The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
20 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 19, The Register – (International) **'Zotob' hacker 'Diabl0' arrested in Bangkok after three-year hunt.** A Moroccan suspected of causing $4 billion in damages to Swiss banking systems was arrested in Thailand and faces extradition to Switzerland. The man was previously arrested and jailed in Morocco for spreading the Zotob worm that infected systems around the world, including a U.S. government Web site. Source: http://www.theregister.co.uk/2014/03/19/diabl0_hacker_arrested_bangkok/

March 17, Health IT Security – (Ohio) **Health Source of Ohio file breach affects 8,800 patients.** Health Source of Ohio reported that 8,800 patients were affected by a data breach after a file containing protected health information was accessible on the Internet from mid-November 2013 through December 2013. The information was gathered through a Web-based program used by the health center's accounting staff and somehow available through Internet searches. Source: http://healthitsecurity.com/2014/03/17/public-file-from-health-source-of-ohio-affects-8800-patients/

March 18, Associated Press – (National) **IRS: Employee took home personal info on 20K workers.** The Internal Revenue Service (IRS) reported March 18 that an employee took home a computer thumb drive containing personal information of about 20,000 IRS workers, former workers, and contractors. The agency's inspector general is investigating the potential breach. Source: http://news.msn.com/us/irs-employee-took-home-personal-info-on-20k-workers

March 19, Softpedia – (International) **Hacked EA server used to host Apple phishing page.** Researchers at Netcraft reported that attackers compromised a server that hosts two Electronic Arts (EA) Web sites and used it to host a phishing page that mimics an Apple login page. Source: http://news.softpedia.com/news/Hacked-EA-Website-Used-to-Host-Apple-Phishing-Page-432977.shtml

March 19, Softpedia – (International) **Expert finds RCE flaw in Yahoo after logging in with "Admin/Admin" credentials.** A security researcher identified and reported a flaw in a Hong Kong subdomain of Yahoo that allowed him to gain read/write/execute permissions by entering a default login name and password. The issue was reported February 20 and fixed February 21. Source: http://news.softpedia.com/news/Expert-Finds-RCE-Flaw-on-Yahoo-After-Logging-in-with-Admin-Admin-Credentials-432956.shtml

March 19, Softpedia – (International) **Mozilla releases Firefox 28, fixes vulnerabilities presented at Pwn2Own.** Mozilla released Firefox 28, the newest version of its Web browser, adding new features and closing 18 vulnerabilities identified during the Pwn2Own 2014 security competition. Source: http://news.softpedia.com/news/Mozilla-Releases-Firefox-28-Fixes-Vulnerabilities-Presented-at-Pwn2Own-432912.shtml

March 18, SC Magazine – (International) **$30 RAT, WinSpy, involved in two phishing campaigns.** FireEye researchers identified two phishing campaigns utilizing the WinSpy remote access trojan (RAT) and the GimmeRAT Android malware that comes packaged with the first RAT. One campaign used spear phishing emails targeting U.S. financial institutions while a second was an indiscriminate spam campaign. Source: http://www.scmagazine.com/30-rat-winspy-involved-in-two-phishing-campaigns/article/338770/

Linux Worm Darlloz Infects over 31,000 Devices in Four Months

SoftPedia, 20 Mar 2014: Back in November 2013, Symantec revealed identifying a Linux worm capable of infecting a wide range of Internet-enabled devices, including security cameras, routers, set-top boxes, printers and industrial control systems running Linux. In January, Symantec spotted a new variant of the worm dubbed Linux.Darlloz. Experts say that a total of over 31,000 devices have been infected with the threat. The author of Darlloz is constantly updating the code and adding new features to his creation. The worm is designed to infect computers running Intel x86 architectures, but it's also capable of infecting devices running MIPS, ARM, PowerPC architectures. Routers, set-top boxes and other devices usually have this kind of architecture. Based on its investigation, Symantec has determined that the main goal of Darlloz is to abuse infected devices for crypto-currency mining. Once it's installed on a computer, the worm installs open source mining software (cpuminer). At the end of February, the attackers mined over 42,000 Dogecoins ($46 / €33) and 282 Mincoins ($150 / €108). This isn't much, but experts expect the attacker to evolve in the upcoming period. It's worth noting however that the crypto-currency mining component is only installed on devices with Intel x86 architecture. One explanation as to why the miner isn't running on "Internet of Things" (IoT) devices is the fact that they don't have the processing power required for such operations. Researchers believe that the cybercriminals are focusing on mining Dogecoins and Mincoins because unlike Bitcoins, they can be mined on home PCs. When it comes to targeting IoT devices, Darlloz uses 13 username/password combinations to access them. Earlier versions only relied on 9 default or common credential sets to access devices. Currently, the Linux worm only targets IP cameras, computers, set-top boxes and routers, but it could one day be improved to target wearable technology and automation devices as well. Symantec has gathered some information regarding current infections. Experts have identified a total of 31,716 IP addresses that open port 58455 (on which Darlloz communicates) and host malware files on static paths. The infections are spread out across 139 regions. Most affected are China, the US, South Korea, Taiwan and India. These countries account for 50% of all infections. 43% of infected devices are computers or servers (Intel-based) running Linux. Printers, cameras, set-top boxes, routers and other smart devices represent 38% of the total number of infections. The large number of impacted IoT gadgets is due to the fact that users seldom scan them for malware. To read more click **HERE**

New ZeuS Generates Income for Its Masters by Displaying Sites on Infected Computers

SoftPedia, 20 Mar 2014: ZeuS, the notorious banking malware, continues to evolve. One new version spotted by experts appears to engage in pay-per-click activities to generate income for its masters. According to Trend Micro researchers, the TROJ_ZCLICK.A variant of ZeuS is designed to display arbitrary websites on infected computers. The sites opened by the threat occupy the entire screen, preventing users from opening other windows or files. Websites are opened every time the victim performs an activity like opening a window or a file. If the user doesn't do anything when these arbitrary websites are displayed, the malware takes control of the mouse, moving the cursor and scrolling the screen. Victims can access the desktop by pressing the Windows key+D combination, but the sites still run in the background. Furthermore, more windows will continue to pop up as users perform other activities. Interestingly, unlike other versions of ZeuS, this one isn't designed to steal sensitive information from infected devices. Instead, it's only designed to load these clickbot routines. "In this light, it's only logical to assume that the main motivation for this variant is to generate income via the pay-per-click model," Mark Joseph Manahan, a threat response engineer at Trend Micro, explained in a blog post. "This malware proves that cybercriminals are continuously tweaking familiar or known malware to deliver new payloads, all in the name of generating income from victimizing users," the expert added. This isn't the only interesting ZeuS variant uncovered this week. Researchers from F-Secure have also spotted a new variant of the notorious threat. While they haven't completed their analysis, it appears that a new version of Gameover ZeuS contains procedures for stealing Bitcoin wallets from infected PCs. Gameover is the peer-to-peer version of ZeuS. Around three weeks ago, experts reported that a variant of the malware came with a kernel-mode rootkit apparently borrowed from the Necurs malware family. The kernel-mode rootkit makes Gameover more difficult to remove from both the disk and memory. There are a number of types of malware part of the ZeuS/ZBOT family. Some of them are designed to download ransomware or other threats onto infected computers. As far as Bitcoin stealers are concerned, they're becoming more and more popular, which isn't surprising considering that a single Bitcoin is worth a lot of money these days. In fact, Bitcoin stealers have become so popular that they're even designed to target Mac OS X users. One example is OSX/CoinThief, which has been distributed via a number of high-profile websites, including Download.com, GitHub and MacUpdate. To read more click **HERE**

Mozilla Thunderbird 24.4.0 Gets Important Security Fixes
SoftPedia, 20 Mar 2014: Mozilla has officially released Thunderbird 24.4.0, an email and RSS client, for all the available platforms, including Linux. A new version has been released in the Thunderbird 24.x branch, but there is nothing to be excited about, a fact that has unfortunately become the norm for new Thunderbird releases. If you aren't up to speed with what's happening with Thunderbird, then you must know that Mozilla has pretty much abandoned the project. It's now in the hands of the community, and the current developers are only interested in making sure that all the security problems are taken care of. The days of Thunderbird are probably numbered. The release comes with just a major fix for the application. According to the changelog, the handling of BCC when replying to messages has been improved. All the rest of the fixes are just security-related. They are important, of course, but not as interesting. For example, a use-after-free issue in TypeObject has been fixed, an out-of-bounds write through TypedArrayObject after neutering has been corrected, and privilege escalation using WebIDL-implemented APIs has been prevented. To read more click **HERE**

21-Year-Old Australian Arrested for Hacking US Online Gaming Company
SoftPedia, 20 Mar 2014: Australia's Queensland Police Service has revealed that a 21-year-old resident of the agricultural town of Kingaroy has been arrested and charged with fraud and hacking-related offences. The man is suspected of hacking into the systems of a US-based company that develops online games. Officers from the State Crime Command's Fraud and Cyber Crime Group arrested the man on Wednesday. Neither the suspect nor the company he attacked has been named for privacy reasons. "We would like to acknowledge the assistance of the FBI and the US based gaming company for their assistance in bringing this investigation to a successful close," said Detective Superintendent Brian Hay of the Fraud and Cyber Crime Group. The suspect has been charged with three counts of computer hacking and misuse, and five counts of fraud, including dishonestly obtaining property from another, dishonestly apply property to own use, and dishonestly cause detriment and possessing equipment for purpose of committing or facilitating the commission of an offence. The arrest comes after police executed a search warrant in November 2013. At the time, they seized laptops and a hard drive, which have been forensically analyzed. On the same day as the arrest, law enforcement authorities also executed a search warrant at a property in Poona, where they seized items located within an encrypted container found on a computer. The man is believed to have hacked into the US company's networks, accessing files and databases. He also hijacked the game developer's Twitter account from which he posted information stolen from the company. Part of the stolen data was used to set up a website that allowed people to search a player database for a certain fee. Police have told Fairfax Media that the database contained players' IP addresses. Other gamers could use these IP addresses to launch DDOS attacks against their opponents' routers to prevent them from playing. The suspect has been released on bail. His next court appearance is scheduled for April 8 at the Maryborough Magistrates Court. That's when we'll find out his name and the name of the company he targeted. The attacks are said to have taken place between July 14 and July 26, 2013. As far as we could determine, the only attack reported against a gaming company at the time was the one against Riot Games, the publisher of League of Legends.

However, it's difficult to say for sure if this is the attack for which the 21-year-old has been charged. To read more click HERE

Windows 8 Leaker Arrested by the FBI

SoftPedia, 20 Mar 2014: Alex Kibkalo, a former Microsoft employee who left the company in 2012, was arrested today after one year of investigations for allegedly leaking copies of Windows 7 and Windows 8 to the Internet. According to a report published by the Seattle Post-Intelligencer, Kibkalo obtained copies of Windows 7 and Windows 8, uploaded them to his personal cloud-storage account and then allowed a French blogger, who was hiding his identity online, to download all files and post information on the web. The report states that Kibkalo, who had been working for Microsoft for a total of 7 years, "uploaded proprietary software including pre-release software updates for WIndows 8 RT and ARM devices, as well as the Microsoft Activation Server Software Development Kit (SDK) to a computer in Redmond, Washington and subsequently to his personal Windows Live SkyDrive account." What's more, it appears that this wasn't the first time when Kibkalo leaked information regarding Microsoft's projects to the Internet, as he previous posted several screenshots and details on his Twitter accounts and blogs. Unsurprisingly, before leaving the software giant in 2012, Kibkalo received a poor performance review and according to the same source, he threatened to resign "if the review was not amended." A conversation between the former Microsoft employee and the French blogger confirms that Kibkalo was the one behind the leaks, even though he clearly knew that it was illegal to disclose the information. "I would leak enterprise today probably," Kibkalo allegedly told the blogger on August 2, 2012 before providing access to Windows 8 leaks. Asked if he really wants to do this because "it's pretty illegal," Kibkalo briefly replied: "I know :)." What's more, the same conversations between the former Microsoft worker and his blogger friend show that Kibkalo was even trying to get into Building 9 in the Redmond campus and copy one of the servers, which was then supposed to be leaked to the Internet just like the previous files. Kibkalo was arrested on Wednesday and is charged with theft of trade secrets, with the initial hearing scheduled to take place this week. As for the French blogger himself, Microsoft Trustworthy Computing Investigations, a special team created by the Redmond software giant to help track him down, managed to discover the Hotmail account he used to communicate with Kibkalo, but his identity was pretty hard to be discovered. He used false details and contact information, claiming to be in Quebec and choosing a nickname to hide his identity during the conversations. To read more click HERE

Oracle Releases Java 8, Several Security Improvements Included

SoftPedia, 20 Mar 2014: Oracle has announced the availability of Java SE 8 and JDK 8, the company's implementation of Java SE 8. Changes have been made in the Java Programming Language, Collections, JavaFX, tools, and other components. As far as security enhancements are concerned, the list is fairly long. First of all, the TLS 1.1 and TLS 1.2 protocols have been enabled by default on the client. The SunJCE provider has been fitted with stronger algorithms for Password-Based Encryption. The list of AES-based algorithms includes PBEWithSHA256AndAES_128 and PBEWithSHA512AndAES_256. SL/TLS Server Name Indication (SNI) extension support has been added to JSSE Server, the SunJSSE provider has been enhanced to support AEAD mode-based cipher suites, and the SunJSE provider now supports AES/GCM/NoPadding cipher implementation and GCM algorithm parameters. "-importpassword" is a new command that's been added to allow users to store a password security as a secret key with the aid of the keytool utility. The list of security improvements also includes enhanced support for NSA Suite B cryptography, better support for high entropy random number generation, PKCS 11 provider support for Windows includes 64-bit, two new rcache types added to Kerberos 5, and weak Kerberos 5 encryption disabled by default. Previous versions of Java have been so vulnerable that it has been often named the most vulnerable software on the market. At the recent Pwn2Own competition, none of the contestants tried to hack Java. The reward for finding exploitable vulnerabilities in the software was only $30,000 (€22,000). Adam Gowdiak, the CEO and founder of Security Explorations, and his team have identified numerous security holes in Java over the past years. While it remains to be seen how secure Java 8 really is, Gowdiak highlights the fact that "what usually matters is the code quality and implementation." To read more click HERE

20% of all malware ever created appeared in 2013

Heise Security, 19 Mar 2014: According to the latest PandaLabs report, malware creation hit a new milestone. In 2013 alone, cyber-criminals created and distributed 20 percent of all malware that has ever existed, with a total of 30 million new malicious strains in circulation, at an average of 82,000 per day. Despite Trojans have continued to be the most common security threat, the company's anti-malware laboratory has observed a wide variety of attacks, with a notable resurgence of ransomware (CryptoLocker being one of the nastiest examples). The proportion of infected computers around the world was 31.53 percent, very similar to the 2012 figures. Besides offering an overview of the most significant events in the computer security field, the 2013 Annual Security Report also forecasts future trends for 2014. Much of 2014's headlines will focus on the Internet of Things (IoT) and Android devices, which will continue to be exploited by attackers to steal users' data and money. PandaLabs expects to see hundreds of thousands of new strains of Android-targeting malware in circulation. 2013 saw a large number of Android scams that used malicious ads in legitimate apps, and it has been estimated that last year alone cyber-criminals released more than two million new malware threats for Android. Social media attacks also grabbed headlines. The number of account hijacking attempts rose spectacularly, affecting companies, celebrities and even politicians. Looking at the types of malware that were created, PandaLabs identified Trojans as being the top threat, accounting for 77.11 percent of all new malware. There was a significant growth in the number of viruses in circulation, rising from 9.67 percent in 2012 to 13.30 percent in 2013. "This increase is mainly down to two particular virus families: Sality and Xpiro. The first virus family has been around a long time, whereas the second one is more recent and capable of infecting executable files on 32-bit and 64-bit systems," said Luis Corrons, technical director of PandaLabs. When it comes to the number of infections caused by each malware category, data gathered by Panda Security's Collective Intelligence platform indicates that three out of every four malware infections were caused by Trojans (78.97 percent), followed by viruses (6.89 percent) and worms (5.83 percent). "It seems that cyber-criminals managed to infect more computers with Trojans in 2013 than in previous years. In 2011, Trojans accounted for 66 percent of all computer infections, whereas this percentage rose to 76 percent in 2012. This growing trend was confirmed in 2013," said Corrons. To read more click **HERE**