Cyber Threats and Security

Barriers archive

Chapter 1 : Olympics Malware attack may have been part of larger cyber espionage scheme 2018-0

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Cyber Espionage Scheme
Today I came across this story from scmagazineuk.com that details an interesting that Researchers found new details in the ?Olympic Destroyer? malware for the PyeongChang Winter Olympics to provide a clearer picture of the malware?s intentions and background.
Olympic malware attacks could be part of a large scale cyber espionage program
Researchers found new details in the ?Olympic Destroyer? malware targeting the PyeongChang Winter Olympics in Korea, revealing more clearly the intention and background of malware attacks.
According to a recently updated blog post, Cisco Talos researchers initially thought malware was only for a single terminal, but malware is now thought to also erase files on shared network drives.
In addition, researchers believe the only purpose of the attack is to shut down the gaming system rather than steal information. The malware contains a binary whose target machine has a pair of ?steal modules,? one for obtaining user credentials embedded in a popular web browser and one for stealing them from the Windows ?Local Security Agency Subsystem Service? .
The updated blog also states that the threat behind the malware actors know many technical details of the Olympic game infrastructure, such as username, domain name, server name, and password, suggesting that a compromise has taken place before the initial attack, according to Talos researcher Craig Williams.
Researchers at Cyber scoop came to a similar conclusion, finding that Olympic IT provider Atos was hacked before the Olympics endangered Atos employees? usernames and passwords, suggesting that the recent attacks are part of a bigger cyber espionage activity based on 14 reported in February.
The researchers said the violation was most likely to target hackers in the Olympics, with hackers entering Atos at least until December 2017.
Despite new information, although some speculate that Russia may be banned from competing as a country for the doping scandal, it is still not clear who is behind the attack. However, non-participating Russian athletes are still allowed to compete under the Olympic flag .
Priscilla Moriuchi, director of strategic threat development, said Recorded Future?s Insikt Group told SC Media that it is important not to jump to conclusions as accurate attribution is more important and harder to pin down than ever before.
?This cold attribution to attacks such as the Pyeongchang Winter Games could have material negative consequences, and therefore deserves in-depth, expert and meaningful analysis,? Moriuchi said.
The researchers also warned that more attacks may be coming as the Olympics provide opportunities for a wide range of attacks, including phishing mail, domain name theft, ransomware and fake social media posts.
?The IT team should warn employees to click on the links or attachments for the Olympic-related e-mail,? Enginger Kirda, Lastline co-founder and chief architect, told SC Media. ?It is also a good idea to use state-of-the-art technology to prevent cyber attacks such as behavior-based detectors like sandboxes from checking for possible attachment to a system.?
Read More?
Researchers discovered new details in the ?Olympic Destroyer? malware which targeted the Winter Olympics in Pyeongchang, South Korea shedding more light on the malware?s intentions and background information on the attack. Cisco Talos researchers originally thought the malware only targeted single endpoints but now believe the malware also wipes files on shared network drives, according to a recently updated blog post detailing the malware. Furthermore researchers believe the sole purpose of the attack was to shut down systems at the games and not to steal information. The malware includes a binary that targets machines with a pair of ?stealing modules,? one designed to grab user credentials embedded in popular web browsers and another to

steal them from Windows? Local Security Authority Subsystem Service. The updated blog also noted that the threat actors behind the malware knew a lot of technical details of the Olympic Game infrastructure such as usernames, domain name, server names and passwords suggesting a prior compromise had taken place before the initial attack, Talos researcher Craig Williams tweeted. Cyberscoop researchers came to a similar conclusion and found that Atos, the IT provider for the Olympics, was hacked months before the Olympics compromising Atos employee usernames and passwords suggesting the most recent attack was part of a larger cyber-espionage initiative, according to a 14 February report. Engaging post, Read More?
thumbnail courtesy of scmagazineuk.com.

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Olympics Malware attack may have been part of larger cyber espionage scheme appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 2 : Ransomware-as-a-Service ? Now Anyone can Download Free Ransomware that is Availa

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Ransomware as a Service:
This story from gbhackers.com gives the truth about researchers have discovered a new Ransomware as a service threat on the Dark website without any registration fees.
Malware authors make money by distributing Ransomware as a service that sells malware as a criminal business model instead of distributing malware and infecting computers.
In such cases, ransomware developers typically host their services on dark sites, anyone can buy them, and they can change their edits, such as ransom money and ransom records.
In addition, some sophisticated Ransomware features some advanced features such as evasion techniques to avoid detection and analysis, and users will be provided with a control panel to control every infected victim.
Buyers just need to set their vault address, they need to customize it, and then they will spread malware.Ransomware is as a service
So once the infected victim pays the ransom amount, the percentage of the amount will be delivered to the buyer and the malware author who created the ransomware.
This kind of Ransomware works as a service
This Ransomware as a Service underground process well-organized, well-planned cybercrime operation.
Buyers can obtain ransomware from the secret Tor site (onion), which includes a guide to help buyers make the right configuration.
In this case, before reaching the original version, the buyer can try the demo version of the ransomware. The buyer just needs to add the bitcoin wallet address and ransom amount they want to request from the victim.
After this process is completed, the malware will be successfully generated and the user can download it.
Once the buyer successfully distributes and compromises the victim, and if the victim is to be paid a ransom amount, a 10% ransom amount will be transferred to the original developer?s wallet.
Free Ransomware run process
Once it enters the victim system, initially it checks the internet connection and if it finds an internet connection then it will terminate its process.
But once it finds the connection, it communicates with the specific address and downloads the encryption key.
According to McAfee Labs, once the file is running, it creates multiple files on the system:
Encryption_key: AES-encrypted RSA key
Lock_file: the system has been encrypted indicators
Uuid_file: Reference for the infected machine. Use this ID to generate the TOR address.
After a successful encryption process, it displays the ransom note on the user?s desktop and points to the TOR site hxxp: // kdvm5fd6tn6jsbwh using the ID of the infected machine.]onion.
Once the victim pays, they can download the decryption key to unlock the encryption key.
?The target extensions include many photos and photographic files related to Canon, Kodak, Sony, etc. There are also extensions to AutoCAD, Autodesk projects, scalable vector images and Microsoft Office files, which are created mainly by designers, photographers, architects and Used by others. ?
Read More?
Researchers discovered a new Ransomware as a service threat available in the Dark web with free of cost without any registration. Instead of distributing the Malware and infect the computer, Malware authors are earning money by selling their malware via Ransomware as a service cybercrime business model. In this case usually, ransomware developer host their Engaging post, Read More?
thumbnail courtesy of gbhackers.com.

google_ad_client: "ca-pub-9083755448612431",
enable_page_level_ads: true
});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Ransomware-as-a-Service ? Now Anyone can Download Free Ransomware that is Available on Dark Web appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 3 : How To Stop Ransomware Affecting Your Computer with Six Remedies 2018-02-19 08:

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Ransomware Remedy:
What is most likely to be an overlooked story from irishtechnews.ie explores revealing six listed Ransomware remedies to protect our computers and prevent ransomware from affecting them.
Always keep a backup We all save important data on our computer, whether it is our document or movie collection. What if the data is lost or the drive is damaged? Or in the worst case, your system can not be reached due to ransomware attacks. To avoid all situations, it is advisable to back up all important data. You can back up on the cloud or you can store the data on an external drive. Cloud backup over other backup methods, because you can access data anytime, anywhere. However, keeping it external drives also has its benefits. So, if you run into any trouble, you will always have all the data.

Suspicious emails, websites, and applications

It is said that it is good to always be cautious. Hackers try to trick people by sending e-mail links or redirecting to malicious Web sites. The usual practice is through phishing mail, malicious advertising and so on. Whenever you click on the suspicious link, it will download the malware to your computer. Once the software installation is complete, it will start the attack and encrypt your files.
Therefore, it is recommended that you do not open unsolicited e-mail or problematic links to avoid such attacks. In addition, you should download the application on your computer from the official website. You should download and install the program after reading its comments.
Use Ransomware protection tool
It is always advisable to obtain ransomware protection tools for your computer. Security software acts as a barrier between your computer and the outside world. It does not allow any ransomware or other malware to be downloaded from your computer. In addition, it helps to indicate if there is any malicious content on your computer.
The software can scan the file to check whether the downloaded file is safe. It also blocks unwanted and hidden installations of malicious ads when you?re on the web. It can scan and determine if your computer is infected.
Always install the update
Operating system manufacturers often post software update fix bugs and other vulnerabilities that hackers can use to trick users. It is always recommended to install updates when publishing updates. The same thing applies to software installations on your computer, be sure to install updates for them immediately after they are released.
Secure network configuration
Network devices (such as routers, switches, and other wireless access points) are used in your organization. Suggest that they should use the updated firmware for proper configuration. This helps you when attacked. It is recommended that you create an optimized network for your virtual LAN (VLAN) and that you should process the data this way in order to transfer the data correctly. The security advantage of VLANs is the systematic isolation of malicious traffic to avoid spreading the infection to other devices. This is useful when the administrator has to deal with infected hosts.
Never pay ransom
If you fall into the trap of cybercriminals and they ask you to pay a ransom, do not do that. We do not recommend paying ransom to hackers because you never know if your documents will be recovered after payment. Disconnecting a computer from the network may seem convenient, but not a good idea as it increases the risk of data loss. There are other solutions to this problem ? you can get the program to decrypt the file. However, you can easily recover if you have a data backup.
So these are some of the ways you can effectively stop ransomware from affecting your computer.

Read More?
Useful guest piece by Apoorv Bhatnagar, a SEO analyst from Systweak Software, giving advice on how to protect your files. Ransomware is a popular amongst criminals used to extort a user by keeping your data hostage and asking for ransom. Lately, the world has witnessed a couple of such attacks. It seems that escaping the malware attacks is almost impossible. But it is always wise to take safety measures to protect your computers from such attacks. In this post, we have listed some of the ways to keep our computer protected and stop the ransomware from affecting it. Engaging post, Read More?
thumbnail courtesy of irishtechnews.ie

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post How To Stop Ransomware Affecting Your Computer with Six Remedies appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 4 : ?China?s gift to Africa?: How China spied on the African Union via donated computers 2

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on China Spied on the African Union
This story from thenextweb.com admits the truth about for five years, China continued to monitor all electronic communications from the African Union headquarters in Addis Ababa, Ethiopia. Chinese espionage continued during this period until some network administrators at the African Union headquarters were discovered in January 2017.
This is based on a survey conducted by Le Monde that revealed how Chinese donated and built a new AU headquarters in Addis Ababa equipped the building with a hidden microphone and exported data overnight from the Australian Data Center Transfer to their data center Shanghai server.
In January 2012, a new headquarters in Addis Ababa was built and equipped by the Chinese government. The 200-million-dollar 20-story building and other buildings in the compound are what the Chinese government calls ?China?s gift to Africa.? However, it will be revealed later that it is a gift that will continue to be donated.
Almost five years later, following the opening of the new headquarters in January 2017, it was revealed that the AU headquarters IT team found that their network was transmitting unusually large amounts of traffic after midnight each day. As Le Monder reported, this is a time when AU headquarters is empty and there is not much (if any) activity on their network. After further investigation by the network administrator, it is clear that large amounts of data from the AU data center servers are sent to unknown servers in Shanghai every night. This apparently also includes voice data recorded from microphones hidden in buildings completely installed by Chinese.
According to the AU, since the project was discovered in January 2017, they have replaced all the servers and ICT equipment donated by China at Union headquarters and obtained their own servers. Even more surprising is that according to the African Union?s reply to the ?Le Monde?, China seems to propose to allocate equipment, which is a request rejected by the AU.
The AU also said it has taken additional steps to ensure the security of its communications, including encrypted communications, and to ensure that all AU officials? telephone lines do not pass Ethiopian Ethio Telecom, a company known to need to close when regulatory and co-operation needs authorities The country?s internet.
On the other hand, the Chinese denied any espionage charges. Kuang Weilin, China?s ambassador to the AU, called these ?allegations? ?absurd.?
This revelation raises several questions, one of which is very important, and for the AU: Five years from now, how can your entire IT team find only so much data transfer per night?
More attention is paid to the apparently infrequent or infrequent security checks in the buildings that occasionally house the Afrika leaders to ensure communications security and/or the absence of hidden audio equipment. Perhaps, finally, Afrika will ?despise free lunches.?
For a period of 5 years, China continued to spy on all electronic communications at the African Union?s headquarters in Addis Ababa, Ethiopia. The Chinese spy operation continued throughout this period without being detected until some network administrators at the AU?s headquarters discovered it in January 2017. This is according to an investigation conducted by Le Monde which has gone on to reveal how the Chinese, who donated and built the new AU headquarters in Adis Ababa, fitted the building with hidden microphones and transferred data every night from the AU?s data center to their servers in Shanghai. In January 2012, the This story continues at The Next Web Engaging post, Read More?
thumbnail courtesy of thenextweb.com

});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post ?China?s gift to Africa?: How China spied on the African Union via donated computers appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 5 : Chat app Telegram is tricking users into installing cryptomining malware 2018-02-19 08:

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary Telegram ? cryptomining malware:
A must-read story from techrepublic.com calls out a revealing fact that Telegram users have become the victims of right-to-left coverage attacks, which makes them think of the Javascript file as a .PNG file with encryption and command and control software installed at runtime.
Attacks were reportedly limited to Russia, but, similar to similar attacks, terrorist attacks are likely to spread. The U.S. security team should ensure that anyone who uses Telegram?s work has the latest version and warns employees not to open attachments of unknown origin.
Telegram Vulnerability
Kaspersky Labs reported a zero-day vulnerability found in the popular messaging app Telegram, which allows hackers to install backdoors and encrypt malware.
Telegram attacks are targeted at telegraph desktop applications and are used to display right-to-left alphabets, such as Hebrew and Arabic, by utilizing the right to left overlay (RLO) feature. Using RLO to rename a portion of a file, as in this attack, can convince users to download malicious code disguised as different types of files.
Alexey Firsh, a malware analyst at Kaspersky Lab, analyzed in detail the work of telegraph hackers, saying that such an attack could only be found in Russia, but that it was not the reason for complacency ? an attack that spread easily.
Make a malicious email with Telegram
RLOs can be done on documents or messages just as if right-to-left alphabets were used. The unicode character U + 202E will also reverse any text that follows it and can be used in filenames and documents.
In Kaspersky Lab?s Russian telegraph hacking attacks, unicode RLO completed a javascript file called gnp.js. The full file name photo_high_re * U + 202E * gnp.js is displayed to the recipient as its photo_high_resj.png. The attacker must open the Javascript file and then install the attacker?s malware.
What attackers are installing in Telegram
When investigating Telegram RLO attacks, Kaspersky Lab uncovered two different types of malware: cryptographic software and the back door that used the Telegram API as a command and control protocol.
Like others, the attack-installed encryption software uses the victim?s CPU and GPU to mine cryptocurrencies for the attacker.
Encrypting malware is dangerous and can have a devastating effect on your hardware and extend it to the limit. This is where the danger ends ? nor can command and control software attackers say these attackers are installing.
As shown below, a complete list of commands available to an attacker allows an attacker to install additional malware, steal system information, or terminate a process that threatens its operation.
Kaspersky Lab also reported that its investigation found that the local cache of user telegrams is an attacker, which means that attackers may also be able to steal personal data.
Kaspersky contacted the Telegram team and said zero days no longer apply to the testing of Telegram software updates.
Other chat programs and outdated versions of the telegraph may still have vulnerabilities. IT teams need to ensure that users with telegrams are up to date with the latest version and that all users receive training on the importance of not opening files of unknown origin.

Read More?
Telegram users are being fooled into running malicious Javascript disguised as image files thanks to a unicode text reversal trick. Engaging post, Read More?
thumbnail courtesy of techrepublic.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Chat app Telegram is tricking users into installing cryptomining malware appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 6 : E-waste recycler gets 15 month prison sentence for creating worthless backup discs 201

Your Feed is from https://www.safeharboroncyber.com/Blog/
:
A must-read story from thenextweb.com declares an interesting story.
You may recognize Eric Lundgren?s name. In 2017, he easily earned Tesla with news of more than 380 miles for creating a $ 13,000 DIY electric car. Today, he is entering prison.
Lundgren has been a mechanic. His Los Angeles-based company specializes in managing e-waste of common electronic devices, such as cell phones and PCs. He spent thousands of hours recycling batteries, motors, and circuits to avoid reusing waste products in wheelchairs, vehicles and even other personal computers. At the age of 19, he founded a company that refurbished and sold his computers to corporate clients such as Dell, Asus, and Lenovo.
When the PC is sold (or scrapped), the included Windows license is legally assigned to the new owner, restoring a nonworking PC and resell it to a relatively simple process. With a real Windows license, simply install the operating system from the restore disc and insert a license key to prove that it is a legitimate installation. The license key is usually displayed on shiny stickers on the side (or bottom) of the PC. Simply get a working copy of Windows on a non-operating device for a genuine certificate and license key.
Those without stickers, Lundgren, told the Los Angeles Times that he scrapped and sold parts for other machines.
But here, Lundgren has trouble. After about 28,000 recovery discs have been compiled the same discs used with the purchased PC, at least until the manufacturer begins to deactivate the optical drive-Lundgren attempts to deliver them to his partners to recover devices that do not work properly.
After Microsoft and Dell got involved in the program, Lundgren received 21 indictments seeking $ 420,000 in sales.
Microsoft calculates the value of each disc is 20 US dollars, the average profit of 75%.
Lundgren made the following statement:
In essence, I hampered Microsoft?s profits, so they pushed it into federal court on a false note.
[Microsoft project manager Jonathan McGloin] confirmed that the free recovery CD costs the same price as a licensed new Windows operating system. ? This is evidence of false and inaccurate Microsoft offers and it tries to set a precedent that will deter future recyclers and refurbishers from reusing the computer without having to pay another license to Microsoft again. ? Anyone who succeeds in extending the life cycle of a computer or relocating those computers from landfills to the community will basically hinder Microsoft?s profits.
It is worth mentioning that, although the number of CDs makes people surprise, every CD is worthless. Without a valid license key, the CD cannot install the working version of Windows on any refurbished machine.
Lundgren said expert witness Glenn Weadock, a software expert who testified on behalf of the U.S. government against antitrust protests in Microsoft, explained the matter to the court. Weadock was asked: ?In your opinion, there is no password, whether it be a product key or a COA [Certificate of Authenticity], what is the value of these reinstallation disks?
?Zero or near zero,? he replied.
Nonetheless, the judge in the case found Lundgren?s recovery disc worth $ 700,000, then sentenced him to 15 months? imprisonment and ordered him to pay a fine of $ 50,000.
Lundgren is currently appealing the decision.
This story raises many questions because of big companies suing for their rights.
Remember the Original owner surrenders the property. Does this apply to salvage laws?
What do you think? Is this unfair?
Read more?
You may recognize the name Eric Lundgren. In 2017, he was all over the news for creating a $13,000 DIY electric car with a 380-plus mile range, easily besting a Tesla. Today he?s on his way to jail. Lundgren has always been a tinkerer. His LA-based company specialized in managing

e-waste from common electronic devices like mobile phones and PCs. He?s devoted thousands of hours to recovering batteries, motors, and circuits from discarded items reuse in wheelchairs, vehicles, or even other PCs. At 19, he started a company to refurbish and sell computers given to him by corporate clients like Dell, Asus, This story continues at The Next Web Engaging post, Read More?
thumbnail courtesy of thenextweb.com.

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post E-waste recycler gets 15 month prison sentence for creating worthless backup discs appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 7 : Remove those nasty adware from your PC properly 2018-02-19 08:19:39

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on removing adware from your PC:
What is most likely to be an overlooked story from blog.malwarebytes.com on how to remove adware from your PC
How to delete adware
Your way out is relatively simple. If you think there?s an adware issue on your PC, you can manually delete it in a few easy steps.
Back up your files. When you face a potential infection, it is always a good precaution. Grab the external hard drive or save the most important data to the cloud.
Download or update the necessary tools. In order for your PC to be clean and tidy, you will need to download or run an update that is specific to scanners that remove adware and PUPs (such as Adwcleaner or the free version of Malwarebytes). If you suspect your computer is seriously infected and you do not have them, you need to have it installed on a friend?s computer and transfer it to your computer via CD or USB.
Uninstall unnecessary programs. Before using your security product for scanning, check that your adware program has an uninstaller. To do this, go to the ?Add / Remove Programs? list in your Windows Control Panel. If the unwanted program is there, highlight it and select the ?Delete? button. After deleting the adware, restart your computer even if you are not prompted to do so.
Use adware and PUP removal to run the scan. Once the program scans and finds the adware, it may isolate something, so you can take a look and decide whether or not to remove it. Our suggestion is to delete, delete, delete. This will get rid of adware and any other residual files that may bring back adware.
How to avoid adware infection
Although the above steps eliminate computers for most adware, there are some forms of militancy that are hard to remove ? and the more aggressive adware is increasingly appearing (pun intended). Today, ad software makers have tweaked their technology around a more comprehensive ad blocking tool by mainstream browser developers such as Google, Mozilla and Microsoft. Their previous gray tactics have turned black.
The bad guys bundle their adware with PUPs programs, preventing them from being removed by preventing the security software from running or even being installed, or by preventing users from removing adware themselves. The only known way to prevent these attacks is to prevent them from happening.
Read more?

How to remove adware from your PC
Half the battle in avoiding adware is reading install wizards and EULAs very carefully. But let?s be real: no one does that. Here?s how to remove adware from your PC in a few easy steps.
Categories: 101 How-tos Tags: adwareAdwCleanerhow to removehow to remove adwarewindows adware (Read more? How to remove adware from your PC

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further

CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Remove those nasty adware from your PC properly appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 8 : Rise of the Hivenet Botnets That Think for Themselves 2018-02-19 08:19:39

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Hivenet Botnets:
A must-read story from darkreading.com describes a surprising fact that intelligent botnet clusters can identify and attack different attack vectors at once.
In the past few years, a new development has taken place: Predicting software systems are using artificial intelligence techniques for programming. Recent advances in these tools use clustering technology to leverage the expertise of massive databases, which are made up of billions of continuously updated data to make accurate predictions.
The bad news now is that this technology has not been overlooked by cybercriminals. A recent survey by Fortinet threat researchers showed that intelligent botnets have repeatedly attacked the Apache Struts framework vulnerabilities responsible for Equifax attacks. Attackers use automated and intelligent decision trees to exploit validated vulnerabilities.
Worse, botnets will evolve into honeynets in the future, a type of attack that can leverage peer-based self-learning to target vulnerable systems with minimal oversight. Hivenets is an intelligent cluster built around group technology that creates more effective attack vectors. Traditional botnets wait for orders from zombie herders and Honeywell can make its own decisions.
Hivenets will be able to use the infected device of the cluster to identify and attack different attack vectors at a time. As it identifies and compromises more devices, a Hivenet will multiply and expand its ability to attack multiple victims simultaneously.
Repeatedly Hivenet Botnets Infected
The researchers also found that many organizations experienced the same botnet infection many times, although it is not entirely clear why this occurred; this could be because the company did not fully understand the scope of the violation and botnets were dormant, Return to normal business operations once again, or the company never found the root cause. This allows botnets to return with the same vulnerability.
Safety best practice
Organizations that use cloud services for online transactions can reduce their exposure to cellular or botnets by following the following basic practices:
Inventory Authorization / Unauthorized device. This should include cataloging authorized and unauthorized assets in your environment, including consumer devices such as mobile phones and laptops. You must know what you are protecting.
Limit user rights: Not everyone needs administrator rights
Restrict Applications in Your Environment: Use only those applications that have business needs and keep these applications and systems up-to-date and fully patched. Using unnecessary applications can increase the attack surface and increase the complexity of protecting the environment.
Larger companies will also be good at following these recommendations. Good cyber hygiene: Beyond keeping a watch out for new threats and vulnerabilities in the wild, make sure you do not ignore what?s happening in your environment. Network hygiene and equipment hygiene may be the most overlooked factors in today?s security. Constantly removing unnecessary services, eliminating holes and maintaining good order is not the most interesting or sexiest part of security, but it is a very important part.
Read More?
These intelligent botnet clusters swarm compromised devices to identify and assault different attack vectors all at once. Engaging post, Read More?
thumbnail courtesy of darkreading.com

```
    enable_page_level_ads: true
  });
```

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Rise of the Hivenet Botnets That Think for Themselves appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 9 : North Korean Hacking Group ?Lazarus? Targeting Banks & Bitcoin Users Via Sophi

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Lazarus Hacker Group:
Gbhackers.com reflects the truth about a new malware campaign, called Hao Bao, was launched by North Korean hacker group Lazarus, specifically targeting cryptocurrencies and financial institutions through sophisticated cyber-attacks.
Lazarus hacker group
In early 2017, Lazarus, a North Korean hacker group, actively circulated a large number of spear phishing mail and targeted many people. Last year, the campaign targeted military planning insight or stealing money from defense contractors to financial institutions, including cryptocurrencies.
The current scenario is targeted at Bitcoin users and their activities targeting Bitcoin users and collecting sensitive information to steal bitcoin.
The variants found so far indicate that the contact is an IP address/domain that is used to host malicious documents from the previous campaign in Lazarus in 2017 and the same malicious document, as well as Lazarus Resurfaces.
North Korea hacker organization Lazarus hacker group movement distribution
Initially, it distributed spam campaigns, which contained a link to a Dropbox account for malicious documents.
hxxps: [.] //dl.dropboxusercontent COM / content_link / AKqqkZsJRuxz5VkEgcguqNE7Th3iscMsSYvivwzAYuTZQWDBLsbUb7yBdbW2lHos / file (DL) = 1
hxxps: // www [. dropbox [.] com / s / q7w33sbdil0i1w5 / job description.doc? dl = 1
Once the victim clicks on the link, the malicious document will be downloaded and the document is created in the older version of Microsoft Word.
Malicious files force the victim to enable macros after implantation into the target system.
In this case, three different documents are distributed from the same Dropbox link. Firestone named lsm.exe contacts 210.122.7.129, which also resolves worker.co.kr.
The second distribution has the name csrss.exe, the contact IP address 70.42.52.80 resolves to deltaemis.com, the third communicates with the Korean IP address 221.164.168.185 and resolves to palgong-cc.co.kr.
Malicious files will be distributed in the encrypted payload of Visual Basic macro code.
According to McAfee, VBA macro code is executed automatically and is configured to be executed when OLE documents (MS Word documents) are opened (via ?Sub AutoOpen ()?) to collect system information.
After all the files have been collected, the information is infiltrated from the victim and sent to the command and control server.
Use the same malicious document structure and similar recruitment advertisements that we observed in our past Lazarus activities. The technology, tactics, and procedures are in line with the Lazarus Group?s interest in encrypting currency theft. McCafferty said.
Read More?
A New Malware campaign dubbed HaoBao distributing by North Korean Hacking Group ?Lazarus? that specifically targets cryptocurrency and financial organizations via sophisticated cyber Attack. North Korean hacking group Lazarus actively spreading a huge number of spearphishing Emails and targeting many individuals in Beginning of 2017. Last year this campaign was heavily targeted military program insight or steal Engaging post, Read More?
thumbnail courtesy of gbhackers.com

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further

CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post North Korean Hacking Group ?Lazarus? Targeting Banks & Bitcoin Users Via Sophisticated Malware appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 10 : Cybersecurity Challenges ?Going to Get Much, Much Worse,? NSA Director Warns 20

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on National Cybersecurity Challenges

A must-read story from hstoday.us concludes how the director of the National Intelligence Agency described the ?tech-savvy contest? in the cyberwar, while intelligence chiefs were concerned that smaller companies that are ?less mature? are accelerating the resolution of current cyber threats.

?The internet is clearly the most challenging threat to the country,? Senate Intelligence Committee President Richard Burr (RN.C.) said at a hearing on Tuesday that the hearing spanned a series of Global Threats. ?It?s one of the most worrisome issues, given how much of our daily routine in the United States can be disrupted by well-planned and well-executed cyber attacks.?

Cybersecurity Challenges on China

Vice President Mark Warner (D-VA) said that ?in addition to this ongoing threat from Russia,? he worries that China has developed a society as a whole, not just all of the government, and society ? to acquire our sensitive technologies and intellectual property way. ?

In giving ?great attention? to the rise of China?s technology sector, Warner said he is particularly concerned about ?the close relationship between the Chinese government and Chinese technology companies, especially in monitoring the commercialization of technology and the shaping of telecommunications equipment.?

?I want to make sure ICs are tracking the direction that the Chinese technology giants are moving, especially their commitment to the Chinese government,? he said. ?? most Americans have not heard of all of these companies yet, but as they enter the Western economy we want to make sure they do the right thing and we need to make sure that this is not a new way for China to acquire sensitive technology ?

Dan Coats, director of the National Intelligence Agency, warned that U.S. rivals ?and other vicious actors are using the Internet and other power tools to shape society and markets, international rules and institutions, and international hotspots to their benefit.?

?We have entered a period that best describes our technological superiority as a counter to our rivals who are trying to sow split in the United States and weaken the U.S. leadership,? Coetz said, warning that the country was ?physically attacked? The Internet is being used to penetrate every major operation in the United States ? from the U.S. businesses to the federal government to state and local governments, where the United States is threatened daily by cyber attacks. ?

Nation-states Cybersecurity Challenges

The director pointed out that Russia, China, Iran and North Korea pose the greatest cyber threats, but added that ?other countries, terrorist groups, terrorist groups, transnational criminal organizations and more technologically powerful groups and individuals use cyber operations to achieve strategic and malicious Behavioral goals. ?

?Some of these actors, including Russia, may carry out more radical cyber-attacks aimed at reducing our democratic values and undermining our alliance.? The sustained and disruptive network operations will continue to have a bearing on the United States and our European Ally, take advantage of the electoral opportunities to undermine democracy, sow discord and undermine our values, ?Goldsmith continued. ?China?s cyber espionage and cyber attack capabilities will continue to support China?s national security and economic priorities. Iran will try to penetrate the spy networks of the United States and its allies to lay the foundation for future cyber attacks while North Korea will continue to use cyber operations to raise funds and launch attacks And gather intelligence about the United States. ?

Burr asked whether the intelligence community ?is sufficiently vigilant about the threat of the private sector.?

?When we realized that, I thought we were informing them,? NSA director Mike Rogers replied. ?But one thing I?m worried about is that we can only see part of this photo and I?m also interested ? from the private sector point of view, tell us what you see.If we can combine the two, We will

have a broader perspective and deeper knowledge. ?

New Technology Cybersecurity Challenges

Burr asks if the ?new technology company emerges every day,? whether the head of the National Security Agency is ?concerned that this will become an increasingly challenging area.?

Rogers said he was worried and weird, ?How bad would it be before we realized we had to fundamentally change something??

?And, I think, if you look at the Internet of Things, you see the level of security in these components ? one can see ? on the order of magnitude,? Rogers added. ?If we think the issue is a challenge right now, then we just wait, and from a security perspective it will get worse and worse ? exponentially growing.?

FBI director Christopher Wray said the council ?worked very hard to do more in the private sector by offering something almost defensive briefing so that some telecoms companies in the United States and other members of the technology industry.

Read More as the article continues?

The director of National Intelligence described a ?race for technological superiority? in the cyber wars while intelligence leaders expressed concern about ensuring ?less sophisticated? small companies are up to speed on current cyber threats. ?Cyber is clearly the most challenging threat factor this country faces,? Senate Intelligence Committee Chairman Richard Burr (R-N.C.) said at a Tuesday hearing spanning a range of worldwide threats. ?It?s also one of the most concerning, given how many aspects of our daily lives in the United States can be disrupted by a well-planned, well-executed cyber attack.? Vice Chairman Mark Warner (D-Va.) noted that ?in addition to this ongoing threat from Russia,? he?s ?concerned that China has developed an all-of-society ? not just all-of-government, but all-of-society ? approach to gain access to our sensitive technologies and intellectual property.? In paying a ?great deal? of attention to China?s ascending tech sector, Warner said he?s particularly worried about ?the close relationship between the Chinese government and Chinese technology firms, particularly in the area of commercialization of our surveillance technology and efforts to shape telecommunication equipment markets.? ?I want to ensure that the IC is tracking the direction that China?s tech giants are heading, and especially the extent to which they are beholden to the Chinese government,? he said. ?Most Americans have not heard of all of these companies. But, as they enter Western economic markets, we want to ensure that they play by the rules. We need to make sure that this is not a new way for China to gain access to sensitive technology.? Director of National Intelligence Dan Coats warned that America?s adversaries, ?as well as the other malign actors, are using cyber and other instruments of power to shape societies and markets, international rules and institutions, and international hotspots to their advantage.? ?We have entered a period that can best be described as a race for technological superiority against our adversaries, who seek to sow division in the United States and weaken U.S. leadership,? Coats said, warning that the country ?is under attack by entities that are using cyber to penetrate virtually every major action that takes place in the United States ? from U.S. businesses, to the federal government, to state and local governments, the United States is threatened by cyber attacks every day.? The director singled out Russia, China, Iran and North Korea as posing the greatest cyber threats, but added that ?other nation-states, terrorist organizations, transnational criminal organizations and ever more technically capable groups and individuals use cyber operations to achieve strategic and malign objectives.? ?Some of these actors, including Russia, are likely to pursue even more aggressive cyber attacks with the intent of degrading our democratic values and weakening our alliances. Persistent and disruptive cyber operations will continue against the United States and our European allies, using elections as opportunities to undermine democracy, sow discord and undermine our values,? Coats continued.

Engaging post, Read More?

thumbnail courtesy of hstoday.us

Russia by Cyber, North Korea by Nuke: A New Batch of Grim Warnings from US Intel

Questioning on Russian election interference and how the Trump White House handles staff clearances dominated the worldwide threat hearing Tuesday, as the Senate intelligence committee grilled leaders of the FBI, CIA, NSA, DNI, DIA and NGA over the contents of the 2018 Worldwide Threat Assessment of the U.S. Intelligence Community. Russia by Cyber, North Korea by Nuke: A New Batch of Grim Warnings from US Intel

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Cybersecurity Challenges ?Going to Get Much, Much Worse,? NSA Director Warns appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 11 : Salon?s optional coin mining site to ad-blockers: Can we use your browser to mine crypt

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Salon?s optional coin mining
A recent story from arstechnica.com says things we don?t talk about Salon?s optional coin mining site lets you avoid ads, but it can drain your CPU power.
Salon.com has a new, cryptocurrency-driven strategy that earns money when readers intercept ads. If you want to read the salon without advertising, as long as you let the site use your spare computing power to tap some coins.
If you visit the salon with ad blocker enabled, you may see a pop-up that asks you to disable the ad blocker or ?block ads by allowing them to use your unused computing power.?
Sharon explains what?s happening in the new FAQ. ?How can Sharon make money by using my processing power?? Said the FAQ. ?We intend to leverage some of your spare processing power to contribute to technology discovery, evolution and innovation, and for our beta program we will begin leveraging your processing power to help support blockchain growth and growth technologies And cryptocurrency. ?
A whole lot of websites and applications are consuming your CPU to mine cryptocurrencies
Although this is a little vague, a second Salon.com popup shows that Salon is using Coinhive for ?calculations that are safely performed in the browser?s sandbox.? The Coinhive pop-up on Salon.com offers the option of canceling or allowing digging in a browser session. Click More Info to bring you to the Coinhive page.
Salon?s optional coin mining site ?provided by Coinhive? pops up.
We wrote an article about Coinhive in October 2017. Over 2,000 WordPress Sites infected by 2nd Keylogger CoinHive Campaign to monetize Monero cryptocurrencies, which in turn, contributed a fraction of the relatively small revenue to participating sites.?
It does use a lot of CPU power
Today I enabled digging on Salon.com to see how much computing power it used. In Chrome?s Task Manager I got the salon tag 426.7 and higher CPU readings:
The Chrome Assistant?s CPU usage is up to 499 on my 2016 MacBook Pro, which is unusual on my computer and even on Chrome. This accounted for 800% of the total, accounting for four cores, each running two threads:
The bottom of my laptop started to warm up, but the computer still worked fine otherwise. With high Chrome usage, Mac Activity Monitor said that 24% of my CPU power is still idle. After I disabled Salon?s cryptocurrency mining, my idle CPU power rose back to the more typical 70% to 80%.
The computer I used for this experiment had a quad-core Intel Core i7 Skylake processor. Obviously different people will get different results. Although the Sharon digging may not lock your computer, I still do not want it to run in the background, especially when I leave the power outlet.
Salon?s optional coin mining site: There is no security risk
Salon, due to the site?s choice to join the system, readers will not be forced into cryptocurrency mining. However, in other cases, users have no idea that Coinhive is in use on their system. Researchers from security firm Sucuri warned that at least 500 sites running WordPress content management systems have been hacked to run Coinhive mining scripts, ?we wrote in an October 2017 article.
Harmful drove money mining disaster shows no sign of reduction
Cryptojacking is still a problem, as we detail in several other articles, including an article yesterday.
Salons infected with the user should not occur in the salon, indicating that readers do not have to choose mining, and said the user?s security is not affected.
?This happens only when you visit Salon.com,? the site?s FAQ says. ?There is no software installed on the computer and Sharon has never accessed your personal information or files.?
Sharon pointed out that advertising allows sites to make money from readers without having them

pay for subscriptions.
?Back in the 1990s, as it is now, Sharon has provided a common relationship to provide users with ads in exchange for the bulk of the content for free,? Salon wrote. ?The principle behind this is that your readership is of value to us and our advertisers, and the fragile relationship has been more disrupted recently with the increasing popularity of ad blocking technology; as with most media websites, ad blocking Go deep into our earnings and build a more one-sided relationship between readers and publishers. ?
Salon does not seem to offer subscription options at the moment, but said it will soon provide a ?fast, ads-free experience? in new paid apps for mobile phones and tablets.
Read More?
Salon?s optional coin mining lets you avoid ads, but eats up your CPU power. Engaging post, Read More?
thumbnail courtesy of arstechnica.com

Salon Adds Cryptocurrency Malware ? On Purpose
Salon Adds Cryptocurrency Malware ? On Purpose

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Salon?s optional coin mining site to ad-blockers: Can we use your browser to mine cryptocurrency? appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 12 : Protecting the cybersecurity of small businesses and their consumers 2018-02-15 08:4

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on Protect the cybersecurity of small businesses and their consumers

A must read story from thehill.com calls out on protecting the cybersecurity of small businesses and their consumers. Imagine this is your early days. About the time you go home, you open your laptop, log in to your bank account and be shocked to see the balance of your small business: zero. You never thought it would be you. Of course, millions of online banking users, you will never be targeted.

Unfortunately, we see this more often in today?s world of hyperconnects. As Chairman of the Small Business Committee of the House Committee, I heard over and over again the extent of the cyberattack damage to businesses, owners, employees and customers.

With online sales, small businesses can reduce costs, increase sales and improve overall efficiency. However, the same tools and resources that empower small business owners to play a bigger role in the market also provide cybercriminals and foreign actors with more opportunities to steal sensitive and valuable information.

This is unacceptable.

According to a recent survey by the National Association of Small Business, 32,000 U.S. dollars ? the average cost of cyberattacking small businesses. According to Verizon?s report, 71% of cyber attacks target fewer than 100 people. This is a start-up company, mom and pop store, most vulnerable to Internet abuse.

The committee that I chair has held several hearings on the role of the government in protecting small businesses from cyber-attacks. More than 47% of private-sector employees are the backbone of the U.S. economy and can not be ignored in cyber-security dialogue.

One thing is clear: We need to do more to protect the cybersecurity of small businesses and their consumers.

Cybersecurity of small businesses and their consumers Partnership

Although we must address this need in time in Congress, the partnership between the government and small businesses needs to be strengthened. It is essential that entrepreneurs ensure that their systems and servers are protected by domestic and foreign attacks. They are often the target because they have no resources or staff at large companies to protect their assets and customers.

At a recent hearing, representatives from the FBI and the Department of Homeland Security emphasized the importance of protecting small business infrastructures because of the recent revelations that potentially malicious foreign-owned firms have access to millions of small businesses ?data. Aware of these fears, I introduced the two-party H.R. 4668, Advanced Cyber Security Enhancement Act for Small Business, to increase the defensive measures that these start-ups have against foreign attacks.

In the ideological war, innovators also need to protect their own intellectual property. Because these startups do not have room for extravagant lawyers and advisors? boards, they need to know more about protecting company information. One possible solution is cybersecurity. As cyber attacks have increased, large companies are already embracing this tactic ? many small businesses are starting to follow suit.

Last year, the House of Representatives passed the Act to Improve Cybersecurity in Small Business, which helps small businesses face cyberthreats by providing other tools and resources available through existing federal agencies. DHS and other federal agencies are able to work with Small Business Development Centers (SBDC) to provide resources for small businesses.

More than ever before, the cyber security of innovators and small businesses in our country needs to be prioritized. Their ingenuity and courage are the reasons for the strong US economy.

Read More?

CIA expects more election interference Lawmakers to Saudi, UAE ambassadors: Lift Yemen blockade immediately Rosenstein on hot seat as parties allege FBI bias MORE represents Ohio?s

1st District in the United States House of Representatives where he serves as chairman of the House Committee on Small Business. Rate President Donald Trump on His Job Performance Judge Awards 5Pointz Graffiti Artists $6.7 Million for Destroyed Works Judge Upholds Warrant for Julian Assange?s Arrest Reports: Police Recommend Indictments of Netanyahu U.S. Drops to 18th on Global Economic Freedom Index Wray Contradicts WH Timeline on Porter Background Check Intelligence Agencies Expect Russia to Target Midterms Bomber Gets Life in Prison for New York, New Jersey Attacks Report: Letter With Powdery Substance Sent to Building With Obama Office Engaging post, Read More?
thumbnail courtesy of thehill.com

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Protecting the cybersecurity of small businesses and their consumers appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 13 : Android Owner Warning: New AndroRAT Exploits Dated Permanent Rooting Vulnerabilit

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on AndroRAT

What is most likely to be an overlooked story from blog.trendmicro.com dissects how Trend Micro has discovered a new variant of Android Remote Access Tool (AndroRAT), identified as ANDROIDOS_ANDRORAT.HRXC, capable of injecting root attacks for malicious tasks such as silent installation, shell command execution, WiFi password collection and screen capture. This AndroRAT targeted CVE-2015-1805, a publicly disclosed vulnerability in 2016 that allows an attacker to penetrate older Android devices to perform its privilege escalation.

AndroRAT Exploits

RAT has always been a common Windows threat, so it should not be surprising for Android. The RAT must have root privileges ? usually by exploiting the vulnerability ? to control the system. The original author found in 2012 that AndroRAT was originally a university project that, as an open source client / server application, could provide remote control of the Android system, which naturally attracted cybercriminals.

This new variant of AndroRAT disguises itself as a malicious utility called TrashCleaner, which is probably downloaded from a malicious URL. When TrashCleaner first runs, it prompts the Android device to install a Chinese-labeled calculator application similar to a pre-installed system calculator. At the same time, the TrashCleaner icon disappears from the device?s UI and the RAT is activated in the background.

Configurable RAT services are controlled by the remote server, which may mean that commands may be issued to trigger different operations. This variant activates embedded root attacks when performing privileged operations. It performs the following malicious actions in the original AndroRAT:

Record audio
Use your device camera to take a picture
Steal system information, such as phone model, number, IMEI and so on.
Pirates WiFi names connected to the device
Theft of call logs including incoming and outgoing calls
Theft of mobile network cell location
Theft of GPS location
Theft of contacts list
Theft of files on the device
Theft of list of running apps
Theft of SMS from device inbox
Monitor incoming and outgoing SMS

In addition to the original functionality of AndroRAT, it performs new privileged operations:

Theft of mobile network information, storage capacity, rooted or not
Theft of list of installed applications
Theft of web browsing history from pre-installed browsers
Theft of calendar events
Record calls
Upload files to victim device
Use front camera to capture high resolution photos
Delete and send forged SMS
Screen capture
Shell command execution
Theft of WiFi passwords
Enabling accessibility services for a key logger silently
Mobile network information theft, storage capacity, rooted or not
Misappropriation of the list of installed applications

CVE-2015-1805 was patched by Google in March 2016, but no more patches or longer rollouts may be affected by this new AndroRat variation. Older Android versions that are still in use by a large number of mobile users may still have vulnerabilities.

AndroRAT Exploits Countermeasures

Users should avoid downloading applications from third-party application stores to avoid threats such as AndroRAT. When it comes to device security, downloading from a legitimate app store may take a long way. Periodically updating the device?s operating system and applications can also reduce the risk posed by new exploits.

A new variant of the dreaded AndroRAT malware appeared in threat landscape
Security researchers from Trend Micro detected a new variant of the popular AndroRAT Android RAT in the criminal ecosystem. Security experts from Trend Micro reported the availability of a new variant of the popular AndroRAT. The malware was first born in 2012 as a university project, designed as an open-source client/server application to offer remote? A new variant of the dreaded AndroRAT malware appeared in threat landscape

Read More?
Trend Micro detected a new variant of Android Remote Access Tool (AndroRAT) (identified as ANDROIDOS_ANDRORAT.HRXC) that has the ability to inject root exploits to perform malicious tasks such as silent installation, shell command execution, WiFi password collection, and screen capture. This AndroRAT targets CVE-2015-1805, a publicly disclosed vulnerability in 2016 that allows attackers to penetrate a number of older Android devices to perform its privilege escalation. Post from: Trendlabs Security Intelligence Blog ? by Trend Micro? Engaging post, Read More?
thumbnail courtesy of blog.trendmicro.com

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Android Owner Warning: New AndroRAT Exploits Dated Permanent Rooting Vulnerability, Allows Privilege Escalation appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 14 : 700 million cyber attacks financial services and e-commerce hacks last year, more in 20

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on cyber attacks financial services and e-commerce trend
A recent story from techwireasia.com report on a new ThreatMetrix report, last year?s attack rate increased 44% compared with last year, with a total of 700 million cyber attacks.
Businesses in the fields of financial services and e-commerce suffered the worst impact on cyber attacks in the world.
Over the years, Mobile has become the leading way to acquire new clients from financial institutions. More than 57% of customers are now from mobile devices.
Unfortunately, the mobile wallet is also becoming the highest targeted attack target, suffered high login and payment attacks. In 2017 there were 130 million attacks using stolen or fake documents harvested during the most recent violations.
The report shows that nearly 60% of financial services transactions are mobile, with mobile transactions up 70% from a year earlier. In addition, more than 45% of users are mobile-only.
Mobile users are more engaged, with nearly twice as many mobile logins per desktop as desktop users, approaching one each day.
As in previous years, ThreatMetrix noted that e-commerce activity has increased during the holidays, resulting in an increase in financial services transactions as users periodically access their online bank accounts to check balances and pay bills.
Cyber attacks financial services and e-commerce -Online shopping, online banking
The rise of the Black Net makes it easier for cybercriminals to buy, trade, add, and unlock stolen credentials. Source: Shutterstock
The report pointed out that many high-profile violations in 2017 have become a favorable target for cybercriminals to profit from the use of pirated and synthetic vouchers.
The rise of the Black Net makes it easier for cybercriminals to buy, trade, add, and unlock stolen credentials. In addition, since they are created using a bundle of stolen data, false credentials are almost indistinguishable from real objects.
However, here are some of TreatMetrix?s projections for the coming year:
Changing consumer behavior will impact the way business grows: Mobile usage in all use cases will continue to grow and will take up more traffic than desktop trading.
Cross-border traffic will create digital commerce for a growing number of key retailers, while businesses in other regions want to trade or try to access restricted goods and services
Non-traditional gifts and one-click payments will force retailers to better balance fraud and friction: Retailers expect non-traditional tailored non-traditional methods such as gift / gift card transactions, online ordering and travel bonuses.
The adoption of digital gifts and same-day shipments will better support last-minute shoppers.
Cyber fraud and financial crime will continue to converge: fraudulent new account creation in financial services has increased by 240% in two years.
In 2018, cybercrime is expected to be combined with traditional financial crimes and take the form of fraudsters, using robotic attacks to apply for fraudulent loans or to hijack existing ones and then transfer funds to other countries.
The digital and emerging industries will be the main target: P2P and shared economy are expected to get into trouble next year.
Fraudsters are using the new platform to monetize vouchers between fake driver / driver accounts and create fraudulent new accounts for counterfeit loan applications that are never going to be repaid.
The digital models of many of these emerging P2P and shared economy companies make them particularly vulnerable to fraud.
Violations will spread worldwide, triggering mobile attacks Initiators: Identity certificates will continue to be sold at low prices, resulting in a breach of identity in global cyber attacks.
This trend will be more pronounced in growing economies and areas where there is less static authentication service.

Read More?
23 October, 2017 Breached data will disseminate globally, sparking shifting attack originators: Identity credentials will continue to be sold at bargain prices, causing breached identity credentials to appear in cyberattacks worldwide. This trend will be more pronounced in growth economies and areas with fewer static identity verification services?. Engaging post, Read More?
thumbnail courtesy of techwireasia.com

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post 700 million cyber attacks financial services and e-commerce hacks last year, more in 2018? appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 15 : Spectre and Meltdown Fixes ?massive overhead? will slow Linux systems, warns Netflix

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary Spectre and Meltdown Fixes
A recent story from techrepublic.com proposes a revealing two main affects from Spectre and Meltdown Fixes.
Due to performance overhead between 1% and 800%, changes to the Linux kernel have been found to reduce system speed in order to mitigate the effects of the crash.
Systems that use large numbers of system calls or have a high page error rate are particularly badly affected.
Netflix engineers warn that patches based on Linux systems can cause ?huge overhead? in response to Meltdown CPU defects.
Brendan Gregg found that depending on the nature of the workload, there is a 1% to 800% overhead increase anywhere updating the Linux kernel to mitigate the risks associated with Meltdown.
Spectre and Meltdown Fixes Impacts
Spectre and Meltdown are vulnerbilities in modern chip design that could allow attackers to circumvent system protection on nearly all recent PCs, servers and smartphones, enabling hackers to read sensitive information (such as passwords) from memory.
?Due to extra CPU cycle overhead and memory work set size,? your position on this spectrum depends on system calls and page-error rates due to TLB refresh of system calls and context switches, ?he wrote. Continuing the assessment could affect Netflix?s AWS-based system.
?In fact, due to our system call rates, I expect my cloud system from Netflix to experience a 0.1% to 6% overhead on KPTI and I expect we will reduce this system to less than 2% .
The severity of KPTI?s patch impact depends on:
System Call Rate: The system call rate goes up. Gregg estimates that there are 50,000 system calls / second per CPU, and the overhead may be 2%.
Page Error Rate: High rates increase spending again.
Working Set Size (Hot Data): Exceeds 10MB of overhead translates from 1% overhead to 7% overhead due to TLB (Conversion Lookaside Buffer) flushing.
Cache Access Mode: The worst-case scenario is a 10% reduction in performance overhead if the workload switches to access inefficient caching mode.
To reduce the impact of KPTI on Linux-based systems, Gregg suggests a number of measures: including using 4.14 for PCID support, large pages (which may also provide some gain), and system call reductions, as described in more detail here.
Gregg added that the actual performance impact of protecting Linux-based systems from Meltdown and Specter will be even greater because changes to KPTI are part of a series of updates to prevent vulnerabilities. In addition, there are Intel firmware updates, cloud provider hypervisor changes, and Retpoline compiler changes ? all of which may further affect performance.
In an eager patch release, multiple instances of Spectre and Meltdown related updates lead to computer instability and performance issues-specifically, Intel firmware updates for variant 2 of the Spectre defect.
According to AMD chief executive Brian Krzanich, Intel is developing new designs for its processors to mitigate threats posed by Spectre and Meltdown vulnerabilities, and AMD is also reducing the specter risk.
IBM also released Meltdown and Specter patches for systems running on Power family of processors. Although IBM can provide operating system and firmware updates because Power4, Power5, and Power6 series systems are out of support, IBM does not patch these systems.
For more CyberWisdom articles on Spectre and Meltdown Fixes
Malware POC Analysis exploiting Spectre and Meltdown flaws

CyberWisdom Safe Harbor Commentary on Spectre POC Malware Analysis I couldn?t believe this story from securityaffairs.co that believes Malware exploits Spectre, crash flaws may come by proof-of-concept analysis. Researchers at AV-TEST, an anti-virus testing company, have

uncovered more than 130 malware samples specifically developed to exploit the Spectre and Meltdown CPU vulnerabilities. The good news is
Read More
Intel?s Meltdown and Spectre patch hold up. What to do while you wait.

CyberWisdom Safe Harbor Commentary Waiting on Meltdown and Spectre Patch: I couldn?t believe this story from scmagazine.com that talks about the truth about while Intel pausedMeltdown and Spectre patch and we are waiting, what should we do when we are waiting Intel earlier this week suggested that users using processors that may be affected by Specter / Meltdown
Read More

Meltdown and Spectre Report: A Guide for Awareness

Meltdown and Spectre Report: A Guide for Awareness Now for almost three weeks, the legendary patch and resolution continue. This article is an update of the Implementation Guide to Meltdown and Spectre CPU Design Flaw or Chip Flaw. Currently, the world is still waiting for the ?sure? fixes from Intel?s recently released bungled patch. However,
Read More

Update: Meltdown and Spectre Flaw and Vulnerability Implementation Guide ? Intel Stops Bungled Patches
Intel Halts Meltdown and Spectre Chip Flaw/CPU Patches Over Unstable Code An update from my Meltdown and Spectre Flaw and Vulnerability Implementation Guide ? by David S. Eng Meltdown and Spectre Flaw and Vulnerability Implementation Guide Now for almost three weeks, the legendary patch and resolution continue. This article is an update of the Implementation Guide to Meltdown
Read More
Meltdown and Spectre Chip Flaw and Vulnerability Implementation Guide Update: Intel holding off Patches

Intel Halts Meltdown and Spectre Chip Flaw/CPU Patches Over Unstable Code An update from my Meltdown and Spectre Flaw and Vulnerability Implementation Guide Meltdown and Spectre Flaw and Vulnerability Implementation Guide Now for almost three weeks, the legendary patch and resolution continue. This article is an update of the Implementation Guide. Currently, the world is still waiting
Read More

Why Meltdown and Spectre are ripe for ransomware attacks
CyberWisdom Safe Harbor Commentary: Today I came across this story from csoonline.com that declares a little known possibly that Meltdown and Spectre vulnerabilities are a path and ripe for ransomware attacks Before we study the solution, let?s take a closer look at Spectre and Meltdown. Specter breaks the isolation between different applications. It allows attackers to

Read More
Meltdown and Spectre patches varies performance impact and can cause unwanted reboots, Intel warns

CyberWisdom Safe Harbor Commentary: I couldn?t believe this story from securityaffairs.co that details Intel?s announcement that the test results on the Meltdown and Spectre patches and their impact on performance, confirming serious problems.Running Meltdown and Spectre patches based on S & G systems with several types of processors may experience more frequent restarts. Performance Hit A few days
Read More

Industrial systems scrambling to catch up with Meltdown, Spectre patch vulnerability

CyberWisdom Safe Harbor Commentary: Today, theregister.co.uk lays out things we don?t talk about that many industrial system vendors joined the vendor?s long list of performance and stability vulnerabilities that Meltdown and Spectre processors responded. So far, a dozen vendors have told ICS-CERT that they use a vulnerable processor, and The Register thinks there?s a
Read more?
Brendan Gregg describes the impact of updates to the Linux kernel that work around Meltdown as demonstrating the ?largest kernel performance regressions I?ve ever seen??. Engaging post, Read More?
thumbnail courtesy of techrepublic.com

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Spectre and Meltdown Fixes ?massive overhead? will slow Linux systems, warns Netflix engineer appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 16 : New Twists In ?Olympic Destroyer? Malware ? Found Credential Theft and Erase Files

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on more Olympic Destroyer
This story from threatpost.com talks about how researchers found new wrinkles in the ?Olympic Destroyer? malware attack on the PyeongChang Winter Olympics in South Korea.
Cisco Talos researchers now believe the Olympic Destroyer malware will also erase files on shared network drives. Initially, researchers thought malware was only for a single endpoint. Researchers now also believe malware voucher components are more dynamic than originally thought.
The Olympic destroyers were deployed at the Olympic Games opening ceremony on February 9 and were accused of disrupting the television coverage of the event and canceling the official website of the Winter Olympics. The result of the attack was so profound that conference attendees were unable to print the bill and destroyed the WiFi network used by journalists covering the opening ceremony.
Researchers at Cisco Talos said the only purpose of the attack was to cancel the system rather than steal information.
Cisco Talos first wrote that the Olympic Destroyer?s goal was to make the system unusable by ?deleting shadow copies, event logs, and attempting to use PsExec & WMI to move further around the environment,? similar to the Bad Rabbit and Nyeyta ransomware.
Olympic Destroyer includes a binary file whose target machine has a pair of ?steal modules.? One to crawl any user credentials embedded in Internet Explorer, Firefox and Chrome, the other from the Windows Local Security Licensing Subsystem service, and the Windows process to handle security policies. ?The malware parses the registry and it queries sqlite files to retrieve stored credentials,? Talos said.
Craig Williams
@security_craig
Our posts have been updated to include effects on network sharing ? Shocker ? They are effectively eliminated: Olympic Destroyer aiming at the Winter Olympics, and there are signs of compromise before ? http://blog.talosintelligence.com/2018/02 / olympic-destroyer .html ? #OlympicDestroyer @SecurityBeard @ r00tbsd @TalosSecurity
Tarox researcher Craig Williams pointed out in his tweet that an analysis of the attacks shows the ?previous compromise? of the targeted Olympic system. ?Our posts have been updated to include the impact on the share of the network ? Shocker ? they were effectively eliminated: the Olympic Destroyers aimed at the Winter Olympics and pointed to previous compromises,? he wrote.
Talos?s updated blog says, ?Malware authors know many technical details of the Olympic Games infrastructure, such as usernames, domain names, server names, and obvious passwords.?
When researchers scrutinized the Olympic destroyer binaries associated with the attack, they found that every new certificate of infection was added to the code.
?The new version of the binary is generated from the newly discovered certificate,? Talos wrote in an update first mentioned by Bleeping Computer. ?This new binary, which will be used for the new infection system by transmission, explains why we found several samples with different sets of certificates collected from previously infected systems.?
However, the delivery of malware is still unknown, Talos added: ?If an attacker has access to the environment, the attack may have been remotely performed, allowing actors to pinpoint the timing of the opening ceremony and have them control their impact time ?
The report said: ?Vandalism is the clear goal of such attacks and gives us the confidence that the actors behind them will embarrass the Olympic Committee during the opening ceremony.?
Read More?
Researchers now believe attackers may have had prior access to networks and that malware was more sophisticated than originally believed. Engaging post, Read More?
thumbnail courtesy of threatpost.com

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post New Twists In ?Olympic Destroyer? Malware ? Found Credential Theft and Erase Files appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 17 : Ex-Mossad head: Israeli cybersecurity isn?t enough?Puzzling Scenario by Pardo Speec

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on Pardo Speech

What is most likely to be an overlooked story from jpost.com report that Pardo made a speech at the Tel Aviv Exhibition Center at Muni-Expo, the first international cybersecurity conference for municipalities. He drew a dystopian picture of a cyber attack that could undermine the functioning of smart devices: ?Let?s assume that tomorrow morning we are talking about all the air-conditioning in all Israeli hospitals in the summer of Israel, [?] or If all data for all schools and universities will be deleted, who is responsible?

Padel predicts that chaos will erupt, and ministries and agencies accuse each other and people of taking to the streets.

In view of Pardo?s confidential information and the efforts of government and non-state hackers (groups such as Hezbollah and Hamas), the former spy at the helm did not consider it beyond the scope of the cyberattack to paralyze the Israeli economy.

Puzzling Scenario by Pardo Speech

Pardo cites other possible scenarios where telecom providers are attacked and unavailable on all smartphones. He used Russian allegations in Georgia as a template, and Internet access was interrupted for a few days during the 2008 war.

?At some point you will not be able to call anyone and you will not be able to send any messages. Think about the chaos that can go to any society,? he said.

Top Israeli spies say they take the risk seriously ? a quick glance Mossad and the security chief who recently retired said many of them are now hired by cyber-security companies. But Pardo said these preparations are not enough.

He suggested that hackers work together with hostile countries and criminally-oriented young people on so-called ?dark networks,? to help each other and to shift coding errors.

?When we talk about the internet, everything is possible, I heard about the [agency] trying to isolate jewelery in certain regions or crowds; we live in a revolutionary era and there is no way to stop the infiltration.?

Although cyber attacks may not leave physical impressions, their impact may even be far-reaching and unstable. In other words, cyber attacks can lead to social confusion.

?Now, if I try to define the web: the web is a weapon, a soft, silent nuclear weapon,? said Pardo. ?I can compare it with the introduction of Japan?s atomic bombs by Americans after World War II ? [and networks] You can destroy society, you can destroy the country, you can win the war without firing a bullet. ?

Pardo Speech depicts several dark scenes and warns against ignoring the cyber security team?s funding and staffing.

?We do not understand how threatening it is and we do not understand the consequences of what a threat might be (cyber attack), and we do not understand what the consequences of those threats are,? he said.

While banks are the first huge industry to recognize the threat ? and they are investing heavily in cybersecurity ? these efforts keep financial institutions ?scarcely protected?, Pardo insisted.

Sovereign governments face many challenges in establishing cyber attacks, especially months or years to develop and install defensive software.

Remedy

One possible antidote is offensive, hiring ?good? hackers to constantly try to infiltrate infrastructures and methodically fix defenses. But this requires a lot of expenses.

Pardo served as head of Mossad between 2011 and 2016 and retired from the intelligence service 35 years later. Today, he advises cybersecurity companies as chairman and chairman of XM and chairman of the board of Sepio Systems.

Read More?

A man holds a laptop computer as cyber code is projected on him. (photo credit: KACPER PEMPEL/REUTERS) Please insert a valid email address Engaging post, Read More?

thumbnail courtesy of jpost.com.

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Ex-Mossad head: Israeli cybersecurity isn?t enough?Puzzling Scenario by Pardo Speech appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 18 : DoubleDoor, a new IoT Botnet bypasses firewall using two backdoor exploits 2018-02-

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on IoT Botnet Bypasses Firewall
Today I came across this story from securityaffairs.co that looks to Security researchers that have discovered a new type of IoT botnet bypass firewall known as DoubleDoor, which can bypass firewalls and modem security using two backdoor vulnerabilities.
IoT devices remain the privileged target of cybercriminals and cyber attackers targeting so-called smart objects have seen rapid growth. Security researchers at NewSky Security (NewSky Security) have uncovered a new IoT botnet called DoubleDoor that can bypass firewalls and modem security with two backdoor vulnerabilities.
The analysis of honeypot logs enabled researchers to detect new threats, using two known backdoor vulnerabilities to manage two levels of authentication.
The first malicious code was a Juniper SmartScreen OS Vulnerability that triggered the CVE-2015-7755 vulnerability to bypass firewall certification.
CVE-2015-7755 Hard-coded backdoors affect Juniper Networks ScreenOS software, which provides support for its Netscreen firewall.
?Essentially, the Netscreen firewall?s telnet and SSH daemons can be accessed with any user name, using the hard-coded password
Powered by WPeMatico

Chapter 19 : When Western Union wired customers? money, hackers transferred their personal deets

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Western Union:
A must read story from theregister.co.uk concludes a hidden breach announcement discovery on Western Union has confirmed that one of its IT vendors was hacked, and that customer information is exposed to gangsters.
A registered reader who wishes to remain anonymous has shown us a copy of the January 31 letter he received from the remittance agency. The rumor acknowledged that a supposedly secure data storage company used by Western Union was damaged: a database filled with records of wire giant accounts was vulnerable to plundering and hackers would soon assume responsibility.
The letter reads: ?We found that some of your information may be unauthorized to access because of computer intrusions into an external supplier system used for secure data storage in the Western Union.?
?We immediately moved our external secure storage to another vendor?s system and we immediately notify law enforcement and are actively engaged in the investigation and immediately provide expert assistance to determine which personal information may have been compromised.
In other words, it sounds like a cloud-based or off-site backup storage provider is getting hacked. Now that the system is down, the police are on guard, and the digital forensics team is detecting network intrusion.
Suspicious Activity on Western Union
A spokesman for Western Union told a ?registered? reporter today: ?After detecting suspicious activity, Western Union permanently suspended all uses of the vendor?s system and took the system offline.
?Western Union immediately took steps to inform law enforcement agencies that the affected individuals and regulators have been notified and affected individuals receive a customized notification of the specific types of personal data that may affect him or her.?
According to the letter, the stored file contains the customer?s contact information, bank name, internal customer ID number of the Western Union, and transaction amount, time and ID number. It emphasizes that credit card data will never be adopted.
El Reg released a revised letter earlier this week:

@WesternUnion has been sending out letters warning of a computer security hack, blaming 3rd party data storage. Which vendor could it be?

12:06 PM ? 12 Feb 2018

View pictures on Twitter: registered
@TheRegister
@WesternUnion has been sending letters to warn computer security hackers of accusations of third-party data storage. It may be which supplier?
3:06 PM ? February 12, 2018
See other registered tweets
Twitter Ads information and privacy
Red-faced businessmen quickly pointed out that neither their internal payments nor their financial

systems were affected in the attack. Nor does it mean that third-party storage providers are the ones who give inconvenient providers of other clients time to check if they are hacked.
Western Union said it has so far not been aware of any fraud caused by data security problems, but it just recruits affected clients for one year in free identity fraud protection just to be on the safe side.
Read More?
Outside storage outfit blamed for data leak blunder Western Union has confirmed one of its IT suppliers was hacked, and that customer information was exposed to miscreants. Engaging post, Read More?
thumbnail courtesy of theregister.co.uk

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post When Western Union wired customers? money, hackers transferred their personal deets appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 20 : Russian hackers expose vulnerabilities in US cybersecurity: ?Our defense is compromis

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary US Cybersecurity:
A survey of Russian hackers led by the Associated Press revealed major problems in US cybersecurity.
Hackers, known as Fancy Bear, also allegedly disrupted the 2016 US presidential election by getting access to e-mail accounts of at least 87 top defense contractors, disclosing information about drones, stealth fighters, cloud computing, computing platforms, missiles And the rocket.
Most accounts are personal Gmail accounts, although a few are corporate accounts.
U.S. defense contractors of all sizes, including Lockheed Martin, Raytheon, Boeing, Airbus and General Atomics, as well as a number of trading groups and foreign contractors, were attacked.
Officials have not figured out what hackers have been stealing, but hackers have exposed the vulm in U.S. cyber security. According to the Associated Press, only one of the 31 contractors who spoke to the exporter got any warning from U.S. officials.
The Associated Press approached Charles Sowell, senior adviser to the director of the National Intelligence Agency.
?What they seem to be targeting and who are working on these options are some of the most advanced and advanced technologies that will have an impact on our competitive edge and our defense if any of these programs are affected,? said Sowell. ?This is really terrible.?
Hackers have used fake notifications to access email accounts.
Major General James Poss, a retired Air Force general who has conducted UAS studies for the FAA, received a notice from Google that warned him of a security breach.
?I clicked it and immediately knew I already had it,? Poss said. He quickly realized that the hacker had designed the alarm so he could enter his certificate.
The AP also talked to drone consultant Keven Gambold, who also targeted hacking. He pointed out that hackers are increasingly threatening U.S. cybersecurity and giving them technological advantages. He said: ?This will allow them to skip the years of rare experience.?
He said the threat from Russian hackers has alarmed his company, saying that if we?re dealing with client-specific data, they ?have almost returned to using a standalone system ? we?re around FedEx?s hard drive.
Read More?
An Associated Press-led investigation into Russian hackers revealed major susceptibilities in U.S. cybersecurity. The hackers, known as Fancy Bear, who also allegedly interfered with the 2016 U.S.?? Engaging post, Read More?
thumbnail courtesy of theblaze.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Russian hackers expose vulnerabilities in US cybersecurity: ?Our defense is compromised? appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 21 : Warning:Well-positioned Reddit clone is out to grab users? login credentials 2018-02-1

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Reddit Clone
A must-read story from helpnetsecurity.com defines a little known that the popular social news aggregator Reddit site have been convincingly cloned as the reddit.co domain. The author apparently does not expect the user to discover for what it is: a website designed to collect the user?s username and password.
HEADSUP: People should be cautioned on information security at @Reddit. (Phishing?) The domain reddit (.) Uses the Columbia TLD website together ? is a perfect visual Reddit for MITM.
Share this with Reddit users.
Reddit clone site
Security researcher Alex Muffett sounded the alarm on Sunday instead of noticing the Reddit team and was still waiting for Google?s secure browser to mark the site as malicious.
The fake website home page looks very much like Reddit, although clicking any non-Reddit photo or video post will return the HTTP ERROR 500 page.
:

As the author is writing this, the site is still up.
People behind fake websites also get SSL certificates so that users can see HTTPS and trust them on the ?secure? site for encrypted connections:
As I was writing this, the site is still there.
Bigger problem on Reddit clone
?Do not misunderstand, this is a valid scam,? said Azeem Aleem, RSA?s director of advanced cyber-defense practices for Europe, the Middle East, and Africa.
?They spent a lot of time and effort creating a very realistic website and even displaying a secure SSL certificate in a browser window, which is well designed and enforced, underlining the real dangers of modern spoofing attacks. It is troubling that these complex scams collect personal information, but what is even more worrisome is that these stolen data will be used to steal information because the stolen credentials are used to undermine the victims? other accounts, and to friends, colleagues And family complex phishing attacks. ?
He pointed out that time is of the essence for Reddit, and companies need to warn users about the site.
?It?s not just websites like Reddit.co ? last year, more than 14,000 certificates were used to set up phishing sites that cheated PayPal, which shows the power of the cybercriminals to padlock them to deceive unsuspecting victims The case is credible and undermines the brand?s reputation via the Internet, ?said Kevin Bocek, chief cybersecurity officer at Venafi.
?This attack is part of a bigger problem that harms the trust system used throughout the internet and explains why there is a need to build a new trust system based on reputation.The answer is a certificate credit rating to help people know What is trustworthy. ?
?This site was previously hosted by Porno, which is not a real Reddit-owned domain, was issued by Comodo, and genuine Reddit uses DigiCert-produced certificates, all of which were rated as long ago by Reddit as being flagged for repair Things, ?he explained.
?Free certificates provide very little validation, but users think they are sacred. If people can not believe the websites they visit are real, our digital world may start to crash.? Now the corporate security team needs to take action because no one else will protect you from bad guys. ?
Read more?
A convincing clone of the popular social news aggregation and discussion
(adsbygoogle = window.adsbygoogle || []).push({});
site Reddit has been spotted on the reddit.co domain. The author is obviously counting on users not to spot it for what it is: a site meant to harvest users? username and password. HEADSUP: Looking for infosec people at @Reddit. Website at (phishing?) domain reddit(.)co ? using the Colombian TLD ? was acting a pitch-perfect apparent MITM of the actual Reddit. Now returning 500 More ? Engaging post, Read More?

thumbnail courtesy of helpnetsecurity.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Warning:Well-positioned Reddit clone is out to grab users? login credentials appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 22 : For the second time CISCO issues security patch to fix a critical vulnerability in CISCO A

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Cisco ASA Vulnerability
The securityaffairs.co finds out how Cisco has tracked new security patches for a serious vulnerability (CVE-2018-0101) in its CISCO ASA (Adaptive Security Appliance) software.
The company released the same security update as the Cisco ASA software at the end of January. An attacker who is remotely unauthenticated can exploit this vulnerability to execute arbitrary code or to trigger Denial of Service (DoS) situations that result in a system reload.
The vulnerability is located in the Secure Sockets Layer (SSL) VPN feature implemented by CISCO ASA software and was discovered by Cedric Halbronn, a researcher at the NCC Group. This vulnerability earned a General Vulnerability Score of 10.0 system score.
According to CISCO, when the ?webvpn? feature is enabled on the device, it is about trying to free memory. An attacker could exploit this vulnerability by sending specially crafted XML packets to the webvpn-configured interface.
Further investigation into this vulnerability revealed more attack vectors and for that reason, the company released a new update. Researchers also found denial of service issues affecting the Cisco ASA platform.
A blog post from Cisco Systems wrote: ?After the survey was expanded, Cisco engineers discovered additional attack vectors and features that were affected by the vulnerability and were not initially identified by the NCC Group and subsequently updated for security Suggest.
Experts have noticed that this vulnerability is related to the XML parser in CISCO ASA software, and an attacker can trigger this vulnerability by sending a specially crafted XML file to a vulnerable interface.
CISCO ASA attack
The list of affected Cisco ASA products includes:
3000 Series Industrial Safety Equipment (ISA)
ASA 5500 Series Adaptive Safety Equipment
ASA 5500-X Series Next-Generation Firewall
ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
ASA 1000V cloud firewall
Adaptive Security Virtual Appliance (ASAv)
Firepower 2100 Series Security Appliance
Firepower 4110 Security Appliance
Firepower 9300 ASA Security Module
Firepower Threat Defense Software (FTD)
According to Cisco experts, there is currently no news about exploiting vulnerabilities, and it is important to apply security updates anyway.
Read more?
Cisco has rolled out new security patches for a critical vulnerability, tracked as CVE-2018-0101, in its CISCO ASA (Adaptive Security Appliance) software. At the end of January, the company released security updates the same flaw in Cisco ASA software. The vulnerability could be exploited by a remote and unauthenticated attacker to execute arbitrary code or trigger Engaging post, Read More?
thumbnail courtesy of securityaffairs.co
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post For the second time CISCO issues security patch to fix a critical vulnerability in CISCO ASA appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 23 : Malicious Trends: Cryptojacking Could Surpass Ransomware as Primary Money Maker

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Cryptojacking
What is most likely to be an overlooked story from securityboulevard.com reviews a surprising
Encryption currency is very hot. According to https://coinmarketcap.com, there are now over 1,300 cryptocurrencies accelerated with the new Initial Coin Products (ICO). Even Kodak is working with Kodak. At the moment Bitcoin is still priced higher than North Korea?s rocket, Blockchain saves only one application for the world at a time.
Cybercrime Swiftly adopting cryptocurrencies as a payment method for ransom plague is now turning to other ways to encrypt money technology. We see that stolen accounts and credit card shops use peer-to-peer DNS in the blockchain as a defense against their products.
Cypto-coin-enabled JavaScript has been placed on vulnerable websites and the #minevertising advertising campaign has begun to take off.
As a result, anyone accessing the compromised site is infected with malware that hijacks 100% of the CPU cycles and stole Monero cryptocurrencies on behalf of criminals. This event is named cryptojacking.
Read More?
Cryptocurrencies are hot. According to https://coinmarketcap.com, there are now over 1300 cryptocurrencies with new initial coin offerings (ICOs) accelerating all the time. Even Kodak is getting into the act with KODAKcoin. And currently, the price trajectory of Bitcoin is higher than a North Korean rocket, with Blockchain saving the world one application at a time?. Engaging post, Read More?
thumbnail courtesy of securityboulevard.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Malicious Trends: Cryptojacking Could Surpass Ransomware as Primary Money Maker appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 24 : A Faraday cage or air gap can?t protect your device data from these two cyberattacks

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Air Gap
This story from techrepublic.com details researchers have found a way to get around the Faraday cage and the air gap by using low-level magnetic fields that can not be stopped by traditional methods.
For safety professionals in a highly-safer environment, it is important to take the recommended steps to resist a magnetic field attack before it appears in the wild.
In two papers published by researchers at Ben-Gurion University, two common methods of physical cybersecurity, air gap, and Faraday cage were uncovered.
Faraday cage is a cage made of conductive material that completely blocks the electromagnetic fields and signals. Gap computers are computers that are completely isolated from external networks and signals. Air gap settings usually include a Faraday cage.
Anyone who interacts with a Faraday battery can prove it works ? place your smartphone in a Faraday cage and you can immediately see the signal fall. However, researchers found that normally overlooked low-level magnetic fields can still penetrate the air gap and Faraday cage, allowing attackers to intercept and steal data.
Blame magnet ?
low-frequency magnetic radiation
Dr. Mordechai Guri, research director, said that it would still work if a basic compass was brought into Faraday cage. He said: ?Although Faraday rooms can successfully block the electromagnetic signals emitted by the computer, low-frequency magnetic radiation is transmitted through the air and penetrates the metal shield in the room. This is a low-level area where attackers can hide any device that has a CPU hidden in a Faraday cage or void room. It is worth reiterating that anything that has a CPU can be manipulated by the method Guri and his team call Odini.
2. low-level magnetic fields
Devices infected with Odini malware can control the low-level magnetic fields emitted by the CPU by adjusting the CPU core load. The data can then be carried on the CPU?s magnetic field, outside the Faraday cage or air gap, and picked up by a receiving device designed to detect magnetic field manipulation. The team called Magneto?s second attack using the same CPU magnetic field method of operation but allowed it to be picked up by nearby smartphones.
Do not think sticking a smartphone in a Faraday bag or placing it in airplane mode will prevent it from detecting a signal: it is magnetic so it passes and is picked up by the device?s magnetic field sensor, which is the standard for most modern devices Feature smartphone.
Read more?
Long thought impenetrable, these forms of physical security continue to be found vulnerable. The latest attack vector is low-level magnetic fields. Engaging post, Read More?
thumbnail courtesy of techrepublic.com

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post A Faraday cage or air gap can?t protect your device data from these two cyberattacks appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 25 : Hackers Could Crack Millions of Samsung and Roku Smart TVs 2018-02-10 00:31:26

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on Samsung and Roku Smart TVs

This story from fortune.com finds out millions of so-called smart TVs have exploits that hackers can exploit.

It is based on consumer reports, which released some of the security censorship results for some smart TVs Wednesday, the name of the internet connected TV set. Among them are models sold by Samsung and Chinese TV maker TCL, which use specific features of Roku, a streaming media device company.

Although hackers can not steal sensitive data such as credit card numbers through security breaches, they can use it to manipulate people?s TVs, play offensive videos, install unwanted apps, or scroll through channels suddenly.

Consumers report: ?The process is rough, like someone with a closed-eye remote control.? But for a television viewer who does not know what happened, it can be creepy, like a hacker lurk nearby or peek at you through this set.

The Consumer Report study highlights the growing popularity of network-connected TVs and makes it easy to watch streaming video services such as Netflix on television. But connecting online makes these TVs vulnerable to hacking if they have exploits that hackers can exploit.

According to technology news site Ars Technica, in 2012, for example, security researchers said they could crack and gain control of certain Samsung smart TVs.

Consumer Reports tested a TCL smart TV with a Roku streaming software release that contains a security hole. The publication said other TV makers using Roku software include Hisense, Hitachi, Insignia, Philips, RCA, and Sharp, all of which may be affected except for some Roku streaming media devices.

Samsung and Roku Smart TVs

Roku?s streaming video software includes a so-called application programming interface or API that third-party developers can use to build their own smartphone applications like TV remote controls. However, hackers may use this API, which consumers report as ?unsafe.?

To be hacked, users must use a smartphone or a personal computer on the same Wi-Fi network to which the smart TV is connected, then visit a malicious Web site or download an application containing software code to allow hackers to take over the report.

However, Roku argues against the Consumer Reports assertion in a blog post that it proposes ?a misrepresentation of functionality.?

Roku said: ?With this API, our customer account or Roku platform has no security risks and customers can turn off this particular remote control feature.

When asked about a similar mistake that was not found on Samsung smart TVs using Roku software, a Samsung spokesman told consumers that it is investigating the issue and will release a software update this year that will probably address other Related errors.

Read More:

Millions of so-called smart TVs have security vulnerabilities that hackers could exploit. That?s according to Consumer Reports, which released results on Wednesday of a security review of certain smart TVs, the name given to Internet-connected televisions. They included models sold by Samsung as well as Chinese-TV maker TCL that use a particular feature by the streaming media device company Roku. Although hackers are unable to steal sensitive data like credit card numbers through the security holes, they could use it to manipulate people?s televisions and play offensive videos, install unwanted apps, or suddenly scroll through channels. ?The process was crude, like someone using a remote control with their eyes closed,? Consumer Reports said. ?But to a television viewer who didn?t know what was happening, it might feel creepy, as though an intruder were lurking nearby or spying on you through the set.? The Consumer Reports study highlights the growing popularity of web-connected televisions that make it easy for people to watch streaming video services like Netflix on their TVs. But being connected online puts these

televisions at risk of potential hacking if they have bugs that hackers can exploit. Engaging post, Read More?
thumbnail courtesy of fortune.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Hackers Could Crack Millions of Samsung and Roku Smart TVs appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 26 : New POS Malware, UDPoS , Steals Credit Payment Data via DNS Traffic 2018-02-10

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on UDPoS
This story from darkreading.com believes a surprising new POS malware called UDPoS that disguises as LogMeIn service pack.
Forcepoint researchers have discovered a new type of point-of-sale (POS) malware disguised as a LogMeIn service pack designed to steal data from a magnetic stripe on the back of a payment card.
UDPoS malware
Forcepoint is calling UDPoS malware differently than the usual POS tools because it uses UDP-based DNS traffic to steal credit and debit card data through firewalls and other security controls. According to the company, this is one of the few new POS malware tools.
In recent years, the United States, like many other countries, has moved away from magnetic cards based on the Europay, Mastercard, and Visa (EMV) standards for chips and PIN cards. This transition made it more difficult for criminals to use POS malware to steal payment card data, just as they did when massive theft was stolen from Target in 2013.
However, malware like UDPoS shows that criminals still have the opportunity to steal data from POS systems. For example, Trend Micro reported last year that MajikPOS, a POS malware family, was used to steal data from more than 23,300 payment cards. The retailer Forever 21, which is investigating data breaches, recently released some malware for the POS system in November last year.
Forcepoint special investigator Luke Somerville said there is no evidence that UDPoS is currently being used to steal credit or debit card data. However, Forcepoint?s testing shows that malware does indeed complete successfully.
In addition, one of the command and control servers that communicate with malware is active while Forcepoint investigates the threat. ?[This] means that the author is at least ready to deploy such malware in the field,? Somerville said.
Possible targets for malware include POS systems for hotels and restaurants and any other location with a handheld device for swiping credit and debit cards.
Somerville said: ?This malware targets Windows systems, which are typically variants of the Windows XP kernel, and large retailers have not recently updated their systems and may have hundreds or even thousands of vulnerabilities The machine. ?
Forcepoint discovered the malware while investigating an obvious LogMeIn service pack, which generated a large number of unusual DNS requests. The company?s analysis of the malware showed that it contacted a command and control server that also had LogMeIn?s themed identity.
Somerville said there is no evidence that LogMeIn?s remote access service or product was in any way abused as part of the malware deployment process. In contrast, the authors of UDPoS seem to use the LogMeIn brand as a disguise. He said: ?The use of the names of legitimate products as the subject of documents and service names is, in fact, an attempt to limit the suspicion of the presence of these artifacts on infected computers.
Forcepoint itself does not understand the process that malware authors use or plan to deliver UDPoS on point-of-sale systems. But using the LogMeIn brand to disguise malware is not by accident. Many retailers and other organizations use LogMeIn?s software to enable remote management of their POS systems.
Given the filenames already selected, it is clear that malware authors want to sneak their malware into these systems in the name of LogMeIn software updates, Somerville said.
LogMeIn issued a warning this week warning its users not to fall into scams. ?According to our investigation, the purpose of the malware is to trick a savvy user into performing a malicious e-mail, link or file that may contain the name of LogMeIn,? the company states.
Read More?
UDPoS is disguised to appear like a LogMeIn service pack, Forcepoint says?. Engaging post, Read More?
thumbnail courtesy of darkreading.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post New POS Malware, UDPoS , Steals Credit Payment Data via DNS Traffic appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 27 : Amazon issues security patch for Key Service after researcher claims hack 2018-02-10

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on key service vulnerability patch
SC media reveals Amazon will release a security patch for its ?critical? service in the upcoming update, and a researcher posted a video demo claiming they are using Raspberry Pi to attack Amazon devices.
Researcher MG, who placed a device called ?Break & Enter dropbox? near Amazon devices without any configuration or network access and claimed to have carried out an attack that allowed them to take delivery of a fake Entering a door simulates a delivery but does not ensure that the door is locked before leaving.
It is unclear which methods are used or which ones are exploited. MG also said he will not release all the technical details of the attack until Amazon releases a patch, telling Forbes to interfere with the Wi-Fi connection used by the Key system instead of Amazon software.
Key service vulnerability
An Amazon spokesman told SC Media that the key service vulnerability in the video indicates a problem with the Wi-Fi protocol. Instead of Amazon software, it?s important to note that this is a mock attack wherein real-life scenarios the device?s security settings have informed Amazon that the door is unlocked. The spokesman added that a real delivery driver would be trained to ensure that the door was locked before leaving the site.
This update addresses the unlikely scenario described as a user opening the door, a deauthorization occurs, and then the user cannot enter or leave after a predetermined number of seconds trigger the deauthorization.
Amazon is issuing a security patch for its Key services shortly after a researchers posted a video demonstration of them claiming to hack the Amazon device. Engaging post, Read More?
thumbnail courtesy of scmagazine.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Amazon issues security patch for Key Service after researcher claims hack appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 28 : Alert to Google Chrome users: Don?t fall prey to this fake tech support scam 2018-02-1

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Google Chrome users don?t fall prey to this fake tech support scam
I couldn?t believe this story from techrepublic.com that discovers things we don?t talk about but according to Malwarebytes, fake Google Chrome warnings require users to contact a fake tech support scam hotline, which has seen an increase in the number of Windows users in the past quarter.
Technical support scams may use the API to freeze the user?s browser, prompting them to call the fake support line and share their credit card information.
According to a blog post from Malwarebytes on Tuesday, technical support fraud is increasingly reaching Windows users on Google Chrome, even as it has been upgraded to the latest version.
Fake tech support scam
These frauds take the form of browser alerts that require users to contact a fake Helpline to attempt to obtain credit card information. The attack on Google Chrome is far from reaching the web first: January 2017, when you Google search for ?Facebook Customer Support,? the hottest is a scam. And in February 2017, Google search results appear to be an advertisement for Amazon.com, which is actually a malicious link to Windows Support Scam.
The U.S. Federal Trade Commission recently launched a campaign called ?Operational Technology Traps? to stop these scams, but as our sister site ZDNet has pointed out, they may still be ubiquitous. This means that businesses must be particularly vigilant in employee training to identify fraud, phishing attacks, and other cybersecurity issues.
According to Malwarebytes, there was an increase in false browser alerts that prompted these technical support scams in the last quarter. Most of these attacks come from malicious advertising and threatened websites, and criminals want to scare users of calling numbers-sometimes even completely locking up the browser.
For example, using the history.pushState API technique, hackers abused HTML5 to freeze the computer. According to Malwarebytes, other tools, known as pop-up downloads, can get users stuck between different tabs.
Since these attacks do not seem to slow down, companies must train end users to recognize them. The best way to deal with this type of attack is to avoid panic and use Task Manager to close the browser. The pop-up window itself is usually harmless, as long as the user does not dial the number provided.
Read More?
Fake browser alerts pushing tech support scams increased last quarter, even in the latest version of Chrome. Engaging post, Read More?
thumbnail courtesy of techrepublic.com

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Alert to Google Chrome users: Don?t fall prey to this fake tech support scam appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 29 : Spectre security patch by Intel, currently only for Skylake chips 2018-02-08 16:23:16

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on Spectre Security Patch

Today I came across this story from securityaffairs.co that finally reviews a partial Spectre security patch is on its way. Intel is releasing a new firmware update to address the Skylake Processor Spectre Vulnerability CVE-2017-5715.

Intel is releasing a new firmware update limited to the Skylake processor to address the spectre vulnerabilities and expects patches for other platforms to be released soon.

Spectre Attack Capability to stop by Spectre security patch

Spectre attacks allow user-mode applications to extract information from other processes running on the same system. It can also be used to extract information from your own processes via code, for example, you can use malicious JavaScript to extract login cookies from other browsers? memory.

Spectre attacks break the isolation between different applications, allowing information to leak from the kernel to the user program and from the hypervisor to the guest system.

The company offers a beta version to update customers and partners that work with other processors for extensive testing prior to final release.

We all know the disturbing story about security patches released by Intel. On January 3, the whitelist hackers at Google Project Zero disclosed features on Intel chips called Meltdown (CVE-2017-5754) and spectre (CVE-2017-5753) And CVE-2017-5715), Intel immediately released security patches, but in many cases, they created problems for the system.

Many companies have introduced patches to reinstate Intel updates, including Red Hat and Microsoft.

Spectre security patch update

Intel now seems to have a clearer idea of the reasons for the problems observed after deploying the initial update and releasing the new microcode update.

?For those who care about system stability, we?re also working with our OEM partners as we complete newer solutions, opting to use the previous version of microcode, but does not show these issues, but deletes Variant 2 (spectre) Mitigation This will be provided by the BIOS update and will not affect the mitigation of Variant 1 (spectre) and Variation 3 (Melting). ?Identifies the microcode revision guide released by Intel.

Spectre Impacts

Do Spectre and Meltdown patches hurt performance?

These patches generally mitigate the vulnerabilities by altering or disabling how software code makes use of the speculative execution and caching features built into the underlying hardware. The downside of this, of course, is that these features were designed to improve system performance, and so working around them can slow your systems down. While there were initial reports of performance hits up to 30 percent, benchmarks from Phoronix indicate that 5 to 10 percent seems more typical.

Frequent restarts and other issues

Frequent restarts and other issues related to fixing CVE-2017-5715 spectre Variant 2 affect virtually any platform, including systems running on Broadwell Haswell CPUs, as well as Ivy Bridge-, Sandy Bridge-, Skylake- and Kaby-based Lake?s platform. Read Cyberwisdom: Embarrassed Microsoft rolled out another Spectre patch on top of the patch to disable mitigations for Spectre v2 attacks

Although many users choose not to install patches to avoid problems, security companies are reporting the first PoC malware exploiting ?Meltdown and Spectre.?

Vulnerability explanation

The so-called Meltdown and Specter hardware vulnerabilities allow so-called bypass channel attacks: in the case of Meltdown this means that there is a risk of malicious access to sensitive information in kernel memory, and for Spectre user applications may read kernel memory and others Application memory. Therefore, an attacker can read sensitive system memory that may

contain passwords, encryption keys, and e-mail, and use that information to make a local attack.
Systems with microprocessors that make use of speculative execution and indirect branch prediction may allow for unauthorized disclosure of information to an attacker with local user access through sidechannel analysis.
On January 17, AV-TEST?s experts reported that they have found 77 malicious software samples that are clearly related to the Intel vulnerability ? Read Cyberwisdom: Meltdown and Spectre Chip Flaw and Vulnerability Implementation Guide Update: Intel holding off Patches
What is speculative execution?
Speculative execution essentially involves a chip attempting to predict the future in order to work faster. If the chip knows that a program involves multiple logical branches, it will start working out the math for all of those branches before the program even has to decide between them. For instance, if the program says, ?If A is true, compute function X; if A is false, compute function Y?, the chip can start computing both functions X and Y in parallel before it even knows whether A is true or false. Once it knows whether A is true or false, it already has a head start on what comes after, which speeds up processing overall. Or, in another variation, if a chip learns that a program makes use of the same function frequently, it might use idle time to compute that function even when it hasn?t been asked to, just so it has what it thinks the answer will be on hand.
What is caching?
Caching is a technique used to speed up memory access. It takes a relatively long time for the CPU to fetch data from RAM, which lives on a separate chip, so there?s a special small amount of memory storage called CPU cache on that lives on the CPU chip itself and that can be accessed very quickly. This memory gets filled with data that the chip will need soon, or often. What?s relevant for our situation is that data that?s output by speculative execution is often stored in a cache, which is part of what makes speculative execution a speed booster.
The problem arises when caching and speculative execution starts grappling with protected memory.
What is protected memory?
Protected memory is one of the foundational concepts underlying computer security. In essence, no process on a computer should be able to access data unless it has permission to do so. This allows a program to keep some of its data private from some of its users and allows the operating system to prevent one program from seeing data belonging to another. In order to access data, a process needs to undergo a privilege check, which determines whether or not it?s allowed to see that data.
But a privilege check can take a (relatively) long time. So ? and this is the key to the vulnerability we?re discussing ? while the CPU is waiting to find out if the process is allowed to access that data, thanks to speculative execution, it starts working with that data even before it receives permission to do so. In theory, this is still secure because the results of that speculative execution are also protected at the hardware level. The process isn?t allowed to see them until it passes the privilege check, and if it doesn?t pass the check, the data is discarded.
The problem arises because the protected data is stored in CPU cache even if the process never receives permission to access it. And because CPU cache memory can be accessed more quickly than regular memory, the process can attempt to access certain memory locations to find out if the data there has been cached ? it still won?t be able to access the data, but if the data has been cached, its attempt to read it will be rejected much more quickly than it otherwise would. Think of it as knocking on a box to see if it?s hollow. Because of the way computer memory works, just knowing the addresses where data is stored can help you deduce what the data is. This is what?s known as a side-channel attack.
What?s the difference between Spectre and Meltdown?
If you want a much more technical description of how Spectre and Meltdown work, you should check out the post on Google?s Project Zero site that was most of the world?s introduction to it. To keep it short and simple, both Spectre and Meltdown could allow potential attackers to get

access to data they shouldn?t have access to using the techniques outlined above, but their effects are somewhat different:

Meltdown got its name because it ?melts? security boundaries normally enforced by hardware. By exploiting Meltdown, an attacker can use a program running on a machine to gain access to data from all over that machine that the program shouldn?t normally be able to see, including data belonging to other programs and data that only administrators should have access to. Meltdown doesn?t require too much knowledge of how the program the attacker hijacks works, but it only works with specific kinds of Intel chips. This is a pretty severe problem but fixes are being rolled out.

By exploiting the Spectre variants, an attacker can make a program reveal some of its own data that should have been kept secret. It requires more intimate knowledge of the victim program?s inner workings, and doesn?t allow access to other programs? data, but will also work on just about any computer chip out there. Spectre?s name comes from speculative execution but also derives from the fact that it will be much trickier to stop ? while patches are starting to become available, other attacks in the same family will no doubt be discovered. That?s the other reason for the name: Spectre will be haunting us for some time.

Why are Spectre and Meltdown dangerous?

Meltdown and Spectre both open up possibilities for dangerous attacks. For instance, JavaScript code on a website could use Spectre to trick a web browser into revealing user and password information. Attackers could exploit Meltdown to view data owned by other users and even other virtual servers hosted on the same hardware, which is potentially disastrous for cloud computing hosts.

But beyond the potential specific attacks themselves lies the fact that the flaws are fundamental to the hardware platforms running beneath the software we use every day. Even code that is formally secure as written turns out to be vulnerable because the assumptions underlying the security processes built into the code ? indeed, built into all of the computer programming ? have turned out to be false.

Mitigating now is to wait and patch our system.

Read more?

Intel is releasing new firmware updates that should address Spectre vulnerabilities CVE-2017-5715 for Skylake processors. Intel is releasing new firmware updates limited to Skylake processors to address Spectre vulnerabilities, patches for other platforms are expected very soon. The Spectre attack allows user-mode applications to extract information from other processes running on the same system. It can also be exploited? Engaging post, Read More?

thumbnail courtesy of securityaffairs.co

more?

?I can?t emphasize enough how critical it is for everyone to always keep their systems up-to-date,? wrote Navin Shenoy, executive veep and general manager of Intel?s data centre group, bemoaning the fact that punters are slow to install patches and criminals use that tardiness to do their worst.

Intel adopts Orwellian irony with call for fast Meltdown-Spectre action after slow patch delivery

For now, have some code that won?t crash Skylakes and stay close to your Telescreens Intel?s offered the world some helpful advice about how to handle the Meltdown and Spectre chip design flaws it foisted on the world.?? Intel adopts Orwellian irony with call for fast Meltdown-Spectre action after slow patch delivery

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing

list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Spectre security patch by Intel, currently only for Skylake chips appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 30 : Elizabeth Warren: Equifax hid hackers? theft of passport numbers, Equifax said no 201

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary:
The nypost.com guides a revealing on US Senator Elizabeth Warren said on Wednesday that the number of online thieves who hacked the Equifax database in 2017 is an unknown number of passports ? a hidden theft by credit reporting agencies.
But the running company opened fire on lawmakers and said it did not reveal the theft because it never happened.
The company said Warren may be the most outspoken Equifax critic.
The prospect of the hijacking of passport numbers disclosed in a report from a four-month investigation conducted at the office in Warren has drawn widespread concern throughout the country.
The hijacking of passport numbers is a serious matter, as these figures may allow hackers to sell information to terrorists who can then make fake U.S. passports.
Warren?s office will not say that there is evidence that the passport number was one of the 145.5 million adults stolen from Equifax last year ? just the ?passport? folder in the corporate database.
The report said: ?Equifax did not disclose the fact that hackers get the consumer passport number.
Meanwhile, Equifax says there are no numbers in the folder.
An Equifax spokeswoman confirmed that the thief passed through this folder, but no passport information was ?visited? ? since there has never been any passport information.
In an interview with the Post, Equifax spokesman Meredith Griffanti said: ?The easiest way to understand this is to have a passport-affixed field with no actual data.
Last year, credit reporting agencies found the database hacked in the country, stolen the credit card verification numbers and tax numbers of 147.5 million adults and shaken the country.
In a Senate hearing last fall, Warren deprived former Equifax chief executive Richard Smith of trying to maintain his passion for the company through her report.
It claimed that the cyber attack was worse than first thought ? the company?s response has been poor.
Reuters reported this week that the Consumer Financial Protection Agency is relaxing its investigation of Equifax hackers.
Warren spokesman Lacey Rose said in a statement: ?Equifax concealed the irregularities from the public for weeks and then confused consumers with information about their data being stolen and told Congress One thing, and is talking about something totally different.
?Equifax needs to talk directly to the Senate Banking Committee and the American people,? Rose added.
Read More?
Thanks for contacting us. We?ve received your submission. Sen. Elizabeth Warren (D-Mass.) on Wednesday said cyber thieves who hacked Equifax?s database in 2017 made off with an unknown number of passport numbers ? a theft the credit-reporting agency has kept hidden. But the embattled company shot right back at the lawmaker, saying it didn?t disclose the theft because it never happened. Warren, perhaps the most outspoken Equifax critic, is working from outdated information, the company said. The prospect of the passport number heist ? revealed in a report that resulted from a four-month investigation by Warren?s office ? got plenty of attention across the country. A passport-number heist is serious business because the data could allow hackers to sell the information to terrorists who could then create phony US passports. When pressed, Warren?s office would not say that it had proof that passport numbers were among the information on 145.5 million adults that was stolen from Equifax last year ? just that the passport information folder in the company?s database was ?accessed.? ?Equifax failed to disclose the fact that the hackers gained access to consumers? passport numbers,? the report said. Meanwhile, Equifax said there were no numbers in the folder?. Engaging post, Read More?
thumbnail courtesy of nypost.com

Equifax failed to offer basic security, senator says
Equifax (EFX) ignored warnings ahead of a massive security breach of data on more than 145 million Americans, then failed to quickly inform consumers, regulators and investors afterwards. That?s according to a report from Sen. Elizabeth Warren, D-Massachusetts, who?s calling for ?real consequences? when credit reporting agencies ?screw up.? The missive by Warren, a vocal critic of banks and other Wall Street entities, comes days after Reuters reported that the Consumer Financial Protection Bureau, or CFPB, had put a probe of the Equifax breach ?on ice.? Started by former CFPB Director Richard Cordray, the agency?s efforts regarding Equifax have derailed under its new head, Mick Mulvaney, the wire service reported. ?Equifax set up a flawed system to prevent and mitigate data security problems, ignored numerous warnings of risks to sensitive data, failed to notify consumers, investors, and regulators about the breach in a timely fashion, took advantage of federal contracting loopholes and failed to protect IRS taxpayer data, and inadequately assisted consumers following the breach,? a four-month investigation found, according to a news release. ?The American public deserves answers ? and Mick Mulvaney needs to let the CFPB do its job and investigate Equifax?s massive data breach, not shut it down,? stated? Equifax failed to offer basic security, senator says

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Elizabeth Warren: Equifax hid hackers? theft of passport numbers, Equifax said no appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 31 : Cybercriminals exploiting traditional trust measures for business compromises, study 2

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Web Site Vulnerabilities
A must-read story from scmagazine.com and techrepublic.com evaluate hidden facts on web site vulnerabilities:
42% of the 100,000 sites on the network are using software that is vulnerable or has been attacked in some way. ? Menlo Security, 2018
4,600 phishing sites use legitimate hosting services to avoid detection. ? Menlo Security, 2018
According to the latest Menlo Security report, many of the places we think are the safest places on the Internet are actually quite dangerous to business people and consumers. The report found that about 42% of the sites in the top 100,000 sites use software that turns them on or has been attacked in some way.
Cybercriminals use long-term confidence trust measures, including the reputation or category of certain websites, to avoid being detected and to increase the effectiveness of the attacks. This means that businesses must be vigilant and ensure that cyber health measures are in place, including employee education and multilayered protection.
Cybercriminals are using traditional methods of trust to gain a foothold on user systems through back-office requests, phishing sites, and cybersquatting that endanger credible sites.
Although many companies have used categories like business and economics, shopping, news and media, and malware to help shape security policies, researchers warn that depending on the Menlo security posture of the network, treating any category as inherently no longer valid It is advisable that the 2017 annual report be released on February 5, 2017.
The researchers said in the report: ?Many companies have used these categories to help shape their safety policies.? Unfortunately, taking into account that any category is inherently ?safe? is no longer desirable. According to our research, more than a third of all websites in the news, media, entertainment and arts, shopping, travel, etc., are at risk. ?
Web site vulnerabilities from the third party
The problem stems from third-party vulnerabilities, which are generally linked to 25 content background sites such as video clips and online advertisements, and corporate security administrators do not have the tools to monitor these connections. Anyone of them will make them vulnerable to backdoor attacks. Cybercriminals use long-term confidence trust measures, including the reputation or category of certain websites, to avoid being detected and to increase the effectiveness of the attacks. Now businesses must be vigilant and ensure that third party together with their cybersecurity health measures are in place, including employee education and multilayered protection and keep the business in the safe harbor on cyber from threats.
A Remedy for keeping your business safe harbor on cyber from vulnerabilities
In order to keep your business safe harbor on cyber, you need:
Log Collection & Aggregation
Security Incident Event Management (SIEM)
Incident Response & Reporting
Continuous Monitoring / Detection (24×7)
Malware Forensic Examination
Advanced Indicator Sharing (AIS)
Automation of Defense Countermeasure Deployment (DC&T)
Indicators of Attack (IOAs)
Indicators of Compromise (IOCs)

Multiple Storage Options and Retention Lengths Available
Legislative Regulation Compliance
I have found an external cybersecurity service partner, called R&K Cyber Solutions LLC (R&K) that provides both much needed cybersecurity 24×7 operation center and solutions to meet the legislative requirements. R&K has affordable solutions that allow its partners to establish real budgets when dealing with the cost of a Cyber Program. R&K also specializes in [providing

affordable solutions for meeting tough Legislative Regulations such as Defense Federal Acquisition Regulation Supplement (DFARS), the Federal Acquisition Regulation (FAR), the Health Insurance Portability and Accountability Act (HIPAA), (PCI DSS) Payment Card Industry Data Security Standard and the EU General Data Protection Regulation (GDPR). R&K exceeds expectations with their reputation and history of awards.

To learn more about their services, contact your next cybersecurity operations provider today by visiting www.rkcybersolutions.com, or R&K Cyber Solutions LLC, Office: 703.326.0755, or Email: inquiries@ rkcybersolutions.com.

***For a limited time, Mention the code: ?David Eng February? to get 5% off for the initial trial special.

Web site vulnerabilities

The report notes that ordinary websites connect to 25 content background sites, such as video clips or advertisements. Most enterprise security administrators lack the necessary resources to monitor these back-office connections, leaving organizations vulnerable to backdoor attacks.

The report also found that efforts to categorize locations into different categories were largely ineffective. For example, websites belonging to the ?Business and Economics? category have had the highest number of security incidents in the past year and have hosted more phishing websites and more sites that run vulnerable software (such as PHP 5.3.3), But not any other category ?gambling.?

advertising

The report found that about 49% of ?News & Media? websites were considered risky, with 45% of ?Entertainment & Arts? websites and 41% of ?Travel? websites considered as at-risk.

Increasingly sophisticated phishing attacks: The report found that some 4,600 phishing sites use legitimate hosting services to avoid detection. Instead of using other alternatives, attackers can more easily set up subdomains on legitimate hosting services, which are often whitelisted by the company.

The report found that domain name registrations or the existence of fake domain names that contain misspelled words for phishing and malware delivery still exist. About 19% of the domain names are found in trusted categories such as financial services, news, and media.

The report found that 49% of news and media sites, 45% of entertainment and art sites, 41% of travel sites, 40% of personal websites and blogs, 39% of social sites, 39% of businesses and economies are at risk, Not as safe as they seem, is a phishing website or a phishing website.

Vulnerable software used on trusted sites also poses a significant risk. The report found that according to Alexa?s rankings, 42% of the top 100,000 websites use software that makes them vulnerable or has been attacked in some way.

Some of the most popular software put these sites at risk, 32,669 sites put Microsoft IIS 7.5 users in jeopardy, 26,796 sites put PHP/5.45.15 users in jeopardy, 18,379 sites put users in apache / 2.2.15 risk.

The predominantly vulnerable website categories included 51,045 commercial and economic sites, 25,977 websites, 20,675 personal blog sites, 1,7083 news media sites and 1,669 adult porn sites.

The researchers said that business and economics websites have experienced the most security incidents, and they contain more websites that run vulnerable software such as PHP 5.3.3 than any other category.

To avoid potential threats, the researchers advised site owners to ensure that their servers run the latest software updates and to investigate technologies such as content security tactics. The researchers added that consumers should devoutly download software updates to avoid vulnerable technologies such as Adobe Flash and use Chrome as much as possible.

Cybercriminals exploiting traditional trust measures for compromises, study

Cybercriminals are exploiting traditional measures of trust to gain a foothold on users systems by

compromising trusted sites?. Cybercriminals exploiting traditional trust measures for compromises, study

and

Phishing attacks continue to grow more sophisticated, as 4,600 phishing sites use legitimate hosting services, according to Cybercriminals exploiting traditional trust measures for business compromises. Engaging post, Read More?

thumbnail courtesy of techrepublic.com.

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Cybercriminals exploiting traditional trust measures for business compromises, study appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 32 : iPhone ? Apple iBoot Source Code Leaked on Github 2018-02-08 16:23:15

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Apple iBoot code
A recent story from thehackernews.com focuses a surprising situation on the source code for the core components of the Apple iPhone operating system is said to have been leaked on GitHub, which could allow hackers and researchers to discover a now unknown zero-day vulnerability in order to develop ongoing malware and iPhone jailbreak.

The source code seems to be iBoot ? a key part of the iOS operating system that takes care of all security checks and ensures that trusted versions of iOS are loaded.
In other words, it?s just like the iPhone?s BIOS. As long as you turn on your iPhone, it ensures that the kernel and other system files have been fully signed by Apple and will not be modified.
The iBoot code was originally shared online a few months after Reddit, but it just reappeared on GitHub today (the repository is now unavailable due to the DMCA removal). Motherboard consulted a number of security experts to confirm the legitimacy of the code.
However, it is unclear whether the iBoot source code is completely real, who is behind this major vulnerability, and how the leaker managed to get his / her code first.
The leaked iBoot code appears to come from a version of iOS 9, which means the code is not completely related to the latest iOS 11.2.5 operating system, but parts of the iOS 9 code may still be used by iOS in iOS 11.
?This is a 9.x SRC that you might get confused with the source code to find vulnerabilities as a security researcher and even bootrom source code for some devices ? even if it?s not possible to compile due to missing files ?? Twitter said.
Leaked source code was listed as ?the biggest loophole in history? by many of the book authors Jonathan Levin inside iOS and MacOS. He said the leaked code appears to be the real iBoot code because it matches the code that he decompiled himself.
Apple has opened up some of the macOS and iOS parts in recent years, but the iBoot code has been carefully kept secret.
As Motherboard points out, the company has iBoot as an integral part of the iOS security system and classifies the secure boot component as a top-level vulnerability in the loophole-bounty program, providing $ 200,000 for each reported vulnerability.
As a result, leaked iBoot code can present a serious security risk as hackers and security researchers dig deeper into the code to look for undisclosed vulnerabilities and write persistent malware vulnerabilities such as rootkits and bootkits.
In addition, jailbreakers can find useful stuff from the iBoot source to jailbreak iOS and provide a wired jailbreak for iOS 11.2 and later.
It is worth noting that newer iPhone and other iOS devices come with Secure Enclave to prevent potential problems with the leaked iBoot source code. So, I really suspect the leak code will be of great help.
Although Github has disabled the repository hosting the iBoot code after the company issued a DMCA takedown notice, Apple has not commented on the recent leak. However, the code is already there.

Read more?

Apple source code for a core component of iPhone?s operating system has purportedly been leaked on GitHub, that could allow hackers and researchers to discover currently unknown zero-day vulnerabilities to develop persistent malware and iPhone jailbreaks. The source code appears to be for iBoot?the critical part of the iOS operating system that?s responsible for all security checks and Engaging post, Read More?

thumbnail courtesy of thehackernews.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
?

```
(adsbygoogle = window.adsbygoogle || []).push({});
```

The post iPhone ? Apple iBoot Source Code Leaked on Github appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 33 : Cyber Espionage Group Targets Asian Countries With Bitcoin Mining Malware ? PZCha

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on PZChao Operation:
Today I came across this story from thehackernews.com that security researchers discovered a tailor made piece of malware as the PZChao operation has caused major damage in Asia in the past few months and is able to perform nasty tasks such as password stealing, Bitcoin mining and full remote access to compromised systems for hackers.
PZChao operation
Known as the PZChao operation, attacks discovered by security researchers at Bitdefender have been targeted at organizations in the government, technology, education and telecommunications sectors in Asia and the United States.
The researchers believe that the nature, infrastructure, and payloads used in the PZChao attack, including variants of the Gh0stRAT Trojan, are reminiscent of the infamous Chinese hacker group Iron Tiger.
However, this movement has evolved into its payload to lower Trojans, conduct cyber espionage and encrypt my bitcoins bitcoin.
According to the researchers, the PZChao operation campaign attacked the goals of Asia and the United States with attacks similar to the Iron Tiger, signaling the possible return of the notorious Chinese APT team.
The organization that PZChao has been targeting has been a malicious VBS file attachment since July last year and is delivered through a highly targeted phishing email.Cyber ??spyware malware
If executed, the VBS script downloads additional payloads from the distribution server hosting ?down.pzchao.com? to the affected Windows machines, which resolves to the IP address in Korea (125.7.152.55) upon investigation.
Threats behind an attacker At a minimum, the controller can control five malicious subdomains in the ?pzchao.com? domain, each of which is used to perform specific tasks such as downloading, uploading, RAT-related operations, and malware DLL delivery.
The researchers point out that the payloads that threaten the deployment of actors are ?diverse, including the ability to download and execute additional binaries, gather private information, and execute commands remotely on the system.?
The first payload on the compromised machine was a bitcoin miner disguised as a ?java.exe? file that mined encryption at 3 am every three weeks (when most people were not in front of their system) currency.
For password theft, the malware also deploys one of the two versions of the Mimikatz password scanning utility (depending on the operating architecture of the affected computer) to obtain the password and upload it to the command and control server.
The final payload of PZChao operation includes a slightly modified version of the Gh0st Remote Access Trojan (RAT), which is designed to be backdoor implanted and has very similar versions detected in cyber-attacks associated with the Iron Tiger APT group.
Gh0st RAT is equipped with a large number of network spy features, including:
Real-time and offline remote key record
List all active processes and open the window
Listen to the conversation through the microphone
Eavesdropping real-time video camera source
Allow remote shutdown and reboot the system
Download binary files from the Internet to a remote host
Modify and steal documents.
All of the above features allow remote attackers full control over an infected system, monitor victims and easily leak confidential data.
The researchers said that although PZChao?s tools have been used for several years, they have been tested for combat and are better suited for future attacks.
Iron Tiger, known since 2010 as ?Emissary Panda? or ?Threat Group-3390,? is China?s Advanced Contingency Threat (APT) group whose activities have led to the theft of large numbers of

directors and managers of U.S. defense contractors.
Similar to the PZChao campaign, the group also attacked entities in China, the Philippines and Tibet and attacked the U.S. targets.
Read more?
Security researchers have discovered a custom-built piece of malware that?s wreaking havoc in Asia for past several months and is capable of performing nasty tasks, like password stealing, bitcoin mining, and providing hackers complete remote access to compromised systems. Dubbed Operation PZChao, the attack campaign discovered by the security researchers at Bitdefender have been targeting Engaging post, Read More?
thumbnail courtesy of thehackernews.com

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Cyber Espionage Group Targets Asian Countries With Bitcoin Mining Malware ? PZChao operation appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 34 : Alert: Unable to detected new Shurl0ckr. Zero-day ransomware on Microsoft & Goo

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on Shurl0ckr. Zero-day Ransomware:

This story from itproportal.com lays out a revealing that Bitglass, the next-generation cloud access security broker (CASB) company, today announced the results of its latest study, P.I., a malware tracking cloud infection. While cloud and mobile are a boon to productivity and agility, they are also a compelling goal for hackers seeking to distribute malware and steal sensitive data.

As businesses have adopted cloud services to increase their productivity and agility, hackers view cloud services as their next important goal of distributing malware and stealing sensitive data from businesses and individuals.

Undetected Shurl0ckr. Zero-day ransomware:

Both Google Drive and Microsoft Office 365 have built-in malware protection, but failed to identify a new Gojdue ransomware called the Shurl0ckr. Zero-day ransomware sidestepped most of the major anti-virus platforms: only 7% of 67 test tools detected it.

Researchers at the Bitglass Threat Research team discovered Shurl0ckr while scanning malware in the cloud. It is recognized by Cylance as a form of ransomware-as-a-service.

Shurl0ckr works the same way as Satan ransomware. Hackers create ransomware payloads and distribute them through phishing or driver downloads. Malicious software encrypts files on disk in the background until the victim pays bitcoin ransom. Hackers pay authors a certain percentage.

Together with Cylance, Bitglass identified a new Gojdue ransomware known as ShurL0ckr on the Blacknet. Two well-known cloud platforms, Google Drive and Microsoft Office 365, with built-in malware protection, did not identify ransomware. In addition, Bitglass also tested VirusTotal, a malware-capable malware that detects files containing the ransomware of the ShurL0ckr. Only 7% of test AV engines successfully detected new malware.

To analyze the proliferation of malware in the cloud, Bitglass Threat Research also scans tens of millions of files and finds high rates of infection in cloud applications. For applications with built-in malware protection, such as Microsoft Office 365 and Google Cloud hard disk.

Mike Schuricht, vice president of product management, said: ?Malware is always a threat to the enterprise, and cloud applications are an increasingly attractive distribution mechanism. ?Most cloud providers do not provide any malware protection and those efforts to detect zero-day threats.Only an artificial intelligence-based solution to discover new malware and ransomware to ensure cloud data security.?

Bitglass threat research highlights Shurl0ckr. Zero-day ransomware Capability:

A new kind of ransomware goes to the cloud near you: Bitglass Threat Research Group found a new Gojdue ransomware on the dark network and tested built-in malware protection for Google Drive and Microsoft Office 365. The ShurL0ckr, ransomware-as-a-service functions in much the same way as the widely-spread Satan ransomware. Generate and distribute the ransomware load on the encrypted disk file, the hacker to pay a certain percentage of the author.

Native Cloud AV can not detect zero-day malware: Both Google Drive and Microsoft Sharepoint can not detect ShurL0ckr ransomware using their built-in threat engine. When scanning antivirus engines, only 7% or one-fifth detect malware ? one of them is Cylance, which protects Bitglass customers.

Malware spreads in the cloud: 44% of the organizations being scanned have some form of malware at least in one of its cloud applications.

Malware can not be distinguished and all SaaS applications suffer: on average, one-third of SaaS application company instances contain malware. Among the four major SaaS applications OneDrive, Google Drive, Box and Dropbox,

Microsoft OneDrive has the highest infection rate of 55%. Google Drive had the second highest infection rate with 43% affected, followed by Dropbox and Box, at 33%.

Which file types are malware disguised? : Bitglass identifies the first five file categories by infection rate. Scripts and executables that launch malicious applications by clicking the button

(42%) are the most common types of infected files. Most users trust Microsoft Office files open without hesitation, with the second most common business file type (21%).
Additional Information:
Read the full Malware PI report: bitglass.com/malware-pi
Download the solution brief for more on Bitglass? Advanced Threat Protection: https://pages.bitglass.com/CASB-Threat-Protection-Cylance.html
By Anthony Spadafora an hour agoNews As organisations have adopted cloud services to increase their productivity and agility, so to have hackers who see cloud services as the next big target for distributing malware and stealing sensitive data from businesses and individuals. In its latest research report titled ?Malware, P.I., Tracking Cloud Infections?, the cloud access security broker Bitglass has identified a new strain of ransomware that is able to elude detection from a majority of anti-virus (AV) engines and well-known cloud applications including Google Drive and Microsoft Office 365. Working together with the data protection company Cylance, the firm was able to identify a new strain of the Gojdue ransomware on the dark web dubbed ShurL0ckr.
This ransomware-as-a-service operates in a similar way to the popular Satan ransomware and the hackers who deploy it pay a percentage of the funds it collects from victims to its author after creating and distributing a ransomware payload that encrypts users? files. Both Google Drive and Microsoft Office 365 were unable to identify ShurL0ckr. Bitglass also utilised the service VirusTotal to see if 67 of the top malware engines could detect the new strain ransomware contained within a file and only seven percent of the? Engaging post, Read More?
thumbnail courtesy of itproportal.com

New Zero-Day Ransomware Evades Microsoft, Google Cloud Malware Detection
Shurl0ckr, a form of Gojdue ransomware, was not detected on SharePoint or Google Drive?. New Zero-Day Ransomware Evades Microsoft, Google Cloud Malware Detection

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Alert: Unable to detected new Shurl0ckr. Zero-day ransomware on Microsoft & Google Cloud appeared first on Safe Harbor on Cyber.

Chapter 35 : 42% of the most popular websites are vulnerable to cyberattacks 2018-02-07 18:19:26

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Web Site are Vulnerable:
A must read story from techrepublic.com evaluates a hidden facts on web site vulnerabilities:
42% of the 100,000 sites on the network are using software that is vulnerable or has been attacked in some way. ? Menlo Security, 2018
4,600 phishing sites use legitimate hosting services to avoid detection. ? Menlo Security, 2018
According to the latest Menlo Security report, many of the places we think are the safest places on the Internet are actually quite dangerous to business people and consumers. The report found that about 42% of the sites in the top 100,000 sites use software that turns them on or has been attacked in some way.
Cybercriminals use long-term confidence trust measures, including the reputation or category of certain websites, to avoid being detected and to increase the effectiveness of the attacks. This means that businesses must be vigilant and ensure that cyber health measures are in place, including employee education and multilayered protection.
The report notes that ordinary websites connect to 25 content background sites, such as video clips or advertisements. Most enterprise security administrators lack the necessary resources to monitor these back-office connections, leaving organizations vulnerable to backdoor attacks.
The report also found that efforts to categorize locations into different categories were largely ineffective. For example, websites belonging to the ?Business and Economics? category have had the highest number of security incidents in the past year and have hosted more phishing websites and more sites that run vulnerable software (such as PHP 5.3.3) , But not any other category ?gambling.?
advertising
The report found that about 49% of ?News & Media? websites were considered risky, with 45% of ?Entertainment & Arts? websites and 41% of ?Travel? websites considered as at-risk.
Increasingly sophisticated phishing attacks: The report found that some 4,600 phishing sites use legitimate hosting services to avoid detection. Instead of using other alternatives, attackers can more easily set up subdomains on legitimate hosting services, which are often whitelisted by the company.
The report found that domain name registrations or the existence of fake domain names that contain misspelled words for phishing and malware delivery still exist. About 19% of the domain names are found in trusted categories such as financial services, news and media.
Read More?
Phishing attacks continue to grow more sophisticated, as 4,600 phishing sites use legitimate hosting services, according to Menlo Security. Engaging post, Read More?
thumbnail courtesy of techrepublic.com.

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post 42% of the most popular websites are vulnerable to cyberattacks appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 36 : MacUpdate hacked on MACs, cryptocurrency miner apps installedOSX.CreativeUpdate

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on MacUpdate
This story from scmagazine.com analyzes the truth about Cybercriminals have managed to infiltrate MacUpdate, a Mac app download site, and maliciously install Firefox, OnyX and Deeper app, which are actually cryptocurrencies miner.
The event took place on February 1, when SentinelOne released a blog warn the reader about mine, the Thomas Reed blogger for Malwarbytes. The malware, called OSX.CreativeUpdate, is a new miner who spends time in the background of computer resources that mine for Monero.
MacUpdate apologizes and explains how to remove malware from comments in each of the applications affected.
Malicious Impact on MacUpdate
With each changed application, the threat actor redirects those click-link clicks to a malicious website that slightly alters the URL to help confuse the behavior.
Both OnyX and Deeper are products made by Titanium Software (titanium-software.fr), but the site has been maliciously changed to point to the download site titaniumsoftware.org, the first domain name registered on January 23, with its ownership overridden Fake Firefox applications are released from download-installer.cdn-mozilla.net, ?Reed said.
When the end user is asked to drag the application into the computer?s application folder, it will be injected. However, the .dmg (disk image file) that contains the malware was moved. Once malware moves to a new folder, it installs a payload from the legitimate website public.adobecc.com as bait. This activity in turn means that malware is activated.
Reed pointed out some of the problems with malware, sometimes causing it to fail.
For example, a malicious OnyX application will run on Mac OS X 10.7, but a tricky OnyX application would require macOS 10.13, which means that malware will run on any system between 10.7 and 10.12, but the decoy application will not Will open to cover up the malicious incident. ?
MacUpdate Remedy
Fortunately, the malware can be removed, but Reed also advises end-users to download applications directly from the developer?s site, not from integrators or Apple. And, because malware is often trendy, he said a warning sign that if there is no advertisement or no effect on the downloaded app, there may be something wrong with some of the new software. This is a good idea if this happens.
Finally, Reid tried to say that Macs will not let malware fall asleep.
Finally, note that the never-ending old adage ?Mac computers do not get viruses? turned out to be more hypocritical, saying that this is the third Mac malware so far this year, following OSX.MaMi and OSX. After CrossRAT.
Read More?
A cybercriminal managed to infiltrate the Mac app download site MacUpdate and install maliciously- copies of the Firefox, OnyX, and Deeper applications that actually were cryptocurrency miners. Engaging post, Read More?
thumbnail courtesy of scmagazine.com
More supporting articles?

Apple, Android Attacked by Monero Mining Malware
Apple, Android Attacked by Monero Mining Malware

MacUpdate Hacked to Distribute Mac Cryptocurrency Miner
MacUpdate Hacked to Distribute Mac Cryptocurrency Miner

MacUpdate hacked, cryptocurrency miner apps installed
MacUpdate hacked, cryptocurrency miner apps installed

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

More Remedy?

Hidding MacUpdate Remedy

As with many of these things, there are two ways to do one thing ? though one of them has some different side effects.

Option A

Option A asks you to open System Preferences, select the Store icon, and ensure that the boxes titled Download the Latest Available Updates in the Background and Install MacOS Updates are selected.

As you can guess, this will mean that before this notification disappears into the background, you get a subtle background notification of what?s happening.Here?s how to make those annoying Mac update notifications disappear

Option B

But what about option B? If you prefer, you can leave the two options unchecked ? you will not even get a subtle popup.

Of course, this means that you will miss even more important patches, although you will not get stuck with unnecessary updates.

So far, so good, right? Then there is a little alpine update that (a) can not be handled in the same way, (b) if you have an old machine that will slow you down.Here?s how to make those annoying Mac update notifications disappear 1

There are two ways to get out of the notification

If the above does not work try this

As MakeUseOf explains, there is a way to do this.

The ?simple? approach includes updating, clicking Ctrl + click on the Mac OS High Sierra banner at the top, and selecting ?hide update.?

If for some reason the above method is not valid, then the ?hard? way is what you need. Start.

Step 1: Open your Mac Finder and click Go> Go to Folder

Step 2: Enter ?/ Library / Bundles? (minus the quotes) in the dialog box.

Step 3: The icon labeled ?OSXNotification.bundle? should be visible. Drag it elsewhere (you can move it back later if you need to).

Step 4: Enter your administrator password when prompted

Step 5: Restart.

Only. Now you will never be bothered by unwanted notifications.

Here?s how to make those annoying Mac update notifications go away
Here?s how to make those annoying Mac update notifications go away

The post MacUpdate hacked on MACs, cryptocurrency miner apps installedOSX.CreativeUpdate appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 37 : FBI sounds alarm over malware-laden phishing email making the rounds 2018-02-07 1

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Phishing Scams:
What is most likely to be an overlooked story from securityboulevard.com mentions that phishing is still the biggest threat to online services, though it is one of the oldest techniques in this book. The FBI warned that phishing scams will continue to headline news in 2018, as bad actors even send out the name of the malware mail sent by the FBI cybercrime department.
In a public service announcement, the agency said it had received a clear complaint about phishing scams on the Cybercrime Complaints Center (IC3). Surveys of these claims over the past seven months show that the claims are real.
Typically, email templates (three, lastly counted by the FBI) ??try to persuade victims to provide sensitive personal information that attackers can use to access their finances. If everything fails, the e-mail relies on a plan B computer infected with the victim?s malware.
Cybercriminals tricked victims into providing personal information and downloading malicious files by posing as the Internet Crime Complaint Center (IC3). ?
In a recent scam, unidentified actors emailed victims to e-mail asking recipients to provide additional information in return for compensation.In order to make e-mail appear legitimate, these swindlers included hyperlinks to news articles, Detailing the arrests or arrests of internet fraudsters unknown unknown actors have also attached a text file (.txt) to download, complete and return to the perpetrator. The text file contains malicious software designed to further victimize the victim. ?
Intelligence agencies have released examples of email templates being used by three attackers, one of which is related to typical phishing scams.
These clues-from crappy English, scribbled punctuation to exaggerated remarks-and a full-fledged juvenile narrative-are enough to allow untrained users to think twice before giving up their personal information.
The council has recommended that anyone who believes they might become a victim of an online scam complains to IC3 at www.ic3.gov.
A joint cyber security study conducted by Google and the University of California last year showed that phishing is the single biggest threat to account-based online services.
Recently, data compiled by email analytics experts show that online retailers face huge risks to their customers by maintaining a weak email verification system. Specifically, the root zone where the top e-tailers in the United States and the EU operate is 87.6%. The study found that their consumers could potentially steal data through phishing attacks.
Read more?
Phishing remains the greatest threat to online services, even though it?s one of the oldest tricks in the book. A warning by the FBI suggests phishing scams will continue to make headlines in 2018, as bad actors go as far as to impersonate the FBI cybercrime division, sending out malware-laced emails in its name. In Engaging post, Read More?
thumbnail courtesy of securityboulevard.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post FBI sounds alarm over malware-laden phishing email making the rounds appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 38 : Warning: Looming Google Chrome HTTPS certificate apocalypse! 2018-02-07 18:19:25

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on HTTPS Certificate Credentials
Today I came across this story from theregister.co.uk that sheds light on thousands of sites will be found to be marked as unsafe unless they have exchanged their HTTPS certificate credentials within the next two months.
Since Google decided in September to stop trusting SSL/TLS certificates from Symantec, beginning in mid-April, Chrome browser users will be using security agencies issued before June 1, 2016 or after December 1, 2017 Certificates issued Visit websites Their connections are not private and someone may try to steal their information. They will have to click past warnings to reach the site.
Chrome will release its version 66 on April 17 ? a version that will be publicly available on April 17 ? and the problem will get worse after the 70 version is released on October 23, and all Symantec certifications will be Listed as untrustworthy.
Of course, not everybody uses Chrome, and not everyone will immediately upgrade to the latest version, but for those websites that do not get a new HTTPS certificate from other agencies, it quickly becomes a headache.
The question is: how big is a headache?
Early versions of Chrome beta testers have warned they will keep browsing websites with untrusted certificates and see dangerous information. Fortunately, one experienced the hassle of running the script so much that it got ugly things.
According to his blog, Arkadiy Tetelman, a security engineer working on Airbnb at Airbnb, decided to conduct a test where he took the certificate information from one million of the largest websites on the Internet and tested it against Alexa-rated traffic, break in.
The script, which took 11 hours to run, showed some very interesting results: out of 1 million websites, only 11,510 will enter TITSUP in April and 91,627 on the cutting board in October.This issue does not raise the disturbing fact that Google has basically declared the entire company?s certificate issuance business as no longer accepting Symantec certificates, thereby invalidating the company?s certificate issuance business. This is a terrible power to have.
But on the other hand, if Symantec does not mistakenly publish SSL/TLS certificates (including, unfortunately, google.com?s certificate), it will not screw it up and sabotage trust in its products. Not a clever move.
If you are an organization purely for ensuring that people can trust you then you should expect some consequences if you can not trust you. Certainly not very happy Symantec, and in a blog post on it uses a series of angry words: irresponsible, exaggerated and misleading words.
It claimed that only 127 certificates were issued incorrectly instead of the previous 30,000 copies. But here we are. A few months after the blog post was posted, Google declined to approve Symantec for its part to sell the certificate business to DigiCert.
Do not say you are not warned.
Read More?
Well, melee. Dust-up? Minor inconvenience? But it?s coming!! Tens of thousands of websites are going to find themselves labeled as unsafe unless they switch out their HTTPS certificate in the next two months. Engaging post, Read More?
thumbnail courtesy of theregister.co.uk
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Warning: Looming Google Chrome HTTPS certificate apocalypse! appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 39 : Researcher Found Bypasses on Windows Controlled Folder Access Anti-Ransomware F

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary:
This story from bleepingcomputer.com revealed a security researcher has discovered a way to get around the ?controlled folder access? feature added to Windows 10 in October 2017, which Microsoft said is a credible counter-raster software defensive measure.
This feature, which is detailed in this Bleeping Computers evaluation, is part of the Windows Defender anti-virus software built into all versions of Windows 10.
Users who update to Windows 10 Fall Creators Update receive a Windows Defender update called Controlled Folder Access (CFA) that allows them to block any changes to the files found in the user-specified directory.
Users must manually approve any application that allows editing of files located in the CFA folder by adding each application?s executable to the whitelist managed by the Allow access to applications through controlled folders option.
Controlled Folder Access ? Application Whitelist
However, Yago Jesus, security researcher at SecurityByDefault, a Spanish security researcher, found that Microsoft has automatically whitelisted all Office applications in the list. This means that Office applications can modify files that reside in the CFA folder, whether or not the user likes it.Ransomware can bypass the CFA using Office OLE objects
Jesus said ransomware developers can easily bypass the Microsoft CFA anti-ransomware functionality by bypassing the CFA by adding simple scripts through OLE objects in Office files.
In a research note published over the weekend, Jesus listed three examples of using fraudulent office files (received via spam) to overwrite the contents of other Office files stored in the CFA folder, password-protecting the same files, or copying and pasting Go to a file outside the CFA folder, encrypt it, and delete the original.
Although the first example is only destructive, the last two will be used as actual ransom and the victim will have to pay the ransomware author for the password / decryption code to unlock the file.Jesus is dissatisfied with Microsoft
Jesus said he informed Microsoft of what he found. In an email screenshot from Microsoft that Jesus received from Microsoft, operating system manufacturers did not classify the issue as a security breach, but instead said they would improve the CFA in future releases to address reported bypassing.
?This really means that Microsoft will fix this loophole and should be categorized as mitigating detours without recognition,? Jesus said, referring to the issues he pointed out that he did not get any credit or wrong bounties.
Read more?
Bitdefender Ironically Stopped Working on Safer Internet Day CSS Code Can Be Abused to Collect Sensitive User Data Scammers Use Download Bombs to Freeze Chrome Browsers on Shady Sites InsaneCrypt (desuCrypt) Decrypter Remove the FF Web Surety Adware & Miner Firefox Addon Remove the My PC Mechanic System Optimizer PUP Remove the Color Filter Miner & Adware Firefox Addon Remove Security Tool and SecurityTool (Uninstall Guide) How to remove Antivirus 2009 (Uninstall Instructions) How to Remove WinFixer / Virtumonde / Msevents / Trojan.vundo How to remove Google Redirects or the TDSS, TDL3, or Alureon rootkit using TDSSKiller Locky Ransomware Information, Help Guide, and FAQ CryptoLocker Ransomware Information Guide and FAQ CryptorBit and HowDecrypt Information Guide and FAQ CryptoDefense and How_Decrypt Ransomware Information Guide and FAQ How to Rename a Hyper-V Virtual Machine using PowerShell & Hyper-V Manager How to Install Hyper-V in Windows 10 How to Enable CPU Virtualization in Your Computer?s BIOS How to open a Windows 10 Elevated Command Prompt How to start Windows in Safe Mode How to remove a Trojan, Virus, Worm, or other Malware How to show hidden files in Windows 7 How to see hidden files in Windows A security researcher has found a way to bypass the ?Controlled

Folder Access? feature added in Windows 10 in October 2017, which Microsoft has touted as a reliable anti-ransomware defensive measure. This feature, described in more depth in this Bleeping Computer review, is part of the Windows Defender antivirus built into all versions of Windows 10. Users who updated to the Windows 10 Fall Creators Update received an update for Windows Defender named Controlled Folder Access (CFA) that allows them to block any modifications to files found in user-designated directories. The user must manually approve any app that?s allowed to edit files located in CFA folders by adding each app?s executable to a whitelist managed through the ?Allow an app through Controlled folder access? option. But Yago Jesus, a Spanish security researcher with SecurityByDefault, has discovered that Microsoft has automatically whitelisted all Office apps on this list. This means that Office apps can modify files located in a CFA folder, either the user likes it or not. Engaging post, Read More?
thumbnail courtesy of bleepingcomputer.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Researcher Found Bypasses on Windows Controlled Folder Access Anti-Ransomware Protection appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 40 : Adobe: Two critical Flash Player 28.0.0.161 security bugs fixed 2018-02-07 18:19:25

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on Adobe Patch Urgent Update

This story from theregister.co.uk recaps that Adobe released an urgent update to Flash Player to fix major zero-day vulnerabilities that have been used to target targeted North Korean hackers.

Last week, South Korea?s Computer Emergency Response Team (KR-CERT) issued a warning that a security company?s follow-up confirmed that the vulnerability had been exploited and involved malicious Microsoft Excel file attacks.

Urgent Updates Flash Player 28.0.0.161 Two Vulnerabilities

Flash Player 28.0.0.161, released on February 6, fixed a zero-day vulnerability identified as CVE-2018-4878 and a similar vulnerability named CVE-2018-4877 that was exposed privately to Adobe through Adobe?s Zero-Day Action Plan report.

Both of these pitfalls are key to releasing memory errors after use and may result in remote code execution, so users should update to the new Flash Player version as soon as possible. Flash plug-ins provided with Google Chrome, Microsoft Edge, and Internet Explorer 11 are automatically updated through the browser?s update mechanism.

The latest version of Flash also patches CVE-2018-4877, which is also a free-to-use vulnerability for remote code execution. Bo13oy of Qihoo 360 Vulcan Team reported the vulnerability to Adobe through Trend Micro?s Zero Day Initiative (ZDI). Adobe does not seem aware of any exploits of CVE-2018-4877.

FireEye has analyzed the attack involving CVE-2018-4878 and thought it was used as a TEMP.Reaper by a group it tracks on a zero-day basis. The security firm has determined that the hackers may be located in North Korea based on the IP addresses used to access Command and Control (C & C) servers.

?Most of their goals are focused on South Korea for government, military and defense industrial bases and other industries.? ?They are also interested in predictable North Korean interests such as reunification efforts and defectors,? FireEye said.

Vulnerability Impact

FireEye observed attacks, including malicious Office documents and spreadsheets, designed to leverage Flash Player Zero Time Difference to deliver the malware tracked by DOGCALL.

Cisco Talos also analyzed the movement and classified it as a group of 123 characters. Although Cisco did not explicitly accuse North Korea of ??attacking 123 groups, the company has targeted some of South Korea?s campaigns in detail as a temptation-related theme in the delivery of malware.

The researchers point out that adding a zero-day attack to their arsenal shows that the group has become very positive and mature.

Researchers at security company FireEye used the new vulnerability to analyze the recent attacks and attribute the attacks to a known North Korean threat organization, called TEMP.Reaper.

?Historically, most of their targeting has been focused on the Korean government, military and defense industry bases, however, last year they have expanded to other international goals,? FireEye researchers said in a blog post. ?They are already interested in issues of immediate importance to the Democratic People?s Republic of Korea (DPRK), such as North Korea?s unification efforts and North Korean defectors.?

TEMP.Reaper Hacker

FireEye also warned that TEMP.Reaper has developed and deployed some erase-targeted disk-erasure malware, although there is currently no evidence that the organization has used it to destroy data. North Korean hackers have in the past launched wiping attacks against South Korea and other international targets, including the 2014 attack on Sony Pictures? computer network.

Researchers at the Cisco Talos team also tracked the latest Flash Player zero-day attacks and attributed them to what they call a group of 123 threat actors. The attack payload is a remote management tool called ROKRAT that can be used to infiltrate documents and manage infected

systems.
In a blog post, researchers at Talos said: ?The 123 Group has now added some of the latest payloads for the criminal elite and ROKRAT.? They?ve used 0 days of Adobe Flash, which goes beyond their predecessors ? they Indeed, exploits were used in previous activities, but never before have a net new exploitation hole been exploited. This change represents a significant shift in the 123 levels of maturity, and we can now evaluate 123 groups from a confidential perspective with a highly skilled, highly motivated and well-established team.
Adobe admitted that its software will remain a security breach shortly thereafter and promises a patch this week.
Now that the update has landed ? it?s not just a programming bug, it also includes a fix, thanks to the Qihoo 360 Vulcan team of researchers. Qihoo staff found a remote code execution vulnerability in Flash, this update has been resolved. Both errors were rated as critical for all supported operating systems except the Linux version of the Adobe Flash Player Desktop Runtime.
Essentially, now patch your Flash installation to stop taking advantage of two newly discovered bugs, one of which is used by North Korea and the other by Qihoo?s Information Finder. Using a malicious Flash file embedded in a vulnerable computer to open a web page or other document is sufficient to trigger a malware infection.
?These updates address critical vulnerabilities that could cause remote code execution, and Adobe recommends that users update their product installations to the latest version,? Photoshop said today.
The remote code execution error exploited by Nork was CVE-2018-4878 and the Vulcan team found CVE-2018-4877.
Read More?
Emergency patch lands, shuts pair of remote exploitable holes, one used by Norks Adobe has issued an emergency security patch for two bugs in its Flash player ? after North Korea?s hackers were spotted exploiting one of the flaws to spy on people investigating the creepy hermit nation.?? Engaging post, Read More?
thumbnail courtesy of theregister.co.uk

Adobe Fixes Flash Player Zero-Day Vulnerability
Adobe has released an emergency update for Flash Player to fix a critical zero-day vulnerability that already has been used in targeted attacks by North Korean hackers. News of the vulnerability broke last week with an alert from the South Korean Computer Emergency Response Team (KR-CERT) and follow-up confirmations from security companies that an exploit.. The post appeared first on Security Boulevard?. Adobe Fixes Flash Player Zero-Day Vulnerability

Adobe: Two critical Flash security bugs fixed for the price of one
Emergency patch lands, shuts pair of remote exploitable holes, one used by Norks Adobe has issued an emergency security patch for two bugs in its Flash player ? after North Korea?s hackers were spotted exploiting one of the flaws to spy on people investigating the creepy hermit nation.?? Adobe: Two critical Flash security bugs fixed for the price of one

Adobe Patches Flash Zero-Day Exploited by North Korean Hackers
Adobe updated Flash Player on Tuesday to address a zero-day vulnerability exploited by what experts believe to be a North Korean hacker group in attacks aimed at individuals in South Korea. read more? Adobe Patches Flash Zero-Day Exploited by North Korean Hackers

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Adobe: Two critical Flash Player 28.0.0.161 security bugs fixed appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 41 : Alleged Cyber Espionage by Russian and North Korean State Sponsors on 2018 Olymp

Your Feed is from https://www.safeharboroncyber.com/Blog/

Alleged Cyber Espionage activities by Russian and North Korean Hackers on 2018 Olympics

The 2018 Olympics have long been a microcosm of geopolitics, which, in addition to athletics, have provided means for diplomacy and propaganda, sometimes even pronouns of war. Well, in 2018, they also become hacker trick links. The Olympic Games next week in Pyeongchang may have been the most thorough hacking in game history, with more surprises coming.

More than any previous Olympic Games, Pyeongchang has been plagued by apparently state-sponsored hackers: a sport with ties to Russia has stolen embarrassing documents that leaked Olympic organizers, and security researchers have followed another move, Probably North Korea, appears to be monitoring the Olympic organization in South Korea.

Security researchers track both operations, saying that the full scope of both operations is still far from clear, and leaving them can still raise the question of upcoming problems with themselves starting a new interruption in the game. More generally, signals of intrusion indicate that geopolitical tensions for the Olympics have long been extended to the digital arena.

Gain Foothold at 2018 Olympics with Email Phishing

E-mails were disguised as coming from the National Counter-Terrorism Center of Korea (NCTC). At that time, NCTC was conducting a sports anti-terrorism exercise to prepare for the Olympics, indicating that e-mail is legitimate and increasing the chances of people opening e-mails.

Malicious documents that contain obfuscated Visual Basic macros prompt the recipient to open it in their Microsoft Word version and start the PowerShell script when they click Enable Content. Attackers use Invoke-PSImage, an open-source steganography tool released on December 20, to hide malicious PowerShell code on remote servers.

The process eventually provides an implant that creates an encrypted channel for the attacker?s server so they can execute commands on the victim?s machine. The researchers explained that the goal is to evade detection techniques that rely on pattern matching.

Researchers at the company say they have linked these samples of malware to a phishing campaign that lures victims with Korean e-mail, pointing to South Korea?s goal. McAfee said the messages cheated a piece of information from the Korean national counter-terrorism center, which, according to McAfee, said the messages were made during the actual conduct of the terrorist demonstration in Pyeongchang ? targeting the more than 300 Olympic Games-related targets of BOCOG . Only the address ?icehockey@pyeongchang2018.com? is visible in its ?to? line. However, by analyzing the email?s metadata, McAfee identifies victims of other intentions, including the Pyeongchang local tourist organization, ski resorts, transportation and key sectors of the PyeongChang Olympics.

Hackers attach Korean Word documents to e-mail for running malicious scripts on the target machine. If a victim clicks ?Enable Content? after opening a contaminated attachment, an attacker can remotely access the computer. An attacker could use the initial temporary foothold to install spyware in order to have a deeper look at hacked computers. McAfee pointed out that the script hidden in an innocent image file, with clever steganography and other obfuscation strategies.

McAfee traces its fishing program to remote servers in the Czech Republic and registers forged certificates with South Korean authorities. And they found a publicly accessible log on this remote server showing that the victim?s machine was actually connected to it from South Korea, which is a sign of the actual infection. Raj Samani, chief scientist at McAfee, said: ?Is this a successful campaign? The answer is yes.? We know it?s the victim. ?

Despite all these discoveries, the origin and ultimate goal of this relatively complex malware movement remain unclear. However, based on North Korean language and goals, Samani hinted that his work theory points to North Korean espionage efforts and closely follows his southern neighbors.

This spy appears to run counter to South Korea?s recent disintegration of diplomatic relations and

has even led to a combination of national women?s hockey teams from both countries. But North Korea may not give up its attack on a temporary olive branch. Samani said: ?I guess this is a? let your friends close, your enemies closer ?approach.

First evidence emerged last month that sighting Fancy Bear, Russian hackers move to new political targets has launched a cyber campaign targeting Olympic organizations following Russia?s ouster from the 2018 Winter Olympics for state-sponsored doping. A hacker persona linked to the group released purported emails and documents from the International Olympic Committee earlier this month.

Malware Laced Word Doc for 2018 Olympics attendees

McAfee has discovered an implant that they believe was being used as a second-state payload in a recent document-less attack on the upcoming organization of the PyeongChang Korea Olympics.

In early January, McAfee security researchers warned that hackers have begun e-mails infected with malware for the PyeongChang Games. It is reported that the first such attack took place on December 22, and the sender?s address was faked, it seems from the South Korean national anti-terrorism center.

Hackers are using PowerShell?s plug-in tools to create a channel for the attacker?s servers and collect basic system-level data, but McAfee cannot immediately determine what an attacker did after first visiting the victim?s system.

McAfee later released a report detailing other implants used in the attack that were used to obtain sustained target systems and sustained data breaches, including the Golden Dragon, the Brave Prince, Ghost419 and RunningRat.

Involved Espionage Groups with 2018 Olympics

December 24, 2017 Observed Korean Planting a Golden Dragon is considered to be the second phase of the Olympic payload, with a more robust persistence mechanism than the original PowerShell implant.

As a data collection implant design, Golden Dragon has a golddragon.com hard-coded domain name that acts as a scout tool and downloader for subsequent payloads. It also generates a key to encrypt the data collected from the system and then sends it to the server ink.inkboom.co.kr.

Golden Dragon is not a complete spyware, because it only has limited reconnaissance and data collection capabilities. The malware released the first variant in Korea in July 2017 with features that include similar elements, codes and behaviors as McAfee?s tracked Ghost419 and Brave Prince since May 2017.

Malware lists the user?s Desktop folder, the files the user has recently accessed, and the directories in the system?s% programfiles% folder and associates this information with the system details, the ixe000.bin file in the current user?s UserProfiles, and the registry Item, and the value of the current user?s run key, encrypts the data, and sends it to the remote server.

Malicious software can check the system for processes related to anti-virus products and cleaning applications, and then terminate the process to evade detection. In addition, it supports the download and execution of other components retrieved from a command and control (C & C) server.

There is also a Korean planting system similar to Gold Dragon, Brave Prince dedicated to systems analysis that collects information about directories and files, network configuration, address resolution protocol cache, and systemconfig. The malware first appeared on December 13, 2017. It also terminates processes related to tools that block malicious code.

For the first time in the field on December 18, 2017, the Ghost419 is a Korean implant dating back to July 29, 2017, with samples representing only 46% of the December sample. This malware, based on the Golden Dragon and the Brave Prince, shares elements and code, especially with system reconnaissance.

Security researchers said attackers also used the Remote Access Trojan (RAT) during the PyeongChang Olympics. Known as RunningRat, this tool has two DLLs, the first to kill any anti-malware solution on the system, and in addition to being persistent, unpack and execute the primary RAT DLL.

The second DLL that uses anti-debugging technology is decompressed in memory, resulting in a fileless attack because it never touches the user?s file system. The malware gathers information about the operating system as well as driver and processor information and begins to capture user keystrokes and send them to the C & C server.

?From our analysis, the theft button is the main function of RunningRat; however, the code for the DLL has a wider range of functions. The code includes copying the clipboard, deleting the file, compressing the file, clearing the event log, shutting down the machine, etc. However , Our current analysis shows that such a code can not be executed, ?McAfee revealed.

All of these implants can be established perpetually on the victims? systems, but they require the first phase of malware that provides an initial foothold for the victim?s system. If you run Hangul Word (a Korean-specific replacement for Microsoft Office) on your system, some implants can only achieve persistence.

?With the discovery of these implants, we now have a better understanding of the scope of this operation.? Golden Dragon, brave prince, Ghost419 and RunningRat show a wider range of motion than ever before. Lasting data breaches can potentially create some potential for attackers during the Olympics, ?McAffee concludes

Additional Group in 2018 Olympics, Anti-Doping Bears

A far louder and more explicit hacker threat has come from a notorious outfit linked with the Kremlin?s GRU military intelligence agency, known as Fancy Bear, or APT28?according to many security researchers, almost certainly the same Fancy Bear that hacked the Democratic National Committee and Clinton campaign in the midst of the 2016 election.

Fancy bear may have more leaks in store. Security companies Trend Micro and ThreatConnect have linked the organization?s campaign to a list of deceptive domain names they discovered that could be exploited by the organization for serious phishing attacks. Many of these fake realms have not caused any leaks yet, but may lead to compromise by the Organizing Committee. They have found that the purpose of the domain name registration fraud is to mimic the United States anti-doping agency, the British rival Britain?s anti-doping, OCA, the European ice hockey federation, the International Ski Federation, the International Winter Biathlon, International Sled And skeleton alliance.

More Malware

In early January a reported anatomy of the targeted email campaign with Kill Chain and fileless malware attacks footprints from Olympics in Pyeongchang, South Korea. Already more than 300 organizations associated with the 2018 Olympic Games have been hit by these campaigns, even before the game starts next month. Analysts at McAfee Advanced Threat Research have reported a fileless malware activity for the 2018 Winter Olympics in Pyeongchang, South Korea. An attacker in an unknown nation-state may be responsible as researcher shows front end kill chain and typical nation-state behavior from phishing campaigns.

In addition, malware can check whether the system has processes related to anti-virus products and cleaning applications, and then terminate the process to evade detection. In addition, it supports the download and execution of other components retrieved from a command and control (C & C) server.

There is also a Korean planting system similar to Gold Dragon, Brave Prince dedicated to systems analysis that collects information about directories and files, network configuration, address resolution protocol cache, and systemconfig. The malware first appeared on December 13, 2017. It also terminates processes related to tools that block malicious code.

For the first time in the field on December 18, 2017, the Ghost419 is a Korean implant dating back to July 29, 2017, with samples representing only 46% of the December sample. This malware, based on the Golden Dragon and the Brave Prince, shares elements and code, especially with system reconnaissance.

Security researchers said attackers also used the Remote Access Trojan (RAT) during the PyeongChang Olympics. Known as RunningRat, this tool has two DLLs, the first to kill any

anti-malware solution on the system, and in addition to being persistent, unpack and execute the primary RAT DLL.

The second DLL that uses anti-debugging technology is decompressed in memory, resulting in a fileless attack because it never touches the user?s file system. The malware gathers information about the operating system as well as driver and processor information and begins to capture user keystrokes and send them to the C & C server.

?From our analysis, the theft button is the main function of RunningRat; however, the code for the DLL has a wider range of functions. The code includes copying the clipboard, deleting the file, compressing the file, clearing the event log, shutting down the machine, etc. However , Our current analysis shows that such a code can not be executed, ?McAfee revealed.

All of these implants can be established perpetually on the victims? systems, but they require a first phase of malware that provides an initial foothold for the victim?s system. If you run Hangul Word (a Korean-specific replacement for Microsoft Office) on your system, some implants can only achieve persistence.

?With the discovery of these implants, we now have a better understanding of the scope of this operation.? Golden Dragon, brave prince, Ghost419 and RunningRat show a wider range of motion than ever before. The arrival of persistent data infiltration can potentially give attackers an advantage over the Olympics, ?concluded McAffee.

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor News Post. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Alleged Cyber Espionage by Russian and North Korean State Sponsors on 2018 Olympics appeared first on Safe Harbor on Cyber.

Chapter 42 : Cyber Scammers Do It For You to File Your IRS Taxes Before You 2018-02-06 11:54:1

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on IRS Taxes:

A must-read story from krebsonsecurity.com notes that today, one day after January 29, officially the first day of the 2018 reporting season, is also known as the day cyber tax scammers began to demand a false tax rebate on behalf of the victims of identity theft which is stealing your tax returns. Want to minimize the chance of this year?s tax fraud? Give the tax before the bad guys!
Hundreds of thousands (or even millions of U.S. dollars) of U.S. citizens suffer tax rebates every year. Victims usually know about crimes only after they are denied because the liar assaulted them. Even those who do not need to submit a return can be victims of refund fraud, as do those who do not actually have a refund from the IRS.
According to the IRS, consumers? complaints about tax fraud have been steadily declining for years, as the IRS and the states have enacted stricter measures to screen potential fraud applications.
If you submit taxes electronically and the returns are denied, and if you are a victim of identity theft (for example, if your social security number and other information occurred during the Equifax spill last year), you should file an identity theft Affidavit form 14039). The IRS recommends that if you suspect that you are the victim of identity theft, even if you have to continue paying the tax paper and submitting the tax return.
If the IRS considers you may be the victim of tax fraud for the preceding tax year, they may send you a special application password, which you will need to enter with this year?s tax return before you can electronically obtain IRS accept. This year is the third of the last five I received from the IRS for one of the PINs.
Of course, submitting taxes early to beat fraudsters requires one person to have all the tax forms. As a wholly-owned company, this is a big challenge as many companies have spent their sweet time sending 1099 forms etc. (even if they were asked to do so on January 31).
Many companies are now turning to online services to provide tax forms to contractors, employees, and others. For example, I received several emailed notifications about the online availability of Form 1099; most said they were using snail mail to send the form, but if I just created an account or entered some personal information on a third-party site, Well if I need them earlier, I can get them online.
Having seen so many websites deal with personal information, I am not very interested in more volunteers. According to Bankrate, even if the taxpayers do not yet have the full 1099, they can still submit returns ? as long as you have the right information and how much you have.
Bankrate explains: ?Unlike the W-2, you typically do not need to append 1099s to your tax returns.? They?re just shipping, so you know how many reports and copies you have to the IRS, so the return processor can double-check your entry. As long as you have the correct information, you can put it on your tax form without the need for a hand statement. ?

IRS Taxes W2
The IRS started to remind its employers in January that they wanted to limit the proliferation of fraud during the tax season, so the IRS simplified the process by which employers reported such scams and took extra steps to protect their employees.
The statement said: ?The IRS can take steps to protect employees, provided that employers immediately notify employers of theft.
This is how the W-2 scam works
Unlike most scams targeting as many potential victims as possible, the W-2 form is much more narrow-minded. Once a goal is identified ? whether small or large ? the fraudster looks at the company and finds the name of the payroll manager or employee responsible for the file. As one of the organization?s top executives, these crooks request payroll staff members a copy of the W-2

form for all employees.
Once the information is sent from the company, the thief has everything needed to file a false tax return, including the employee?s name, address, social security number, income and withholding information. Once you submit your return, the refund will be credited directly to your account. These fake returns may give rise to refunds, or the information can be posted for sale on dark sites.
Employers need to exercise caution when handling employee records
Employers need to be more cautious about employee records and thoroughly check all requests for information before posting to protect their personal information.
Taxpayers? identity theft is not limited to the unsuspecting salary staff who post employee information to crooks because identity thieves use data illegally obtained from various third-party and government sites to file false tax rebates.
Surge in Email, Phishing and Malware Schemes on IRS Taxes
Phishing is a hoax by which scammers lure unsuspecting victims by sending e-mail to reveal personal and financial information that can be used to steal the identity of the victim.
The IRS has issued a number of warnings about fraudulent use of the IRS name or logo by fraudsters seeking to obtain consumer financial information in order to steal their identity and assets.
Fraudulent emails are designed to trick taxpayers into thinking that these are official communications from the IRS or other people in the tax industry, including tax software companies. These phishing programs may seek information related to refunds, application status, confirmation of personal information, order transcripts, and verification PIN information.
Watch out for fake emails that appear to come from tax professionals, asking for information on the IRS form. The IRS does not require life insurance and annuity updates from taxpayers or tax experts. Beware of this scam.
Changes can be seen by text message. IRS knows email phishing scams, including links to fake websites on the official IRS website. These emails contain instructions for ?You want to update IRS electronic files now?. These emails are not from the IRS.
These sites may ask for information to provide false tax returns or may carry malicious software that could infect a computer and allow criminals to access your files or track your keystrokes for information.

In past tax years, identity thieves used data collected from various third-party and government websites to file false tax rebates ? including from the IRS itself! One of their longstanding favorites is the Get Transcript service from IRS, which had quite relaxed certification before.
Read more?
Today, Jan. 29, is officially the first day of the 2018 tax-filing season, also known as the day that fraudsters start requesting phony tax refunds in the names of identity theft victims. Want to minimize the chances of getting hit by tax refund fraud this year? File your taxes before the bad guys can! Tax refund fraud affects hundreds of thousands, if not millions, of U.S. citizens annually. Victims usually first learn of the crime after having their returns rejected because scammers beat them to it. Even those who are not required to file a return can be victims of refund fraud, as can those who are not actually due a refund from the IRS. Engaging post, Read More?
thumbnail courtesy of krebsonsecurity.com

The post Cyber Scammers Do It For You to File Your IRS Taxes Before You appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 43 : Spy agency warns North Korea may be behind 520 Million cryptocurrency heist 2018-0

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on major cryptocurrency heist:
A recent story from cnbc.com highlights by people familiar with the situation, South Korean state espionage agencies told parliamentary committees that North Korean hackers may break into a digital currency exchange in Japan to steal $520 million worth of digital coins. First reported by Rueter News.
People familiar with North Korea?s intelligence commission procedures told Reuters reporters: ?North Korea is likely to be stolen.?
Because of the sensitivity of the issue, those who declined to be named added that the virtual coin market remains a possible target for North Korean hackers because of its size and scale, but there is no conclusive evidence that North Korea is behind the theft.
Japan?s electronic moneychanger Coincheck raided Friday to fix a loophole in computer networks before hackers stole $ 530 million in electronic money in January.

The source said the virtual currency market remains a possible target for North Korean hackers because of its size and small size, but there is no definitive evidence of North Korea?s responsibility.
Last month, Coincheck, one of Japan?s largest electronic currency exchanges, said it had stolen about 58 billion yen (533 million U.S. dollars) of NEM virtual coins and it would have returned 46.3 billion yen Investors who lost money.
Another person who spoke with Reuters said that ?it is possible, but not possible, based on evidence? that North Korea is behind the theft.
Reuters said both men declined to be named due to the sensitivity of the issue. A spokesman for the National Intelligence Service declined to comment.
The reporter saw the sign beside Encrypted Currency Exchange Coincheck, while the Japanese financial regulator conducted a field inspection of Coincheck on February 2, 2018 in Tokyo, Japan. Reuters / Kim Kyung-HoonThe report sparked speculation that Pyongyang may once again release cyber attacks.The United States publicly accused North Korea of launching the so-called WannaCry cyber attack, which paralyzed hospitals, banks and other companies around the world by 2017.
A South Korean lawmaker said on Monday that North Koreans were responsible for the theft of billions of dollars in a locally encrypted currency exchange in 2017.
Kim Jong-Ki, a member of the South Korean Parliamentary Intelligence Committee, said on Monday: ?E-mail sent by North Korea may invade the private information of cryptocurrencies and their clients and steal billions of cryptocurrency.
Cryptocurrency Exchange Coincheck?s signboard was in front of the building where the office in Tokyo, Japan was located on February 2, 2018. REUTERS / Kim Kyung-HoonKim did not say which exchanges were hacked.
These reports also appeared as Japan quickly cleaned up the cryptocurrency market after the Theft in Coincheck.
Japanese authorities raided its system Friday at Coincheck and said it has already called for a clearinghouse to fix bugs in the computer network before the theft.
Japan?s top government spokesman and chief cabinet secretary Hideki Jizuka said Tuesday that Japan collected and analyzed information about North Korea?s cyber attack capacity but declined to comment on a specific analysis.
?We recognize that how we deal with cyber attacks is an important issue for our country?s

security, crisis management, and economic growth,? he told reporters on regular morning stress. ?We want to work with the international community with a sense of urgency.?

($ 1 = 1,093.1300 won) The source said the virtual currency market remains a possible target for North Korean hackers because of its size and small size, but there is no clear evidence that North Korea is responsible.

Last month, Coincheck, one of Japan?s largest electronic currency exchanges, said it had stolen about 58 billion yen (533 million U.S. dollars) of NEM virtual coins and it would have returned 46.3 billion yen Investors who lost money.

Another person who spoke with Reuters said that ?it is possible, but not possible, based on evidence? that North Korea is behind the theft.

Reuters said both men declined to be named due to the sensitivity of the issue. A spokesman for the National Intelligence Service declined to comment.

The reporter saw the sign beside Encrypted Currency Exchange Coincheck, while the Japanese financial regulator conducted a field inspection of Coincheck on February 2, 2018, in Tokyo, Japan. Reuters / Kim Kyung-HoonThe report sparked speculation that Pyongyang may once again release cyber attacks.The United States publicly accused North Korea of launching the so-called WannaCry cyber attack, which paralyzed hospitals, banks, and other companies around the world by 2017.

A South Korean lawmaker said on Monday that North Koreans were responsible for the theft of billions of dollars in a locally encrypted currency exchange in 2017.

Kim Jong-Ki, a member of the South Korean Parliamentary Intelligence Committee, said on Monday: ?E-mail sent by North Korea may invade the private information of cryptocurrencies and their clients and steal billions of cryptocurrency.

Cryptocurrency Exchange Coincheck?s signboard was in front of the building where the office in Tokyo, Japan was located on February 2, 2018. REUTERS / Kim Kyung-HoonKim did not say which exchanges were hacked.

These reports also appeared as Japan quickly cleaned up the cryptocurrency market after the Theft in Coincheck.

Japanese authorities raided its system at Coincheck on Friday and said it had already called for clearing the flaws in computer networks before the burglary occurred.

Japan?s top government spokesman and chief cabinet secretary Hideki Jizuka said Tuesday that Japan collected and analyzed information about North Korea?s cyber attack capacity but declined to comment on a specific analysis.

?We recognize how we deal with cyberattacks is an important issue for us

Read more?

South Korea?s spy agency reportedly said North Korean hackers may have stolen $520 million in digital tokens?. Engaging post, Read More?

thumbnail courtesy of cnbc.com.

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Spy agency warns North Korea may be behind 520 Million cryptocurrency heist appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 44 : Grammarly Patches Chrome Extension Bug That Exposed Users? Docs 2018-02-06 11

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary:
I couldn?t believe this story from threatpost.com that thinks a surprising
Grammarly has fixed a Chrome Extensions vulnerability that exposes its authorization token to a website, allows the website to assume the identity of a user and view the documentation for their account.
Tavis Ormandy, a researcher at Google?s Project Zero, wrote in a February 2 forum: ?I call this a serious mistake because it seems to be a serious violation of the user?s expectations.? Users do not expect to visit a web site to allow Access documents or data that they enter into other websites. ?However, Grammarly has addressed the issue and introduced an update to the Chrome Web Store and Mozilla to show ?a very impressive response time,? Ormandy wrote in a follow-up post on Monday. ?I call this question fixed.?
Grammerly said on Twitter, thanks to Ormandy for his help, ?We were aware of the security implications of our extension on Friday and we worked with Google to launch a fix within a few hours,? find and educate the community about this Kind of complex error. ?The company added that more details are coming.
Grammarly?s Chrome extension has more than 20 million users, and the company also offers a Web-based editor. Its software scans users for grammar, spelling, punctuation and style, providing corrections and suggestions.
Read more?
The grammar-checking web service fixed the problem with ?impressive? speed, a Google researcher says?. Engaging post, Read More?
thumbnail courtesy of threatpost.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Grammarly Patches Chrome Extension Bug That Exposed Users? Docs appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 45 : Scam Alert: Beware Twitter Accounts Impersonating Cryptocurrency Firms and Figures

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Twitter Accounts Impersonating:
What is most likely to be an overlooked story from inc.com announces things we don?t talk about but to steal money from innocent people, scammers have started using various Twitter accounts to simulate large companies and numbers in the cryptocurrency world.
For example, on January 30, Charlie Lee, the founder of Litecoin, sent a response to Twitter whose Twitter certificate is @SatoshiLite and is named ?Charlie Lee (LTC)? and is almost the same Handle, @ SatoshiLitev (of course, this handle is not validated). This reply solicited contributions and contained a promise that Lee would donate ten times the amount they donated:
?I?m donating 240 Litecoin to the LTC community. The 0.4 LTC for the first 60 trades is sent to the following address. Each LTC receives an LTC of 4 LTCs at its address of 0.4 LTC. LdJsGa9NLzL7QkkLzEkMsn94UodEfZKLUz Claim your LTC now!
Of course, @StaoshiLitev is not Litecoin founder Charlie Lee, and the donation promise is a scam. At this point, over 11.5 Litecoin (I wrote this article about $ 1,600 in value) has been sent to the address of a crook ? all of which have been sent by crooks to another address. For some reason, Twitter has not deleted the post, so there may be more people will continue to plunder the scream.
Similarly, fake cryptocurrencies Ripple (with verified account @Ripple) and Ripple founder Brad Garlinghouse (using a verified account @ bgarlinghouse) and cryptocurrency Ethereum (verified account @ethereumproject) and its founder Vitalik Buterin (Verified Account @VitalikButerin).
Remedy: So here are some guidelines to help you stay safe from Twitter Accounts Impersonation:
Do not simply ask for any tweet request, send you any address of any type of cryptocurrency. Instead, just like the phishing attacks that I?m talking about in Cryptocurrencies, be sure to check your address and the reason for making a payment through any questions related to cryptocurrencies by connecting them to the official website The addresses of addresses and promotions are allegedly issued by Twitter and are listed in any previous correspondence from that party. You should also verify the address and offer by contacting the parties at a known, valid contact address or phone number. If anything does not match exactly, or seems ?closed,? be cautious or do not continue. Also, given that most major cryptographic electronic money publishers and data have validated Twitter accounts ? so if you find that a major cryptocurrency issuer or celebrity email was created from an unverified account, please Look again at the handling of the account and, by the fact, you are visiting tweets made from a valid Twitter account.
Read More?
Bogus Twitter accounts with similar names to crypto-stars are requesting that people make small ?donations? in exchange for much greater paybacks. Engaging post, Read More?
thumbnail courtesy of inc.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Scam Alert: Beware Twitter Accounts Impersonating Cryptocurrency Firms and Figures appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 46 : Unpatched DoS Flaw Could Help Anyone Take Down WordPress Websites 2018-02-06

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on DoS Flaw:
A recent story from thehackernews.com features how a simple but serious application-level denial of service ? DoS Flaw -vulnerability was discovered on the WordPress CMS platform that allows anyone to shut down most WordPress sites, even with one machine, as the network requires DDoS attacks that consume a large amount of bandwidth are implemented in the same way.
As the company declined to patch this issue, the vulnerability (CVE-2018-6389) has still not been patched and affects almost all WordPress releases released in the past nine years, including the latest version of WordPress (version 4.9.2).
Israeli security researcher Barak Tawily found that the vulnerability resides in the WordPress CMS built-in script ?load-scripts.php? that handles user-defined requests.
For those who do not know, the load-scripts.php file is designed for admin users and helps the site improve performance and load pages faster by consolidating (on the server side) multiple JavaScript files into one request.
Depending on the plug-ins and modules you install, the load-scripts.php file optionally calls the required JavaScript files by passing the required JavaScript name into the ?load? parameter, as the URL below Show:

https://your-wordpress-site.com/wp-admin/load-scripts.php?c=1&load=editor,common,user-profile,media-widgets,media-gallery
When loading a website, ?load-scripts.php? (mentioned at the top of the page) tries to find each of the JavaScript file names given in the URL, appends their content to a single file and sends it back to the user browser.
According to the researchers, you can simply force load-scripts.php to pass all the possible JavaScript files (181 scripts) to the URL above in one go, causing the target site to consume high CPU and server memory.
Read more?
A simple yet serious application-level denial of service (DoS) vulnerability has been discovered in WordPress CMS platform that could allow anyone to take down most WordPress websites even with a single machine?without hitting with a massive amount of bandwidth, as required in network-level DDoS attacks to achieve the same. Since the company has denied patching the issue, the vulnerability (Engaging post, Read More?
thumbnail courtesy of thehackernews.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Unpatched DoS Flaw Could Help Anyone Take Down WordPress Websites appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 47 : New Monero Crypto Mining Botnet Leverages Android Debugging Tool 2018-02-06 11:

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Mining Botnet:
What is most likely to be an overlooked story from threatpost.com analyzes a surprising
According to researchers at Qihoo 360 Network, a new botnet distributes malware to mine Monero cryptocurrencies and infect Android devices through ports linked to operating system debugging tools.
Botnets, called 360B.Net by 360 Netlab, are entering Android devices via port 5555 associated with the Android Debug Bridge ? primarily smartphones and TV boxes ? a command-line tool for debugging, installing applications, and other purposes.
The ADB usually communicates with the device over USB, but depending on the Android document it may also be set up using wifi. The botnet spread in a ?worm? fashion, looking for open 5555 ports on other devices, most of which 360 Netlab researcher Wang Hui said in a blog post.
It is noteworthy that it uses some of the port scan code in the Mirai Botnet which is the first time the Mirai code has been used to target Android devices. Mirai appeared in August 2016 and has historically been used to attack Linux devices.
Most of the Android devices targeted by ADB.Miner is located in China and South Korea, but 360 Netlab has not identified any of them yet.
?In general, we think there is a new worm that targets the adb debug interface for the android system, which may have infected more than 5,000 devices in 24 hours. In fact, according to 360 Netlab?s own scan data, 5555 Port scanning traffic has entered the top 10.
The botnet is distributing malicious code and is digging for Moro coins, but so far no fees have been paid.
Increasingly, cybercriminals are turning to cryptocurrency mining through botnets, while Monetar is a favored target. According to Proofpoint, people behind the massive Smominru botnet have generated up to $ 3.6 million in revenue from more than 500,000 infected machines since May.
Encrypting mined botnets offers significant advantages over other types of attacks such as ransomware, as they do not necessarily require social engineering, and their nature also means that they run sneaky and do not steal anything from the victim. In fact, encrypting miners could be a ?new option? for cybercriminals, researchers at Cisco Talos said recently.
Read more?
The botnet uses port scanning code from Mirai, a first for Android-related attacks, according to researchers. Engaging post, Read More?
thumbnail courtesy of threatpost.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post New Monero Crypto Mining Botnet Leverages Android Debugging Tool appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 48 : Cisco and FireEye Pointing Finger at North Korea Hacking Group For Adobe Flash 0-Da

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary:
A must-read story from securityaffairs.co notes that an interesting
According to Cisco and FireEye security researchers, North Korean hacking groups are behind the attacks exploiting the recently discovered Adobe Flash 0-Day vulnerability
There have been over 1,000 Adobe Flash vulnerabilities since it was released. Designed to simplify website development and deliver other features not available with standard web browsers, this adds complexity and broader scope of an attack. Web browsers no longer support Flash by default, but users often re-enable it for convenience. Just installing it on your system is enough to make this latest zero-day Adobe Player exploit available.
KISA, South Korea CERT released a security bulletin on January 31, 2018, warning that the ?free to use? vulnerability in Adobe Flash Player is widely exploited. The next day, Adobe released security advisory APSA18-01, confirming that CVE-2018-4878 is a potential remote code vulnerability and announced plans to release a security patch on February 5, 2018. The attack is on a malicious SWF file in a Microsoft Office or Hancom Hangul document or spreadsheet. Once opened, the victim?s computer will execute malicious SWFs through Adobe Flash if installed.
FireEye said: ?After being open and successfully utilized, the encryption key to encrypt the embedded payload will be downloaded from the compromised Korean third-party website.
The embedded load is likely to be DOGCALL malware, which helps to install ROKRAT commands and control Trojans, allowing remote attackers to access the victim?s system.
Experts warn that users should be very careful about opening unexpected spreadsheet and document files while waiting for a patch from Adobe on February 5. In fact, for any unexpected or suspicious files, especially those that support embedding, you should always be on your guard to hide all kinds of malware. You should also strongly consider uninstalling Adobe Flash. Even if it is disabled in your browser, simply installing it on your system is sufficient to allow the latest exploit to execute successfully. Maybe you do not need Adobe Flash anymore. As Sophos explains,
?The most common requirement we hear is watching online video, but if you do not have Flash, almost all websites use HTML5 as a video. If you uninstall it, your browser will use its built-in video player ? so you probably do not need Flash at all. ?
Both Cisco and FireEye are investigating and warned that the North Koreans they?ve been tracking may lag behind this latest attack. Known by FireEye as TEMP.Reaper, Cisco calls Group 123 and groups that have ties with North Korea were very active in 2017.
FireEye said: ?Historically, most of their goals are focused on the Korean government, military and defense industrial bases, however, last year they have expanded to other international goals.?
In addition to expanding its targets, hackers also seem to be expanding their skills to deploy disruptive wiper malware and command and control Trojan horses using a variety of different technologies.
In the past few years, North Korea has had many accusations of hacking. With the tense situation in 2017 and the upcoming Olympic Games in South Korea this month, there are many opportunities and potential motivations for some important things. This latest attack shows that this hacker group is ready to take advantage of these opportunities.
Read more?
According to security researchers at Cisco and FireEye a North Korea Hacking Group is behind the attacks that exploited the recently discovered Adobe Flash 0-Day vulnerability. There have been over 1,000 Adobe Flash vulnerabilities since it was released. Designed to make website development easier and providing additional features not supported by standard web browsers, it also adds Engaging post, Read More?
thumbnail courtesy of securityaffairs.co
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing

list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Cisco and FireEye Pointing Finger at North Korea Hacking Group For Adobe Flash 0-Day In The Wild appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 49 : Russian dark web ad for new GandCrab ransomware-as-a-service discovered 2018-02

Your Feed is from https://www.safeharboroncyber.com/Blog/

A recent story from scmagazineuk.com reveals a little-known researchers investigating newly discovered GandCrab ransomware have learned how their authors have sold malware as malicious potential buyers as ransomware as a service pack.

Russia?s Black Internet Advertising Newly-Found GandCrab Ransomware as a Service

Researchers investigating newly discovered GandCrab ransomware have learned how their authors have sold malware as blackmagic potential buyers as ransomware as a service pack.

Last Friday, LMNTRIX, the Australian cybersecurity company, shared their findings with SC Media. After revealing a GandCrab Russian ad, an unusual ransomware, it used RIG and GrandSoft exploits as a distribution mechanism, asking for Use cryptocurrency Dash and use a server hosted on a .bit domain.

According to LMNTRIX, the ad offers a partnership program whereby members divide GandCrab?s profit with the developer into 60:40. In addition, large partners have the opportunity to increase their share to 70%. The author also provides technical support and updates for buyers.

However, there are a few caveats: Partners must not target countries that are now members of the former Soviet republics of the Commonwealth of Independent States, or their accounts will be deleted. In addition, ?Partners must apply to use ransomware and have a handful of ?seats? available,? LMNTRIX explained in an email to SC Media.

According to LMNTRIX?s English translation of ads, the authors also touted the ability to manually configure ransom size, individual robots and encryption masks; a ?handy admin panel? on the TOR web and the ability to access victim pages from regular web browsers; This significantly increases the amount of payments. ?The ad further states that the amount of ransom automatically doubled if the victim did not pay on time.

As an additional selling point, GandCrab?s author also posted a teaching video demonstrating how ransomware avoids antivirus testing.

Read more?

Researchers investigating the newly discovered GandCrab ransomware have learned how its authors are marketing the malicious program as a ransomware-as-a-service package to potential buyers on the dark web. On Friday, Australian cyber-security firm LMNTRIX shared with SC Media its findings, after uncovering a Russian-language advertisement for GandCrab ? an unusual ransomware in that it uses the RIG and GrandSoft exploit kits as a distribution mechanism, demands payment using the cryptocurrency Dash, and employs a server hosted on a .bit domain. According to LMNTRIX, the ad offers a partner programme, whereby members split GandCrab?s profits with the developers 60:40. Additionally, large partners are given the opportunity to increase their share to 70 percent. The authors also offer technical support and updates to buyers. However, there are caveats: Partners must not target countries in the former Soviet Republics that now comprise the Commonwealth of Independent States, or their accounts will be deleted. Engaging post, Read More?

thumbnail courtesy of scmagazineuk.com

The post Russian dark web ad for new GandCrab ransomware-as-a-service discovered appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 50 : Alleged Kelihos Botnet Mastermind Extradited to U.S. 2018-02-06 11:54:12

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Kelihos Botnet Mastermind:
A recent story from securityweek.com explains a surprising
A 37-year-old Russian is accused of being the Kelihos Botnet Mastermind of the notorious Kelihos botnet that has been extradited from Spain to the United States.
The United States Department of Justice announced that Peter Yuryevich Levatov of St. Petersburg, Russia, also known as Peter Levatov, Peter Severa, Peter Severa and Sergey Aspen Tahov, was convicted Friday in Connecticut. He was unconvinced over the charges against him.
Le Vatov was arrested in April 2017 by the Spanish authorities under a U.S. arrest warrant and has since been held in custody. The suspect was on holiday while apprehended, coinciding with the removal of the Kelihos botnet. About two weeks later, he was indicted in a federal grand jury in Connecticut.
Russia tried to stop him from extraditing to the United States. Levatov said he had previously worked for President Putin?s United Russia party and feared it would be killed if extradited to the United States. Initial media reports said his arrest may be related to the U.S. election, but officials denied the connection.
Eight counts were alleged of causing damage to the protected computers, conspiracy, access to protected computers for fraud, wire fraud, threats to sabotage protected computers, fraudulent e-mail, and increased identity theft. Faced with these allegations, he faced more than 50 years in prison.
According to U.S. authorities, Levashov controls and operates the Kelihos botnet, using it to send spam, gather personal information, and spread other malware. When arrested, investigators said the botnet sometimes contains 100,000 computers, including many in the United States.
Although some security companies tracked Kelihos as Waldac, many listed it as the successor to Waledac, a botnet that was intercepted by authorities in 2010.
Another Russian national to be extradited to the United States is Alexander Vinnik, owner of BTC-e, the cryptocurrency exchange. The Greek Supreme Court recently approved the extradition of Vinnik, who allegedly used bitcoin to clean up $ 4 billion.
After the High Court of the Czech Republic upheld the original mandate to extradite the United States authorities, Yevgeni Nikulin, who violated the LinkedIn, Formspring and Dropbox systems, will soon be extradited.
Read more?
A 37-year-old Russian national accused of being the mastermind behind the notorious Kelihos botnet has been extradited from Spain to the United States. read more Engaging post, Read More?
thumbnail courtesy of securityweek.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Alleged Kelihos Botnet Mastermind Extradited to U.S. appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 51 : Western Digital My Cloud flaws allows local attacker to gain root access to the devices

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary:
A recent story from securityaffairs.co explains how Trustwave researchers revealed that two new Western Digital vulnerabilities My Cloud network storage devices may be used by local attackers to delete files stored on the device or execute shell commands as root.
These two Western Digital My Cloud vulnerabilities are an arbitrary command execution vulnerability and an arbitrary file deletion problem. This arbitrary command execution vulnerability affects the public gateway interface script ?nas_sharing.cgi?, which allows local users to execute shell commands as root. Hard-coded credentials allow any user to authenticate the device with the user name ?mydlinkBRionyg?.
?The first discovery was the discovery of hard-coded administrator credentials in nas_sharing.cgibinary that allow anyone to authenticate the device with the username? mydlinkBRionyg. ?State the Trustwave-published analysis.? Considering how many devices were affected This is very serious. Interestingly, another researcher released the same issue independently less than a month ago. ?
The arbitrary file deletion vulnerability is also bound to the public gateway interface script ?nas_sharing.cgi?.
Another issue I have found in nas_sharing.cgi is to allow any user to execute shell commands as root. To take advantage of this issue, you can use the ?artist? parameter. ?Continue to analyze.
Western my cloud account
By linking these two flaws, you can execute the command as root, a local attacker can log in with hard-coded credentials and use base64 encoding to execute the commands passed in the ?artist? parameter.
The affected Western Digital models include My Cloud Gen 2, My Cloud PR2100, My Cloud PR4100, My Cloud EX2 Ultra, My Cloud EX2, My Cloud EX4, My Cloud EX2100, My Cloud EX4100, My Cloud DL2100 and My Cloud DL4100.
Trustwave reported these issues to Western Digital in 2017 and, according to the researchers, the vulnerabilities were fixed in an update to the firmware (version 2.30.172) released on November 16, 2017.
Read more?
Trustwave disclosed two vulnerabilities in Western Digital My Cloud network storage devices could be exploited by a local attacker to gain root access to the NAS devices. Researchers at Trustwave disclosed two new vulnerabilities in Western Digital My Cloud network storage devices could be exploited by a local attacker to delete files stored on devices or to? Engaging post, Read More?
thumbnail courtesy of securityaffairs.co
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Western Digital My Cloud flaws allows local attacker to gain root access to the devices appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 52 : Malware Attack On National Stores Inc. Exposed Payment Data 2018-02-04 18:08:08

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary:
Today I came across this story from pymnts.com that reveals things we don?t talk about but
After malware attacks allowed ?unauthorized parties? to access customer credit card information, low-priced retailer National Stores was trying to prevent fraud and increase the security of its point-of-sale (POS) system. announcement.
?We have worked closely with the FBI, cybersecurity experts and payment card brands to curb this incident and to protect our customers? payment cards,? said Michael Falas, the country?s chief executive, last Monday (January 22) Announced. ?Malicious software has been removed from our system and no customer is responsible for any fraudulent charges on their account.We are strengthening the security of the point-of-sale system to prevent this from happening in the future.?
According to a national store survey, the company believes customers who use credit cards at their locations from July 16 to December 11 may be suspected of breaking the rules. Affected information may include name, payment card number, expiration date, and security code.
Following the violation, the company hired Digital Network Security to assist in the investigation, saying it ?will continue to provide any necessary cooperation to ensure the responsibility of malicious actors.?
Equifax, the credit scoring company that posted cybersecurity incidents, could affect about 143 million consumers in the United States and about 209,000 credit card numbers. According to Equifax, unauthorized visits occurred between mid-May 2017 and July 2017.
Five years after the nationwide store incident, there has been a massive irregularity in Target, with 40 million cards stolen, 70 million customer records stolen and 1 to 3 million cards successfully sold and used for fraudulent transactions. A total of $ 200 million has been spent on cards reissued by banks and credit unions, with an estimated $ 57.3 million flowing directly into the pockets of criminals trying to lift them.
read more?

Following a malware attack that allowed ?unauthorized parties? to access customer credit card information, off-price retailer National Stores is seeking to prevent fraudulent activity and improve the security of its point-of-sale (POS) systems, the company said in an announcement. ?We have been working closely with the FBI, cybersecurity experts and payment card brands to contain the incident and protect our customers? payment cards,? National Stores Chief Executive Officer Michael Fallas said an announcement last Monday (Jan. 22). ?The malware has been removed from our system, and no customers will be responsible for any fraudulent charges to their accounts. We are in the process of strengthening the security of our point-of-sale systems to prevent this from happening in the future.? Based on National Stores? investigation, the company believes customers who used their credit cards at its locations between July 16 and Dec. 11 may be involved in the breach. Affected information might have included names, payment card numbers, expiration dates and security codes. Following the breach, the company hired digital cybersecurity firms to assist with its investigation, stating it ?will continue to provide whatever cooperation is necessary to hold the malicious actors accountable.? News of the National Stores? breach comes less than? Engaging post, Read More?
thumbnail courtesy of pymnts.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Malware Attack On National Stores Inc. Exposed Payment Data appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 53 : 0-Day Adobe Flash Vulnerability Exploited In The Wild on Chrome and Browsers 2018-

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary:
A recent story from darknet.org.uk opens up another 0-day Flash vulnerability was exploited in the field, a previously unknown vulnerability that was marked as CVE-2018-4878, affecting versions 28.0.0.137 and earlier for Windows and Mac (desktop runtime), and Basically all in Chrome (Windows, Mac, Linux and Chrome OS).
The heavy use of this approach, which appears to have used the Korean goal by North Korean hackers, apparently has been in use since November 2017.
This is a rather complex attack chain, so I was surprised it was a very reliable hole because it targeted Flash content embedded in Microsoft Office documents.
Most current browsers of this generation do not have Flash support at all, or make ?Ask First? when Flash content tries to display. This, I suspect, is why attackers choose to embed Flash into Microsoft Office documents because it is so commonplace to software, not to frequently update or patch individuals or organizations.
This is not the first Flash zero day, it will not be the last, we have already reported the last time, I think as more and more sites are phasing out Flash and ported to local HTML5, the impact should be getting smaller .
Read more?
APSA18-01 Adobe warned on Thursday that attackers are exploiting a previously unknown security hole in its Flash Player software to break into Microsoft Windows computers. Read the rest of now! Only available at Darknet?. Engaging post, Read More?
thumbnail courtesy of darknet.org.uk
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post 0-Day Adobe Flash Vulnerability Exploited In The Wild on Chrome and Browsers appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 54 : Round-up Cybercriminals are using new tactics to spread Ransomware GandCrab 201

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Ransomware GandCrab
The komando.com guides a revealing a new ransomware elusive tactic to spread their malicious payload of hacks and extortion to rob unaware victims like us.
Ransomware is rapidly rising to become the largest threat to software security. Ransom software so attractive to cybercriminals, in addition to profitability, but also one thing is its adaptability.
It continues to evolve as cybercriminals change their code to suit their needs and evasion of security software. And not just the code that changes regularly, the media and methods of ransomware distribution are constantly changing.
In fact, the software security company Malwarebytes recently discovered a new way of distributing ransomware.
Often ransomware is provided through poison files and attachments embedded in spam and phishing emails ? you know, click on the receipt! Or ?Read This PDF!? Variety.
Ransomware is malware that infects computers and restricts users? access to it until the payment of a ransom can be unlocked.
Why so effective?
The authors of ransomware instill fear and panic among victims, causing them to click on links or pay the ransom, and user systems can become infected with other malware. Ransomware shows horrifying news similar to the following:

?Your computer is already infected with the virus. Click here to solve the problem.?

?Your computer was once used to visit sites that contain illegal content, and to unlock your computer you have to pay a fine of $ 100.?

?All files on your computer have been encrypted and you must pay this ransom within 72 hours to regain your data.?

Ransomware GandCrab version is distributed through exploit kits.
GandCrab uses two vulnerability kits, distributed by RIG EK and GrandSoft EK. GandCrab opted not to require payment of ransom in bitcoin but instead used Dash to encrypt money to find payment.
What is the exploit kit?
Exploit Toolkit is an automated hacking tool, usually sold on the Dark Web, meaning novices often cannot write their own malicious code.
These easy-to-use tools typically propagate malware load for vulnerabilities in widely used software, such as Web browsers, Microsoft Office, Java and Adobe Flash Player.
You may already see your exploit kit on the web. Cybercriminals typically embed malicious ads, fake Flash updates, video plug-ins, and pop-ups to lock out-of-date software on vulnerable computers.
These kits first check for available vulnerabilities on your computer and continue to install malware automatically if they are found. This is why it is important to always have updated software!
Vulnerability Pack activities are known for spreading malicious code, including trojans, cryptographers, and crypto-attackers, but Malwarebytes notes that it is ?unusual? to use them to distribute ransomware.
Ransomware GandCrab
The ransomware in question is called GandCrab. For the first time, Malwarebytes researchers found on January 26 that two separate exploits, RIG and GrandSoft, are currently being distributed.
The RIG Attack Toolkit is known as a browser-based exploit using vulnerabilities in Adobe Flash

Player and Internet Explorer. Malwarebytes pointed out that ?RIG will spread GandCrab to victims using malicious advertisements on compromised websites.?
GrandSoft Exploit Kit is a pre-2012 suite that leverages remote execution of code in vulnerabilities in the Java runtime environment.
This means that both of these exploits can install GandCrab on an unpatched machine, and access to a compromised site requires no user interaction at all! Quite horrible, indeed.
Once installed, GandCrab is just like any other ransomware. It uses RSA encryption to lock Windows files and displays ransom instructions requesting payments for ?GandCrab Decryptor? needed to unlock the files.
However, GandCrab does not require bitcoin payments like other ransomware scams. It tends to use Dash, a little-known encrypted currency. The current ransom rate is 1.5 Dash (about $ 1,200), but double if you do not pay the price in a few days.

Image Credit: Malwarebytes

How to protect yourself from toolkits and ransomware GandCrab attacks
Unfortunately, if you are infected with GandCrab, there is currently no free decryption key, so prevention is your best defense.
As I mentioned earlier, always keep all software updates that include the latest patches for your web browser, plug-ins, operating systems, and software.
Although hackers are always looking for the next zero-day vulnerability, having the latest version of the software will protect you from widely used exploits such as RIGs and GrandSoft, which are often targeted at those who are most likely to be patched Vulnerability.
Another powerful protection policy, ransomware is a good online backup solution! As ransomware threats continue to emerge, a reliable backup will always give you the peace of mind you need. We recommend our sponsor IDrive for all your cloud backup needs! Go to IDrive.com and use the promotional code to get exclusive offers.
Ransomware Remedies

Remedies
What can you do for this?On the one hand, ransomware can be very scary ? encrypted files can basically be thought of as irreparable damage. However, if you have already prepared your system, that is really too much trouble. Here are some tips to help you avoid ransomware destruction of your day:

1. Back up your dataThe most important thing to beat ransomware is to regularly update your backups. You should backup all your data and documents and have a recovery plan for all critical information. Perform and test regular backups to limit the impact of data or system loss and speed recovery. Note that backups of network connections may also be affected by ransomware; critical backups should be isolated from the network for optimal protection.

If you are attacked by ransomware, you may lose the documentation that you started using this morning, but you can easily do it if you can recover your system to an older snapshot or clean your machine and restore other missing documents from your backups. Remember, Ransomware like Cryptolocker will also encrypt the files on the mapped drive. This includes any external drive, such as a USB thumb drive, and any network or cloud file storage to which you have assigned drive letters. So, what you need is a regular backup plan, external drive or backup service, no drive letter assigned, or a drive or backup service that was disconnected while the backup was not taking place.

Infection can be devastating to individuals or organizations and recovery can be a difficult process that may require the services of a reputable data recovery specialist.
US-CERT recommends that users and administrators take the following precautions to protect computer networks from ransomware:
Use application whitelists to help prevent malware and unapproved programs from running. An application whitelist is one of the best security policies because it only allows specified programs to run while blocking all other programs, including malware.
Keep your operating system and software up-to-date with the latest patches. Vulnerable applications and operating systems are the targets of most attacks. Ensuring that these patches and the latest updates greatly reduce the number of entry points available to an attacker.
Maintain the latest anti-virus software and execute before scanning all software downloaded from the internet.
Restrict users? ability to install and run unneeded software applications (permissions), and apply the ?least privilege? principle to all systems and services. Restricting these rights may prevent malware from functioning or limit its ability to propagate over the network.
Avoid opening macros from email attachments. If the user opens the attachment and enables the macro, the embedded code will execute the malware on the machine. For businesses or organizations, it is best to block emails from attachments of suspicious sources. For information on safely handling email attachments, see Identifying and
Avoiding Email Scams. Follow safe practices when browsing the web. See good safety practices and protect your data for more details.
Do focus on unsolicited web links in emails.

If you like to read more on my blog titled Ransomware Effectiveness and Solution ? URl is https://www.safeharboroncyber.com/cryptoransomware/ransomware-effectiveness-and-solution/

Read more?
? Engaging post, Read More?
thumbnail courtesy of komando.com

Cybercrooks are using this new scheme to spread ransomware
? Cybercrooks are using this new scheme to spread ransomware

GandCrab blends old and new threat resources as ransomware evolves
GandCrab blends old and new threat resources as ransomware evolves

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Round-up Cybercriminals are using new tactics to spread Ransomware GandCrab

appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 55 : Why the Russian Government Turns a Blind Eye to Cybercriminals 2018-02-04 18:08:0

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Russian Government:
A must-read story from slate.com proposes a revealing why the Russian government turns a blind eye to cybercriminals? As long as they target the victims of other countries, that will be alright.
If you?re a hacker committing cybercrime, posting your limousine photo on social media may not be the best idea. However, this is exactly what Karim Baratov did. As a result, the 22-year-old Canadian was arrested in November and admitted that it is no surprise that he was involved in the Yahoo hacker operations (the largest data breach so far). The lucrative cybercrime is certainly not news, but the Balatov case is outstanding because the indictment details his relationship with the FSB of the Russian Federation intelligence service.

As the son of Kazakhstan?s immigrants, Balatov was paid by two FSB officials as part of a larger movement aimed at Yahoo, which also involved Alexsey Belan, who is already on the FBI?s Web Most Popular List But managed to avoid being extradited to the United States. Used as a network agent: a middleman who attacks cyber attacks benefits Russian intelligence agencies. The stories of Bratov and Beyram provide insight into the agency relations between Russian states and hackers, and how agencies are organized and structured differently from one agency to another. What we now know is mainly to confirm the rumors circulating over the past two decades.
Read more?
By Tim Maurer Future Tense is a partnership of Slate, New America, and Arizona State University that examines emerging technologies, public policy, and society. Posting photos of your luxury cars on social media is probably not the best idea if you are a hacker committing cybercrime. Yet that?s exactly what Karim Baratov did. It is therefore not surprising that the 22-year-old Canadian got caught and pleaded guilty in November to being involved in the Yahoo hack, the biggest data breach ever (to date). That cybercrime is lucrative isn?t news, of course, but the Baratov case stands out because the indictment details his relationship with the FSB, a Russian intelligence service on the other side of the planet. Baratov, the son of Kazakh immigrants, was paid by two FSB officials as part of a larger operation targeting Yahoo that also involved Alexsey Belan, who had already been on the FBI?s Cyber?s Most Wanted list but managed to avoid being extradited to the U.S. The two were used as cyber proxies: intermediaries who conducted an offensive cyber? Engaging post, Read More?
thumbnail courtesy of slate.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Why the Russian Government Turns a Blind Eye to Cybercriminals appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 56 : U.S. Gov posts Cybersecurity US-CERT aAvisory for Pyeongchang Winter Olympic Atte

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary US-CERT Advisory:
A recent story from scmagazine.com sheds light on a US-CERT Advisory released the Pyeongchang Winter Olympics participants network security advice Just over a week more to go to the torch lighting at the PyeongMing Olympic Winter Games, CERT has released a guide to online games that can also be used in any public environment.
Considering the nature of the Olympic Games, all the following recommendations are centered on mobile safety and hygiene, much like the participants at Black Hat and Def Con.
Turn off Wi-Fi and Bluetooth connection when not in use.
Use credit cards to pay for online goods and services.
When using public or unsecured wireless connections, avoid using websites and applications that require personal information such as logins.
Update mobile software.
Use strong password and password.
Other suggestions include setting up two-factor authentication for your account, keeping the screen lock on your device active, and above all, spending a little bit of time before clicking the link.
There have been several Olympics-focused hacking attacks and files and emails stolen from the UML are leaked. McAfee reported in early January that the organizations participating in the PyeongChang Olympics have used the games as a social engineering initiative Part to cheat folks to open phishing emails.
Although cyber-attacks supported by nation-states cannot be ruled out, most experts believe it is unlikely that North Korea will participate in the games now and in this direction, but that does not mean that the games are secure.
Read More?
With the torch lighting for the Winter Olympics in Pyeongchang just over a week away U.S. CERT has issued cybersecuirty guidelines for those visiting the games, tips that can also be used in any public environment. Engaging post, Read More?
thumbnail courtesy of scmagazine.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post U.S. Gov posts Cybersecurity US-CERT aAvisory for Pyeongchang Winter Olympic Attendees appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 57 : Espionage malware snoops for passwords, mines bitcoin on the side 2018-02-04 18:08

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary
A must-read story from zdnet.com encourages things we don?t talk about but a
Customizable password-stealing, Bitcoin-tapped malware discovery, and the ability to give hackers access to compromised systems can mark the return of a notorious hacker organization.
Attacks PZChao targets government, technology, education and telecommunications organizations in North America and Asia. The target of the attack is controlled by a malicious subdomain network, with each subnet named PZChao.
The nature of the attack and the infrastructures and payloads used, including variants of the Gh0st RAT Trojan, have led BitDefender researchers to conclude that they could signal the return of the Iron Tiger APT (Advanced Persistence Threat) operation.
Iron Tiger is said to have been active in China since 2010 and has lagged behind its previous activities, resulting in a large number of US contractors stolen records. The group is said to have espionage activities in China and elsewhere in Asia.
The PZChao campaign attacks similar targets in North America and Asia ? using a similar attack technique ? Iron Tiger, both of which may be the same threat to the work of an actor.
Bogdan Botezatu, a senior cyber threat analyst at Bitdefender, told ZDNet: ?We can only infer the attribution but one thing is certain: the Gh0stRat sample used in the Tiekin APT attachment is very similar to the one identified in the PZCHAO attack.?
CapabilityOne of the key goals of the attacks is to steal passwords, which the malware achieves by deploying one of two versions of the Mimikatz password-scraping utility, depending on whether the operating architecture of the system is x86 or x64. Once extracted, passwords get uploaded to the command and control server.
Free download: IT leader?s guide to reducing insider security threats
The most powerful component of the malware consists of a modified version of the Gh0st RAT trojan, which provides the attackers with a backdoor into compromised systems, allowing almost complete control of the infected system. The behavior of Gh0st RAT is described as ?very similar? to attacks associated with the Iron Tiger attack group.
Gh0sT RAT can log keystrokes, eavesdrop on webcams, remotely listen via microphone, allow the remote shutdown and reboot of the host, the ability to secretly monitor, modify and exfiltrate files, explore the list of all active processes, and more.
It?s ultimately a fully-functioning cyber-espionage tool which can be used to by the attackers to steal information, drop more malware and perform any number of malicious deeds.
While researchers describe the tools used in these attacks as a few years old and ?battle-tested?, the malware is still very much capable of carrying out the espionage it is intended for, as demonstrated by continued infections against targets in technologically advanced industries around the world.
RECENT AND RELATED COVERAGEChinese hacking group returns with new tactics for espionage campaign
?KeyBoy? group drops stealthy malware to steal data from targets in a corporate espionage campaign focused on new targets.
Read more?
Topic: Security Video: 10 key strategies for disaster preparedness and increased IT security The discovery of custom-built malware capable of password-stealing, bitcoin-mining, and providing hackers with complete access to compromised systems could signal the return of a notorious hacker group. Attacks by Operation PZChao are targeting government, technology, education, and telecommunications organisations in North America and Asia. Compromised targets are controlled with a network of malicious subdomains ? each named PZChao. The nature of the attacks, as well as the infrastructure and payloads used ? including variants of the Gh0st RAT trojan ? have led researchers at Bitdefender to conclude that they could signify the return of the Iron Tiger APT

(advanced persistent threat) operation. Iron Tiger is thought to have been active since 2010, to be China-based, and to have been behind previous campaigns that resulted in the theft of large amounts of records from US contractors. The group is also said to have conducted espionage against targets in China and other parts of Asia. Engaging post, Read More?

thumbnail courtesy of zdnet.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Espionage malware snoops for passwords, mines bitcoin on the side appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 58 : Researchers uncover Russian dark web ad for new GandCrab ransomware-as-a-service

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on GandCrab ransomware-as-a-service:
This story from scmagazine.com admits the truth from researchers investigating newly discovered GandCrab ransomware have learned how its authors are marketing the malicious program as ransomware as a service pack.
Last Friday, LMNTRIX, the Australian cybersecurity company, shared their findings with SC Media. After discovering GandCrab?s Russian ads ? an unusual ransomware that uses RIG and GrandSoft exploits as a distribution mechanism, requires payment in crypto-currency Dash and uses servers hosted in .bit domains.
According to LMNTRIX, the ad offers a partnership program whereby members divide GandCrab?s profit with the developer into 60:40. In addition, large partners have the opportunity to increase their share to 70%. The author also provides technical support and updates for buyers.
However, there are a few caveats: Partners must not target countries that are now members of the former Soviet republics of the Commonwealth of Independent States, or their accounts will be deleted. In addition, ?Partners must apply to use ransomware and have a handful of ?seats? available,? LMNTRIX explained in an email to SC Media.
According to LMNTRIX?s English translation of ads, the authors also touted the ability to manually configure ransom size, individual robots, and encryption masks; a ?handy admin panel? on the TOR web and the ability to access victim pages from regular web browsers; This significantly increases the amount of payments. ?The ad further states that the amount of ransom automatically doubled if the victim did not pay on time.
As an additional selling point, GandCrab?s author also posted a teaching video demonstrating how ransomware avoids antivirus testing.
Read more?
Researchers investigating the newly discovered GandCrab ransomware have learned how its authors are marketing the malicious program as a ransomware-as-a-service package to potential buyers on the dark web?. Engaging post, Read More?
thumbnail courtesy of scmagazine.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Researchers uncover Russian dark web ad for new GandCrab ransomware-as-a-service appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 59 : Critical Infrastructure Are More Vulnerable to Hacks Than Ever Before 2018-02-04 18:0

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary
This story from news.hitb.org explores that despite widespread awareness of the physical and data-related dangers inherent in exposing critical infrastructure to cyber attacks, the number of Internet-accessible industrial control systems (ICSs) is increasing every year.
According to Zheng Technology, advanced industrial nations such as the United States, Germany, China, France and Canada have the largest Internet ICS components that run factories, transportation, power stations and other facilities. Among the detected Internet ICS components, there are 176,532, of which about 42% are in the United States, an increase of 10% over the previous year (from 50,795 to 64,287).
For the second year in a row, the German team finished 13,242, ranking second. The PT research team also noted that more and more Internet access ICS components are actually network devices such as the Lantronix and Moxa interface converters, accounting for 12.86% and 5.06% of the test components in 2017. Although these converters are generally considered to be Relatively insignificant, but they may be very useful for hackers, the company pointed out.
Read More?
l33tdawg Fri, 02/02/2018 ? 00:47? Engaging post, Read More?
thumbnail courtesy of news.hitb.org
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Critical Infrastructure Are More Vulnerable to Hacks Than Ever Before appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 60 : Siemens fixed three flaws in plant management product Siemens TeleControl Basic syst

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary:
This story from securityaffairs.co reviews that Siemens has fixed three security holes in its plant management product, the Siemens TeleControl base system.The system is used in water treatment facilities, traffic monitoring systems, and energy distribution plants. TeleControl Basic Control Center runs TeleControl Server Basic software. Siemens TeleControl Basic system enables organizations to monitor and control the operation of industrial processes and municipal facilities in industrial environments.
Siemens TeleControl basic
The TeleControl Server Basic system is attacked by three vulnerabilities. An attacker can exploit these three vulnerabilities to perform different types of attacks, including privilege escalation, bypass authentication, and denial of service (DoS) attacks.
?The latest update to TeleControl Server Basic addresses three vulnerabilities, one of which could allow an authenticated attacker who accesses over the network to upgrade their rights and perform administrative actions.? The security advisory issued by Siemens AG shows.
Siemens recommends updating to the new version. ?
This is the first time Siemens has released a safety bulletin of Siemens and ICS-CERT for vulnerabilities affecting TeleControl products
These defects affect TeleControl Server Basic versions prior to V3.1, the worst of which will be considered as CVE-2018-4836 and will be rated as high severity.
In the list of vulnerabilities and related description below:
Vulnerability ? CVE-2018-4835 [CVSS v3.0 Base Score 5.3] ? An attacker can bypass the authentication mechanism and access limited information by using the network to access TeleControl Server Basic?s port 8000 / tcp.
Vulnerability ? CVE-2018-4836 [CVSS v3.0 Base Score 8.8] ? Port 8000 / tcp for TeleControl Server Basic may be exploited by an authentication-less attacker to elevate privileges and perform management operations.
Vulnerability ? CVE-2018-4837 [CVSS v3.0 Basics 5.3] ? An attacker who accesses a TeleControl Server Basic?s web server (port 80 / tcp or 443 / tcp) can exploit this vulnerability on the web server.
Siemens also offers a number of solutions to mitigate the risk of attack, including blocking of TCP port 8000 via Windows Firewall for CVE-2018-4835, CVE-2018-4836, and blocking of ports 80 and 443-4837 of CVE-2018.
The United States ICS-CERT also released a detailed consultation on the Siemens TeleControl Basic vulnerability.
Read more?
Siemens has patched three security vulnerabilities in its Plant Management Product, the Siemens TeleControl Basic system. The system is used in water treatment facilities, traffic monitoring systems, and energy distribution plants. The TeleControl Basic control center runs the TeleControl Server Basic software. The Siemens TeleControl Basic system allows organizations to monitor and control processes in Engaging post, Read More?
thumbnail courtesy of securityaffairs.co.
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Siemens fixed three flaws in plant management product Siemens TeleControl Basic system appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 61 : Spritecoin ransomware masquerades as cryptocurrency wallet and also harvests victim?

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Spritecoin Ransomware
Securityaffairs.co mentions a hidden ransomware called Spritecoin ransomware. Fortinet discovered a ransomware called Spritecoin ransomware that only allows Monero, the victim, to pay and pretend to be a cryptocurrency-related password store.
Researchers from the Fortinet FortiGuard lab discovered a ransomware that only allows victims Monero to pay and pretend to be a cryptocurrency-related password store.
Ransomware itself is a ?wizard money? wallet, which requires users to create the password they want, rather than downloading the blockchain, which encrypts the victim?s data file.
The malware claims a ransom of 0.3Myero ($ 105 at the time of writing) and ransom ?your file is encrypted? on the target system.
SpriteCoin ransomware
Malware includes an embedded SQLite engine, which leads experts to believe it also implements certificate collection for Chrome and Firefox credential storage. Malicious code appends the encrypted file extension to the encrypted file (ie resume.doc.encrypted).
While decrypting the files, Spritecoin ransomware also deployed another malware that can collect certificates, parse images and control webcams.
?If the victim decides to pay and gets a decryption key, they will be delivered a new malicious executable [W68 / Generic! Tr.
?Although we have not fully analyzed this malicious payload, we can verify that it has the ability to activate a webcam and parse certificates and keys, which may make the victim more compromised than before.
Experts speculate that ransomware is being broadcast through forum spam, targeting users who are interested in cryptocurrencies.
?Ransomware is usually delivered through social engineering techniques but can also be leveraged without user interaction.These are typically arrived via email, using toolkits, maliciously crafted Excel / Word / PDF macros, or JavaScript download programs (but not Limited to).
?Attackers often use social engineering and crafted malicious mail spoofing to entice victims to run these executables, which often use compelling filenames to lure victims to open files. Often, ransomware requires some user interaction to succeed Hazardous to the victim?s machine. ?
In this case, the threat arrives as a SpriteCoin package (spritecoind [.] Exe) in the name of a SpriteCoin encrypted currency wallet.
Once installed on the victim?s machine, the malware prompts the user ?Enter the wallet password you want.?
SpriteCoin ransomware connect to TOR
When the victim provided the document, Spritecoin ransomware informed the user that the blockchain was being downloaded and that it was actually encrypting the document.
Ransomware connects to a TOR site via an onion agent (http: // jmqapf3nflatei35 [.] Onion.link / *), which allows the victim to communicate with the attacker?s website without the need for a TOR connection.
Read more:

Fortinet discovered a strain of ransomware dubbed Spritecoin ransomware that only allows victims Monero payments and pretends to be a cryptocurrency-related password store. Researchers from Fortinet FortiGuard Labs has discovered a strain of ransomware that only allows victims Monero payments and pretends to be a cryptocurrency-related password store. The ransomware poses itself as a ?spritecoin? wallet, it asks? Engaging post, Read More?
thumbnail courtesy of securityaffairs.co

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Spritecoin ransomware masquerades as cryptocurrency wallet and also harvests victim?s data appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 62 : Cryptocurrency HACKERS use YOUTUBE to target computers for bitcoin and ripple min

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Cryptocurrency HACKERS use YOUTUBE
Express.co.uk reveals an interesting fact that Cryptocurrency HACKERS uses YOUTUBE to target computers for bitcoin and ripple mining? Hackers have been targeting users of YouTube to exploit cryptocurrencies such as bitcoin by attacking their computers with video-platform advertising services.
The issue was believed to be the first to be discovered last week when users of Google-owned video sites reported that watching ads on YouTube triggered their anti-virus software.
The ad was found to contain a mining code called CoinHive, which secretly used as much as 80% of the visitor?s computer?s central processing unit to mine the cryptocurrency for anonymous hackers to act as a malware attack.
In addition to trading cryptocurrencies, new coins in online money can also be mined digitally.
However, mining these currencies consumes a great deal of computer power and hackers have begun to steal electricity from other computers instead of their money.
Google has said that their ad services are closely monitoring any malware used by those trying to dig into digital currencies.
Read more?
HACKERS have been targeting users of YouTube to mine cryptocurrencies such as bitcoin by attacking computers through the video platform?s advertising service, it has been reported?.
Engaging post, Read More?
thumbnail courtesy of express.co.uk.

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Cryptocurrency HACKERS use YOUTUBE to target computers for bitcoin and ripple mining appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 63 : Malware POC Analysis exploiting Spectre and Meltdown flaws 2018-02-02 21:15:17

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on Spectre POC Malware Analysis

I couldn?t believe this story from securityaffairs.co that believes Malware exploits Spectre, crash flaws may come by proof-of-concept analysis. Researchers at AV-TEST, an anti-virus testing company, have uncovered more than 130 malware samples specifically developed to exploit the Spectre and Meltdown CPU vulnerabilities.

The good news is that these samples seem to be the result of testing activities, but experts are worried that we will soon begin to observe the field attacks.

Most of the code obtained by AV-TEST is just a recompiled version of the proof-of-concept (PoC) code provided online. AV-TEST?s experts also found the first JavaScript PoC code for the browser in our databases, such as IE, Chrome or Firefox.

?We also found the first JavaScript PoC code in our database for web browsers like IE, Chrome or Firefox,? said Andreas Marx, chief executive of AV-TEST, to Security Week.

Meltdown attacks could allow an attacker to read the entire physical memory of a target machine, steal credentials, personal information, and more.

Spectre

Cracking exploits speculative execution to break the isolation between user applications and operating systems so that any application has access to all of the system memory. Spectre attacks allow user-mode applications to extract information from other processes running on the same system. It can also be used to extract information from your own processes via code, for example, you can use malicious JavaScript to extract login cookies from other browsers? memory.

Spectre attacks break the isolation between different applications, allowing information to leak from the kernel to the user program and from the hypervisor to the guest system.

On January 17, AV-TEST?s experts reported that they have found 77 samples of malware that are clearly related to Intel?s vulnerability.

Read more?

Malware Exploiting Spectre, Meltdown Flaws Emerges Researchers at the antivirus testing firm AV-TEST have discovered more than 130 samples of malware that were specifically developed to exploit the Spectre and Meltdown CPU vulnerabilities. The good news is that these samples appear to be the result of testing activities, but experts fear that we could soon? Engaging post, Read More?

thumbnail courtesy of securityaffairs.co

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Malware POC Analysis exploiting Spectre and Meltdown flaws appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 64 : Ransomware Scammers Get Scammed Themselves By Tor Proxy Hack, called LockerR

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary LockerR:
A must-read story from extremetech.com mentions a hidden ransomware is the most cunning and frustrating malware that flows on the Internet. These programs lock your files by encrypting and threatening to delete them unless you pay for a ransom of encrypted currency. Victims cannot stop the attack, so many people just pay for it. Now, cunning crooks by more cunning online criminals are crooks. Ransomware payments are being diverted through man-in-the-middle attacks, which is an improper justice. However, it will not do anything good for the victims of the original ransomware.
LockerR
Security company Proofpoint discovered a new attack on ransomware cybercriminals and noticed a warning posted called LockerR ransomware payment portal. The service runs on the Tor network, a cobweb of encrypted nodes around the world, that routes traffic anonymously and hosts hidden services. This is where many scammers operate compared to the open internet because of the relative safety. The problem is that most Ransomware victims do not know how to access Tor. As a result, the liar directs them to the Tor agent that can load the Tor service in a standard browser. This is where ransonmare cybercriminals are cheated.
According to a notice posted on LockerR, the onion.top Tor agent has begun redirecting Bitcoin ransomware manufacturer payment to another address. It simply replaces the original Bitcoin wallet address with the one owned by the agency operator. The payment website encourages victims to use the Tor browser to connect directly to LockerR to ensure that bitcoins arrive at the correct address. To date, hijacked bitcoin worth about $ 22,000 has been ?stolen? by ransomware cybercriminals trick innocent computer users.
Read More?
Ransomware payments are being diverted via a man-in-the-middle attack, which is some sort of perverse justice. Still, it won?t do the original ransomware victims any good. Engaging post, Read More?
thumbnail courtesy of extremetech.com.

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Ransomware Scammers Get Scammed Themselves By Tor Proxy Hack, called LockerR appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 65 : North Korea hackers exploit Flash bug to pwn South Koreans. Adobe to issue fix next w

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Flash Bug:
A recent story from theregister.co.uk thinks a surprising Adobe Flash Bug release on a patch next week to compress a flaw in Flash. The flaw could be exploited by malicious web pages and documents to hijack and monitor vulnerable computers when they are opened.
North Korean hackers are now abusing the vulnerability to infect victims? PCs. You should update your browser or Flash installation ? If you are still using Flash, the other criminals will not be able to exploit this vulnerability and may take control your computer if the fixes appear.
Zero-day vulnerability caused by Flash bug
Adobe Flash Player is now severely affected by the new Zero-day vulnerability, which researchers believe can have a serious impact on ActiveX-enabled browsers, compromising the security of Windows PCs.
Zero-day vulnerabilities are attacks that have not been patched or undisclosed.
This important zero-day vulnerability is shown in the current Adobe Flash Player ActiveX versions 28.0.0.137 and earlier.
In this case, this major zero-day vulnerability is primarily spread through Microsoft Office documents or spam messages that contain malicious Flash files.
South Korea?s Computer Emergency Response Team found that programming chaos (CVE-2018-4878) was exposed after the malicious code was hidden in Microsoft Office documents, web pages, and spam, exploiting Flash loopholes to infect Windows PCs with malware.

South Koren Cyber Emergency Response Team(KR-CERT) Released Emergency notes that says, ?This vulnerability only on user?s who all are using Internet Explorer (IE) be influenced chrome (chrome) until a patch is available using Firefox (FireFox) is recommended?

Security Researcher from Hauri, Inc.said, ?Flash 0day vulnerability that made by North Korea used from mid-November 2017. They attacked South Koreans who mainly do research on North Korea.?
Simon Choi, head of the Korea Information Security Research Center, said the vulnerability was abused by North Korea to spy on South Korea?s investigation of the dictatorial regime in the hermit state. Victims are tricked into opening a sly Microsoft Office spreadsheet to crack the PC via flash:
North Korea used a Flash 0day vulnerability in mid-November 2017 to attack South Koreans, mainly North Koreans. (No patch yet)
Adobe said today that it is working on a patch that should be released on the ?February 5? week We can only wait for the Flash bug fix.
All versions of Flash are susceptible to the above issues. Photoshop makers said that so far only Windows machines have been attacked, although Windows, Macintosh, Linux and Chrome operating systems may be attacked.
Read more?
Maybe it?s a good time to just delete the thing Adobe will next week emit patches to squash a security bug in Flash that can be exploited by malicious webpages and documents, when opened, to hijack and spy on vulnerable computers. Engaging post, Read More?
thumbnail courtesy of theregister.co.uk

Beware!! New Zero-day Vulnerability Found in Adobe Flash Player ? Still No Patches Available
Adobe Flash Player now suffering from brand New Zero-day vulnerability with high severity rate and researchers believes that it cause a Severe impact on ActiveX Support browsers which leads to compromise the Windows PC. Zero-day vulnerabilities are referred to attacks on vulnerabilities that have not been patched or made public. This critical Zero-day vulnerability is? Beware!! New

Zero-day Vulnerability Found in Adobe Flash Player ? Still No Patches Available

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post North Korea hackers exploit Flash bug to pwn South Koreans. Adobe to issue fix next week appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 66 : Five ways to check if your router is configured securely 2018-02-02 21:15:17

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on router configured securely:
A must-read story from welivesecurity.com details five ways to check if your router is configured securely. Below are some of the security issues users should focus on in their home networks, especially security issues related to routers connected to the Internet.
Five ways router configured securely
1. Make the router connection and certification test
Recently, we posted information at WeLiveSecurity.com on how to protect your home router against Internet of Things threats. Now let?s review other highlights of router management and configuration, especially about ports and services.
Routers allow management and configuration using some of the ports in the local network; this can be done via an Ethernet cable or a wireless connection. Normally you can configure your router over the web but the router also allows you to connect other services and ports such as FTP (port 21), SSH (22), Telnet (23), HTTP (80), HTTPS (443) or SMB (139,445).
In addition to this, there are various other well-known and well-used services whose default port is identified as the Internet standard defined by the Internet Assigned Numbers Authority (IANA). Although a blocked port configuration may be set in the router by default, you can view it to determine status and configuration settings. In other words, you can only enable the services you need, disable all other services, and block unused ports. Even if a remote connection, unless necessary.
The same logic applies to using passwords to manage services. If possible, you should change the (admin) password and username so neither is the default out of the box. If the router?s default password has not changed, attackers can know or easily guess; if that?s the case, they can log in to your router and reconfigure or compromise the network.
In addition, we recommend using long, complex passwords or pass phrases for these purposes; you can use Password Manager to create and store passwords in a secure place. Therefore, recheck the service and port configuration, user account, and password strength.
2. Perform a vulnerability test on the router
There is another aspect to consider when looking for weaknesses in your router setup ? test whether the router can execute with a tool that automates tasks, such as finding known vulnerabilities. This type of tool includes information, options, and advice on how to resolve these potential problems. Attackers use similar tools to identify vulnerabilities in the router, so it?s also a good idea to use them, so your router is no longer low cost.
Some router tests include scan port vulnerabilities, malicious DNS server reputation, default or easy-to-hack passwords, vulnerable firmware or malware attacks. Some also include vulnerability analysis of the web server components of the router, finding issues such as cross-site scripting (XSS), code injection, or remote code execution.
If you do not know these attacks and irregularities, be sure to find a router test (or a set of tests) that will work for you as hard as possible. Although this is not a complete test, a good way to get started is with the Connected Home Monitor tool.
Verify the connected devices in the network
3. Router configuration
A third aspect of maintaining the normal operation and performance of routers and networks is the identification of connected devices. Occasionally, trusted devices may or may not be trusted to connect without proper authorization due to bad practices and the use of vulnerable protocols.
Therefore, it is a good idea to understand and be able to identify all the devices connected to the router: First, network performance is degraded to prevent unauthorized use of resources by third parties; second, as a security measure to keep your information from being compromised.
Validation is done either through automation tools or through the manual use of the router?s management options. The next steps in the right direction include allowing only allowed devices

and using only filters to restrict access to specific IP addresses or MAC addresses.
To begin this activity, the Connected Home Monitoring Tool provides an easy-to-access list of connected devices, sorted by device type, such as printers, routers, mobile devices, etc. to show what is connected to your home network. Then, you must make your own changes using the router interface.
4. Update all devices on your home network
There was a recent vulnerability called KRACK (key reinstall AttaCK) that allowed interception of traffic between devices connected to access points in a Wi-Fi network, again emphasizing Updated.
For an attack that exploits this vulnerability, the perpetrator must usually be near the expected victim?s Wi-Fi network. An attacker could reconnoitre the communication or install the malicious software. Once the manufacturer has posted a security patch to address the vulnerability, we always recommend updating all devices (such as computers, smartphones or tablets) connected to your network; other patches will be updated in the firmware installed on the router once patches are available, Such as computers in ?public network? mode, add the full level of the device compared to the ?private / home? network mode because it reduces the risk of compromised devices being attacked. We want to emphasize that the most important thing is to keep computers and devices updated.
5. Enabling Security Options
The fifth best practice is to enable the security options available in your router?s configuration, depending on the model and type of device. Regardless of the router model used in your home network, we recommend that you enable security options designed to provide more protection for your devices and networks. For example, some recent routers include configuration options to allow enhanced protection against known Denial of Service (DoS) attacks such as SYN flooding, ICMP echo, ICMP redirection, LAN denial (LAND), Smurfs, and shutting down WinNuke . If you enable these options to prevent the router and the network from functioning properly, selectively disable them to improve performance. Information Protection ? Endless Tasks
We have just touched on five practices that help to improve safety. It is important to check the router?s settings and fully protect the routers, devices, and of course the data as needed. Doing so will help stop many of the entry points used by the current pandemic cyber-security threats.
News, views, and insight from the ESET security community By Miguel Ángel Mendoza posted 23 Jan 2018 ? 01:58PM Cybersecurity nowadays requires more (and better) protective measures than ever before. These measures range from adopting what are acknowledged as best practices, through helping end-users to stay well-informed about upcoming threats and how to avoid them, to implementing internet security technology and keeping it up to date. In a dynamic environment where threats continually evolve and new vulnerabilities are identified almost daily, it is necessary to use the most up-to-date security tools, since they deal with protection measures for new and ever-shifting attack vectors. Whether we are speaking about the work, school or home environment, security must consider and protect all elements that could become gateways for possible attacks. In this article we will review some security aspects users should look at in a home network ?particularly those related to the configuration of its internet-connected router. Recently, we published information at WeLiveSecurity.com about how to secure your home router to prevent IoT threats. Now we will review other important points for the administration and configuration of routers ?in particular, steps pertaining to ports and services. Routers allow administration and configuration using? Engaging post, Read More?
thumbnail courtesy of welivesecurity.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further

CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Five ways to check if your router is configured securely appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 67 : Top 10 Tips to Protect you from Identity Theft 2018-02-02 21:15:17

Your Feed is from https://www.safeharboroncyber.com/Blog/
Malicious actor causing identity theftTop 10 Tips for Identity Theft Protection

Identity thieves use your personal information without your knowledge. The thief may use your name to recover debt and even commit crimes. The following tips can help you reduce the risk of becoming a victim.

Protect your social security number from identity theft.

Do not carry your social security card in your wallet. If your health plan (except Medicare) or another card uses your social security number, ask for a different number from the company. For more information, see your Social Security number: Key to controlling identity theft pages.
Prompt to protect your SSN and identifiable information
Keep your card and any other files showing your social security number in a safe place; do not always carry your card or other documents to display your number.
Be careful to share your number, even if you are required; share your SSN only when absolutely necessary.
Protect your personal financial information at home and on the computer.
Check your credit report once a year.
Check your Social Security income report annually,
Protect your PC by using firewalls, antispam / virus software, updating security patches, and changing the password for your Internet account.
Protect your personally identifiable information; keep it private. Only when you are with you can you provide your SSN.
Source: https://www.irs.gov/identity-theft-fraud-scams/identity-protection-tips

hit ?Phishing? ? do not take the bait.

Do not reply to any request to verify your account or password. Legitimate companies do not require this information in this way.
Bottom line: Never provide your personal information ? unless you contact.
Do not fall because of ordinary scams
An unexpected email from the IRS is always a scam. The IRS does not contact taxpayers by email or social media to request personal or financial information. If you receive a fraudulent mail claiming to be from the IRS, please forward it to phishing@irs.gov.
A phone call claiming to be an agent of the IRS is a scam if you cannot pay immediately or threaten you with arrest or deportation. In another variation, the caller requests your financial information in order to send you a refund. Report these calls and other IRS counterfeit programs to the Treasury?s Director of Tax Management at 1-800-366-4484 or on the IRS Model Fraud Report website.
If you find a website that claims to be IRS but does not start with ?www.irs.gov?, please forward the link to phishing@irs.gov.
Source: https://www.irs.gov/identity-theft-fraud-scams/identity-protection-tips
How to avoid fraud and identity theft fraud
Every day, consumers are given a great deal of fraud, so you must always exercise caution when it comes to your personal and financial information. The following tips may help prevent you from becoming victims.
Beware of incoming emails or text messages asking you to click on a link because the link may install malicious software that allows the thief to peek into your computer and get your information;
Suspect that any email or phone request to update or verify your personal information because lawyers do not obtain updates to existing information in an unsafe manner;
It is legal to contact the sender by contacting the sender (preferably by looking up the sender?s

contact information instead of using the contact information in the email);
Assuming that anything that seems too good is not true, it may be deceptive;
Be wary of the fraudulent check, bank check, money order or e-Fund transfer sent to you requesting that you refund part of the money to you;
Be wary of unsolicited offers that require you to act quickly;
Check the security settings on social networking sites. Make sure they stop people you do not want to see your page;
Before researching any ?apps?, do not assume that ?apps? is legal because it is similar to the name of a bank or other company you are familiar with;
For any pressure to make your remittance by wire transfer quickly or involved in the confidentiality of the other party, and
Beware of disaster-related financial fraud. After a catastrophic event, a crook uses what people claim to be from a legitimate charity that is actually trying to steal money or valuable personal information.
Source: https://www.fdic.gov/consumers/assistance/protection/idtheft.html

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Top 10 Tips to Protect you from Identity Theft appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 68 : Cryptocurrency Mining Smominru Botnet Infected more than 500,000 Windows Machine

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Smominru:
A must-read story from gbhackers.com dissects that security researchers from Proofpoint discovered Monero miners using the notorious EternalBlue Exploit. Attackers using persistent botnets refer to Smominru as spreading the infection through all possible vulnerabilities.
The 2017 Cryptocurrency Exchange, which targets Ransomware, data breaches, and hacking, is known. WannaCry Ransomware used some of the Windows machines with the same EternalBlue exploit in 2017.
Mining cryptocurrencies legally is a resource-intensive process, so attackers demand that ransom payment and infect other computers to mine cryptocurrencies.
Attackers even now abuse Google?s DoubleClick ads and run Malvertising Champaign into high-traffic sites running coinhive cryptographers and other web-based miners, connected to some private tools.
Read simultaneously Coincheck Cryptocurrency Exchange hacking and stealing over $ 500 million
The robot was discovered at the end of May 2017 and miners using the Windows Management Infrastructure are not common in coin-mining malware. Based on the hash rights associated with the payment address of Monero, the fraudster has mined more than 8,900 Monero?s.
The researchers said at least 25 hosts were attacked via EternalBlue (CVE-2017-0144 SMB) to infect the new node and increase the size of the botnet. The hosts seem to be behind the network AS63199.
Smominru C & C Server and Distribution
The Smominru C & C server, hosted by SharkTech, affects over 526,000 window servers with nodes all over the world, mainly in Russia, India and Taiwan.
Read more?
Security researchers from Proofpoint detected Monero miners that spread using the infamous EternalBlue Exploit. Attackers using persistent Botnet dubbed Smominru to spread the infection through all possible exploits. The year 2017 is well known for Ransomware, data breaches and Hacking attacks targetting Cryptocurrency exchanges. In 2017 Wanna cry Ransomware uses the same EternalBlue vulnerability to Engaging post, Read More?
thumbnail courtesy of gbhackers.com

Mining Smominru botnet used NSA exploit to infect more than 526,000 systems
Researchers from Proofpoint discovered a huge botnet dubbed ?Smominru? that is using the EternalBlue exploit to infect Windows computers and recruit them in Monero cryptocurrency mining activities. The number of cyber attacks against the cryptocurrency sector continues, vxers are focusing their efforts on the development of cryptocurrency/miner malware. Recently security experts observed cryptocurrency miners leveraging the NSA EternalBlue SMB exploit? Mining Smominru botnet used NSA exploit to infect more than 526,000 systems

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Cryptocurrency Mining Smominru Botnet Infected more than 500,000 Windows Machines appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 69 : How to remove pesky adware from your PC 2018-02-01 17:41:39

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on removing adware from your PC:
What is most likely to be an overlooked story from blog.malwarebytes.com
How to delete adware
Your way out is relatively simple. If you think there?s an adware issue on your PC, you can manually delete it in a few easy steps.
Back up your files. When you face a potential infection, it is always a good precaution. Grab the external hard drive or save the most important data to the cloud.
Download or update the necessary tools. In order for your PC to be clean and tidy, you will need to download or run an update that is specific to scanners that remove adware and PUPs (such as Adwcleaner or the free version of Malwarebytes). If you suspect your computer is seriously infected and you do not have them, you need to have it installed on a friend?s computer and transfer it to your computer via CD or USB.
Uninstall unnecessary programs. Before using your security product for scanning, check that your adware program has an uninstaller. To do this, go to the ?Add / Remove Programs? list in your Windows Control Panel. If the unwanted program is there, highlight it and select the ?Delete? button. After deleting the adware, restart your computer even if you are not prompted to do so.
Use adware and PUP removal to run the scan. Once the program scans and finds the adware, it may isolate something, so you can take a look and decide whether or not to remove it. Our suggestion is to delete, delete, delete. This will get rid of adware and any other residual files that may bring back adware.
How to avoid adware infection
Although the above steps eliminate computers for most adware, there are some forms of militancy that are hard to remove ? and the more aggressive adware is increasingly appearing (pun intended). Today, ad software makers have tweaked their technology around a more comprehensive ad blocking tool by mainstream browser developers such as Google, Mozilla and Microsoft. Their previous gray tactics have turned black.
The bad guys bundle their adware with PUPs programs, preventing them from being removed by preventing the security software from running or even being installed, or by preventing users from removing adware themselves. The only known way to prevent these attacks is to prevent them from happening.
Read more?

How to remove adware from your PC
Half the battle in avoiding adware is reading install wizards and EULAs very carefully. But let?s be real: no one does that. Here?s how to remove adware from your PC in a few easy steps. Categories: 101 How-tos Tags: adwareAdwCleanerhow to removehow to remove adwarewindows adware (Read more? How to remove adware from your PC

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post How to remove pesky adware from your PC appeared first on Safe Harbor on Cyber. Powered by WPeMatico

Chapter 70 : Samsung confirms it is making ASIC chips for cryptocurrency mining 2018-02-01 17:41

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Samsung:
techcrunch.com announces a hidden news that Samsung has confirmed that it has started production of ASIC chips for digging Bitcoin, ether and other cryptocurrencies.
?Samsung?s foundry business is currently engaged in the manufacture of cryptocurrency mining chips, however, we can not disclose more details about our customers,? a company spokesman told TechCrunch.
Samsung declined to provide more details when we asked.
South Korean media reports said the technology giant has partnered with an unnamed Chinese distribution partner. Samsung has produced mass-storage chips for GPUs, which are often used to process graphics on computers, but are also being deployed for mining purposes.
The news led to big competition in the field of ASIC, which is dominated by China?s Bitmain and Canaan Creative, both of which have teamed up with Taiwan?s giant TSMC. In fact, encryption technology is said to have added $ 354-4 million to TSMC?s (already impressive) quarterly revenue.
How Samsung adapt to this equation is unclear. At a fundamental level, it will be as rival as TSMC, which competes in other industry segments, as a company that builds and markets finished products in the market. However, if Samsung?s move brings in a new partner or if it does its own hardware, then it can make a competitor Bitmain and collaborate.
All of this, some of the key business encryption has a significant impact on Samsung?s bottom line. The Korean company?s chip sales in 2017 reached a staggering 6.9 billion US dollars, mainly due to the smart phone industry.
Read more?
Fresh from toppling Intel as the planet?s biggest seller of chipsets, Samsung has confirmed that it has begun manufacturing ASIC chips which are used to mine bitcoin, ether and other cryptocurrencies. ?Samsung?s foundry business is currently engaged in the manufacturing of cryptocurrency mining chips. However we are unable to disclose further details regarding our??
Engaging post, Read More?
thumbnail courtesy of techcrunch.com

Samsung?s now making chips designed for cryptocurrency mining
Samsung?s semiconductor business is booming, with the company recently overtaking Intel as the world?s biggest chipmaker. But the South Korean firm is not resting on its laurels, and is currently looking to expand into the buzziest contemporary market for processors: cryptocurrency mining. As reported by TechCrunch, Samsung has confirmed it?s in the process of making hardware specially designed for mining cryptocurrencies like Bitcoin and Ethereum. A spokesperson for the firm told TechCrunch: ?Samsung?s foundry business is currently engaged in the manufacturing of cryptocurrency mining chips. However we are unable to disclose further details regarding our customers.? These chips are known as ASICs, or application-specific integrated circuits. ASICs are processors that have been specially designed for a single computational task, as opposed to the multi-purpose processors we use in computers and phones. As the valuation of cryptocurrencies has shot up, so has the demand for these sorts of chips. In the case of Bitcoin, the currency is created by solving mathematical problems, with these calculations also maintaining the integrity of Bitcoin transactions. As more bitcoins are mined, these math problems become increasingly difficult. This has led to miners moving on from using normal integrated graphics cards, to GPUs designed for gaming,? Samsung?s now making chips designed for cryptocurrency mining

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries.

The post Samsung confirms it is making ASIC chips for cryptocurrency mining appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 71 : Scarab ransomware: new variant changes tactics 2018-02-01 17:41:37

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Scarabey:
This story from blog.malwarebytes.com gives a surprising look at Scarab ransomware discovered in June 2017. Since then, several varieties have been created and discovered in the wild. The most popular or widely distributed version is distributed through the Necurs botnet, originally written in Visual C. However, after unpacking, we found a different distribution of Scarabey, another variant found in December 2017, with different payload codes.
Like most ransomware, Scarabey?s goal is to require the victim to request Bitcoin payments after encrypting the files on the system. However, Scarabey was not distributed internally via the internal malspam as the original Scarab was, but was found to target Russian users and be distributed via RDP / manual distribution to servers and systems.
In addition, Scarabey does not seem to be included in any of the samples we encountered. Malicious code is written in Delphi, there is no Scarab C + + package, and the content and language of the ransom note vary.
Sample referenceSCARAB Original: e8806738a575a6639e7c9aac882374aeSCARABEY VARIANT: 9a02862ac95345359dfc3dcc93e3c10eRansom noteIn the case of victims, the main difference between the Scarabey and other Scarab ransomware lies in the language of ransom notes and intimidation used in encrypted information.
Different threatsIn the original Scarab version, it warned: the longer users wait, the higher the price.
On the other hand, for Scarabey, it tells users that they are waiting every day and that more and more files will be deleted until no more files are left for them to recover.
Essentially, criminals imply that they have a copy of the unencrypted file given to the user, or they control the victim?s computer to delete the file. This is not correct for the following reasons:
In addition to the totally unreasonable fact that sending every single file on the victim?s computer, there is no network feature that sends the file to the malware author as a ransom.There is no backdoor or remote access code in the Scarab or its variants, which makes the threat of deleting files on the victim?s computer impossible.According to our understanding, the decryption process is after the payment of the ransom, they will send you a decryption software loaded with a unique key. Then you can run the software and decrypt your files. This means that they have no way to limit decryption because it is done locally and offline.No part of the malware code deletes the user?s files from the computer.Specifically, in this message, you see that the author implies that the code was originally decrypted on the server side, which is untrue:
?Deleted 24 files every 24 hours. (We have their copy.)If you do not run the decryption program within 72 hours, all files on your computer will be completely erased and will not be recovered.
The malware author then gives the decryption step, which references the use of the decryption program sent to the victim after payment. Decryption software received after payment using the unique key will be locally decrypted File:
?- After starting the decoder, the file will be decoded in an hour. ? Other users? decoders are not compatible with each user?s dataUnique encryption key ?
The conclusion here is that the idea that authors can delete files by deleting files or malware is purely an intimidation method used to prompt users to remit money quickly.
Read more?
We?ve found that a variant of the Scarab ransomware, called Scarabey, is distributed via a different technique, with a different payload code, and a new target: Russia. Categories: Malware Threat analysis Tags: Necurs malspamransomwareransomware variantScarabscarabey (Read more? Engaging post, Read More?
thumbnail courtesy of blog.malwarebytes.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further

CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Scarab ransomware: new variant changes tactics appeared first on Safe Harbor on Cyber. Powered by WPeMatico

Chapter 72 : Cyber Blackmail Expanding Beyond Ransomware to IoT and Social Media 2018-02-01

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on Cyber Blackmail

Today I came across this story from darkreading.com that covers digital extortion which really cybercriminal cyber blackmail. When we think of cyber blackmail, we often think of ransomware. But now cybercriminals are looking for new ways to shatter organizations beyond blackmail. Cybercriminals already know that many businesses will pay if ransomware attacks affect their day-to-day operations. Ransomware pushes the peak of cyber blackmail in 2017 and still the weapon of choice for cybercriminals

Internet of Things Cyber Blackmail

Cybercriminals will start using the Internet of Things,IoT, (especially the Industrial Internet of Things) to grow and extort money from victims. Key manufacturing and health care are the best examples of attacks on manufacturing plants and robots and sensitive documents and documents. Enterprises that need to be up and running are particularly vulnerable. He continues: ?Any real-time service organization, real-time operations will be affected.

These plants and machines usually run on legacy systems and various hardware, and patches or upgrades are possible if not impossible. These systems are the main goals for attackers looking for old loopholes. Trend Micro?s report highlights supply chain disruptions, such as an attacker inserting a logical bomb or a Trojan into a specific network location. Victims need to pay to find the bug?s location so they can be disabled.

Digital files, which are usually targeted at ransomware attacks, are not as complete as the key processes. Threatening actors want to ?peel onions,? Cabrera said and get core infrastructure data that businesses will pay to keep. ?They are going deeper and deeper into organizing these processes ? If these processes are affected, you

know they will pay for it.?

Social Media Cyber Blackmail

Social media blackmail is another growing threat. One form is smear activity, which spreads fake information and asks the victim to pay or stop. These more common campaigns among celebrities and politicians have started to target brands and executives. Once a company?s reputation is damaged online, it is hard to rebuild.

Cabrera points out: ?We live in a reputable economy.? CEOs and board members, especially in this era of society, are being promoted, and whatever they say, good or bad, can be immediate Seen online

Computer Cyber Blackmail

Ransomware will not go anywhere. Cabrera said: ?I think extortion software will not disappear, will only continue to evolve. Security experts across the industry have noticed the spike in ransomware, with a 90% detection rate of corporate victims in 2017. Last year, more than 50% of companies were attacked by ransomware, and on the average, they were hit twice.

Ransomware has proven to be a reliable earner for the financial losses of cybercriminals and victims. Sophos found that the median total cost of ransomware attacks was $ 133,000. This includes ransom, downtime, labor, equipment costs, network costs and opportunity costs. Of the 2,700 respondents surveyed, 5% said that the total cost of ransomware varied from 1.3 million to 6.6 million U.S. dollars.

In the following year, Trend Micro predicts that ransomware criminals will add new capabilities to their digital weapons through ?old books? that re-use traditional malware technologies. This may include PE (Portable Executable) infections and more aggressive communication strategies to drive the speed and spread of attacks. Analysts also suggest that criminals will establish a system that minimizes their interaction with victims.

Cabrera said the arrival of GDPR will change the tactics extorted by cybercriminals. They understand the impending changes and if they do not comply, the company will have to pay a fine. He predicts they will use the new rules as a lever for victims to pay for the data.

He explained: ?They are just on the surface of understanding what organizational motivation is.? Not only do they fine-tune their tools for organizing but also understand all the financial aspects ? I absolutely believe that GDPR will be used as Impact payment ransom tool.

Pay or Not Pay the Cyber Blackmail?

The problem persists: should you pay when you are subjected to ransomware? Cabrera said that if your company is in the last place of choice, then you have failed.

He said: ?The days of ransomware attacks on our personal computers are gone, it is more annoying than the risks of business.? You should have a very strong plan to deal with digital ransomware. ?

There are many reasons not to pay, but unplanned organizations find themselves weighing the pros and cons of payments.

If or when they are attacked, businesses need people, processes, and technology to reduce risk. There is no guarantee that you will receive your data when it is retrieved. And, even if you did get it back, there is no guarantee that it is not copied or stolen.

Cabrera said: ?Even a slight change in the data may affect weeks or months of operation.

Read More?

In the future of digital extortion, ransomware isn?t the only weapon, and database files and servers won?t be the only targets. Engaging post, Read More?

thumbnail courtesy of darkreading.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post Cyber Blackmail Expanding Beyond Ransomware to IoT and Social Media appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 73 : Google Deletes 700,000 Malicious Apps From Play Store in 2017 2018-02-01 17:41:36

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Google:
A recent story from gbhackers.com discusses things we don?t talk about but Google deleted about 700,000 malicious applications in 2017, that is in violation of Google Play Store policies and malicious adware applications that silently execute malicious activity on users? Android devices.
The removal of applications was 70% more than the deletion of applications in 2016, clearly demonstrating that cybercriminals distribute many malicious Android applications daily and quickly add Android-based attack vectors. In this case, 99% of the Andoird apps being removed are identified and blocked, and anyone can install them on their Android phone.
The total number of Google Play Store apps is projected to be 2.6 million in December 2016 and 3.5 million in December 2017.
Google play store blocked those 700,000 apps are mainly based on one of the following categories.
Copycats
Inappropriate content
Potentially Harmful Applications (PHAs)
Read more?
Google blocked nearly 700,000 Malicious Apps in 2017 alone that violated Google Play Store policies and Malvertising Apps which silently Performing malicious activities on users Android Device. Removed apps are 70% more than the apps taken down in 2016 that clearly indicate that Cyber criminals are distributing many malicious android applications day by day and Engaging post, Read More?
thumbnail courtesy of gbhackers.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Google Deletes 700,000 Malicious Apps From Play Store in 2017 appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 74 : New Tool Automatically Finds and Hacks Vulnerable Internet-Connected Devices 2018

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on AutoSploit Tool

The motherboard.vice.com summarizes a new tool that ?The name may indicate that AutoSploit is trying to automate the use of remote hosts,? said the Github page of the tool. On Wednesday, Pseudonymous Security Researcher and AutoSploit Tool creator Vector shared this tool on Twitter.

AutoSploit Tool Explained

AutoSploit brings together several different hacks of tools and workflows into one package. Often, a hacker may need to find a server or other target; check if the target is vulnerable to any possible exploits; and then launch a successful attack.

On the other hand, AutoSploit combines Internet device search engines Shodan and Metasploit, a well-known penetration testing tool to perform vulnerability attacks.

?Basically you started the tool and then typed in a search query like? apache ?,? Vector tells the board in Twitter to refer to the popular Web server software. Later, the tool uses the Shodan API to find computers that are described as ?apache? on Shodan.

?After that, load and sort the list of Metasploit modules based on your search query, and once you have chosen the right module, it will start to run them sequentially on the list of targets you?ve got,? they added.

It can be said that this tool reduces hacker barriers to entry because hackers may not have the ability to immediately target a large number of machines. This has given AutoSploit some criticism in the area of information security.

?There?s no need to release this, and the connection with Shodan makes the issue even more prominent,? said Richard Bejtlich, a longtime security expert, who posted Twitter tweets on Twitter.

?There is no good reason to develop a public system on a large scale within the playboy, and it?s not wise to do just because you can do something that will end in tears,? he added. However, vectors are not alarmed.

He added: ?I saw these comments too. What I mean is that the same criticism can be applied to anyone who releases their assault tools.

?I personally think that the information should be free, I am an open source fan, why??

Read more?

Hacking isn?t always hard. Some lower-tier hackers use programs to automatically churn through breached login details to break into other accounts, and some penetration testing tools are designed to streamline processes so hackers can get to the more interesting stuff as quickly as possible. Enter AutoSploit, a program which takes that idea of efficient hacking, but severely ramps up the potential for damage by automating pretty much everything, including the process of finding a vulnerable target to attack. ?As the name might suggest AutoSploit attempts to automate the exploitation of remote hosts,? the tool?s Github page reads. Pseudonymous security researcher and AutoSploit creator Vector shared the tool on Twitter on Wednesday. In short, AutoSploit simply brings together several different tools and workflows for hackers into one package. Usually, a hacker might have to find a server or other target; check whether the target is vulnerable to whatever exploit they may have; and then deliver the attack successfully. AutoSploit on the other hand, combines Shodan, a sort-of search engine for internet-connected devices, and Metasploit, a well-known penetration testing tool for executing of exploits. ?Basically you start the tool, and enter a search query, something like ?apache?,? Vector told Motherboard in a? Engaging post, Read More?

thumbnail courtesy of motherboard.vice.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post

The post New Tool Automatically Finds and Hacks Vulnerable Internet-Connected Devices appeared first on Safe Harbor on Cyber.

Powered by WPeMatico

Chapter 75 : 10 ways to guard against real estate cyber scams from FBI and NAR 2018-01-31 18:54

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary
This story from inman.com guides a surprising event that Realty Executives hosted a webinar to educate agents and brokers about wire fraud, and National Association of Realtors (NAR) senior counsel Finley Maxson and FBI supervisory special agent Martin Hellmer both attended. They said awareness, education, and preparedness are key in safeguarding your business and your clients.
This industry is stepping in the right direction to educate their agents and brokers. Other small businesses should follow to keep their business to be a safe harbor on cyber.

Hellmer said businesses usually focus on having top-notch technology and cybersecurity, but forget to educate employees on best practices, which he called a major mistake.
?We typically think of these magnificent young minds at the command line and typing things we don?t understand ? and a lot of hackers are that good ? however, the primary entryway into the front door is through phishing emails,? Hellmer said in the webinar.
?We as humans are curious, and we are usually the ones who give the bad guys access. Our computer networks and systems may have the best protection in the world, but it doesn?t mean a thing if an employee or you click on that phishing email.?
Here are ten tips for combating cyber scams:

Update the software on your phone, computer, tablet and any other electronic device regularly. It?s often annoying to download and install regular updates of your operating system, but you wait to update your device?s software, Maxson and Hellmer say you?re giving criminals the opportunity to take advantage of any security weaknesses.
Air-gap computers that have sensitive information. Air gapping is when you make sure the computer isn?t connected to the internet or to any other computers that themselves are connected to the internet. It?s much more difficult to remotely hack an air-gapped computer.
Regularly back up all your electronic devices. If you?re hit with ransomware?malicious programs that hackers use to lock your computer and hold it hostage in exchange for money, usually a digital currency?you can restore your computer to the latest backup. Maxon and Hellmer also suggest never paying the ransom to get your information back, even if your computer isn?t backed up.
Make sure no one can access all of your business information. The sales team should only have access to information pertinent to their team. This prevents hackers from being able to access the entire network through one person.
Strengthen your passwords. Use passwords that are 10 characters or more, and take advantage of two-factor authentication to protect your emails.
Be aware of common email scams. For example, escrow scams where criminals pose as a title company and change the wiring instructions, referral scams where criminals promise to send a lead for a small fee, and fake Docusign emails and texts with links. These are all ways criminals can gain access to your information.
Implement state-compliant policies. This includes policies for handling and disposing personally identifiable information (PII), such as social security numbers and bank information. Also create policies for document protection and disposal, breach notifications and cybersecurity. These measures help reduce the risk of being hacked, and they help if you?re ever civilly sued for negligence.
Conduct voluntary security audits. Hire a security expert who can identify weak points in your systems and offer solutions for strengthening them.

Invest in cyber insurance. This will cover the costs of restoring the network and the data, providing breach notifications and credit monitoring.
Make sure your vendors are following proper cybersecurity protocols. Closely read over the security and privacy policies of the companies you work with and rely upon, and find out what recourse you have?if any?if they are hacked and your information is exposed.Read more

Faster. Better. Together.Inman Connect San Francisco, Jul 16-20, 2018 Although technology has made real estate transactions quicker, more seamless and increasingly transparent, it has also made buyers, sellers and real estate professionals vulnerable to cybercriminals looking to cash in. In the past year, $969 million have been stolen from buyers via escrow scams ? something cybercrime professionals say will continue to grow in popularity. Last week, 100-percent commission real estate franchisor Realty Executives hosted a webinar to educate agents and brokers about wire fraud, and National Association of Realtors (NAR) senior counsel Finley Maxson and FBI supervisory special agent Martin Hellmer both attended. They said awareness, education and preparedness are key in safeguarding your business and your clients. Hellmer said businesses usually focus on having top-notch technology and cybersecurity, but forget to educate employees on best practices, which he called a major mistake. Engaging post, Read More?
thumbnail courtesy of inman.com.
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post 10 ways to guard against real estate cyber scams from FBI and NAR appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 76 : Critical Oracle Micros POS Flaw Affects Over 300,000 Payment Systems 2018-01-31 1

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary
I couldn?t believe this story from thehackernews.com that features the truth on Oracle has released a security patch update to address critical remotely exploitable vulnerabilities affecting its hospitality industry MICROS point-of-sale (POS) business solution.The fix has been released as part of the January 2018 update to Oracle and 238 vulnerabilities have been fixed in its various products.
According to the public disclosure of ERPScan, a security company that discovered and disclosed to the company, Oracle?s MICROS EGateway application service is deployed by more than 300,000 small retailers and businesses around the world and is vulnerable to directory traversal attacks.If exploited, the vulnerability (CVE-2018-2636) could allow attackers to read sensitive data and receive information about various services from vulnerable MICROS workstations without requiring any authentication.Using directory traversal vulnerabilities, unauthorized insiders have access to vulnerable applications, reading sensitive files from MICROS workstations, including service logs and configuration files.As the researchers explained, two such sensitive files stored in the application memory (SimphonyInstall.xml or Dbconfix.xml) contain the username and encrypted password connected to the database.
The researchers warned: ?Therefore, an attacker could crawl the database username and password hash, tamper with it and use all business data to gain full access to the database in a variety of ways, resulting in compromise of the entire MICROS system.?If you think visiting the POS URL is a good choice, keep in mind that hackers can find digital scales or other devices that use RJ45, connect it to Raspberry PI, and scan the internal network, which makes them easy to spot POS systems, Remember this fact when you enter the store. ?ERPScan also released a proof-of-concept Python-based exploit which, if executed on a vulnerable MICROS server, sends a malicious request to get the contents of a sensitive file.In addition, Oracle?s January 2018 Patch Update also provides fixes for Specter and Meltdown Intel processor vulnerabilities affecting some Oracle products.
Oracle has released a security patch update to address a critical remotely exploitable vulnerability that affects its MICROS point-of-sale (POS) business solutions for the hospitality industry. The fix has been released as part of Oracle?s January 2018 update that patches a total of 238 security vulnerabilities in its various products. According to public disclosure by? Engaging post, Read More?
thumbnail courtesy of thehackernews.com
If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Critical Oracle Micros POS Flaw Affects Over 300,000 Payment Systems appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 77 : South Korea says it uncovered about $600 million in cryptocurrency crimes 2018-01-31

CyberWisdom Safe Harbor Commentary:

Today I came across this story from cnbc.com that reflects things we don?t talk about but, according to a statement released on Wednesday by South Korean customs officers, South Korea found cryptocurrencies worth 637.5 billion won ($ 594.3 million), including illegal foreign exchange transactions.
The statement said domestic investors have purchased 1.7 billion won worth of cryptocurrencies sent to overseas partner companies through virtual wallets. Then transferred back to the legal tender, which is equivalent to the unrecorded capital outflow.
The custom also said it will continue to oversee the use of cryptocurrencies in the case of illegal currency transactions or money laundering.
Read more?

South Korea has uncovered cryptocurrency crimes worth 637.5 billion won ($594.35 million), which includes illegal foreign exchange trading, a statement released by the country?s customs service said on Wednesday. The statement said domestic investors bought 1.7 billion won worth of cryptocurrencies, which they sent to overseas partner companies through virtual wallets. The transfers were then converted back into fiat currencies, which amount to unrecorded capital outflows. The customs office added that it would continue to monitor the use of cryptocurrencies in cases like illegal currency trading or money laundering. Engaging post, Read More?
thumbnail courtesy of cnbc.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. [wpseo_breadcrumb]

The post South Korea says it uncovered about $600 million in cryptocurrency crimes appeared first on Safe Harbor on Cyber.

Chapter 78 : The Silent Threat That?s Putting Your Network at Risk by DNS Hijacking 2018-01-31 1

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on DNS hijacking:
Today I came across this story from darkreading.com that visualizes a hidden DNS hijacking: silent threat that puts your network in jeopardy. This technique is easy to implement and can cause great damage.
Recently discovered MaMi malware modifies the DNS configuration of infected devices. This is a good reminder that DNS hijacking is a constant threat that enterprise IT organizations need to take seriously. DNS hijacking is easy to achieve, can be hard to find, and surprisingly causes damage. This is what you should know and what you can do to fight it.
DNS hijacking Explained
DNS hijacking is simple: you only have to rewrite the configuration of the devices on the Internet to send DNS queries to malicious DNS servers. Many malwares do this and are often just one of the many consequences of infecting devices. Almost all malware can do this ? modifying DNS settings usually does not require any special permissions. Perhaps the most famous malware in this category is DNSChanger, which may have infected more than 4 million computers. Although DNSChanger was banned in 2011, there are still hundreds of thousands of infected computers on the Internet.
So why change the device?s DNS configuration? In the case of DNSChanger, ads on websites are mostly used to replace advertisements sold by bad guys running rogue DNS servers. This may sound less shocking, but DNS hijackings may also have more serious implications. For example, David Dagon and his company discovered and wrote down malicious DNS servers in their 2008 research report, ?Malicious DNS Resolution Path: The Rise of the Authority for Malicious Solutions,? for example. Dagon found on the Internet a small part of the recursive DNS server open, no matter which domain you look for, always in response. For example, some addresses will always reply to the same set of IP addresses, none of which is the correct address.
What is the purpose of this DNS service?
Well, it turns out that the hosts running these IP addresses (in our case, A, B and C) are running open web proxies. As a result, users of devices that query DNS servers will unknowingly access the Web through open Web proxies that can snoop on their traffic. And DNS servers can easily direct users to sites that look the same as their banks or brokers, where they unknowingly enter their credentials and capture them for later use by bad guys.
Fortunately, there is a simple way to mitigate the threat of these DNS hijacking attacks: Do not let any internal IP address on your corporate network send DNS queries to any IP address on the Internet.
In most DNS architectures, only a fraction of the DNS servers (called Internet transponders) actually need to be able to query DNS servers on the Internet. You should specifically allow only its IP address to exchange DNS messages with the IP address on the Internet. If some of your internal devices are infected with malware that modifies their DNS configuration, they will only stop resolving the domain name, which alerts the user to the fact that they are not paying attention. Hopefully this will lure them to bring the device to IT, and if they are lucky, the infection will be discovered.Read more?
The technique is easy to carry out and can cause much damage. Here?s what you need to know about fighting back?. Engaging post, Read More?
thumbnail courtesy of darkreading.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further

CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post The Silent Threat That?s Putting Your Network at Risk by DNS Hijacking appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 79 : Mozilla plugs critical and easily exploitable flaw in Firefox Browser (not Chrome) 2018-0

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Mozilla flaw in Firefox
Today I came across this story from helpnetsecurity.com that reveals
If Firefox users want to keep their computers safe, it?s best to upgrade to the latest version of your browser.
Fix to CVE-2018-5124 Flaw in Firefox
Firefox 58.0.1, released on Monday, contains a very important security fix that can address vulnerabilities caused by insufficient HTML fragmentation in the Chrome privileges document.The vulnerability (CVE-2018-5124) is considered to be very important because a successful exploit may allow an attacker to execute arbitrary code with the user?s privileges. And, if the user has elevated privileges, the attacker can completely compromise the system.
Another reason for this classification is that exploitation can be triggered by a few clever social projects.
?An attacker could exploit the vulnerability by persuading a user to access a link or file that submits malicious input to the affected software,? Cisco explained in an advisory.
To exploit this vulnerability, attackers may use misleading language or instructions to convince the target user to open the file. ?
Mozilla developer Johann Hofmann found this vulnerability in Firefox versions 56-58. Firefox for Android and Firefox 52 ESR are not affected.
It is recommended that users and administrators apply software updates as soon as possible, as a rule, to avoid the following links or open attachments being included in unsolicited (email) messages from unidentified sources.
Read more?
Firefox users would do well to upgrade to the browser?s latest release if they want to keep their computers safe from compromise. Released on Monday, Firefox 58.0.1 contains one but very important security fix that plugs a vulnerability arising from insufficient sanitization of HTML fragments in chrome-privileged documents. (In this context, chrome is not the popular Google browser, but a component of Firefox.) The vulnerability (CVE-2018-5124) is considered critical because a successful exploit could allow More ? Engaging post, Read More?
thumbnail courtesy of helpnetsecurity.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post Mozilla plugs critical and easily exploitable flaw in Firefox Browser (not Chrome) appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 80 : A Perfect ten scored CVSS rating on 10 Cisco VPNs vulnerability 2018-01-31 13:50:46

Your Feed is from https://www.safeharboroncyber.com/Blog/
CyberWisdom Safe Harbor Commentary on Cisco VPNs vulnerability
What is most likely to be an overlooked story from theregister.co.uk explores the truth about a mis-programming code in Cisco VPNs software exist for more than five year that introduces a highly critical vulnerability to a score of solid ten. The vulnerability is opened for attacks on ten different Adaptive Security Appliances and Firepower Threat Defense software products.
The Cisco VPNs vulnerability scored a perfect rating of 10 on CVSS Scale, and exists in the SSL VPN feature of the product. This is bad news, because if you have already deployed VPNs (especially webvpn) for use by employees in the field, the interface will be exposed on the Internet. If you are lucky, attackers may trigger reloading and denial of service attacks. If you?re not lucky, criminals will be able to execute arbitrary malicious code on your network firewall.
Cisco VPNs vulnerability
Suggestion from Switchzilla: ?This vulnerability was caused by an attempt to double release memory regions when webvpn functionality was enabled on Cisco ASA appliances. An attacker can send multiple elaborate XML packages to the webvpn configuration interface on the affected system Exploit this vulnerability. ?
The issue affects Firewall Modules for the 3000 Series Industrial Firewall, ASA 5500 and 5500-X Firewalls, Catalyst 6500 Switches and 7600 Series Routers, Virtual ASA 1000V and ASAv Products, Three Firepower Appliances (2100, 4110 and 9300 ASA Modules) and Firepower Threads Defense (FTD) software.
Programming vulnerabilities seem to have been introduced in ASA 8.x, at least as early as a few years ago. Cisco has released an affected ASA build table along with the fixes from the above recommendations. This bug also affects Firepower Threat Defense 6.2.2 released last year, as well as subsequent releases (fixed 6.2.2.2-4 or 6.2.2.2-6), depending on your hardware.
Both Adaptive Security Appliance software and Firepower Threat Defense software fixes are available ? if you have a Cisco service contract, or your reseller can provide patches. If not, you will have to ask the Cisco Technical Assistance Center. ®
Patch your Adaptive Security Appliance and Firepower Threat Defense code before they?re utterly p0wned A programming slip in Cisco VPN software has created a critical vulnerability hitting ten different Adaptive Security Appliance and Firepower Threat Defense Software products. Engaging post, Read More?
thumbnail courtesy of theregister.co.uk

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home » Curated SafeHarboronCyber?s CyberWisdom Post
The post A Perfect ten scored CVSS rating on 10 Cisco VPNs vulnerability appeared first on Safe Harbor on Cyber.
Powered by WPeMatico

Chapter 81 : Dutch Banks, Tax Agency Under DDoS Attacks a Week After Big Russian Hack Reveal

CyberWisdom Safe Harbor Commentary on DDoS Attack:

A must-read story from bleepingcomputer.com features an interesting on a coordinated DDoS attack on their respective infrastructure attacks with at least three Dutch banks and the Netherlands Revenue Agency reported Monday. Officials at ABN Amro, Rabobank and ABN Amro reported having suffered a DDoS attack that prevented them from logging in to the web-based dashboard.

DDoS attacks by ABN Amro started per bank statement on Saturday, while two other banks were attacked Monday.

Also Monday, Belastingdienst admitted that it had suffered a DDoS attack, preventing users from logging on to their portal and submitting tax-related documents.

DDoS attack reached 40 Gbps

According to Rickey Gevers, a Dutch security researcher, the number of these attacks reached a peak of 40 Gbps. He also said that these attacks come mainly from the IP address associated with the home router. A report by NL Times citing anti-virus vendors ESET claims that some DDoS attacks were also conducted using Zbot malware, a known (desktop-based) bank Trojan based on the old ZeuS bank trojan.

The same report claimed that the botnet command and control server in Russia.

Many people worry that DDoS attacks are the response to last week?s exposure
The obsession with the Russian media by the Dutch media is not by accident. Last week, a report was published by Dutch newspapers Volkskrant and NOS television, claiming that the country?s AIVD intelligence service violated computers that were part of the hacker for Cozy Bear, also known as APT29, a Russian cyber espionage agency.

GandCrab Ransomware Distributed by Exploit Kits, Appends GDCB Extension Scientists Warn of Transduction Attacks on Sensors Tor-to-Web Proxy Caught Replacing Bitcoin Addresses on Ransomware Payment Sites Teen Sentenced 8 Years in Prison for Buying Bomb on the Dark Web to Kill Parents Cisco Fixes Remote Code Execution Bug Rated 10 Out of 10 on Severity Scale InsaneCrypt (desuCrypt) Decrypter How to remove Www.ab4hr.com Redirects Remove the FF AntiVir Monitoring Firefox Addon Remove the 11 Pumpkin Flavored Foods Chrome Extension Remove Security Tool and SecurityTool (Uninstall Guide) How to remove Antivirus 2009 (Uninstall Instructions) How to Remove WinFixer / Virtumonde / Msevents / Trojan.vundo How to remove Google Redirects or the TDSS, TDL3, or Alureon rootkit using TDSSKiller Locky Ransomware Information, Help Guide, and FAQ CryptoLocker Ransomware Information Guide and FAQ CryptorBit and HowDecrypt Information Guide and FAQ CryptoDefense and How_Decrypt Ransomware Information Guide and FAQ How to Rename a Hyper-V Virtual Machine using PowerShell & Hyper-V Manager How to Install Hyper-V in Windows 10 How to Enable CPU Virtualization in Your Computer?s BIOS How to open a Windows 10 Elevated Command Prompt How to start Windows in Safe Mode How to remove a Trojan, Virus,

Worm, or other Malware? Engaging post, Read More?

thumbnail courtesy of bleepingcomputer.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home

» Curated SafeHarboronCyber?s CyberWisdom Post

The post Dutch Banks, Tax Agency Under DDoS Attacks a Week After Big Russian Hack Reveal

appeared first on Safe Harbor on Cyber

.

Powered by WPeMatico

Chapter 82 : Japan Suffers the Biggest Cryptocurrency Heist in History (Again!) 2018-01-30 21:50:2

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on Cryptocurrency Heist:

A must-read story from thedailybeast.com lays out how on last Friday evening in Japan

, one of the biggest virtual currency exchanges in Asia, Coincheck

, announced that it had lost 58 billion units of the cryptocurrency NEM

, worth roughly $530 million dollars, which may well be the biggest cryptocurrency heist

in history.

For those of us with a long memory, the press conference was eerily reminiscent of Feb. 28, 2014, when Mt. Gox

, once the world?s largest bitcoin exchange, declared bankruptcy and announced that it had lost over $500 million worth of bitcoins to hackers.

This new incident is an embarrassment to the Japanese government, Coincheck at its press conference on Friday, and on its webpage announcements, hackers first broke into the firm?s NEM accounts at 2:57 a.m. Friday, local time, on Jan. 25. The security breach went undetected, however, until almost 11:30 that morning.

According to sources close to Japan?s Financial Services Agency, hackers using overseas servers were able to disguise themselves as authorized users and enter the system. They then withdrew large amounts of NEM, spreading the withdrawals out several times during the eight and a half hours they went undetected.

Yusuke Otsuka, the chief operating officer of Coincheck, confirmed suspicions that the firm?s

cyber security was subpar when, at the press conference, he admitted that the stolen currency had been kept on-line in a ?hot wallet? rather than a much more secure offline storage facility known as a ?cold wallet.?

Read More?

Tokyo wants to be the world center for cryptocurrency trading, but now with the $530 million NEM theft from Coincheck those ambitions could be in ?? Engaging post, Read More?

thumbnail courtesy of thedailybeast.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home

» Curated SafeHarboronCyber?s CyberWisdom Post

The post Japan Suffers the Biggest Cryptocurrency Heist in History (Again!)

appeared first on Safe Harbor on Cyber

.

Powered by WPeMatico

Chapter 83 : Warning: Chrome Extension can hide malware in Android Apps 2018-01-30 21:50:18

CyberWisdom Safe Harbor Commentary on Chrome extensions:

The Google Chrome has handy applets that give you seamless access to services such as Evernote or Password Manager, or Bitmoji for easy access with just a click of a mouse. However, as with Android apps, Chrome extensions can sometimes hide malware or other disasters, even if you install the Chrome extension from the official Chrome Web Store. Google said malicious extensions have been reduced by about 70% over the past two and a half years, but recent research shows that the problem and the risks are far from being solved by users.

William Peteroy, chief executive of security firm Icebrg, said what we?re seeing is an increase in the use of crime. ?When we first started to see criminals, it absolutely matched our needs, and that?s something we need to be aware of, and users need to start paying more attention than usual.

Sneak attack on Chrome extensions

Other browsers suffer a similar impact, but with a market share of nearly 60%, attacks on Chrome users typically affect the most people, making them the primary targets of criminal hackers. Icebrg recently highlighted four malicious extensions in the Chrome Web Store, totaling more than 500,000 downloads. These extensions are disguised as standard tools, with names like ?Stickies? and ?Lite Bookmarks.? The researchers found that they are actually part of click fraud scams to increase the attackers? earnings. And these extensions request sufficient permissions to spy on more, access user data and the like, and track their behavior. After Icebrg privately leaked, Google deleted the four extensions.

Read More?

You already know to be wary of third-party Android apps, and even to watch your back in the Google Play Store. A flashlight app with only 12 reviews might be hiding some malware as well. But your hyper-vigilant download habits should extend beyond your smartphone. You need to keep an eye on your desktop Chrome extensions as well. These handy little applets give you seamless access to services like Evernote or password managers or put your Bitmoji just a click away. As with Android apps, though, Chrome extensions can sometimes hide malware or other scourges, even when you install them from the official Chrome Web Store. Engaging post, Read More?

thumbnail courtesy of wired.com.

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home

» Curated SafeHarboronCyber?s CyberWisdom Post

The post Warning: Chrome Extension can hide malware in Android Apps

appeared first on Safe Harbor on Cyber

.

Powered by WPeMatico

CyberWisdom Safe Harbor Commentary on GandCrab Ransomware

:

Bleepingcomputer.com reveal a post from Malwarebytes exposing a new ransomware, GandCrab, was released late last week and is currently being released through exploits. GandCrab has some interesting features not seen in ransomware, such as the first one to accept DASH currency and the first one to use Namecoin support .BIT tld.

David Montenegro, a security researcher, first discovered that researchers quickly jumped in to analyze ransomware and post their results on Twitter. This article will delve into the content found by myself and other researchers.

Unfortunately, there is currently no way to decrypt files that are freely encrypted by GandCrab. However, this ransomware is under study and we will update this article if new information is available.

Now, if you want to discuss GandCrab, you can read the comments section of this article or our dedicated GandCrab help and support topic.

GandCrab is distributed via the rig attack kit
According to exploit kit researchers nao_sec and Brad Duncan, GandCrab is currently distributing via a malicious advertising campaign called Seamless and then pushing visitors to the RIG exploit kit. The attack kit will attempt to exploit the vulnerability in the visitor software to install GandCrab without their permission.

How to protect your own GandCrab Ransomware

In order to protect yourself from GandCrab ransomware, it is important to use good computing habits and security software. First and foremost, you should always have reliable and tested data backups that you can recover in an emergency, such as ransomware attacks. With a good backup, ransomware has no effect on you.

You should also have security software that includes behavioral detection to deal with ransomware, not just signature detection or heuristics. For example, Emsisoft anti-malware and malware anti-malware all contain behavioral tests that prevent many (if not most) ransomware from infecting encrypted computers.

And last but not least, ensuring that you practice the following safety practices is, in many cases, the most important step:

- Backup, backup, backup!

- If you do not know who sent it, do not open the attachment.

- Until you confirm that the person actually sent to your attachment is turned on,

- Use Accessories such as VirusTotal to scan attachments.

- Make sure all Windows updates are installed Also make sure you update all programs, especially Java, Flash, and Adobe Reader. Older programs contain security holes commonly exploited by malware distributors and utilize toolkits. Therefore, it is very important to keep updating.

- Make sure you are using some kind of security software installed with behavior detection or whitelist technology. Whitelisting can be a painstaking training, but if you are willing to stock it, you can get the maximum return.

- Use a hard password and do not reuse the same password at multiple sites.

Read more:

Fitness Tracking App Accidentally Exposed Military Bases ATM Jackpotting Attacks Hit the US for the First Time Microsoft Issues Windows Out-of-Band Update That Disables Spectre Mitigations Tor-to-Web Proxy Caught Replacing Bitcoin Addresses on Ransomware Payment Sites IOTA Cryptocurrency Users Lose $4 Million in Clever Phishing Attack Lenovo?s Fingerprint Scanner Can Be Bypassed via a Hardcoded Password InsaneCrypt (desuCrypt) Decrypter Remove the 11 Pumpkin Flavored Foods Chrome Extension Remove the FF uBlocker Firefox Addon Remove the S-N-A Chrome & Firefox Extension Remove Security Tool and SecurityTool (Uninstall Guide) How to remove Antivirus 2009 (Uninstall Instructions) How to Remove WinFixer / Virtumonde / Msevents / Trojan.vundo How to remove Google Redirects or the TDSS, TDL3, or Alureon rootkit using TDSSKiller Locky Ransomware Information, Help Guide, and FAQ CryptoLocker Ransomware Information Guide and FAQ CryptorBit and HowDecrypt Information Guide and FAQ CryptoDefense and How_Decrypt Ransomware Information Guide and FAQ How to Rename a Hyper-V Virtual Machine using PowerShell & Hyper-V Manager How to Install Hyper-V in Windows 10 How to Enable CPU Virtualization in Your Computer?s BIOS How to open a Windows 10 Elevated Command Prompt How to start Windows in Safe Mode How to remove a Trojan, Virus, Worm, or other Malware

How to show hidden files in Windows 7 How to see hidden files in Windows A new ransomware called GandCrab was released towards the end of last week that is currently being distributed via exploit kits. GandCrab has some interesting features not seen before in a ransomware, such as being the first to accept the DASH currency and the first to utilize the Namecoin powered .BIT tld. First discovered by security researcher David Montenegro, researchers quickly jumped in to analyze the ransomware and post their results on Twitter. This article will dive into what has been discovered by myself and other researchers. Unfortunately, at this time there is no way to decrypt files encrypted by GandCrab for free. This ransomware is being researched, though, and if any new information is released we will be sure to update this article. For now, if you wish to discuss GandCrab you can this article?s comments section or our dedicated GandCrab Help & Support Topic. Engaging post, Read More?

thumbnail courtesy of bleepingcomputer.com

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home

» Curated SafeHarboronCyber?s CyberWisdom Post

The post GandCrab Ransomware Distributed by Exploit Kits, Appends GDCB Extension

appeared first on Safe Harbor on Cyber

.

Powered by WPeMatico

Chapter 85 : File Your IRS Taxes Before Cyber Scammers Do It For You 2018-01-30 21:50:06

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on IRS Taxes:

A must-read story from krebsonsecurity.com notes that today, one day after January 29, officially the first day of the 2018 reporting season, is also known as the day cyber tax scammers began to demand a false tax rebate on behalf of the victims of identity theft which is stealing your tax returns. Want to minimize the chance of this year?s tax fraud? Give the tax before the bad guys!

Hundreds of thousands (or even millions of U.S. dollars) of U.S. citizens suffer tax rebates every year. Victims usually know about crimes only after they are denied because the liar assaulted them. Even those who do not need to submit a return can be victims of refund fraud, as do those who do not actually have a refund from the IRS.

According to the IRS, consumers? complaints about tax fraud have been steadily declining for years, as the IRS and the states have enacted stricter measures to screen potential fraud applications.

If you submit taxes electronically and the returns are denied, and if you are a victim of identity theft (for example, if your social security number and other information occurred during the Equifax spill last year), you should file an identity theft Affidavit form 14039). The IRS recommends that if you suspect that you are the victim of identity theft, even if you have to continue paying the tax paper and submitting the tax return.

If the IRS considers you may be the victim of tax fraud for the preceding tax year, they may send you a special application password, which you will need to enter with this year?s tax return before you can electronically obtain IRS accept. This year is the third of the last five I received from the IRS for one of the PINs.

Of course, submitting taxes early to beat fraudsters requires one person to have all the tax forms. As a wholly-owned company, this is a big challenge as many companies have spent their sweet time sending 1099 forms etc. (even if they were asked to do so on January 31).

Many companies are now turning to online services to provide tax forms to contractors, employees, and others. For example, I received several emailed notifications about the online availability of Form 1099; most said they were using snail mail to send the form, but if I just created an account or entered some personal information on a third-party site, Well if I need them earlier, I can get them online.

Having seen so many websites deal with personal information, I am not very interested in more volunteers. According to Bankrate, even if the taxpayers do not yet have the full 1099, they can still submit returns ? as long as you have the right information and how much you have.

Bankrate explains: ?Unlike the W-2, you typically do not need to append 1099s to your tax returns.? They?re just shipping, so you know how many reports and copies you have to the IRS, so the return processor can double-check your entry. As long as you have the correct information, you can put it on your tax form without the need for a hand statement. ?

In past tax years, identity thieves used data collected from various third-party and government websites to file false tax rebates ? including from the IRS itself! One of their longstanding favorites is the Get Transcript service from IRS, which had quite relaxed certification before.

Read more?

Today, Jan. 29, is officially the first day of the 2018 tax-filing season, also known as the day that fraudsters start requesting phony tax refunds in the names of identity theft victims. Want to minimize the chances of getting hit by tax refund fraud this year? File your taxes before the bad guys can! Tax refund fraud affects hundreds of thousands, if not millions, of U.S. citizens annually. Victims usually first learn of the crime after having their returns rejected because scammers beat them to it. Even those who are not required to file a return can be victims of refund fraud, as can those who are not actually due a refund from the IRS. Engaging post, Read More?

thumbnail courtesy of krebsonsecurity.com

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. Home

» Curated SafeHarboronCyber?s CyberWisdom Post

The post File Your IRS Taxes Before Cyber Scammers Do It For You

appeared first on Safe Harbor on Cyber

.

Powered by WPeMatico

Chapter 86 : Intel alerted Chinese cloud giants ?before US govt? about CPU bugs 2018-01-30 21:50

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on Intel Alert:

What is most likely to be an overlooked story from theregister.co.uk recaps the truth about Intel warned Chinese companies before they notified the U.S. government at US-CERT about its infamous Meltdown and Spectre processor vulnerabilities.

According to The Wall Street Journal, big customers, including Lenovo and Alibaba.com, were aware of design mistakes sometime before they pass on the information to U.S. government and small cloud providers, citing some unknown people familiar with the matter and a few related companies.

The disclosure schedule has raised the possibility that some Chinese government officials may have known the vulnerabilities before the U.S. technology giant Intel disclosed it to the U.S. government and the public.

Two chip vulnerabilities, Meltdown and Spectre, were first discovered by members of Google?s Project Zero security team before being independently discovered and reported by other security researchers. ?Intel had planned to make the discovery public on Jan. 9? but sped up its timetable when the news became widely known on Jan. 3, a day after U.K. website *The Register*

wrote about the flaws,? the *WSJ*

reports.

Intel is dedicated to addressing vulnerabilities with security researchers at Google and other teams, as well as PC makers (especially large OEMs) and cloud computing companies. Informed persons include Lenovo, Microsoft, Amazon, and Arm.

The Wall Street Journal did not mention when Lenovo and others were notified, but a memorandum Intel leaked to computer makers showed that at least one group of unnamed OEM disclosure agreements, as previously reported.

Lenovo quickly walked out of the portal on January 3 and issued a statement telling customers the reason for the vulnerabilities as it had previously worked with industry processors and operating system partners.

Speculation on Intel Alert

According to one person familiar with the company, China?s largest cloud service provider Alibaba Group was also notified in advance. A spokesman for Alibaba told The Wall Street Journal the idea that the company may share threat intelligence with the Chinese government is ?speculative and unfounded.? Lenovo said Intel?s information is protected by a confidentiality agreement.

Jake Williams, president and former NSA worker for security firm Rendition Infosec, said Beijing is aware that the exchange of information between Intel and its Chinese technology partners is ?near certainty? because local authorities often Monitor all such communications.

An official at the U.S. Department of Homeland Security operating CERT in the United States said it learned of processor vulnerabilities only from earlier news reports. They added: ?We certainly hope to get this notice.

White House chief cybersecurity officer Rob Joyce publicly claimed that the NSA also did not know the chip flaws known as Meltdown and Spectre

Because of their early warnings, Microsoft, Google, and Amazon were able to roll out protection for their cloud computing customers before the details of Meltdown and Specter were made public. This is important because Meltdown, which allows malware to extract passwords and other secrets from Intel-powered computers? memory, can easily be leveraged and cloud computing

environments are particularly exposed as they allow customers to share servers. Someone rented a virtual machine on a cloud box that could fail with Meltdown design and use the same host server to spy on another person.

Small-scale cloud service providers are beaten to ?catch up.? Joyent, a U.S. cloud service owned by Samsung Electronics, is one of the companies that may benefit from the warning but was not included in the advisory group until it was publicly disclosed.

Bryan Cantrill, the company?s chief technology officer, told The Wall Street Journal ?Others are six months ahead.? ?We?re fighting for it.?

?I do not understand why CERT will not be your first stop,? Canterbury added. This is an understatement that Intel put ahead of their big customers before us. Maybe we should follow some of GDPR rules.

El Reg asked Intel to comment on its disclosure policy. Chipzilla told us in a statement that it does not have the ability to notify all those who plan ahead of time ? including the US government ? because of the loopholes that preceded the Jan. 9 announcements:

The Google Project Zero team and affected vendors, including Intel, follow best practices for responsible and coordinated disclosure. The initial disclosure criteria and proven practices are to work with industry participants to develop solutions and deploy fixes prior to publication. In this case, Intel immediately hired the U.S. government and a few others just prior to the public disclosure date of the industry coalition.

US-CERT, under Department of Homeland Security agency initially suggested that this ?Spectre? vulnerability could only be resolved by swapping unaffected processors before repositioning it, suggesting that adequate mitigation is provided by applying the vendor-supplied patches.
US-CERT -Automated Indicator Sharing (AIS) is available for free through the Department?s NCCIC, a 24/7 cyber situational awareness, incident response, and management center which was designated as the central hub for the sharing of cyber threat indicators between the private sector and the Federal Government by the Cybersecurity.

Read more?

?We certainly would have liked to have been notified of this? says Homeland Security Intel warned Chinese firms about its infamous Meltdown and Spectre processor vulnerabilities before informing the US government, it has emerged. *Engaging post, Read More?*

thumbnail courtesy of theregister.co.uk

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. *Home*

» Curated SafeHarboronCyber?s CyberWisdom Post

The post *Intel alerted Chinese cloud giants ?before US govt? about CPU bugs*

appeared first on *Safe Harbor on Cyber*

.

Powered by *WPeMatico*

Chapter 87 : Ploutus.D Malware Variant Used in U.S.-based ATM Jackpotting Attacks 2018-01-30 2

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on Ploutus.D Malware Variant

I couldn?t believe this story from threatpost.com that visualizes how the modern Bank ATM robbery is unfolding. The U.S. Secret Service issued a warning to financial institutions on Friday stating that financial institutions ?systematically? attack ?credible information? on U.S. ATMs that use malware that can quickly drain cash. ATM machine maker Diebold Nixdorf also warned that customers are likely to warn of potential ?ATM? face-up attacks from Mexico to the United States.

Brian Krebs, a reporter in charge of the KrebsOnSecurity website, reports that the U.S. attack has begun. Krebs quoted sources at ATM maker NCR Corp. as saying that the number of ATM ATMs, also known as logic attacks, has reached the U.S. coast.

related articles on Ploutus.D Malware Variant Bank ATM Robbery:

The first ATM ?jackpot? hit the U.S. cash dispenser ? cash robbery

First ATM ?jackpot? Attacks Hit U.S. ATMs ? Cash Robbery

?While at the moment these issues are all focused on non-NCR ATMs, logical attacks are an industry-wide issue, as was the first case of loss identified as a result of the logical attacks by the United States,? Krebs quoted NCR Consultants as saying.

Although the U.S. Secret Service disagrees with the nature of these attacks, Krebs sources within the agency claim recent attacks include the use of Jackpotting malware Ploutus.D.

The source said the secret service warned that in the past 10 days, thieves appear to be using a series of coordinated attacks on Ploutus.D malware targeting the Opteva 500 and 700 series Dielbold ATMs and there is evidence that further attacks are taking place Plan across the country, ?according to Krebs report.

Dielbold and NCR did not immediately respond to this story?s comment request.

In its advisory, the Special Service Agency said that the threat actors were mainly targeted at stand-alone ATMs. ?ATMs are usually located in pharmacies, large retail stores and through ATMs. Criminals go from individual suspects to large groups of organizations, from local criminals to international organized criminal groups,? the Secret Service said.

The agency is authorizing the U.S. cybercrime team to identify ?credible? threats. ?Subsequently, we remind other law enforcement partners and

Financial institutions who may be affected by this crime, ?it said.

Ploutus.D Malware Variant ATM Attack History

Previous attacks targeted ATMs in Mexico, Japan, Thailand and Europe. Bulkhead malware used in these attacks includes Ploutus, Prilex, Green Dispenser, and Ice5.

In the case of Ploutus, malware has been online since 2013. According to an article published in the Bulletin of the Virus by Kaspersky Lab researcher Thiago Marques, in October 2017, malware lost $ 64 million.

Marques said Ploutus needs physical access via USB or CD to deploy malware in order to steal the ATM ID used to activate and identify the ATM and then redeem it.

In a recent attack, Krebs reported that a Secret Service source said the attackers were using medical devices such as endoscopes to navigate inside the ATM to intercept cash dispenser communications Port, ATM computer, and start malware infection.

Krebs said: ?Currently, malware fraudsters will contact conspirators who can remotely control ATMs and force machines to dispense cash.?

According to the January 2017 FireEye Awards, remote attackers can direct ATMs to distribute thousands of dollars in just a few minutes.

FireEye researchers point out that Ploutus-D is often targeted at Diebold ATM devices running multi-vendor Kalignite platforms. ?We identified samples for the ATM supplier Diebold. However, since the Kalignite platform runs 40 different ATM vendors in 80 countries, minimal code changes to the Ploutus-D will significantly extend the ATM vendor?s goals.? Research Staff said.

Leigh-Anne Galloway said: ?The interesting thing about these attacks is that they require a lot of physical space to access the ATM itself, which means there is a high risk of being discovered and the choice of attack vector is much more complex. Positive resilience leads at Positive Technologies.

Krebs reports that the Secret Service warned financial institutions that ATM running on Windows XP is still vulnerable.

Past ATM robbers used different malware. In August 2016, a family of malware known as RIPPER was accused of some ATM robberies in Thailand. Attackers are able to penetrate the target ATM using an ATM card activated by a special EMV (EuroPay, MasterCard and Visa) chip. This card serves as a mechanism to authenticate with existing RIPPER malware on the ATM. The liar in the incident escaped with 378,000 U.S. dollars.

read more?

ATM maker NCR Corp. is warning that cyber criminals are hacking U.S. cash machines with malware that can drain machines dry of cash. *Engaging post, Read More?*

thumbnail courtesy of threatpost.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing

list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. *Home*

» Curated SafeHarboronCyber?s CyberWisdom Post

The post *Ploutus.D Malware Variant Used in U.S.-based ATM Jackpotting Attacks*

appeared first on *Safe Harbor on Cyber*

.

Powered by *WPeMatico*

Chapter 88 : UK to fine critical organizations up to $24M if they fail to put in strong cyber security and

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on GDPR:

What is most likely to be an overlooked story from techcrunch.com highlights the truth about companies gears up to make themselves compliant on GDPR about upcoming data protection regulations in Europe.

As businesses have filed compliance on the forthcoming data protection legislation on GDPR, businesses operating in member states will face another wave of cybersecurity requirements as part of the NIS Directive on Network and Information Security until 20185 On the 9th of each month, it is implemented in member states.

In the UK, the government announced that organizations that work in key service areas such as energy, transport, water, and health could not prove their cyber-security systems could be fined up to £ 17 million ($ 24 million) to be adequately equipped to withstand attacks.

The main requirements for the organization include having the right people and organizations to deal with cyber attacks; having the right software to protect against attacks; having the proper ability to detect if an attack has occurred; and establishing a proper system that, in the event of system compromise Minimize the impact of the attack (although the other three are in place).

More detailed guidance includes how to secure other aspects of your network, such as your supply chain and the data in the cloud.

The new regulator will evaluate private and public organizations in each sector, not only to review existing infrastructures but also to penalize those who are considered not safe enough and to report violations and promptly make The system of reaction.

Penalties can only be enforced if the system still needs to be improved after the organization is notified. The Ministry of Culture, Media and Sports, which is responsible for implementing the directive as part of its overall responsibility for the digital economy, said this is ?the last resort and does not apply to operators that adequately assess risks, take appropriate security measures, and Regulators contacted but were still attacked.

The National Security Operations Directive (NIS Directive) and the Directives governing how organizations and governments comply are monitored by the National Cyber Security Center (a part of GCHQ). The government has earmarked 1.9 billion pounds of funds and has partnered with companies such as Microsoft in a more unified response to the country?s cyber-security threats.

Ciaran Martin, chief executive of the National Cyber Security Center, said in a statement: ?Networks and information systems provide important support for day-to-day activities, so it is vital that they be as secure as possible.

Contrast on GDPR

An interesting contrast with the decision to force existing traditional organizations to perform their duties better is in contrast with the development of the United States, whose development priorities seem to be expanding to include newer infrastructures.

Yesterday, Axios reported leaked documents from the U.S. National Security Council, advising the U.S. government to build a 5G mobile network. The view is that China?s dominance in wireless networks means that private operators building their own 5G networks tend to buy equipment from Chinese manufacturers.

However, this posed a security threat because of China?s state-sponsored hacking. Therefore, from the ground up ? government-controlled supplier trading, construction, and operations ? is a safer way to help secure the network itself as well as key services in transportation, energy and other areas.

Read more?

Ingrid Lunden (@ingridlunden)?> As companies gear up to make themselves complaint with upcoming data protection regulations in Europe around GDPR, those doing business in Member States will also be facing another wave of requirements around cyber security, as part of the NIS Directive covering network and information security that must be put into place across Member States by May 9, 2018. In the UK, the government has announced that organizations working in critical services like energy, transport, water and health can be fined up to £17 million ($24 million) as a ?last resort? if they fail to demonstrate that their cyber security systems are equipped adequately against attacks. Major requirements for organizations will include having the right people and organization in place to handle a cyber attack; having the right software in to protect against attacks; having the right capabilities in place to detect if an attack has taken place anyway; and having the right systems in place to minimize the impact of an attack if a system is breached (despite the other three being in place). More detailed guidance includes how to secure other aspects of your network, such as your supply chain and how your data in the cloud. Private and public organizations in each sector will be evaluated by new regulators, which will not only vet existing infrastructure and fine those who are deemed to have not had good enough security in place, but help set up systems for reporting breaches and responding to them quickly. The fines will only be applied after organizations are notified of where they are still required to improve their systems. They will be applied, the DCMS said, as ?a last resort and will not apply to operators [that] have assessed the risks adequately, taken appropriate security measures and engaged with regulators but still suffered an attack.? The NIS Directive and managing how organizations and the government will comply are being overseen by the National Cyber Security Centre, which is part of the GCHQ. *Engaging post, Read More?*

thumbnail courtesy of techcrunch.com

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. *Home*

» Curated SafeHarboronCyber?s CyberWisdom Post

The post *UK to fine critical organizations up to $24M if they fail to put in strong cyber security and comply to GDR*

appeared first on *Safe Harbor on Cyber*

.

Powered by *WPeMatico*

Chapter 89 : 2000 WordPress Sites Infected with a Keylogger to steal admin password and Coinhive

Your Feed is from https://www.safeharboroncyber.com/Blog/

CyberWisdom Safe Harbor Commentary on WordPress sites:

Today I came across this story from thehackernews.com that highlights more than 2,000 WordPress sites were once again found infected with an encryption mining malware that not only stole the visitor?s computer resources to dig digital money but also recorded every visitor?s keystroke.

Security researchers at Sucuri discovered a malicious activity that infected WordPress sites with malicious scripts, crypto-currency miners in browsers from CoinHive and a keylogger.

Coinhive is a popular browser-based service that provides site owners with a mechanism for embedding JavaScript to exploit the CPU capabilities of their site visitors to monetize Monero?s cryptocurrency.

Researchers at Sucuri say the threat behind this new campaign is the threat that infected over 5,400 WordPress sites last month, as both used keyloggers/cryptocurrency malware called cloudflare [.]solution.

Cloudflare [. The solution, released in April last year, is cryptocurrency mining malware and has nothing to do with network management and cyber security company Cloudflare. Malware uses cloudflare [.] Solution domain to spread malware initially, so this name is already given.

This malware was updated in November and includes a keylogger. Keyloggers behave in the same way as previous activities and can steal the site?s administrator login page and the site?s public front desk.

WordPress sites keyboard record

If the infected WordPress site is an e-commerce platform, hackers can steal more valuable data, including payment card data. If hackers manage to steal administrator credentials, they can log into the site without relying on the flaws to enter the site.

Read more?

More than 2,000 WordPress websites have once again been found infected with a piece of crypto-mining malware that not only steals the resources of visitors? computers to mine digital currencies but also logs visitors? every keystroke. Security researchers at Sucuri discovered a malicious campaign that infects WordPress websites with a malicious script that delivers an in-browser *Engaging post, Read More?*

thumbnail courtesy of thehackernews.com

(adsbygoogle = window.adsbygoogle || []).push({});

If you like to receive more of these curated safe harbor news alerts then subscribe to my mailing list. and come back soon at https://www.safeharboroncyber.com/Blog/ to read further CyberWisdom Safe Harbor Commentaries. *Home*

» Curated SafeHarboronCyber?s CyberWisdom Post

The post *2000 WordPress Sites Infected with a Keylogger to steal admin password and Coinhive to Mine Cryptocurrency*

appeared first on *Safe Harbor on Cyber*

.

Powered by *WPeMatico*

Chapter 90 : Approaches and opportunities on increasing participation 2010-02-16 22:52:01

THe following are approaches and opportunities on increasing participation.

- We should grant Staff time-off for hosting participation events

- JAM Session with food and fun Events,

- Contest,

- Polls

- Provide Tutorial, Pilots on wiki and blog for practice (explore and getting their feet wet),

- We should have policies and procedures to encourage staff participation without asking their managers for approval.Â Participation to collaborate on and share information should be written in the staff PARS.Â Second there should be awards given on a quarterly basis through the offices to acknowledge successes.Â For this should be two national exemplary awards given to:

- managers - uses innovative approaches and technologies to facilitate collaboration, participation and/or transparency.

- staff or team - onÂ using process and tools to collaborate, participate, and add transparency and meets open government mandates

Chapter 91 : Innovative methods to increase participation, obtain ideas and increase collaboration. 2

Â Ways to Encouragement and Enticement to Change Behavior with Management encouragement

- JAM Session with food and fun Events,

- Contest,

- Polls

- RSS feed to inform new information or comment on their watch or interest page,

- Tutorial, Pilot wiki and blog for practice,

- Personnel Action Incentives

* Add communicative and collaborative duties to employees PARS

* Reward with Awards similar to Suzanne E. Olive Award for Exemplary Leadership in National EEO - Non-Managerial for diversity. We should add another award for individual collaborator facilitator and Monthly Office award to individuals for best collaborator

As I mention earlier that coaching, training, explaining, and leading by example would be appropriate and beneficial activities. But what about measuring? Itâ??s a technical no-brainer to measure how much each individual has contributed and to generate some kind of absolute or relative metric.Â

- Encourage friendly competition. Lots of people are fiercely proud of their PageRanks, TopCoder ratings, number of Wikipedia edits, etc. and work to keep them high only to preserve bragging rights.Â

- Make people strive to improve their scores. I know Iâ??ve been inordinately proud of my Technorati ranking, even though it has no direct bearing on my professional success. The desire to maintain it has definitely driven me to keep blogging regularly.

Chapter 92 : Technology transformation platforms for collaboration. 2010-02-16 22:26:14

Strategically rethink how to deliver on our mission. Individual offices or major programs should strategically develop service-focused uses that may involve using Web 2.0 approaches to reconfigure their business models or services in order to more effectively deliver on their own core missions or outcomes that require collaboration with other agencies. This rethinking should be a part of their required agency-wide strategic planning process and not just within their technology offices.

From Web 1.0
Â Â
Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â to
Â Â
Â Â Â Â Â Â Â Â Â Â Web 2.0

Content publishing by website owner
(business to consumer, government to citizen)Â Â Â Â
Â toÂ Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Content creation by members (peer to peer)

Data extraction by website ownerÂ Â to
Â Blogging, vlogging, and interaction by members

Content management systemsâ??producer Â Â Â Â Â Â Â Â Â Â Â Â Â to
Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Wikisâ??members, consumers, and producers

PortalsÂ
Â Â
Â Â Â Â Â Â Â Â Â to
Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Search engines

Directories and
taxonomyÂ Â
Â toÂ Â Tagging and â??folksonomyâ?•

People, location, Â and data
Â Â Â Â Â Â Â Â Â to
Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â People, location,Â data, and application â??mashupsâ?•

StickinessÂ Â
Â Â Â Â Â Â Â Â Â to
Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Syndication,Â â??open interoperabilityâ?• and

Syntax
Â Â
Â Â Â Â Â Â Â Â Â to
Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Semantics

We should continue to use of open source technologies on a Web 2.0 enterprise platform. For LAMP platform- Linux, Apache, PHP, MySQL we should continue to use MediaWikiÂ and WordPress.Â We should explore the use of Gallery2 or Coppermine for picture, video and multimedia gallery similar to Flickr and YouTube to enable metadata for searching and discovery

of images and file. In addition other wiki like DekiWiki may be use on our lamp server Web 2.0 enable CMS system â?? Drupal or Joomla.Â We could also use ELGG as a social networking application similar to Facebook. We could also use a Microblog software, a WordPress plug-in, to replace twitter.

The second platform is also an open source technology platform with the use of Linix, Apache, Java, MySQL or Oracle for Liferay for social networking application coupled with Xwiki for wiki. This platform will enable us to link with portal through an API.

We should provide RSS feed and social book marking tools.

We should invest in government-wide solutions, such as captioning software to make videos and webcasts on Web 2.0 Platforms accessible to people with disabilities

Chapter 93 : Promote cooperation with other agencies, the public, non-profit organizations and private

Â

First, if your Agency is a leader in Web 2.0 applications, you could promote cooperation with other federal agencies and other organizations to provide best practices, policies, procedures and a framework for open collaboration internally and with the public.Â If other organizations work within our framework we could (in theory) loosely coupled with their application, such as wiki to interlink with their knowledge base that would enrich the collaboration between organizations to discover and access information. Horizontal business processes such as financial management, HR and procurement are subject to increased sharing across agencies and even jurisdictions. This means that government organizations no longer own or control them. Instead they are becoming clients to other organizations leading and ripe on increased adoption of social media. In addition, government IT infrastructure is subject to consolidation efforts and will be progressively commoditized and challenged by cloud-computing solutions.

Second, The "Federal Open Community" should be develop on the virtual cloud of next-gen open social toolsÂ that could share internal blogs, gadgets/widgets, social networks, wiki,Â with common login, profile and contact info with Federal open social tools: anyÂ OpenSocial, Open Ajax API partners portal would be considered part of the "Federal Open Community Social Cloud".Â Once the infrastructure has been developed, information sharing, collaboration and joint projects and efforts may be better facilitated to build a one true One Government, thus meeting the presidentâ??s priority.

Chapter 94 : Key Agency behaviors must change for their staff to be more transparent. 2010-02-16 2

Â

- The Culture of the Management needs to become coaches or inspirer to nourish, participate with and reward their staff. All must given time to first participate, practice and experience by collaborating with tools, such as blogs and wikis internally to further transparency publicly.

- The Agency should be required to fund their â??virtualâ?• office space with remote access as part of their critical infrastructure, in the same way they fund their â??bricks and mortarâ?• office space.

- The Agency should be required to appoint editor-in-chief and content gardener and Web 2.0 Evangelist for every web application they maintain, as do the top commercial websites. This person should be given appropriate funding and authority to develop and enforce web policies and publishing standards, including ensuring that prime real estate on government websites is dedicated to helping people find the information they need.

- The Agency should develop standard job descriptions and core training requirements so agencies can hire and retain highly qualified experts in web content, content gardener, and new mediaâ??not just IT specialists.

- Reward Employees such as 1. Honor Awards similar to Suzanne E. Olive Award for Exemplary Leadership in National EEO - Non-Managerial for diversity. 2. Office awards for individual collaborator, facilitator and /or Monthly Office award to individuals for best collaborators or practioners for enabling transparency

Chapter 95 : Evolution of Managerâ??s Future Role with Open Government Collaborative Culture 2

With the explosion of information, and flattening technologies and organization, starting with e-mail, I think that a future agencyâ??s Manager needs to focus more on the platform that enables collaboration, because and find themselves employees already have all the data. They have access to everything is needed.

In addition the managers should focus on their staff to trust,Â encourage, promote, nourish, reward for those who are practicing, coaching, training, explaining, and leading by example would be appropriate and beneficial activities on increasing transparency, collaboration, participation, tools development, available training and resources, and paving the accomplishing Open Government directive and goals.Â They should learn to trust their staff to do the right thing and accomplish their assignments.Â

So, what will the Manager do with the changing to a social culture?Â The manager will have to work on the structure of collaboration. How do people get recognized? How do you establish a meritocracy in a highly dispersed environment and inspire your employee?

The answer is to allow and trust employees to develop a name for themselves that is irrespective of their organizational ranking or where they sit in the org chart. And it actually is not a question about monetary incentives. They do it because recognition from their peers is, I think, an extremely strong motivating factor, and something that is broadly unused in modern management.

The role of the new collaborative and open and information rich manager/boss is to then work on those collaboration platforms, as opposed to being the one making the decisions. Itâ??s more like the producer of the show, rather than being the lead. By creating an atmosphere of collaboration, the people who are consistently right get a huge following, and their work product is talked about by people theyâ??ve never met.

Example:Â If we continue with todayâ??s management style, staff may find the job is just wasnâ??t as much fun anymore. They felt that they could do more. The result will chase away somebody extremely valuable. If you start micromanaging people, then the very best ones leave.

Otherwise, if the very best people leave, then the people youâ??ve got left actually require more micromanagement. Eventually, they get chased away, and then youâ??ve got to invest in a whole apparatus of micromanagement. Pretty soon, youâ??re running a police state. So micromanagement doesnâ??t scale because it spirals down, and you end up with below-average employees in terms of motivation and ability.

Instead, the trick is to get truly world-class people working directly for you so you donâ??t have to spend a lot of time managing them. Having display this HR Policies, Organizational structure reforming, and Work place transformation may need change to change to adapt to the above relationship.

Chapter 96 : Your Office could conduct work more openly and publish data online including ways to ir

The Agency should use their website including blogs to publish a summary of common customer comments and explain the actions they are taking in response to the feedback. Effort should be made to respond according to responders suggestion or comments. Doing so will create better transparency and accountability.

The Agency should use social media, not just to create transparency, but also to help our Offices, various projects and Staff accomplish their core tasks and meet their information needs. For example, the agency could post instructional videos on Blogs to explain how to apply for stimulus grants. To do this, the government must ensure that Staff as well as Citizen who need access to social media tools have them, and that these new ways of delivering content (i.e. stimulus grants) are available to all, including people with disabilities and multi-lingual needs.

The Agency has developed government-wide guidelines for disseminating content in universally accessible formats (data formats, news feeds, mobile, video, podcasts, etc.), and on non-government sites . To remain relevant, government needs to take our content to where people already are on the Web with communication plan to market and promote the available tools, guidance, and information, rather than just expecting people will come to government websites. Having guidelines will ensure that weâ??re part of the larger online community acting together

Chapter 97 : Government 2.0 16 Dares 2010-01-31 21:42:56

Happy New Year, I came up and want to share with you 16 dares for engaging to Gov 2.0 with Web 2.0 Technologies

- Social media is not just about the technology, but what the technology enables others to collaborate.

- Social media is driven by people, not by your Office.Â Stop trying to deploy by one team or office, and instead think of a way to bring together people from across your organization to engage collaboration.Â Develop Â and nourish your community of practice.

- The risks of social media are greatly outweighed by the risks of NOT engaged in social media.

- Your Government agency/organization/team/branch/division/office may not be unique.Â You do not work in a place that just canâ??t just use social media because your work is not right for public consumption.Â You do not work in an environment where social media will never work. If you work with people then Gov 2.0 can take root. Your challenges, while unique to you, are not unique to the government. Learn from others and adapt and adopt and tried.

- You will work with skeptics or 'can't be done here' and other people who want to see social media fail because the transparency and authenticity will threaten their perceived control and expose their weaknesses. But, be confident.Â Know what you know and donâ??t back down.Â You will be challenged by skeptics and others who do not care and/or understand social media.Â Do not let them discourage you.

- Younger employees are not necessarily any more knowledgeable about social media than older employees.Â Stop assuming that they are. They are more exposed to Web 2.0, not necessarily a practioner.

- Be humble.Â You donâ??t know everything so stop trying to pretend that you do.Â Itâ??s ok to be wrong. Mistakes can and will be made (a lot).Â Stop trying to create safeguards to eliminate the possibility of mistakes and instead concentrate on how to deal with them when they are made.

- You will work with people who want to get involved with social media for all the wrong reasons.Â They will see it as an opportunity to advance their own their careers, to make more money, or to show off.Â These people will be more dangerous to your efforts than the biggest skeptic.

- Before going out and hiring any social media â??consultants,â?• assume that there is already someone within your organization who is actively using social media and who is very passionate about it.Â Find them, use them, engage them.Â These are the people who will make or break your foray into social media.

- Information security is a very real and valid concern.Â Necessary evil, Â Learn to use it with you advantage and live with it.Â It will protect you.

- Policies are not written in stone.Â With justification, passion, and knowledge, policies and rules can and should be changed or waived.Â Sometimes itâ??s as easy as asking, but other times will require a knockdown, drag-out fight.Â Both are important.

- There are true social media champions throughout the government.Â Find them.Â Talk to them.Â Learn from them. Â Work with and corroborate with them not top them.Â

- Todayâ??s employees will probably spend five minutes during the workday talking to their friends on Facebook or watching the latest YouTube video and be intouch.Â Todayâ??s employees will also probably spend an hour at 10:00 at night answering emails or responding to a work-related blog post. It all balance out, because we care about our work and a professional. Â Trust and assume that your employees are good people who want to do the right thing and who take pride in their work.

- Transparency, participatory, collaborative â?? these terms do not refer only to the end state; they refer to the process used to get there as well.Â Itâ??s ok to have debates, arguments, and disagreements about the best way to go about achieving â??Government 2.0.â?•Â Diverse perspectives, opinions, and beliefs strengthen, and Â should be embraced and talked about openly and build concensus and starve skeptics.

- Itâ??s not enough to just allow negative feedback on your blog or website, you also have to do, respond or something about it.Â Donâ??t just listen to what the public has to say, respondÂ because you are concern, If not donâ??t start.

- Use Web 2.0 technologies as tools for communication, sharing, participation, transparency, and collaboration. Todayâ??s technologies that is driving social media will change, but the principles of will not.Â You can either jump on the Government 2.0 Â or get hit by it.Â Which one will you be?

Chapter 98 : Ten Points on Gov2.0 2009-10-16 20:43:43

Government 2.0, as defined onÂ Wikipedia Â is neologism for attempts to apply the social networking and integration advantages of Web 2.0 to the practice of government. William (Bill) Eggers claims to have coined the term in his 2005 book, Government 2.0: Using Technology to Improve Education, Cut Red Tape, Reduce Gridlock, and Enhance Democracy.[1] Government 2.0 is an attempt to provide more effective processes for government service delivery to individuals and businesses. Integration of tools such as wikis, development of government-specific social networking sites and the use of blogs, RSS feeds and Google Maps are all helping governments provide information to people in a manner that is more immediately useful to the people concerned.[2]

A number of efforts have been made to expose data gathered by government sources in ways that make it available for mashups.

Web 2.0 technologies provide opportunities for various Agencies to share, disseminate and collect information from both internal and external customers in new and exciting ways. Technologies such as wikis, blogs and social networking sites all provide unique ways of collaborating electronically. Web 2.0 technologies are especially useful when additional two-way communication or real-time collaboration would be beneficial to the task.
Â
Like any information technology initiative, the business uses, goals and expected benefits should be first established to help guide the selection and use of specific technologies. The inclusion of applicable information technology policies early in requirements gathering process is critical. Also of consideration are the Federal employee requirements to provide content, moderate, and maintain these constructs and the ability of the individual Federal organizations to digest the volume of input received.

1.0 Defines Web 2.0 as,

â??â?¦a term describing changing trends in the use of World Wide Web technology and web design that aims to enhance creativity, information sharing, and, most notably, collaboration among users.â?•

Wikipedia goes on to say â??These concepts have led to the development and evolution of web-based communities and hosted services, including social-networking sites, video sharing sites, wikis, blogs, and folksonomies.

2.0 What does this mean?

Web 2.0 makes the Internet more interactive. Web sites are no longer merely one-way portals and business tranactions but instead can provide an interactive environment for sharing, dialogue and collaboration among a diverse group of people.

3.0 What do I need to do?

Look for opportunities to utilize new technologies and capabilities in a smart and professional manner. Remember that Web 2.0 technologies are subject to same principles and guidance as other internet and communications technologies that an agency may already use to share, disseminate or collect information. An example is that since the site is at an government site the submitted contents by government employee must comply with Accessibility Requirements as dictated in

Section 508.

Federal employees must remember that any time they make a statement on public Web2.0 media with any identifying information attached, they are in effect making a public statement under the guise of their position. Even if the employee does not intend to make a binding or public statement, by including identifying information in the post (such as name, position, or even agency affiliation) the communication may be interpreted in this manner by other end users. Federal employees must ensure that they do not communicate anything that they would not state publicly in a non-virtual context.

4.0 What does this mean?

Care needs to be given to all communications made in an increasingly connected world.

5.0 What do I need to do?

Remember that you are a Federal employee no matter what identifying information you provide. Do not take any actions or make any statements that you would not do openly at work.

6.0 Management of Information Exchange

One of the major enticements of using Web 2.0 technology is the ability to exchange informal ideas among multiple parties with transparency. Agencies should decide up front their policies for collecting and processing incoming information. Some Web 2.0 collaborative tools (blogs, for example) may allow agencies to moderate contributions before they are posted to the public. Agencies should clearly state how their tools are moderated and what users are allowed, and not allowed, to contribute. Other forms of communications (such as virtual worlds) may not provide any viable method of pre-screening contributions. Agencies should be aware of their inability to moderate certain forms of Web 2.0 communications and clearly post disclaimers if necessary.

7.0 Information Quality

The Public places a high degree of trust in .gov content and considers it an authoritative source. Under the Information Quality Act and associated guidelines, agencies are required to maximize the quality, objectivity, utility, and integrity of information and services provided to the public. With regard to Web 2.0 information dissemination products, Agencies must reasonably ensure suitable information and service quality consistent with the level of importance of the information. Reasonable steps include: 1) clearly identifying the limitations inherent in the information dissemination product (e.g., possibility of errors, degree of reliability, and validity) so users are fully aware of the quality and integrity of the information or service, 2) taking reasonable steps to remove the limitations inherent in the information, and 3) reconsidering delivery of the information or services. In short, agency management must ensure that the agency position is reflected in all communications rather than one personâ??s opinion. Resource: Information Quality Act, Pub. L. No. 106-554

6.0 Information Collection

Agencies are required, when practicable, to use electronic forms and filing to conduct official business with the public, and Web 2.0 technologies can be used in many cases to meet this need. Federal public websites must ensure that information collected from the public minimizes burden and maximizes public utility. The Paperwork Reduction Act (PRA) covers the collection of data from the public. The PRA requires OMB approval of all surveys given to ten (10) or more participants. This includes any sort of survey where identical questions are given to ten or more

participants, regardless of the format. The exception to the survey rule is an anonymous submission form where users can provide open ended comments or suggestions without any sort of Government guidance on the content.

Resources: Government Paperwork Elimination Act and Paperwork Reduction Act

7.0 Intellectual Property

The use and management of Web 2.0 technologies raises several questions about the legal concepts of copyright, fair use, and intellectual property ownership. Agencies must be diligent to ensure that they consider existing intellectual property and copyright laws when implementing Web 2.0 technologies. While the Federal government typically provides public data which is not considered copyrightable intellectual property, Web 2.0 technologies that allow public contribution of content may potentially create challenges regarding the protection of intellectual property contributed by visitors. The ease of copying and propagating data from many sources on the internet makes it very easy to unintentionally breach copyright laws. Most commercial media sharing websites warn of the illegal use of copyrighted materials and trademarks. This strategy may or may not prove sufficient to protect the interests of government agencies, depending on specific circumstances. Agencies must establish policies and post clear disclaimers detailing the copyrights that non-government contributors to their sites may retain. Government content on any site is generally public domain and therefore can not become the intellectual property of an individual or be protected by a site provider. Care must be taken to not create the appearance of a copyright on a government created work, unless specifically permitted by statute. Resources: Copyright.gov, U.S. Trademark Law

8.0 Agency Websites Linking to External Services

Many Web 2.0 services are hosted outside government websites. These services include popular media sharing services such as YouTube. If users are connected to these sites from Government websites using hyperlinks, agencies are required to establish and enforce explicit agency-wide linking policies that set out management controls for linking beyond the agency to outside services and websites. Typically the user is notified they are leaving the Government website. Resource: OMB Memo M-05-04

9.0 Usability of Data

Many Web 2.0 technologies allow users to take data from one website and combine it with data from another, commonly referred to as â??Mashups.â?• Agency public websites are required, to the extent practicable and necessary to achieve intended purposes, to provide all data in an open, industry standard format that permits users to aggregate, disaggregate, or otherwise manipulate and analyze the data to meet their needs. Agencies need to ensure that these open industry standard formats are followed to maximize the utility of their data. Resource: OMB Memo M-05-04

10.0 Accessibility to Persons Who Have Disabilities

Section 508 of the Rehabilitation Act of 1973, (as amended), requires that electronic and information technologies purchased, maintained, or used by the Federal Government meet certain accessibility standards. These standards are designed to make online information and services fully available to the 54 million Americans who have disabilities, many of whom cannot possibly access information that does not comply with the Section 508 standards. Agencies are already required by the Federal Acquisition Regulations to modify acquisition planning procedures to ensure that the 508 Standards are properly considered, and to include the standards in requirements documents.

OMB reminds agencies to disseminate information to the public on a timely and equitable basis, specifically mentioning meeting the Section 508 requirements in OMB Memorandum M-06-02. Agencies employing non-Federal Web 2.0 services are required to ensure that persons with disabilities have either accessible access to those services or equivalent access to the information disseminated on those services. Resources: Section 508 of the Rehabilitation Act ,OMB Memo M-06-02

Chapter 99 : Perceived and Real Barriers and Potential Solutions 2009-10-16 19:25:36

Social Media and the Federal Government:

Perceived and Real Barriers and Potential Solutions
December 23, 2008

Produced by the following members of the Federal Web Managers Council: Bev Godwin, GSA/USA.gov (Executive sponsor), Sheila Campbell, GSA/USA.gov (Co-chair), Rachel Flagg, Dept. of Housing and Urban Development (Co-chair), Jeffrey Levy, EPA (Co-chair, Social media sub-council), Joyce Bounds, Dept. of Veterans Affairs (Co-chair, Social media sub-council)

A. The context for using social media within the federal government

Some agencies are already using social media tools with great success. Theyâ??ve shown how these tools can transform how we engage the public, include people in the governing process, and accomplish our agency missions. (See WebContent.gov for examples of agencies successfully using social media:
http://www.usa.gov/webcontent/technology/other_tech.shtml

).

But many agencies are not using these tools, either because of perceived or real lack of resources, cultural resistance, or legal or other
barriers. There are varying interpretations around what is allowed across the federal government, and some agencies do not yet understand how these tools will help them achieve their missions.

The purpose of these recommendations is to address the perceived and real barriers to using social media, and to propose solutions that will result in greater consistency and a clearer understanding of what is expected and permitted across federal agencies.

We hope this paper will facilitate dialogue on these important issues, both within and outside the government. As this topic evolves, weâ??ll use Webcontent.gov and various social media tools to continue the conversation. We also invite you to read the Federal Web Managers Council white paper, "Putting Citizens First: Transforming Online Government," which offers recommendations for transforming online government beyond social media
(*http://www.usa.gov/webcontent/documents/Federal_Web_Managers_WhitePaper.pdf*

).
B. Barriers and potential solutions

1. Cultural issues and lack of a strategy for using these new tools
Issue: Many agencies view the use of social media as a technology issue, instead of a communications tool, and management decisions are often based solely on technology considerations. In many cases, the focus is more on what canâ??t be done rather than what can be done. The default approach should be openness and transparency. For this reason, agencies need to be prepared that the decision to use social media will have cultural implications throughout government. Some agencies have leadership and legal support and have shown that the benefits of using social media outweigh the risks; but many have not. The result: social media is not consistently applied across

Proposed Solution:

The new Administration should communicate a government-wide strategy for using social media tools to create a more effective and transparent government. The new Administrationâ??s Chief Technology Officer (CTO) should require each agency to, within three months, develop their own social media/Web 2.0 communications strategy that describes how it will use their agency website and the larger Web to accomplish its mission, reach new audiences, and engage the public. The strategy should include resources needed to accomplish these goals.

2. Employee access to online tools

Issue: Many agencies block their employees from using sites like YouTube, Facebook, and Wikipedia.

They make one of three arguments, all of which can be addressed through effective policies and management controls:

1. Security: IT security specialists raise concerns that these high traffic sites pose a greater risk for malware and spyware. However, agencies can implement security measures to mitigate these risks, just as they do for other high traffic sites such as Google and Yahoo. Certain agencies may still need to restrict access for specific groups, but this should be the exception, not the rule.

2. Employees will waste time: this is the same argument that has been used to say employees shouldnâ??t have access to phones, email, etc. Itâ??s not unique to Web 2.0. It should be addressed by agency managers as a management issue, not a technology problem.

3. Bandwidth: this is a legitimate concern for sites such as YouTube that consume considerable bandwidth. However, agencies need to budget for this, as they do for other infrastructure needs. If opening all computers to all sites is an issue, agencies should at least provide access to agency staff that need to understand and use these tools to communicate with the public.

Proposed solution: The new Administration should require agencies to provide access to social media sites unless the agency head justifies blocking certain employees or certain sites.

3. Terms of service

Issue: Most online sites require account owners to agree to terms of service that federal agencies can't agree to, in particular:

1. Indemnification and defense: if a federal employee, on behalf of their agency, creates an account on a social media site, they must agree not to sue the site, nor allow the site to be included in suits against the agency. Many sites also require the account owner to pay the site's legal costs arising from such suits. Under the Anti-deficiency Act, federal agencies can't commit to either provision.

2. Applicable law and court jurisdiction: most terms of service also assert that a certain state's laws (usually California) apply to the terms of use and that the stateâ??s courts will adjudicate disputes. This is problematic since federal agencies follow federal law and go to trial in federal court.

Many companies have been willing to negotiate on these issues, but they don't want to negotiate separate agreements with dozens of different agencies. Similarly, itâ??s not efficient for agencies to work out agreements with an unending list of potential companies.

Proposed solution: The new Administration (through the National CTO, GSA, OMB, or some other central organization) should:

a) Establish a single terms of service that covers all social media sites, which excludes the federal government from the provisions described above. (If this isnâ??t possible, at a minimum, create a standard federal terms of service with each site and establish a process for adding new agreements

as new sites are identified.)
b) Alert federal agencies that the benefits of using these sites outweigh the risks and that they should use social media sites pending agreements on terms of service.
4. Advertising
Issue: Many vendor sites place ads on all their pages; this is how they earn money from free accounts.
For some agencies, this raises ethical concerns when government content appears near inappropriate advertisements (pornography, hate, political, etc), because it can give the appearance that the government is endorsing the content. What constitutes â??advertisingâ?• is interpreted differently across government.

Proposed solution: The new Administration should:
1. Issue a memo stating that government agencies should accept this kind of contextual advertising as a byproduct of using social media sites, that advertising online is no different than advertising in a magazine, newspaper, radio, or TV, where you canâ??t control exactly howÂ your content will appear in context. However, if this is not possible:
2. Set criteria for all agencies for when such ads are acceptable. For example, ads could be acceptable when:
ï? They are ubiquitous, appearing on all similar pages on a site, regardless of the account owner
ï? They do not include pornography or violence
ï? There isn't confusing language that implies endorsement by the account owner (e.g., "promoted" or "sponsored" material)

Procurement
Issue: Government procurement rules didn't anticipate the flood of companies offering free tools to anyone who wants to use them. Attorneys at different agencies interpret the rules differently, leading to confusion and hesitation. Agencies that want to use these tools face three issues:
1. Gratuitous services and gift authority: there are rules governing when agencies are allowed to accept free services or gifts. Some agencies have gift authority and others donâ??t. Potential concerns include giving the offering company inappropriate inside information that lets it tailor a later commercial product or possibly coming back later and billing the government.
2. Choosing winners without competition: the government shouldn't arbitrarily decide which companies will be given the cachet of providing our content, which can provide value to their sites. For example, federal agencies should have criteria to determine which video sharing sites they will publish their videos to (YouTube, Yahoo Video, AOL Video, etc).
3. Contract authority: Ordinarily, only specific employees are given authority to bind an agency contractually. This is very cumbersome when trying to establish accounts on social media sites.

Proposed solution: The new Administration should work with procurement and ethics attorneys to ensure that:
1. Agencies can use free Web products and services.
2. Agencies do not need to use all products and services offered, as long as they have criteria for deciding which ones they use.
3. Employees with a clear business need can create accounts to use free services, as long as they have managerial approval.

6. Privacy
Issue: There is no guarantee that social media sites will protect people's privacy to the same degree as federal agencies.
Proposed solution: The new Administration should direct agencies to use a standard disclaimer to display on social media sites where they publish content (i.e. EPAâ??s Facebook page or Twitter page).
The disclaimer would alert the public that they are no longer on a federal site and that the private sector site's own privacy policy applies, with a link to that policy.
7. Persistent Cookies

Issue: Agencies are banned from using persistent cookies without approval from their agency head, which effectively means the federal government isn't using them. This greatly limits our ability to serve customers' needs because our sites can't remember preferences or settings. It also means we canâ??t take advantage of sophisticated web services and analytic tools that rely on persistent cookies.

Proposed solution: The National CTO or OMB should immediately rescind the previous guidanceprohibiting persistent cookies and replace it with guidance that allows agencies to use persistent cookies to better serve customers' needs. The new guidance should state that it's acceptable for agencies to use social media sites that rely on persistent cookies. However, the government should retain the ban on tracking cookies, since they specifically track where visitors go between sites.

8. Surveys

Issue: The Paperwork Reduction Act, subsequent OMB regulations, and OMB draft guidance require that agencies complete a lengthy process to obtain an OMB control number to survey and request information from the public. This requirement is interpreted by most agencies to include voluntary online surveys, polls, and other applications that are intended to improve customer service. The Act predated the Internet and doesn't anticipate the use of social media and other customer service tools.

Proposed solution: The National CTO or OMB should issue immediate guidance that outlines exceptions to the PRA, such as using online surveys to solicit public opinion about federal websites, using social media to have online discussion forums with the public, etc.

9. Access for people with disabilities

Issue: Under section 508 of the Rehabilitation Act of 1973, all information provided to the public via agency websites must be equally accessible to people with and without disabilities. Many social media tools are automatically accessible because they are primarily text (e.g., blogs). However, some multimedia sites do not currently provide the opportunity to include transcripts or captioning, and many agencies lack sufficient resources to provide these services on their own.

9 Proposed solutions:

1. The National CTO should issue guidance requiring agencies to post their materials in accessible formats on their own websites, and that non-governmental sites may not be the sole location where content is posted. This will ensure that people with disabilities always have an accessible version of the content, and that the official version of content is located on a government website.
2. The National CTO and GSA should collaborate on developing a government-wide procurement vehicle to purchase tools that assist with 508 compliance, such as captioning software to make videos and webcasts available to people with disabilities.
3. The National CTO should work with major companies to make Web software, including social media software, fully accessible to people with disabilities.

10. Administrative requirements during rulemaking

Issue: The Administrative Procedure Act (APA) of 1946 sets rules for how agencies can communicate with the public during rulemaking, accept public comment on proposed regulations, etc. The Act didn't anticipate the collaborative tools now available, leading to hesitation and confusion as to how to incorporate them during the rulemaking process.

Proposed solution: The National CTO or OMB should issue guidance to help agencies use collaborative social media tools to enhance the rulemaking process, while still complying with the APA.

We welcome your questions and comments. Please contact the Federal Web Managers Council co-chairs, Sheila Campbell (*sheila.campbell@gsa.gov*

) and Rachel Flagg (*rachel.flagg@hud.gov*

).

Chapter 100 : One Wiki @ EPA 2009-10-16 19:10:54

Environmental Protection Agency's Environmental WikiÂ - One wiki for EPA

Purpose

Environmental Wiki would support the Agencyâ??s knowledge management strategy and enterprise architecture by providing a tool for knowledge acquisition and access for all EPA staff in an easy-to-operate and convenient online encyclopedia of agency and environmental knowledge.

Two Concepts of Proposal
1. Environmental Wiki would be an enterprise wiki designed for EPA employees to collaborate on this one knowledge base and shared the wealth of information among Agency employees. Parts of this wiki could eventually be moved to a public space for national information consumption.
2. EPA is harnessing Web 2.0 technologies tools to adapt to individual office and regional business requirements to meet open-collaboration needs with government transparency, audience engagement, response, and information sharing and access. These mission-oriented applications/technologies interact, share, respond, and collaborate among two or more parties. One of these ever-increasing tools is the wiki, with more than 75 deployed wiki applications within EPA and a growth rate of 8% per month. This growth also increases our overall infrastructure hosting cost, support needs, and presents a management and standardization dilemma.

Impact

How can we apply a wiki tool to our daily EPA business practices effectively, keep it manageable and affordable, and use it with our infrastructure and architecture? The solution is to establish an Agency-wide wiki, called Environmental Wiki. This â?•One Wiki Conceptâ?• has many benefits:

Benefits and Improvement

ï?? Lower cost in infrastructure, wiki deployment, and wiki application management,
ï?? Unified management on implementation, communication, and wiki implementation,
ï?? Collaboration on, communicate and discover agency information among offices
ï?? Establishment of EPA University for new employees to learn about EPA businesses,
ï?? Agency knowledge acquisition from staff knowledge and expertise,
ï?? Standard approach of knowledge search, access, and presentation
ï?? Integration with other enterprise applications
ï?? Cost savings from application improvements and integration with added values

Applying Web 2.0 technology, such as a wiki, may affect the Agency and may change its business methods, its procedures, and even its culture and practices. A wiki tends to flatten the vertical workflow/process hierarchy, which may prove to be challenging given that traditional government organizations are hierarchal. However, the final benefits outweigh the cultural impact. We need a versatile, unified, and easy-to-use framework, extending to social networking practices within EPA. When a portion of the Environmental Wiki becomes publicly accessible, the public will be better served and informed and will have a tool to respond or interact with EPA, which will

promote trust and transparency to its audiences and stakeholders.

Deployment

The Environmental Wiki would become a collaborative Web space, such as Community of Practice forum, for the various program offices, partnered governmental entities, and trusted environmental organizations to access and contribute their knowledge on particular subject matter, collaborate, and integrate their staff expertise works onto a single â??blackboard,â?• with a series of dimensional sub-blackboards of wikis to accommodate the various different programmatic needs, congressional mandates, and judicial decrees.

As a starting point, we may use EPA OEIâ??s taxonomy and glossary as seedlings; ask each of the program offices to include their programmatic regulations, knowledge, subject matter, and deliverables; and work with other government agencies to learn and deploy the Environmental Wiki. It is important to have a standard governance body to establish, modify, and maintain policies and guidelines for the Environmental Wiki.

Hopefully, Environmental Wiki will become a â??living knowledge baseâ?• for EPA staff to access and will become a future reference for all federal government agencies to use on environmental subjects. Environmental Wiki may be a gateway for environmental information access for all and may reap the benefits of collaborative works/effort, components, shared experience, a social network for contribution, and knowledge management. Eventually, Environmental Wiki may become the source and clearing house of environmental information similar to Wikipedia.

Steps

1. Partner with various program offices, partnered governmental entities, and trusted environmental organizations.
2. Establish an Environmental Wiki project team with initial funding.
3. Establish a governance body for Environmental Wiki to establish policy and guidelines.
4. Prepare plans and strategy for Environmental Wiki development.
5. Develop Wiki Pilot with supporting blog, Web sites, and portlets.
6. Encourage all Agency offices to build and collaborate on OEIâ??s taxonomy and glossaries of terms to seed the Environmental Wiki.