THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

12 November 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

Microsoft patches critical bug that affects every Windows version since 95
TheVerge, 12 Nov 2014: Microsoft has patched a critical flaw in Windows that has existed in every version since the introduction of Windows 95 more than 19 years ago. IBM security researchers discovered the flaw earlier this year and notified the software giant privately in May. The rare bug allows attackers to remotely execute code on an affected system just by convincing Windows users to visit a URL in Internet Explorer. IBM says the exploit can be triggered on Internet Explorer 3.0 onwards, and every currently supported version of Windows is affected. "This vulnerability has been sitting in plain sight for a long time despite many other bugs being discovered and patched in the same Windows library," says IBM researcher Robert Freeman. While Microsoft is providing patches for Windows 8.1, Windows 7, Windows Vista, and its various server releases, the company stopped supporting Windows XP earlier this year so consumers will not be protected if attackers attempt to exploit the bug. There's no evidence this bug is being exploited in the wild yet, but it has been rated 9.3 out of 10 on the Common Vulnerability Scoring System (CVSS) so it's well worth patching through Windows Update if you haven't already. To read more click **HERE**

November 10, Reuters – (National) **U.S. Postal Service says data breach hits employees, call center.** The U.S. Postal Service (USPS) announced November 10 that the personal information, including Social Security numbers, of more than 800,000 employees and customers who called the Postal Service Customer Care Center between January and August 16 was potentially accessed in a cyberattack. The USPS is investigating and reported that the intrusion is limited in scope and operations are functioning normally. Source: http://www.reuters.com/article/2014/11/10/us-cybersecurity-usps-idUSKCN0IU1P420141110

November 7, Securityweek – (North Carolina) **N.C. dermatology center discovers hacked server two years after attack.** Central Dermatology Center in Chapel Hill announced November 7 that one of its servers was breached and compromised by malware in August 2012. The health center discovered the breach September 25 and continues to investigate the attack in order to determine what information was compromised, which could include patients' personal and medical information. Source: http://www.securityweek.com/nc-dermatology-center-discovers-hacked-server-two-years-after-attack

November 8, Associated Press – (Wyoming) **Hackers breach Wyoming library system.** Officials announced November 7 that the Statewide online catalog of the Wyoming State Library was taken offline for 2 days for remediation after authorities learned the system was breached October 7 by unknown hackers. The attack was discovered after unusual activity was detected on the system and there is no indication that personal data was compromised. Source: http://www.kansas.com/news/business/article3661611.html

November 10, Securityweek – (International) **Darkhotel attackers target business travelers via hotel networks.** Kaspersky Lab researchers identified an advanced persistent threat (APT) group dubbed Darkhotel APT that has targeted travelers in the Asia-Pacific region in addition to the U.S. using malicious hotel WiFi networks, spear phishing, and malicious torrent files. The group's hotel attacks involve prompting users with a software update notice that installs a backdoor, and the group has targeted guests associated with industries and sectors including government organizations, the defense industry, energy industry, pharmaceutical industry, electronics manufacturers, medical providers, and non-governmental organizations. Source: http://www.securityweek.com/darkhotel-attackers-target-business-travelers-hotel-networks

November 10, The Register – (International) **BrowserStack HACK ATTACK: Service still suspended after rogue email.** Browser testing service BrowserStack stated that it was temporarily suspending service to recover after an attacker managed to gain access to a list of email addresses and the company's official email account, using it to send out a fake message to developers. Source: http://www.theregister.co.uk/2014/11/10/browserstack_hack_attack_service_still_suspended_after_rogue_email/

November 10, The Register – (International) **Emoticons blast three security holes in Pidgin.** Researchers at Cisco reported that the instant messaging client Pidgin contained three security vulnerabilities that could have allowed attackers to overwrite files or cause a denial of service (DoS) situation. The vulnerabilities have since been patched. Source: http://www.theregister.co.uk/2014/11/10/cisco_security_bods_hunt_pidgin/

Critical Flaw in Secure Channel Package Affects All Windows Versions
Softpedia, 12 Nov 2014: The latest set of monthly updates from Microsoft includes a patch for a privately disclosed security vulnerability in the Security Channel (schannel) component of Windows, impacting all current versions of the operating system. Schannel is responsible for implementing the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) authentication protocols used for encrypted communication between a client and a server over the web. If exploited, the vulnerability, which is now identified as CVE-2014-6321, offers the possibility of remote execution of arbitrary code on the affected machine. The glitch consists in failure to properly filter specially-crafted packets in malicious traffic intended for a Windows server. Workstation systems are also impacted by the flaw because they can run server software that listens to specific ports and accepts connections from different clients. In a security bulletin from Microsoft, it is stated that no workarounds are available for mitigating the problem, applying the update being the only solution to fix the issue. No evidence of attacks in the wild leveraging the flaw Apart from solving this problem, the company also included new TLS cipher suites that would secure customer information with stronger encryption. "These new cipher suites all operate in Galois/counter mode (GCM), and two of them offer perfect forward secrecy (PFS) by using DHE key exchange together with RSA authentication," the bulletin informs. Perfect forward secrecy (PFS) is a feature in public-key cryptography that ensures the safety of a session key in the event of having a private key compromised. All versions of Windows, Server 2003 through Windows 8.1, both 32-bit and 64-bit versions – RT included, are susceptible to attacks based on exploiting CVE-2014-6321. At the moment, there is no evidence pointing at the flaw being leveraged in the wild, but the public bug disclosure on Tuesday may result in an effort from cybercriminals to create an exploit and start scanning for vulnerable machines. Crooks are quick at creating exploits for recently uncovered weaknesses Last month, a week after Adobe released a security update for Flash Player, exploits for two of the glitches were incorporated into browser-based crimeware Angler and Fiesta. This goes to show that cybercriminals are quick at taking advantage of serious security weaknesses, as they are ready to invest the necessary resources to reverse engineer the patches and come up with a way to compromise vulnerable machines. The Schannel flaw fix is part of the November round of updates from Microsoft, which included no less than 16 security bulletins for different Windows components and products. To read more click **HERE**

18 Critical Vulnerabilities Patched in Flash Player 15.0.0.223

Softpedia, 12 Nov 2014: The latest revision of Adobe Flash Player incorporates a set of 18 security fixes, all for critical vulnerabilities; most of them (15) would allow a potential attacker to execute arbitrary code on the affected machine. Previous versions of the software are susceptible to glitches ranging from memory corruption, use-after-free and heap buffer overflow to double free, information disclosure and permission issues. Exploiting some of them would give an attacker the possibility to gain elevated privileges or access to session tokens. According to the security bulletin from Adobe, in the case of two weaknesses (CVE-2014-8442 and CVE-2014-0583), malicious actors could increase their privileges on the impacted system from low to medium integrity level. Their discovery has been attributed to Haifei Li of McAfee Labs IPS Team (CVE-2014-0583) and researchers Behrang Fouladi and Axel Souchet of Microsoft Vulnerability Research. Other contributors to the increased security of the latest Flash Player are from Google's Project Zero (Ian Beer, Natalie Silvanovich, Tavis Ormandy and Chris Evans), Venustech ADLAB, TrendMicro, and Chinese company KnowSec. The browser plug-in is updated automatically in Google Chrome, where it is synonymous with a version bump. The same can be said in the case of Internet Explorer, which receives the update through the built-in mechanism in Windows. The desktop release can also be updated automatically if the feature has been turned on in the client. To read more click **HERE**

New DNS Amplification Attacks Use Text from White House Press Release

SoftPedia, 12 Nov 2014: Cybercriminals have started a new trend for conducting distributed denial-of-service (DDoS) attacks and rely on a type of DNS (Domain Name System) amplification that leverages text records for making the operation more effective; in some campaigns, parts of a press release from the White House have been observed by researchers. The tactic is not new, but more and more incidents of this sort have been recorded by the PLXsert (Prolexic Security Engineering and Research Team) of Akamai, which observed it in an October 4 incident. "Attackers have used large TXT records in reflection attacks in the past. Previous victims of DNS amplification attacks using TXT records include sites such as isc.org and many .gov sites. With this new threat, malicious actors are now crafting the TXT records to provide the largest response size possible, thereby having as much impact as possible," a report from the researchers informs. A DDoS attack is designed to bring a service down by delivering a large amount of requests to its server. When the information can no longer be processed, the machine can no longer do its job. According to PLXsert, the most targeted entities are from the entertainment (75%), education (12.5%), and high tech consulting (12.5%) sectors. The snippets of the official text originate from the guessinfosys.com domain, and are used in what is called a DDoS reflected attack. Cybercriminals often use intermediate victims to reflect the bad traffic to their target. Largest incident lasted for more than 15 hours In the observed incidents, the systems from PLXsert revealed that DDoS attacks leveraging the DNS TXT amplification technique was involved in longer-lasting events (more than five hours), with the most serious such event peaking at over 15 hours. The statistics gathered from the incidents show that the source port used for the attacks is 53, while the targeted one is 80, but it can also be a random one. A DNS amplified DDoS incident relies on sending a request to a server from the spoofed IP address of the victim. Thus, when the server returns the response, which is larger than the initial request, the packets are sent to the victim, causing a denial-of-service condition. It appears that the peak bandwidth was recorded by PLXsert at 4.3 Gbps. Researchers say that using an access control list (ACL) should be a good form of defense, but only if there is more bandwidth than the attack can generate. To read more click **HERE**

Crooks Still Scan for Shellshock Vulnerable Machines, over 630,000 Incidents in 2 weeks

Softpedia, 11 Nov 2014: Almost one and a half month since its publishing, the Shellshock vulnerability in Bash, the default command line interpreter in Linux, has become mainstream, with scans in excess of 630,000 being recorded in the wild in a period of just two weeks. The incidents originate from more than 15,000 IP addresses across the world (more than 95% being malicious requests), showing an exponential increase in the number of attackers compared to the early days of the disclosure, when over 890 IPs carried out attacks, as per Incapsula's reports. According to the statistics from the company, its systems

were hit at the beginning at a rate of 1,970 attacks per hour, although some of them were the result of legitimate scanning tools. Over one month after the initial incidents, the attack rate has not come down too much, over 1,870 being carried out. However, the difference consists in the fact that the amount of IP addresses deploying them has increased incredibly, by more than 1,600%. This means that the crooks are scanning the Internet systematically in search of vulnerable machines that can be used for malicious activities. One would think that, after all this time, most of the machines have been immunized against Shellshock; but not all systems online are taken care of on a regular basis, leaving them susceptible to attacks. More than this, the initial patch for Shellshock did not mitigate the issue completely and the risk still existed. "The media may have moved on, but the hackers haven't. Shellshock remains an extremely dangerous vulnerability, having the ability to cause direct damage to unprotected devices, in addition to downstream collateral damage to others (e.g., as the result of a subsequent DDoS botnet attack)," Ofer Gayer and Igal Zeifman say in a blog post. Any machine is an asset for cybercriminals, no matter how old it is, as the simple fact that it is connected to the Internet is enough for initiating or spreading an attack. The attacks leveraging the Shellshock bug differ in purpose and in many cases the goal was to enslave the systems into a botnet; subsequent uses of the botnet range from launching distributed denial-of-service (DDoS) attacks to spreading malware. Servers were among the most targeted because an attack on them requires less resources and the effect is the delivery of malware to visiting customers. NAS devices were also in the crosshair because of the slew of files they store. Attackers could use the bug to plant crimeware with encryption capabilities in order to get a ransom fee in exchange for the decryption key. To read more click **HERE**