THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

18 August 2014

Purpose
Educate recipients of cyber events to aid in protecting electronically stored DoD, corporate proprietary, and/or Personally Identifiable Information from theft, compromise, espionage

Source
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
To receive this newsletter please send an email to scott.daughtry@dtra.mil

Disclaimer
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

NMCIWG Members
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, and Sandia National Labs

Distribution
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings. Credit is given to the NMCIWG for the compilation of this open source data

August 15, Securityweek – (International) **New Bugat malware uses HTML injections taken from Gameover Zeus.** A researcher from IBM Security reported August 14 that a new variant of the Bugat financial malware (also known as Cridex or Geodo) was spotted infecting computers in the U.K. and the Middle East region. The new variant uses HTML injections and scripts and an attack structure similar to that used by the Gameover Zeus malware and attempts to redirect victims to fake financial institution Web sites in order to steal login information. Source: http://www.securityweek.com/new-bugat-malware-uses-html-injections-taken-gameover-zeus

August 14, Softpedia – (International) **New Gameover Zeus botnet forming, the US sees most infections.** Arbor Networks researchers observed two new variants of the Gameover Zeus financial malware using 8,494 IP addresses to attempt to connect to command and control (C&C) servers in July in order to build a new botnet after a law enforcement and industry takedown of the original botnet. The new variants no longer use the peer-to-peer (P2P) command and control architecture of the original and instead utilize a domain generation algorithm (DGA) to contact C&C servers. Source: http://news.softpedia.com/news/New-Gameover-Zeus-Botnet-Forming-the-US-Sees-Most-Infections-455112.shtml

August 14, SC Magazine – (National) **Vitamin seller website attacked, payment cards and other info compromised.** Vitamin seller TheNaturalOnline.com reported August 12 that an undisclosed number of their customers may have had their payment and personal information compromised during a breach of the company's systems that was identified July 15. The information included names, addresses, email addresses, account passwords, phone numbers, and payment card numbers, expiration dates, and CVV codes. Source: http://www.scmagazine.com/vitamin-seller-website-attacked-payment-cards-and-other-info-compromised/article/366314/

August 15, The Register – (International) **Don't think you're SAFE from Windows zombies just 'cos you have an iPhone - research.** Researchers at the Georgia Institute of Technology reported finding that Apple iOS devices can be compromised with iOS malware after being connected to a Windows computer by exploiting weaknesses in the iTunes syncing process, allowing attackers to steal data, install malicious apps, and replace existing apps. The researchers plan to demonstrate their findings August 20 at the Usenix Security Symposium. Source: http://www.theregister.co.uk/2014/08/15/infecting_ipads_new_how_to/

August 15, SC Magazine – (International) **50% of corporate passwords crackable within a few minutes.** Trustwave released the results of research that analyzed 620,000 passwords compiled over 2 years and found that around 50 percent of U.S. corporate passwords could be cracked using a brute force method within a few minutes, while 92 percent could be cracked within 31 days. The research found that a longer password containing only letters took much longer to brute force compared to a shorter password that also includes numbers and special characters. Source: http://www.scmagazineuk.com/50-of-corporate-passwords-crackable-within-a-few-minutes/article/366470/

New Phishing and Malware Campaigns Use Ebola Virus Epidemic as Bait

SoftPedia, 18 Aug 2014: Security researchers have identified multiple malicious campaigns leveraging mostly fake news or reports about the Ebola virus, in order to deliver malware or steer users to phishing websites. A phishing operation caught by researchers Symantec impersonates a communication from CNN containing breaking news about the virus, luring the potential victim to click on a link for access to additional details that had not been disclosed. The experts have analyzed the email delivering the malicious link and determined that the crooks are after the log-in details for major webmail providers. “If the user clicks on the links in the email they are sent to a Web page, asked to select an email provider, and asked to input their login credentials. If the user performs this action, their email login credentials will be sent directly to phishers. The victim is redirected to the real CNN home page,” they write in a blog post. Another three campaigns spotted by the researchers to rely on news about the Ebola virus as bait would deliver malware. In one case, an attachment with a fake report about the virus adds Zeus Trojan, also known as Zbot, to the computer. Fortunately, all reputable antivirus products can now catch it before damage is done. However, a campaign more complex in nature is also currently claiming victims; posing as an email from a major telecommunications service provider, there is an attachment purporting to be a PDF presentation of the virus. Once executed, a newly discovered Trojan is released on the system, identified by Symantec as Blueso. It appears that Blueso is not the final payload. “The malware is also crafted to inject W32.Spyrat into the victim’s Web browser,” say the researchers. Its functionality ranges from logging key strokes, recording from the built-in webcam, grabbing screenshots or opening web pages to deleting data from the hard disk and enumerating files and folders. It can also communicate with a command and control server to send and receive data. The experts note that the malware collects information about the applications installed on the computer as well as the underlying operating systems, and it can also remove itself from the machine. The third malware campaign discovered by Symantec uses Zmapp as bait, an experimental drug for Ebola, claiming that it can kill the virus. The malware delivered is called Breut and it has functions such as capturing webcam activity, modifying hosts files, keylogging, password stealing and downloading and executing arbitrary programs and commands. Unsolicited email most often contains some sort of threat, which can lead to compromising the computer and stealing sensitive details. Users are advised not to open links or attachments provided in such messages. To read more click HERE

Over 10,000 Fall Victim to Intensified Cyber Attacks Targeting Syria

SoftPedia, 18 Aug 2014: An intensification of cyber attacks in Syria has been observed as security researchers find remote access Trojans (RAT) being delivered through activist websites and social networking pages relating to the political conflict in the area, to individuals seeking news or tools for ensuring private communication. The most prevalent RATs malware operators rely on are ShadowTech, Xtreme, NjRAT, Bitcomet, Dark Comet and Blackshades, some of the malicious files being downloaded more than 2,000 times, according to a new report from Kaspersky researchers. They say that the attacks did not increase only in number but also in complexity, leveraging powerful social engineering techniques that created more than 10,000 victims. Lack of technology awareness, coupled with trust in social networking and other communication channels, is among the main factors leading to effective infection vectors. Kaspersky tracked the methods employed by the threat actors and discovered that the malicious files allowing complete compromise of the computer were received by unsuspecting users through download links offered through Skype, Facebook posts, and YouTube videos. Victims are delivered links to fake programs claiming to provide encrypted communication (SSH VPN), antivirus solutions (Ammazon Internet Security) or firewalls, and fake Whatsapp and Viber applications for PC. In plenty of cases, users are lured with documents claiming to disclose wanted activists, videos presenting victims of recent bombings or images of leaked papers from Syrian officials warning military units of chemical attacks. Once accessed, these files deliver the malware on the computer giving the threat actor unrestricted access to the system. Keylogging, recording of audio and video, executing arbitrary programs, downloading files, exfiltrating data, remote shell and executing denial-of-service attacks are among the functions provided by the RATs. Although cyber attacks in Syria are nothing new, the novelty in this case is that the malicious campaigns have become more organized as malware operators started to create "highly stealth and graphically-enticing applications." "Among the most popular RAT found in the samples subset is Dark Comet, a free remote administration tool that provides a comprehensive command set for the attackers to use in their malicious purposes," the researchers write in the report. In their investigation, Kaspersky managed to identify a group with a highly organized structure (dubbed the Resistant Syrian Electronic Army) broken into multiple teams in charge of specific tasks: Team Hacker and Assad Penetrations Unit (Team 1), Anonymous Syria Al Assad Unit (Team 2) and Management of Electronic Monitoring and Central Tracking Unit (Team 3). Kaspersky predicts that, because of the rapid evolution of the cyber attacks against Syrian citizens (over 100 samples have been collected), the attackers may soon proceed to writing their own malware instead of relying on known threats. "With enough funding and motivation they might also be able to get access to zero day vulnerabilities, which will make their attacks more effective and allow them to target more sensitive or high profile victims," they conclude. To read more click HERE

Microsoft Tells Users to Uninstall Windows August Updates

SoftPedia, 18 Aug 2014: This weekend, Microsoft removed the manual download links for two different patches rolled out on Update Tuesday, and although no reason was provided at first, it was very clear that the decision was made after hearing about problems and issues experienced by users after installing the updates. In an updated advisory on Microsoft Support, the company says that links for a total of four different updates released last week have been removed until the reported issues are being investigated. Here's the list of updates that are no longer available for download due to bugs:

- 2982791 MS14-045: Description of the security update for kernel-mode drivers: August 12, 2014
- 2970228 Update to support the new currency symbol for the Russian ruble in Windows
- 2975719 August 2014 update rollup for Windows RT 8.1, Windows 8.1, Windows Server 2012 R2
- 2975331 August 2014 update rollup for Windows RT, Windows 8, and Windows Server 2012

Microsoft says that all those who have already installed the updates and experienced issues should go over to Control Panel, open "Programs and Features" and click on "View installed updates." Then, you should remove "any of the following updates that are currently installed": KB2982791, KB2970228, KB2975719, and KB2975331. In a statement sent this morning, the company also said that it was indeed investigating reports pointing to botched updates, but no other specifics were provided. Windows 8.1 August Update was launched last week to introduce a series of new options in Microsoft's modern operating system, but everything quickly became a fiasco due to these bugs. Here are the three main improvements that are part of Windows 8.1 August Update:

- Precision touchpad improvements – three new end-user settings have been added: Leave touch pad on when a mouse is connected; allow right-clicks on the touchpad; double-tap and drag.
- Miracast Receive – exposes a set of Wi-Fi direct APIs for Independent Hardware Vendor (IHV) drivers or OEM drivers to develop Windows 32-bit applications that run on all supported x86-based or x64-based versions of Windows 8.1, enabling the computer as a Miracast receiver.
- Minimizing login prompts for SharePoint Online – reduces the number of prompts with federated use in accessing SharePoint Online sites. If you select the "Keep me signed in" check box when you log on for the first time, you will not see prompts for successive access to that SharePoint Online site.

A complete list of Windows 8.1 August Update improvements (link) is also available if you'd like to find out all features that are part of this release.

To read more click HERE

2.1 Million Stolen Credit Card Numbers Found on Seleznev's Laptop, Bail Denied

SoftPedia, 18 Aug 2014: During a bail hearing on Friday for Roman Valerevich Seleznev, prosecutors revealed that a laptop computer containing 2.1 million stolen credit card numbers was seized from the defendant. Roman Seleznev is the son of a State Duma member representing the Liberal Democratic Party, Valery Seleznev, and is accused of breaching point-of-sale system of US retailers and trading financial information on forums under his control. At the moment, there is no information about the source of the credit card numbers on his laptop, or if they were to be sold to cybercriminals on underground forums. According to Q13 FOX, the lawyers of the defendant asked for Seleznev to be placed under house arrest in a furnished apartment in Seattle, on a $1 million (€747,000) bond secured by $100,000 / €75,000 in cash. However, the US Magistrate James P. Donohue denied the bail on the grounds that Seleznev presents a serious flight risk, as he has no ties to Western Washington, where the court holding the trial is located. More importantly, the hacker is known to have travelled internationally on a frequent basis and has the necessary knowledge for forging false identification documents that would permit him to cross the border. "Today was another important step in ensuring the charges against this defendant are tried in this community," U.S. Attorney Jenny A. Durkan was quoted by the publication. "The defendant is entitled to every protection offered by our system, but will be afforded no special privileges. Our investigation into the scope of defendant's actions is ongoing," she added. Roman Seleznev was charged by the Western District of Washington in absentia in March 2011 with a total of 29 counts that included bank fraud, hacking into protected computers, possession on unauthorized devices and trafficking unauthorized devices. If found guilty on all counts, the maximum penalty he faces is of at least 65 years of jail time and payment of a fine totaling $2.75 million / €2 million. The hacker was arrested on July 5 by the US Secret Service at the Male International Airport in Maldives and taken immediately to a US facility in Guam Island. This operation is considered by the Russian government as a kidnapping act and authorities in Maldives should not have allowed "another country's special service to kidnap a Russian citizen and take him out of the country." The date of Seleznev's trial has been set for October 6, 2014, and the defendant will plead "not guilty" to the charges. To read more click HERE

BadUSB Is Not as Bad as It Looks, for Now

SoftPedia, 18 Aug 2014: The BadUSB talk at the Black Hat security conference and the media coverage of the subject, before and after the event, sure stirred up the spirits of the regular users, who have been seeded the idea that malware in the firmware can propagate from one USB device to another without options to prevent infection. Each USB device is powered by a micro-controller chip, programmed to identify its type and functionality, allowing the system to load whatever drivers are needed. SR Labs researchers Karsten Nohl and Jakob Lell demonstrated at the Las Vegas conference how easy it is for a USB storage device, reprogrammed as a keyboard or as a portable network adapter, to compromise the computer; the malicious code would be present in the firmware and executed when the gadget is plugged in. In one example, the duo demonstrated on stage how a regular thumb drive was passed to the system as a keyboard. In another, they showed a device of the same class posing as an Ethernet adapter; in both cases, the end result would be compromising the systems. The implications of this discovery bring even more bad news because there is the possibility for the malicious firmware to spread to other USB controllers, which would make the infection persistent; basically, any USB device (mass storage, webcam, mobile phone) hooked to that machine should be considered compromised. At a first look, there does not seem to be too much to be done to protect against attacks perpetrated this way, especially since even the BIOS of the computer may be replaced in this manner. On the same note, malware scanners are useless because they cannot check the firmware without its help, and malicious firmware could impersonate a legitimate one, making security products useless. Indeed, a USB device reprogrammed for malicious purposes would be serious pain to deal with, but there is some silver lining. The two researchers went through plenty of difficulties to complete their study and demonstrate the dangers of tampering with the firmware of USB controller chips. They did not come up with this security glitch overnight. To reflect such digital apocalypse where there is no apparent line of defense, save for not using USB devices at all, against threat actors taking control over users' computers, Nohl, Lell and their colleague Sascha Krißler chose to reprogram a type of USB controller chips that is widely used in USB gadgets. Months were required to reverse engineer the firmware for the devices used in the demonstration, showing that the task is not easy to carry out. However, before this can be done, a version of the firmware is required and the tool for flashing the controller. Neither of them is readily available on the Internet. Understanding how the firmware works and being able to alter it to add different functionality to the device is also work that requires time and effort. Apart from this, distributing BadUSB malware can be done only to compatible items. Using different products with different controller chips should ensure a higher degree of protection against this threat. But one solution that stands out is relying on secure USB devices that have the controller firmware locked and protected against unauthorized modifications. This is achievable through a tamper-proof mechanism. "In order to block BadUSB, USB storage devices need to prevent a hacker from reading or changing the firmware and ensure that the firmware is digitally signed so if it did get modified, the secure device will not operate with the modified firmware," said via email Ken Jones, vice president of engineering and product management Imation Mobile Security. Cryptographic code-signing is not an approach that can be easily adopted by all manufacturers. At the moment, only devices aimed at professionals and for enterprise environment provide this sort of security. IronKey from Imation relies on FIPS 140-2 Level 3 certification for ensuring the integrity of the product; products from Spyrus adopted the same standard and also make available selective hardware disabling of update processes. Jones also said that because of the challenges posed by securing firmware in the device, USB manufacturers will start to "differentiate themselves by offering secure solutions." Another solution against BadUSB is to rely on simpler hardware that does not need firmware updates after leaving the factory. "Note however, that unless a device is tamper-proof/tamper-evident, there may still be the possibility that a device can be compromised physically and firmware modified," says Jones. On the same note, Bogdan Botezatu, senior threat analyst at Bitdefender, said that there is no guarantee that the USB device has not been tampered with in the production or delivery chain. In the Black Hat presentation, the researchers say that USB devices can be built with some sort of software lock that prevents reprogramming it. However, this type of attack has just been made public and this may have already sparked a few wrong ideas. Because most (read "billions") of the USB devices on the market do not enforce any type of protection against firmware tampering, cybercriminals will, at some point, take advantage of this slip-up. But this won't happen too soon – finding the tools and understanding how everything works is a long-term investment not many will be ready to make right now. Replacing the vulnerable devices requires both time and an alternative that is both secure and cheap, in order to be adopted en masse. To read more click HERE

Seven WebKit Vulnerabilities Fixed in Safari Browser

SoftPedia, 18 Aug 2014: A new version of Safari web browser has been released to repair a set of seven security glitches in the WebKit component, all of them leading to unauthorized disclosure of information through remote execution of arbitrary code. The report from Apple is very scarce in details, and apart from providing the Common Vulnerabilities and Exposures identification, it says that the browser update for OS X eliminates memory corruption problems in WebKit by improving the way the memory is handled. Five of the issues were discovered by Apple engineers, while one was reported by the Google Chrome Security Team and another is credited to an anonymous researcher. If exploited, any of them would have the same effect. Vulnerable versions of Safari (earlier than 6.1.6 and 7.0.6) could allow a potential remote attacker to execute code on the affected system as well as cause a denial of service condition of the application. User interaction is required to achieve this, because the victim has to be convinced to visit a maliciously crafted website. As far as the severity of the issues is concerned, they were given a 6.8 CVSS (Common Vulnerability Scoring System) score, which stands for "medium." The latest versions of Safari browser are available through the update mechanism on Mac systems. To read more click HERE