The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
11 - 13 March 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

March 7, WBAL 11 Baltimore – (Maryland) **FBI probes Johns Hopkins University data breach.** Johns Hopkins University officials reported a data breach after the personal information of as many as 1,307 current and former students in the Department of Biomedical Engineering's Design Team course was stolen from a web server at the Baltimore school. The hackers attempted to extort the university out of server passwords and posted the information they obtained online. Source: http://www.wbaltv.com/news/fbi-probes-johns-hopkins-university-data-breach/24858850

March 8, Softpedia – (International) **Statistics company Statista hacked, email addresses and passwords possibly stolen.** Statistics and studies company Statista reported that attackers may have compromised its systems and accessed a user database containing email addresses and encrypted passwords. Source: http://news.softpedia.com/news/Statistics-Company-Statista-Hacked-Email-Addresses-and-Passwords-Possibly-Stolen-431173.shtml

March 8, Softpedia – (International) **BAE Systems publishes white paper on "Snake" cyber espionage campaign.** Researchers at BAE Systems Applied Intelligence published a white paper on the Snake cyberespionage campaign, which they believe the Uroburos rootkit is a part of. The researchers stated that the campaign may have been in development since 2005, may still be active, and also contains components known as "snark" and "sengoku." Source: http://news.softpedia.com/news/BAE-System-Publishes-White-Paper-on-Snake-Cyber-Espionage-Campaign-431214.shtml

March 7, Softpedia – (International) **Ransomware authors: We are not scammers, we don't need your files.** Researchers at Symantec identified a version of the Trojan.Ransomscript ransomware that encrypts victims' files and demands a ransom to decrypt them, but also offers to decrypt the files for free after a month has passed. Source: http://news.softpedia.com/news/Ransomware-Authors-We-Are-Not-Scammers-We-Don-t-Need-Your-Files-431053.shtml

March 11, Softpedia – (Washington) **Hackers steal details of thousands of individuals from Archdiocese of Seattle.** The Archdiocese of Seattle warned volunteers and employees that their personally identifiable information, including Social Security numbers, may have been compromised when attackers breached the archdiocese's systems. The archdiocese advised those affected to check and see if fraudulent tax returns have been filed in their names. Source: http://news.softpedia.com/news/Hackers-Steal-Details-of-Thousands-of-Individuals-from-Archdiocese-of-Seattle-431508.shtml

March 10, Krebs on Security – (International) **Experian lapse allowed ID theft service access to 200 million consumer records.** A Vietnamese national pleaded guilty the week of March 3 to running an identity theft service from his home in Vietnam by tricking an Experian subsidiary into giving him access to personal and financial data belonging to over 200 million U.S. citizens by claiming to be a private investigator. Source: http://krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records/

March 7, KGAN 2 Cedar Rapids – (Iowa) **Iowa DHS data breach of personal info.** The Iowa Department of Human Services announced March 7 that 2,042 individuals were impacted by a breach of personal information related to some Polk County social work assessments after two workers used personal email accounts, personal storage accounts, and personal electronic devices for work purposes. The workers transmitted information through unsecured networks over a 5-year period starting in 2008. Source: http://www.cbs2iowa.com/news/features/top-stories/stories/iowa-dhs-data-breach-personal-info-25429.shtml

March 11, Softpedia – (International) **162,000 WordPress sites abused to amplify DDoS attack.** Researchers at Securi found that attackers used around 162,000 WordPress sites to indirectly launch a distributed denial of service (DDoS) attack on a client's WordPress site by abusing the sites' XML-RPC feature, which is enabled by default on WordPress sites. Source: http://news.softpedia.com/news/162-000-WordPress-Sites-Abused-to-Amplify-DDOS-Attack-431590.shtml

March 11, Threatpost – (International) **Apple iOS 7.1 fixes more than 20 code-execution flaws.** Apple released an update for its iOS mobile operating system, closing several code execution vulnerabilities and other issues. The Webkit framework underlying the Safari browser also received fixes for 19 memory corruption issues. Source: http://threatpost.com/apple-ios-7-1-fixes-more-than-20-code-execution-flaws/104705

March 10, SC Magazine – (International) **Saboteurs slip Dendroid RAT into Google Play.** A researcher at Lookout found that the Dendroid remote access trojan (RAT) had been uploaded into the Google Play store disguised as other apps, but was quickly removed. Source: http://www.scmagazine.com/saboteurs-slip-dendroid-rat-into-google-play/article/337607/

March 10, IDG News Service – (International) **Joomla receives patches for zero-day SQL injection vulnerability, other flaws.** The Joomla Project released security updates for its Joomla content management system, addressing a SQL injection vulnerability that could be used to steal information from databases on Joomla-based Web sites, as well as addressing two cross-site scripting (XSS) vulnerabilities and an unauthorized log-in flaw. Source:http://www.computerworld.com/s/article/9246849/Joomla_receives_patches_for_zero_day_SQL_injection_vulnerability_other_flaws

March 12, Softpedia – (International) **Adobe updates Flash Player 12 to address two vulnerabilities.** Adobe released updates to for its Flash Player for Windows, Mac, and Linux, addressing two vulnerabilities.. Source: http://news.softpedia.com/news/Adobe-Updates-Flash-Player-12-to-Address-Two-Vulnerabilities-431700.shtml

March 12, Softpedia – (International) **Hackers can steal private WhatsApp chats with other Android apps.** A security researcher identified a security flaw in WhatsApp that could allow any Android app installed on the device with access to the SD card to retrieve the WhatsApp database containing private chat logs. The database is encrypted, but a legitimate app that can decrypt the file is available. Source: http://news.softpedia.com/news/Hackers-Can-Steal-Private-WhatsApp-Chats-with-Other-Android-Apps-431783.shtml

March 12, Softpedia – (International) **Chrome updated to 33.0.1750.149, 7 security issues fixed.** Google released the 33.0.1750.149 update of its Chrome browser, closing seven security issues. Source: http://news.softpedia.com/news/Chrome-Updated-to-33-0-1750-149-7-Security-Issues-Fixed-431708.shtml

March 11, IDG News Service – (International) **Microsoft Patch Tuesday rounds up IE flaws.** Microsoft released its monthly round of Patch Tuesday updates March 11, containing 5 bulletins addressing 23 vulnerabilities. Two were marked as critical, including an Internet Explorer vulnerability that has been used in targeted attacks. Source:http://www.computerworld.com/s/article/9246895/Microsoft_Patch_Tuesday_rounds_up_IE_flaws

March 11, IDG News Service – (International) **Researchers attack secured Internet activity to mine personal data.** Researchers at the University of California, Berkeley developed an attack that could allow governments and Internet service providers to bypass HTTPS traffic protections and determine the Web pages a user has visited with 89 percent accuracy. Attackers would need to be able to visit the same Web pages as the user, which would enable them to identify packet patterns in the encrypted traffic. Source: http://www.networkworld.com/news/2014/031114-researchers-attack-secured-internet-activity-279594.html

Pwn2Own 2014: Firefox, Internet Explorer and Safari Hacked on Day One

SoftPedia, 13 Mar 2014: Pwn2Own 2014, an event that takes place these days alongside CanSecWest in Vancouver, has started. On the first day, contestants already found vulnerabilities in Safari, Firefox, Internet Explorer, Adobe Flash and Reader. The payouts made after the first day total $400,000 (€286,000). Most of the money went to French research firm VUPEN. The company's researchers have managed to find a total of four vulnerabilities. They found a use-after-free with an Internet Explorer sandbox bypass in Flash. The issue can be exploited to execute arbitrary code. A heap overflow and PDF sandbox escape in Adobe reader also resulted in code execution. VUPEN experts have also found a use-after-free that can be leveraged for code execution in Firefox. In addition, they've managed to bypass the sandbox in Internet Explorer 11 on Windows 8.1 with a use-after-free vulnerability that causes object confusion in the broker. For their work, VUPEN researchers have been rewarded with $300,000 (€215,000). Researchers Jüri Aedla and Mariusz Mlynski each managed to "pwn" Firefox. Aedla found an out-of-bound read/write resulting in code execution. Mlynski found two security holes: a privilege escalation flaw and one that could be exploited to bypass the web browser's security measures. Each of the experts has been rewarded with $50,000 (€35.850). TippingPoint's Zero Day Initiative (ZDI) and Google, the co-sponsor of Pwn2Own 2014, have taken part in a new challenge called Pwn4Fun. Experts from Google and ZDI presented their own exploits, all the proceeds being donated to the Canadian Red Cross. "At Pwn4Fun, Google delivered a very impressive exploit against Apple Safari launching Calculator as root on Mac OS X. ZDI presented a multi-stage exploit, including an adaptable sandbox bypass, against Microsoft Internet Explorer, launching Scientific Calculator (running in medium integrity) with continuation," the competition's organizers explained. A total of $82,500 (€59,000) has been donated to the Canadian Red Cross. IDG's Gregg Keizer reports that most of the contestants managed to demonstrate their exploits within 5 minutes, despite having 30 minutes to do it. Once the exploits were demonstrated, the security researchers headed to the disclosure room where they presented the details of their exploits to vendors. This is one of the main conditions of Pwn2Own. All vulnerabilities must be disclosed to respective vendors so that they can fix the security holes. We can expect Mozilla and Microsoft to patch the vulnerabilities found by contestants in the upcoming days. It remains to be seen if anyone manages to break Chrome in the second and last day of Pwn2Own. To read more click **HERE**

EC-Council Admits Hacker Compromised Some Email Accounts

SoftPedia, 13 Mar 2014: Back in February, a hacker managed to deface the website of EC-Council, an organization that provides IT security training and certification. Now, three weeks after the incident, EC-Council has provided additional details about the attack. In a statement posted on its website, EC-Council maintained the fact that the defacements were a result of DNS poisoning. The hacker, calling himself Eugene Belford (the name of a character in the movie "Hackers"), managed to deface the site three times because the organization was having trouble getting in touch with the appropriate domain registrar personnel. The domain registrar in question was unable to secure its servers, so EC-Council was forced to shut down its website while it migrated services to a different company. After hijacking the certification company's domain, the attacker leveraged a vulnerability in the password reset policy of an email service provider used by EC-Council to compromise "a small number of email accounts." "This resulted in unauthorized access to messages in those specific email boxes for a short duration of time. The potentially compromised accounts represent approximately 2% of their customer base." EC-Council representatives stated. It's uncertain if the hacker has stolen any data from the compromised email accounts. However, EC-Council is notifying them. Credit card information has not been obtained, the company says. "As a precaution, EC-Council strongly recommends that their affected customers remain vigilant for any unauthorized use of the information shared with EC-Council and that they alert EC-Council if they find any reason to suspect any," the statement reads. The organization says it's working with law enforcement agencies across three continents to track down the attacker. In the meantime, it has rolled out additional security measures to prevent future incidents. r000t's Blag has conducted an investigation and has determined that the perpetrator is a 16-year-old Finnish individual who's a former member of Hack the Planet (HTP), a group that breached the systems of web hosting and cloud computing provider Linode back in April 2013. The hacker in question was excluded from the group after the Linode hack. Shortly after, HTP disappeared from the hacking scene. r000t's Blag has found evidence that the server to which EC-Council's visitors were redirected during the hack attack is owned by this individual from Finland. The teen who has targeted EC-Council is said to already be on the FBI's radar. The agency reportedly arrested him in Las Vegas at DEF CON 2013. However, they had to let him go. To read more click **HERE**

North Dakota University System Hacked, Details of 290,000 People Possibly Stolen

SoftPedia, 11 Mar 2014: In February, the North Dakota University System (NDUS) discovered that one of its servers had been breached. According to the organization, the impacted server stored the details of 290,000 individuals. NDUS believes that the hackers gained unauthorized access to the server sometime in late October 2013. They compromised an existing account's login credentials in order to access the machine. However, for the time being, it's not known how the attackers obtained the login credentials. The server stored the social security numbers and other details of 291,465 current and former students, including Fall 2014 applicants. It also contained the social security numbers and employee IDs of 784 faculty and staff members. After conducting a forensic analysis of the breached server, NDUS hasn't found any evidence to suggest that the cybercriminals stole any of the information. In fact, it's believed that they might have targeted the server for other purposes, not to steal data from it. "Based on the forensic investigation, it is likely the intruder's intent was only to use the server's processing power to launch attacks on other computers and systems. The intruder may not have even been aware that the sensitive information was stored on this server," reads the FAQ published by the university. However, since there are no guarantees that no information has been stolen, the educational institution has signed a contract with AllClear ID to provide free Identity Protection Coverage for one year to those whose information was contained on the breached server. All those who receive notification letters from NDUS can sign up for the service. A call center will be available starting with March 14 to answer any questions that affected individuals might have. The university warns students to watch out for any phishing scams that might leverage the incident. Since NDUS is notifying them via email (at least those whose email addresses the organization has), it's possible that cybercriminals will also take the opportunity to harvest some information. It's important for impacted individuals to remember that they will not be asked to provide their social security numbers to verify their identities, not on the phone and not via email. "Information security is of the utmost importance to us, and it is very unfortunate this has

happened.We are working diligently to help make sure this doesn't happen again. It's disturbing that higher education is often targeted by criminal elements in today's global assaults on IT systems," said NDUS Interim Chancellor Larry C. Skogen. "We completely understand that this incident could be distressing. We certainly hope that no one experiences any negative impact from this intruder's actions, but we are providing resources for those who would like them, and we will keep people apprised of any new developments." To read more click **HERE**

162,000 WordPress Sites Abused to Amplify DDOS Attack

SoftPedia, 11 Mar 2014: Sucuri has been called in to mitigate a major distributed denial-of-service (DDOS) attack aimed at a popular WordPress site. What's interesting about this incident is that 162,000 other WordPress sites were used to amplify the attack. DDOS attacks are becoming more and more common. However, every once in a while, cybercriminals come up with an interesting way to amplify them. According to experts, in this particular attack, the 162,000 WordPress sites were indirectly used as amplification vectors. After the company, which hasn't been named, subscribed to their CloudProxy Website Firewall service, Sucuri immediately started analyzing the operation. They soon discovered that tens of thousands of WordPress sites were sending random requests at the targeted websites in an effort to make it inaccessible. So how could cybercriminals abuse such a large number of WordPress sites? The attackers are actually abusing the XML-RPC feature. XML-RPC is used for trackbacks, pingbacks, remote access and other operations. Because XML-RPC is enabled by default on WordPress websites, it's not difficult for malicious actors to abuse it. They simply have to send a ping back request to the website's XML-RPC file. The request looks something like this: $ curl -D - "www.anywordpresssite.com/xmlrpc.php" -d '<methodCall><methodName>pingback.ping </methodName> <params><param><value><string> http://victim.com</string></value></param> <param><value><string> www.anywordpresssite.com/postchosen </string> </value></param></params></methodCall>' With this simple Linux command, many WordPress websites become amplification vectors for a DDOS attack. Sucuri experts advise the owners of WordPress websites to check their logs for any POST request to the XML-RPC file. If they find pingbacks to random URLs, the site is most likely used to target others. Alternatively, there is an online WordPress DDOS Scanner tool made available by Sucuri. In order to protect your website from being abused in such a manner by cybercriminals, you can disable the XML-RPC pingback functionality, or add the following piece of code to your WordPress theme:

```
add_filter( 'xmlrpc_methods', function( $methods ) {
unset( $methods['pingback.ping'] );
return $methods;
```

To read more click **HERE**

Virgin Media Promises Fix for Wi-Fi Vulnerability in Super Hub Routers

SoftPedia, 11 Mar 2014: Last week, security researcher Paul Moore reported that a vulnerability in Virgin Media's Super Hub and Super Hub 2 routers (produced by Netgear) could be exploited to hijack the devices. Virgin Media representatives say they're working with Netgear on addressing the issue. Moore has found that when these routers are started, there's a 7 second window in which Wi-Fi is enabled, but encryption is not. An attacker can use this window to gain access to the encryption key. A hacker needs the password to the user interface in order to obtain the information. However, there is a default password that people rarely change, so the task is not difficult. Moore has also found a way to force the reboot of the device, so an attacker would not have to wait around for the target to restart the router. In a response to a discussion on this topic on the Virgin Media forum, Jim Meadows, a member of the Help and Support Forum team, provided the following statement: "The security of our services is of the highest importance and we are working with Netgear to develop and test a software update which will initialise encryption immediately from reboot and this is close to being issued. We encourage all our customers to change their default passwords when they are installed, if anyone is unsure whether they have made this change, instructions on our website provide an easy guide on how this can be done at any time on our help pages at http://virg.in/sh2pass If customers are concerned, then we

would recommend that after changing the default password, they should also change the WiFi passphrase for additional security." So Virgin Media agrees with Moore's recommendations. On the other hand, in his statement, Meadows downplays the seriousness of the security hole. "To confirm, the issue only relates to the Netgear VMDG485 device (SuperHub2) and, although we agree with the person who identified it that this is highly unlikely to happen; we have thanked them for bringing this to our attention," he noted. In a statement provided to The Register, Virgin Media representatives reiterate the recommendations and advise users to change their default passwords. They've also promised a permanent fix for the issue, but it's uncertain when it will be rolled out. "The security of our services is of the highest importance and we have been working with our supplier to develop and test a software update which is close to being issued," they noted. To read more click **HERE**