THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

16 October 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

October 14, Dallas Morning News – (Texas) **Dallas warns that 'small number' of laptops containing patient information are missing from ambulances.** Dallas City Hall officials reported October 14 that an unknown number of laptops containing patient information disappeared from Dallas Fire-Rescue ambulances between January 2011 and August 29. The city is contacting patients who were transported on the ambulances or attended to by emergency technicians while they continue to investigate the disappearance. Source: http://cityhallblog.dallasnews.com/2014/10/dallas-warns-that-small-number-of-laptops-containing-patient-information-are-missing-from-ambulances.html/

October 15, Help Net Security – (International) **Microsoft patches two more 0-days actively used by attackers.** Microsoft released its monthly Patch Tuesday round of patches for October, closing several critical vulnerabilities including the SandWorm vulnerability and others exploited by attackers. Source: http://www.net-security.org/secworld.php?id=17498

October 15, Softpedia – (International) **Flash Player 15 update plugs remote code execution bugs.** Adobe released patches for three critical vulnerabilities in its Flash Player consisting of two memory corruption issues and one integer overflow vulnerability. Source: http://news.softpedia.com/news/Flash-Player-15-Update-Plugs-Remote-Code-Execution-Bugs-462158.shtml

October 15, Softpedia – (International) **Mozilla fixes critical bugs in Firefox 33.** Mozilla released the latest version of its Firefox browser, closing 33 critical vulnerabilities and adding improved functionality. Source: http://news.softpedia.com/news/Mozilla-Fixes-Critical-Bugs-in-Firefox-33-462211.shtml

October 15, Softpedia – (International) **SSL 3.0 falls in the face of POODLE attack, needs to be disabled.** Researchers with Google designed an attack named POODLE that can exploit a flaw in the design of the Secure Sockets Layer 3.0 (SSL 3.0) protocol that can allow the extraction of data from secure connections using the protocol. SSL 3.0 has been superseded by several other protocols but is still used in some clients and servers and as a backup protocol by Web browsers if modern protocols are unavailable. Source: http://news.softpedia.com/news/SSL-3-0-Falls-In-Face-of-POODLE-Attack-Needs-To-Be-Disabled-462136.shtml

October 14, Softpedia – (International) **Malware-like browser pop-ups used by advertisers to push apps on Android.** A researcher at Malwarebytes reported that some advertisers are using fake warning or update notifications directed at Android users in an attempt to get them to download legitimate but potentially unwanted programs in an affiliate marketing scheme. Source: http://news.softpedia.com/news/Malware-Like-Browser-Pop-Ups-Used-By-Advertisers-to-Push-Apps-On-Android-462103.shtml

October 14, Threatpost – (International) **BlackBerry 10 devices open to bug that allows malicious app installation.** BlackBerry released a patch for a vulnerability in BlackBerry 10 devices that could allow an attacker with a man-in-the-middle position to replace legitimate apps downloaded through the BlackBerry World app store with malicious apps. Source: http://threatpost.com/blackberry-10-devices-open-to-bug-that-allows-malicious-app-installation/108830

October 14, Help Net Security – (International) **Malicious YouTube ads lead to exploits, ransomware.** Trend Micro researchers identified and reported a malvertising campaign where attackers appeared to have bought traffic from legitimate ad providers in order to place malicious ads on popular YouTube videos to redirect users through several sites to a server hosting the Sweet Orange exploit kit. The exploit kit then attempts to infect users with the Kovter ransomware via an Internet Explorer vulnerability. Source: http://www.net-security.org/malware_news.php?id=2883

Average company now compromised every four days, with no end to the cybercrime wave in sight
ZD Net, 16 Oct 2014: The cost and regularity of digital attacks against business continue to rise steadily, with no obvious end to the assault on the horizon. The average cost of cybercrime to business, as reported by a sample population of 257 organizations, is $7.6m per year. Actual costs range from $500,000 to $61m per company — a rise of 10 percent rise on last year's survey. The 257 companies canvassed by HP said they had experienced 429 "discernible cyber attacks", which equates to 1.7 successful attacks per company per week, on average. Some attacks are easier to perform (but less painful) than others: over a four-week period, virtually all organizations experienced attacks relating to viruses, worms and/or Trojans and malware. More than half — 59 percent — suffered botnet attacks, while just under half complained of stolen devices. Only 35 percent of companies reported that a malicious insider was the source of the cybercrime. Types of cybercrime experienced by respondents, according to the HP/Ponemon Institute survey:

- Viruses, worms, Trojans: 98 percent
- Malware: 97 percent
- Botnets: 59 percent
- Web based attacks: 58 percent
- Phishing: 52 percent
- Malicious code: 51 percent
- Denial of service: 49 percent
- Stolen devices: 49 percent
- Malicious insiders: 35 percent

But those malicious insiders were also the most costly type of attack — costing $213,542 on average. Denial-of-service attacks cost $166,545, while web-based attacks cost $116,424 to clear up. Business disruption, followed by loss of data, and then revenue lost account for the vast majority — 94 percent — of the cost of a cyber attack. The report is keen to point out that smart tools like intrusion prevention systems and network intelligence systems can help cut the cost of such attacks, but the reality is that cybercrime cannot be solved by hardware and software. A bigger problem is that, for now, many cybercriminals remain untouchable: most live far from the companies they are attacking, which means that police are unlikely to have any way of arresting them — even if they had the skills to discover the culprits in the first place. Around 85 percent of the cases dealt with by the European Cybercrime Centre involve Russian-speaking organised crime groups, for example, but getting cooperation across border is rarely straightforward. To read more click **HERE**

Easily exploitable Drupal bug can lead to total site compromise

Heise Security, 16 Oct 2014: Admins of sites that run Drupal 7 are advised to update to the latest version of the platform - version 7.32 - because it fixes a critical SQL injection vulnerability that can ultimately lead to site hijacking and data theft. Urgency is needed as the vulnerability in question is easy to exploit and because proof of concept exploits have already been made public. "While we do not have reports of actual usage, the nature of this vulnerability is such that the attack can be difficult to detect," the Drupal security team warned. Ironically enough, the bug has been found in the database abstraction API that is used to ensure that queries executed against the database are sanitized to prevent SQL injection attacks. "A vulnerability in this API allows an attacker to send specially crafted requests resulting in arbitrary SQL execution. Depending on the content of the requests this can lead to privilege escalation, arbitrary PHP execution, or other attacks," they explained in the security advisory, and added that the vulnerability can be exploited remotely, without any kind of authentication required. The vulnerability was discovered and flagged a month ago by Stefan Horst, a researcher with German PHP security firm Sektion Eins, which was hired to audit Drupal by a customer. But, according to Robert Horton, European managing director of security consulting at NCC Group, the flaw was discovered and "was independently sitting in the public domain in Drupal's public bug tracking database since November 2013. To read more click **HERE**

How to Fix KB2952664 Installation Error 80242016 on Windows 7?

SoftPedia, 16 Oct 2014: KB2952664 is a Windows 7 update that was first released by Microsoft in April this year, but revised for this month's Patch Tuesday and delivered to all computers running this particular OS version. The only problem, however, is that on some PCs, the KB2952664 is causing quite a lot of trouble, mostly because it fails to install with an error code that says basically nothing about the thing that went wrong. Users who encountered this error said that KB2952664 installation failed with code 80242016, which in most cases means that installation couldn't be completed because another installation was in progress. From what we've heard until now, it appears that KB2952664 installation fails after copying some files on the target computer, so the best way to deal with it is to uninstall all files and try to get it one more time. To do this, navigate to the following path: "?codeControl Panel\Programs & Features\View installed updates" Once you're there, search for KB2952664, right-click it and hit the "Uninstall" option. Windows should automatically remove all of its files in a second. After that, search for new updates once again, and the KB2952664 should show up on your computer, with the installation process to be performed correctly this time. There's one major issue, however: we're receiving reports from some users that the KB2952664 patch fails to install from the very beginning, so the "Uninstall" option won't be available. In this case, a Fix it solution from Microsoft to clean your computer and make the update available in Windows Update is clearly required, but the company hasn't yet provided any statements on this. Fortunately for those who have already deployed a newer Windows version on their computers, Windows 7 is the only OS build that's affected by this issue because the KB2952664 patch is only delivered to PCs running it. To read more click **HERE**

FBI Calls for Help Catching Cyber Offenders

Heise Security, 16 Oct 2014: The FBI has resorted to publicizing a list of cybercriminals who have been indicted for cyber offenses ranging from identity theft, computer fraud, hacking and wire fraud to distribution and creation of malware. After compiling information in their database, the Bureau created the Cyber's Most Wanted section on the public website. Members of the Chinese People's Liberation Army included on the list First on the list is John Gordon Baden, a monetary reward of $5,000 / €4,000 being offered for information leading to his capture. This is not the largest bounty offered by the FBI, as the reward in the case of other individuals reaches $50,000 / €39,000. Evgeniy Bogachev, the individual indicted for the creation of the Zeus botnet that stole financial information from victimized computers, is second on the list. The next three places are occupied by members of the Chinese People's Liberation Army (PLA) activating in Unit 61398, an advanced persistent threat (APT) division believed to be behind multiple cyber-espionage activities against organizations around the world. Each of the PLA members (Sun Kailiang, Huang Zhenyu and Wen Xinyu) has been indicted for 31 criminal counts, economic

espionage and theft of trade secrets being among them. As per the FBI's summary of the offenses, "each provided his individual expertise to an alleged conspiracy to penetrate the computer networks of six American companies while those companies were engaged in negotiations or joint ventures or were pursuing legal action with, or against, state-owned enterprises in China." The list of the most wanted cyber offenders continues with individuals involved in selling fraudulent software in more than 60 countries (Bjorn Daniel Sundin and Shaileshkumar P. Jain) or in breaking into the accounts of a major investment services company (Alexandr Sergeyevich Bobnev). Reports of cyber-attacks hailing from China increase In recent news, multiple security firms joined forces to crack down on a cyber-espionage group believed to operate out of China for at least four years. Working under the name Operation SMN, the companies used collective intelligence to connect the dots between various attacks orchestrated by a group Symantec calls Hidden Lynx. They uncovered a set of backdoor and Trojan programs that were used to penetrate the defenses of public infrastructure providers and government organizations in the US and Asia. The malware was also employed for lateral movement across the network and for exfiltrating sensitive information. Despite the fact that only private companies were involved in the project, the FBI was probably provided information about methodology and tools used by the group. As a result, the Bureau sent a warning on Wednesday to different companies about cyber-attacks believed to originate from China. According to Reuters, the alert included descriptions of the tools and methods employed by the attackers to reach their goal. The news agency obtained a copy of the document which included details about "a group of Chinese government affiliated cyber actors who routinely steal high-value information from U.S. commercial and government networks through cyber espionage." To read more click **HERE**

FBI Director Says: Chinese Hackers Are Not That Good, "They're Just Prolific

Softpedia, 16 Oct 2014: The director of the Federal Bureau of Investigation, James Comey, said that the success of Chinese hackers isn't owed to their skills but to the frequency of their attacks. In an interview on 60 Minutes, among the topics touched were that of hackers and the nations initiating attacks against the US. The director would not disclose a top five of the states attacking the US online, but placed China at the top of the list, saying that its hackers would steal anything that could take the stress of inventing new technology off their shoulders. "There are two kinds of big companies in the United States: there those that have been hacked by the Chinese and those who don't know they've been hacked by the Chinese," Comey said during the interview. However, this is not because they are adept cyber intruders but because they are so prolific in their attacks; "their strategy seems to be 'we'll just be everywhere, all the time', and there's no way they can stop us," he added, likening them to a "drunk burglar" carrying out a loud intrusion and leaving all sorts of clues behind. Referring to the assets coveted by the Chinese intruders, Comey said that they would take "information that is useful to them so that they don't have to invent," and anything "they can copy or steal." The financial loss generated by these incidents cannot be quantified, but billions of dollars are being spent to deal with them. Although great progress has been made in the past years, Comey admits that the FBI still has some steps to take in order to become better at fighting cyber threats. He compared the good guys and the bad guys with soccer teams playing in different leagues. "We're about high school soccer now; we've spread out, we pass well, but the bad guys are moving at World Cup speed, so we have to get better." Reducing the amount of crime online is not a business just for authorities, as users can also protect against cyber-attacks by paying more attention to emails carrying attachments coming from unknown persons. Although China is named top cyber-attacker, recent news shows that Russia may also be involved in events targeting important corporations in America. To read more click **HERE**

Security Firms Form Coalition to Crack Down on Cyber Espionage Group

Softpedia, 15 Oct 2014: A group of security vendors joined forces to combat malware used by a group of hackers linked to various cyber-espionage campaigns for at least four years. The adversary is a China-based team of hackers believed to consist of up to 100 operatives that seem to engage in on-demand attacks. They are referred to by Symantec as "Hidden Lynx," and security researchers say they are well-resourced and that they are one of the first groups to use the "watering hole" attack method to spread

malicious software to their targets. This is the first initiative of this kind against an APT (advanced persistent threat) group, and it included intelligence from Cisco, FireEye, F-Secure, iSIGHT Partners, Microsoft, Tenable, ThreatConnect, ThreatTrack Security, Volexity, Novetta, and Symantec. Dubbed Operation SMN, the action was coordinated by Novetta, a company offering advanced analytics technology solutions, under Microsoft's Coordinated Malware Eradication program. Worth noting is that all the members of the coalition are from the private sector and most of them are competitors for customers; however, they agreed to share intelligence about the malicious tools used by Hidden Lynx to infiltrate organizations. As such, this initiative is a step forward from individual threat reporting and towards a centralized system to identify threat actors involved in espionage campaigns. APT group relies on multiple tools and techniques to achieve their goal Hidden Lynx's main goal seems to be maintaining a foothold into the network of the target, looking for ways to infiltrate deeper without triggering detection mechanisms. According to Novetta, the targets range from large public network infrastructure providers to holders of extensive IP portfolios, and government entities from various countries in Asia and the United States. Researchers observed that apart from malicious software, Hidden Lynx often resorts to compromising the security of the supply chain for the targeted organization in order to work their way into the network. Novetta refers to the threat actors by the name "Axiom," and says that they rely on "compromised mid-point infrastructure within Korea, Taiwan, Japan, Hong Kong and the United States to conduct exploitation operations." The threat group is capable of gaining privilege escalation, moving laterally on the network, and using custom backdoors. During Operation SMN, the group has been observed to target and exploit human resource management agencies, individuals in law enforcement organizations, media agencies in the US, Europe and Japan, international law firms, and a Ministry of Finance. All these have been targeted since September 2013. A comprehensive report regarding the activities of Operation SMN is scheduled to be released towards the end of the month, on October 28. To read more click **HERE**

Month-Long Breach Targeted Card Data of Kmart Customers

Softpedia, 13 Oct 2014: The IT team from Kmart discount store identified on Thursday an intrusion on its payment data system that lasted since early September. An investigation was immediately initiated in order to learn the extent of the attack and the customer information that was affected. The company was quick at disclosing the breach, as the announcement about the compromise came a day after learning about it, on Friday. Owned by Sears Holdings Corp., Kmart is among the largest discount store chains in the world, with at least 1,200 locations, as of February 2013. The brand also exists in Australia and New Zealand, although there no longer is a relation with the American counterpart since the 70s. According to the results of the investigation, social security numbers, PIN codes or email addresses have not fallen in the hands of the attackers, and only the "track 2" card data of in-store shoppers was swiped by the cybercriminals. The stolen information, which includes card numbers, allows cloning of the cards and making online purchases. According to the official Kmart announcement about the breach, "Kmart store payment data systems were infected with a form of malware that was undetectable by current anti-virus systems." The company informed that the threat was removed from their payment systems and transactions should be carried out securely at the moment. There are no details on the security solution used or the type of malware responsible for extracting the data, but a healthy way to prevent such events would be to learn from the mistakes of others. Recent news covered data breach events affecting customers of major retailers, most of them hit by the Backoff POS malware. Last week, Dairy Queen confirmed that this threat was present on the payment systems of almost 400 franchised stores. The company received alerts about a possible breach back in August, and in the case of some of the stores, the intrusion lasted until October 6. In early September, Home Depot discovered malware infiltrated in their payment systems, and in the wake of the investigation, a startling number of unique cards impacted was revealed: about 56 million. To read more click **HERE**

Cyber Espionage Group Exploits New Windows Zero-Day to Get Elevated Privileges

Softpedia, 14 Oct 2014: A cyber espionage group known as Hurricane Panda has taken advantage of a zero-day vulnerability in Windows that gave them administrative privileges on the affected systems. The group is believed to be from China and targets infrastructure companies. Multiple vulnerabilities have been exploited in their attacks, the most severe of them, a previously unknown security glitch now identified as CVE-2014-4113, being leveraged to infect 64-bit Windows platforms in order to gain a foothold in the network of the target. CVE-2014-4113 affects all Windows operating systems from Windows 2000 through Windows 7, and exploiting it allows elevated privileges when the objects in memory are not handled correctly by the Windows kernel-mode driver (Win32k.sys); this could lead to remote execution of arbitrary code in kernel mode. CrowdStrike, one of the two companies working with Microsoft to prepare a patch for Windows users, says that they found the Hurricane Panda attack when one of their systems picked up suspicious activity on a 64-bit Windows Server 2008 R2 machine. Further exploration of the matter led to the discovery of Win64.exe, which was used from a webshell to elevate privileges for a command that added a new administrator account to the local group of the targeted machine. "Subsequent analysis of the Win64.exe binary revealed that it exploits a previously unknown vulnerability to elevate its privileges to those of the SYSTEM user and then create a new process with these access rights to run the command that was passed as argument," CrowdStrike co-founder and CTO, Dmitri Alpetrovich writes in a blog post. At 55 kilobytes, the item is very small and contains a limited set of functions that allow it to execute a command as new process with system privileges. The steps it goes through to achieve this include creating a memory section for storing a pointer to a function, profiting from a memory corruption vulnerability in the window manager, and replacing the access token pointer in the EPROCESS structure with one in the system process. Attackers took advantage of the vulnerability for at least five months If Hurricane Panda is a Chinese group, then they are a very different adversary than the one described by FBI director James Comey recently. Alpetrovich notes that "the exploit code is extremely well and efficiently written, and it is 100 percent reliable." Moreover, the threat actors went to great lengths to make sure that it was not easy to discover, deploying the malicious tool only when it was required. The result was an exploitation duration of at least five months, according to CrowdStrike, since the build timestamp of the Win64 executable was May 3, 2014. The vulnerability was privately reported to Microsoft by both CrowdStrike and FireEye, who conducted a separate study of the attack. A patch for it is available as part of the monthly security updates released by Microsoft on Tuesday. Important to note is that this vulnerability is different than the one reported earlier by iSight Partners (link), which is tracked as CVE-2014-4114 and was leveraged by a Russian cyber-espionage group that has been dubbed Sandworm for the many references to the science fiction series Dune. To read more click **HERE**