The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

18 February 2014

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

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, Sandia 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 open source data

February 14, Softpedia – (International) **IE zero-day served by DeputyDog cybercriminals from US Veterans of Foreign Wars site.** Researchers at FireEye identified a cyberattack campaign dubbed SnowMan utilizing a zero-day vulnerability affecting Internet Explorer (IE) 9 and IE 10 being served from the U.S. Veterans of Foreign Wars Web site. The researchers believe the same group behind the DeputyDog and Ephemeral Hydra campaigns is also responsible for SnowMan and may be targeting military personnel. Source: http://news.softpedia.com/news/IE-Zero-Day-Served-by-DeputyDog-Cybercriminals-from-US-Veterans-of-Foreign-Wars-Site-426909.shtml

February 14, Softpedia – (International) **Cybercriminals abuse Twilio and Ow.ly for SMS phishing attack.** Cloudmark researchers reported that cybercriminals are using Twilio and URL shortening service Ow.ly in an SMS message phishing campaign attempting to steal mobile service provider account login credentials. Source: http://news.softpedia.com/news/Cybercriminals-Abuse-Twilio-and-Ow-ly-for-SMS-Phishing-Attack-426840.shtml

February 14, Help Net Security – (International) **Thousands of FTP sites compromised to serve malware and scams.** Researchers at Hold Security reported that around 7,000 FTP sites and servers have been compromised and are being used by cybercriminals to host malware or to compromise connected Web services. Source: http://www.net-security.org/malware_news.php?id=2709

February 13, Help Net Security – (International) **Fake SSL certificates used to impersonate Facebook, Google, banks.** Netcraft researchers discovered a large number of fake SSL certificates in the wild purporting to be from banks, social networks, payment providers, and other services which could be used by attackers to conduct man-in-the-middle attacks. The researchers warned that mobile banking apps are especially vulnerable because they may not adequately check the validity of SSL certificates. Source: http://www.net-security.org/secworld.php?id=16360

Iranian hacking of Navy computers reportedly more extensive than first thought
FoxNews.com, 18 Feb 2014: An Iranian hack of the Navy's largest unclassified computer network reportedly took more than four months to resolve, raising concern among some lawmakers about security gaps exposed by the attack.   The Wall Street Journal, citing current and former U.S. officials, reported late Monday that the cyberattack targeted the Navy Marine Corps Internet, which is used by the Navy Department to host websites, store nonsensitive information, and handle voice, video, and data communications.   The paper reported that the hackers were able to remain in the network until this past November. That contradicts what officials told the Journal when the attack was first publicly reported this past September. At the time, officials told the paper that the intruders had been removed. "It was a real big deal," a senior U.S. official told the Journal. "It was a significant penetration that showed a weakness in the system." The quoted official said that the Iranians were able to conduct surveillance and compromise communications over the unclassified computer networks of the Navy and Marine Corps. However, another senior official told the Journal that no e-mail accounts were hacked and no data was stolen. There is also no evidence that Iran was able to penetrate classified

U.S. computer networks. The cyberattack is one of the one of the most serious infiltrations of government computer systems by the Iranians. The Journal reported that U.S. defense officials were surprised at the skill of the hackers, who were able to enter the network through a security gap in a public-facing website. The military response to the hack was over seen by Vice Adm. Mike Rogers, President Obama's pick to be the next head the NSA. Congressional aides told the Journal that Rogers would likely face questions on plans to fix security issues that have surfaced as a result of the attack. A confirmation hearing for Rogers has not yet been scheduled. To read more click **HERE**

Microsoft Finds Exploits for Patched Adobe Flash Vulnerability
SoftPedia, 18 Feb 2014: Microsoft has warned that exploits for a known Adobe Flash vulnerability have been spotted in the wild and could affect users running Flash Player versions 12.0.0.43 and earlier. According to an advisory rolled out this morning, the exploits are based on a malicious .swf file that can be hosted on a web server in order to be loaded when the user visits the website. "When the .swf is loaded, the vulnerability is triggered," Microsoft warned. "Version 12.x (12.0.0.43 and earlier) is known to contain the vulnerability used by the attack, but it also carries a mitigation that prevents building the ROP gadget from the Flash Player DLL. The sample we analyzed does not support version 12.x for this reason," the company warned. "If you're using Flash Player version 12.0.0.43 or earlier, you need to update your Flash Player now to be protected against these attacks." Of course, all users are highly recommended to download and install the latest Flash Player version, just to make sure that you're on the safe side and no effective exploits are being developed. To read more click **HERE**

ZeuS Trojan Configuration File Disguised as Harmless Image
SoftPedia, 18 Feb 2014: Security researchers have analyzed a new version of the notorious ZeuS banking Trojan. The new variant, ZeusVM, is designed to retrieve its configuration file from an image. Experts from Malwarebytes and French security researcher Xylitol have noticed that alongside other components, the malware is retrieving a JPG image from a server. A closer analysis of the file revealed that it was an image copied from the web, but with some additional code appended to it. By using steganography, the cybercriminals have added the malware configuration data to the image without damaging it. After decrypting the appended data, experts found a list of financial institutions targeted by ZeusVM. The fact that the configuration file is disguised as an image has a number of advantages, including the fact that the malicious code can bypass security systems. Furthermore, a webmaster whose server is used to host the file would probably not suspect that the image is actually part of a cybercriminal operation. Additional technical details are available on Malwarebytes' blog [**LINK**]. To read more click **HERE**

Hackers Send Out Text File to Warn Users of Vulnerable Asus Routers
SoftPedia, 18 Feb 2014: Last week, we informed you that Asus released firmware updates for a number of router models. It turns out that some hackers are leveraging the security holes fixed with the new firmware to send out a text file to the owners of affected devices warning them of the risks. According to Ars Technica, a user found a mysterious text file on his external hard drive. The file contained a message that read, "This is an automated message being sent out to everyone affected. Your Asus router (and your documents) can be accessed by anyone in the world with an Internet connection." The individuals responsible for sending out the files also instruct users to read an article that contains information on how to protect themselves against attacks that leverage vulnerability in their routers. On February 4, someone published a list of close to 13,000 IP addresses reportedly associated with vulnerable Asus routers. Lists containing the names of files stored on the hard drives of impacted users have also been published online. The existence of the vulnerability was revealed by security researcher Kyle Lovett in June 2013. He had made his findings public after being told by Asus that "it was not an issue." Later, Asus promised to address the problem, but since the company failed to warn customers, Lovett published additional technical details, along with ways to mitigate potential attacks. The list of affected routers includes RT-N66R, RT-N66U, RT-AC56U, RT-N56R, RT-N56U, RT-N14U, RT-N16, RT-N16R, RT-AC66R and RT-AC66U. Owners of these models are advised to update their firmware as soon as possible since

this is clearly a critical vulnerability. It appears that Asus has released firmware updates for all of the impacted models. You can download the latest firmware variants for Asus routers from Softpedia. To read more click **HERE**

Fake "New Payment to Skype" Emails Lead to PayPal Phishing Site
SoftPedia, 18 Feb 2014: Phishing emails carrying the subject line "New Payment to Skype" have been seen landing in inboxes these days. They inform recipients that they've sent a payment to Skype via PayPal. "You sent a payment of 42.98 GBP to Skype (support@skype.com)," the emails read. Both PayPal and Skype users have reported receiving such emails. Of course, the notifications don't have anything to do with either of the companies. Cybercriminals are sending them out in an effort to lure users to a phishing site. The phishing page I've seen is hosted on a hijacked sports site. As you can see in the gallery below, the page is well designed. Victims are asked to hand over not only their PayPal login credentials, but also their personal and financial information. If you come across such pages, make sure you're on a legitimate PayPal domain, such as paypal.com. If you're a victim of this scam, change your PayPal password immediately. Also, keep a close eye on your credit card activity since fraudsters will probably attempt to use the stolen information for fraudulent transactions. To read more click **HERE**

Syrian Electronic Army Leaks Details of over 1 Million Forbes Readers
SoftPedia, 15 Feb 2014: Forbes confirms that the Syrian Electronic Army has breached its publishing platform. In addition to gaining access to the company's WordPress admin console and hijacking some Twitter accounts, the Syrian hacktivists have also gained access to readers' information. "Users' email addresses may have been exposed. The passwords were encrypted, but as a precaution, we strongly encourage Forbes readers and contributors to change their passwords on our system, and encourage them to change them on other websites if they use the same password elsewhere," Forbes wrote in a statement posted on Facebook. "We have notified law enforcement. We take this matter very seriously and apologize to the members of our community for this breach." Initially, the Syrian Electronic Army offered to sell user email addresses and passwords taken from Forbes. However, one hour later, they announced that the data would be published for free. Two hours ago, the hackers uploaded a file containing the details of more than 1 million users, including usernames, email addresses and encrypted passwords. The information has been uploaded to what the SEA calls a "secure host." This probably means it will more difficult for Forbes to remove it. The IP address of the server to which the data has been uploaded is 91.227.222.39. The server, located in the United Kingdom, was previously used by the Syrian hackers when they defaced marines.com. Even if the passwords are encrypted, the large number of email addresses published online could still be useful to cybercriminals. The Syrian Electronic Army has told Softpedia that they've attacked Forbes because of the publication's reports about the hacker group and Syria. The hacktivists have suggested that Forbes Social Media Editor and staff writer Alex Knapp is the one they've tricked into providing them with the information needed to compromise the company's systems. The Syrian Electronic Army has attacked numerous media organizations over the past years. However, they rarely leak user data. To read more click **HERE**

Half a million Belkin WeMo users are wide open to attackers
Heise Security, 18 Feb 2014: IOActive has uncovered multiple vulnerabilities in Belkin WeMo Home Automation devices that could affect over half a million users. Belkin's WeMo uses Wi-Fi and the mobile Internet to control home electronics anywhere in the world directly from the users' smartphone. Mike Davis, IOActive's principal research scientist, uncovered multiple vulnerabilities in the WeMo product set that gives attackers the ability to:

- Remotely control WeMo Home Automation attached devices over the Internet
- Perform malicious firmware updates
- Remotely monitor the devices (in some cases)
- Access an internal home network.

Davis said, “As we connect our homes to the Internet, it is increasingly important for Internet-of-Things device vendors to ensure that reasonable security methodologies are adopted early in product development cycles. This mitigates their customer’s exposure and reduces risk. Another concern is that the WeMo devices use motion sensors, which can be used by an attacker to remotely monitor occupancy within the home. The vulnerabilities found within the Belkin WeMo devices expose users to several potentially costly threats, from home fires with possible tragic consequences down to the simple waste of electricity. The reason for this is that, after attackers compromise the WeMo devices, they can be used to remotely turn attached devices on and off at any time. Given the number of WeMo devices in use, it is highly likely that many of the attached appliances and devices will be unattended, thus increasing the threat posed by these vulnerabilities. Additionally, once an attacker has established a connection to a WeMo device within a victim’s network; the device can be used as a foothold to attack other devices such as laptops, mobile phones, and attached network file storage. The Belkin WeMo firmware images that are used to update the devices are signed with public key encryption to protect against unauthorized modifications. However, the signing key and password are leaked on the firmware that is already installed on the devices. This allows attackers to use the same signing key and password to sign their own malicious firmware and bypass security checks during the firmware update process. Additionally, Belkin WeMo devices do not validate Secure Socket Layer (SSL) certificates preventing them from validating communications with Belkin’s cloud service including the firmware update RSS feed. This allows attackers to use any SSL certificate to impersonate Belkin’s cloud services and push malicious firmware updates and capture credentials at the same time. Due to the cloud integration, the firmware update is pushed to the victim’s home regardless of which paired device receives the update notification or its physical location. The Internet communication infrastructure used to communicate Belkin WeMo devices is based on an abused protocol that was designed for use by Voice over Internet Protocol (VoIP) services to bypass firewall or NAT restrictions. It does this in a way that compromises all WeMo devices security by creating a virtual WeMo darknet where all WeMo devices can be connected to directly; and, with some limited guessing of a ‘secret number’, controlled even without the firmware update attack. The Belkin WeMo server application programming interface (API) was also found to be vulnerable to an XML inclusion vulnerability, which would allow attackers to compromise all WeMo devices. IOActive worked closely with CERT on the vulnerabilities that were discovered. CERT made several attempts to contact Belkin about the issues, however, Belkin was unresponsive. To read more click **HERE**

Removing admin rights mitigates 92% of critical Microsoft vulnerabilities

Heise Security, 18 Feb 2014: Avecto analyzed data from security bulletins issued by Microsoft throughout 2013 and concluded that 92% of all vulnerabilities reported by Microsoft with a critical severity rating can be mitigated by removing admin rights. The results also revealed that removing admin rights would mitigate 96% of critical vulnerabilities affecting Windows operating systems, 91% critical vulnerabilities affecting Microsoft Office and 100% of vulnerabilities in Internet Explorer. If malware infects a user with admin rights, it can cause incredible damage locally, as well as on a wider network. Additionally, employees with admin rights have access to install, modify and delete software and files as well as change system settings. Paul Kenyon, co-founder and EVP of Avecto said: "The dangers of admin rights have been well documented for some time, but what's more concerning is the numbers of enterprises we talk to that are still not fully aware of how many admin users they have. Without clear visibility and control, they are facing an unknown and unquantified security threat." Paul concluded: "This analysis focuses purely on known vulnerabilities, and cyber criminals will be quick to take advantage of bugs that are unknown to vendors. Defending against these unknown threats is difficult, but removing admin rights is the most effective way to do so." To read more click **HERE**

Most organizations are unable to resolve a cyber-attack

Heise Security, 14 Feb 2014: The lack of incident detection and investigation puts companies and their CISOs' jobs at significant risk, according to a new Ponemon Institute study. In fact, when a CEO and Board of Directors asks a security team for a briefing immediately following an incident, 65% of respondents believe that the briefing would be purposefully modified, filtered or watered down. Additionally, 78% of respondents believe most CISOs would make a "best effort guess" based on limited information, and they would also take action prematurely and report that the problem had been resolved without this actually being the case. This disconnect results from several critical shortcomings in the current point solution approach to cybersecurity and incident response (IR), namely:

- Lack of timely compromise detection: 86% of respondents say detection of a cyber-attack takes too long;
- Inability of point solutions to prioritize alerts as they come in: 85% say they suffer from a lack of prioritization of incidents;
- Lack of integration between point solutions: 74% say poor or no integration between security products negatively affects response capabilities; and
- An overwhelming number of alerts paralyzing IR efforts: 61% say too many alerts from too many point solutions also hinders investigations.

"When a cyber-attack happens, immediate reaction is needed in the minutes that follow, not hours or days," said Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. "It's readily clear from the survey that IR processes need to incorporate powerful, intuitive technology that helps teams act quickly, effectively and with key evidence so their companies' and clients' time, resources and money are not lost in the immediate aftermath of the event." Further, the respondents also shared growing concerns about the inability to find the root cause of a compromise. While 66% of respondents believe determining root cause of prior incidents enables them to strengthen defenses, 38% of respondents say determining the root cause of a compromise could take a year while an alarming 41% believe they would never be able to identify the root-cause of security events with certainty. Lastly, integrated threat intelligence – a hugely promising approach to arming CISOs with the latest indicators of compromise (IOC) information and ability to confirm threats – appears to be largely unusable by current security products, with a full 59% of respondents saying they are not able to efficiently and effectively use threat intelligence with their existing security products. Additional key findings revealed that current security products make it difficult to import multiple threat intelligence feeds or quickly investigate mobile devices:

- 40% say none of their security products support imported threat intelligence from other sources
- 86% rate the investigation of mobile devices as difficult
- 54% say they are not able to or unsure of how to locate sensitive data such as trade secrets and personally identifiable information (PII) on mobile devices.

To read more click **HERE**