THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

16 September 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

September 15, Help Net Security – (International) **Dragonfly malware targeting pharmaceutical companies.** Belden and RedHat Cyber researchers determined the Dragonfly (Havrex) malware is likely targeting pharmaceutical companies after findings uncovered that the malware contained an Industrial Protocol Scanner module that searched for devices often found in consumer packaged goods industries and that the Dragonfly attack is similar in nature to the Epic Turla campaign, among other findings. Source: http://www.net-security.org/malware_news.php?id=2865

September 12, Tampa Bay Business Journal – (Florida) **TGH fires worker accused in data breach.** Personal and health information for 675 Tampa General Hospital patients were accessed without authorization by a former employee between October 2011 and August 2014, the Florida hospital announced September 12. The patients were notified and the employee was terminated. Source: http://www.bizjournals.com/tampabay/news/2014/09/12/tgh-fires-worker-accused-in-data-breach.html

September 15, Help Net Security – (International) **Freenode suffers breach, asks users to change their passwords.** IRC network Freenode notified users that it experienced a security breach September 13 and advised all users to change their passwords as a precaution. Source: http://www.net-security.org/secworld.php?id=17362

September 15, Securityweek – (International) **Vulnerabilities found in website of Google-owned Nest.** A security researcher identified and reported several security vulnerabilities in the Web site of home automation company Nest, including a file upload vulnerability that could allow attackers to upload a shell and gain access to personal and financial details of Nest customers. Google stated that the issue was addressed by restricting access to the affected domain and redirecting visitors to a different domain. Source: http://www.securityweek.com/vulnerabilities-found-website-google-owned-nest

September 12, Threatpost – (International) **Four vulnerabilities patched in IntegraXor SCADA.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an advisory September 11 advising users of Ecava Sdn Bhd's IntegraXor supervisory control and data acquisition (SCADA) server software to patch their systems after four remotely exploitable vulnerabilities were discovered. The software is primarily used for industrial automation in firms managing railways, sewage systems, telecommunications, and heavy engineering. Source: http://threatpost.com/four-vulnerabilities-patched-in-integraxor-scada-server

75% of mobile apps will fail basic security tests

Heise Security, 15 Sep 2014: Through 2015, more than 75 percent of mobile applications will fail basic security tests, according to Gartner. Enterprise employees download from app stores and use mobile applications that can access enterprise assets or perform business functions, and these applications have little or no security assurances. These applications are exposed to attacks and violations of enterprise security policies. "Enterprises that embrace mobile computing and BYOD strategies are vulnerable to security breaches unless they adopt methods and technologies for mobile application security testing and risk assurance," said

Dionisio Zumerle, principal research analyst at Gartner. “Most enterprises are inexperienced in mobile application security. Even when application security testing is undertaken, it is often done casually by developers who are mostly concerned with the functionality of applications, not their security.” Mr. Zumerle said that existing static application security testing (SAST) and dynamic application security testing (DAST) vendors will modify and adjust these technologies to address mobile application cases and meet mobile application security testing challenges. Although SAST and DAST have been used for the past six to eight years and have become reasonably mature, mobile testing is a new space, even for these technologies. In addition to SAST and DAST, a new type of test, behavioral analysis, is emerging for mobile applications. The testing technology monitors a running application to detect malicious and/or risky behavior exhibited by an application in the background (e.g., when an audio player application plays music — at the same time, it also accesses a user's contact list or geolocation, and initiates data transmission to some external IP address). Testing the client layer — the code and GUI — of the mobile application that runs on the mobile device is not enough. The server layer should be tested as well. Mobile clients communicate with servers to access an enterprise's applications and databases. Failure to protect a server poses the risk of losing the data of hundreds of thousands of users from the enterprise's databases. Code and user interfaces of these server-side applications should therefore be tested with SAST and DAST technologies. “Today, more than 90 percent of enterprises use third-party commercial applications for their mobile BYOD strategies, and this is where current major application security testing efforts should be applied,” said Mr Zumerle. “App stores are filled with applications that mostly prove their advertised usefulness. Nevertheless, enterprises and individuals should not use them without paying attention to their security. They should download and use only those applications that have successfully passed security tests conducted by specialized application security testing vendors.” Gartner predicts that by 2017, the focus of endpoint breaches will shift to tablets and smartphones – already there are three attacks to mobile devices for every attack to a desktop. The security features that mobile devices offer today will not suffice to keep breaches to a minimum. Gartner recommends that enterprises focus on data protection on mobile devices through usable and efficient solutions, such as application containment (via wrapping, software development kits or hardening). To read more click HERE

Hacker exploits printer Web interface to install, run Doom

ARS Technica, 15 Sep 2014: On Friday, a hacker presenting at the 44CON Information Security Conference in London picked at the vulnerability of Web-accessible devices and demonstrated how to run unsigned code on a Canon printer via its default Web interface. After describing the device's encryption as "doomed," Context Information Security consultant Michael Jordon made his point by installing and running the first-person shooting classic Doom on a stock Canon Pixma MG6450. Sure enough, the printer's tiny menu screen can render a choppy and discolored but playable version of id Software's 1993 hit, the result of Jordon discovering that Pixma printers' Web interfaces didn't require any authentication to access. "You could print out hundreds of test pages and use up all the ink and paper, so what?" Jordon wrote at Context's blog report about the discovery, but after a little more sniffing, he found that the devices could also easily be redirected to accept any code as legitimate firmware. A vulnerable Pixma printer's Web interface allows users to change the Web proxy settings and the DNS server. From there, an enterprising hacker can crack the device's encryption in eight steps, the final of which includes unsigned, plain-text firmware files. The hacking possibilities go far beyond enabling choppy, early '90s gaming: "We can therefore create our own custom firmware and update anyone’s printer with a Trojan image which spies on the documents being printed or is used as a gateway into their network," Jordon wrote. It's a solid reminder that the most seemingly innocent devices in a home or work network can become gateways to all matter of exploits, beyond the ones publicly disclosed at hacking conferences. Years ago, for example, a series of Hewlett-Packard printers were subject to their own remote-access hack, though HP denied the researchers' assertion that it could be used to set printers on fire. The Canon exploit, meanwhile, could reach far and wide if affected users don't pay attention to upcoming firmware updates to fix the issue. Shortly before the exploit became public, Context scanned the Internet for vulnerable Pixma printers whose Web interfaces could be accessed. The group was able to log into six percent of them; by that estimate, "at least 2,000 vulnerable models" are sitting online as we speak, ready to receive Doom (or something scarier). Jordon's post goes into less detail about the version of Doom he got running on Pixma printers; in an interview with the BBC, he clarified that the printer had a 32-bit ARM processor and 10 MB of memory, but modifying the ARM version of Doom to work required months of his spare time. As a result, he told the BBC he was "so sick of" working on the game port and would not further optimize it (sorry, printer gamers!). Context reached out to Canon after discovering the exploit in March of this year, and the companies have been in active conversations since then. Immediately after the presentation, Canon issued a statement indicating that all affected Pixma models in the wild will receive a firmware update to add a login prompt. In the meantime, Context suggests users "not put your wireless printers on the Internet, nor any other 'Internet of Things' device." The security company isn't aware of any active exploits aimed at printers, "but hopefully we can increase the security of these types of devices before the bad guys start to." To read more click HERE

Protecting Servers from Remote Attacks

GovInfo Security, 16 Sep 2014: When IBM unveiled BIOS - Basic Input/Output System - in 1981 with the introduction of its personal computer, few perceived it as a security vulnerability. Fast-forward more than three decades, and security researchers have identified vulnerabilities to servers posed by BIOS. So the National Institute of Standards and Technologies has published new guidance to mitigate the threat. NIST's Special Publication 800-147B: BIOS Protection Guidelines for Servers (LINK) is aimed at mitigating unauthorized modification of BIOS firmware by malware. Corrupting BIOS is seen as a significant threat because of its privileged position on the computer architecture. The protections offered in the guidance are designed to help mitigate remote attacks but wouldn't necessarily stop dedicated attackers who try to tamper with BIOS in systems they have "unfettered physical access to," says Andrew Regenscheid, a NIST mathematician who authored the guidance. "In practice, depending on how the manufacturer implements BIOS protections, these mechanisms would provide some protection against certain attacks," he says, "but wouldn't necessarily stop an attacker willing and able to pull and replace chips on the motherboard." BIOS is a de facto standard defining a firmware interface built into IBM-compatible PCs and servers; it's the first software run when a computer based on IBM PC technology is turned on. Essentially, BIOS initializes and tests the system hardware components and boots up the operating system from mass memory. "Historically, BIOS has not been the primary target of attackers; however, in recent years we've seen more activity focusing on lower-level attacks," Regenscheid says. As the security of operating systems improved, Regenscheid says attackers began looking for entry into systems by going lower in the computer systems stack, creating what some cybersecurity researchers have coined as "a race to bare metal" between attackers and security professionals, with each group trying to gain or maintain control of the system before the other side does. "You can't really get any closer to bare metal than the BIOS," he says. Regenscheid provides a brief history of BIOS vulnerabilities: In the late 1990s, malware known as the CIH virus attempted to erase BIOS on infected systems. When successful, the computer would not start. In 2011, the Mebromi rootkit attempted to insert malware in the BIOS that would continue to re-infect systems, even after clearing the malicious code with anti-virus software, reinstalling the operating system or replacing the hard drive. "Storing the malicious code inside the BIOS ROM could actually become more than just a problem for security software, given the fact that even if an anti-virus detects and cleans the MBR infection, it will be restored at the next system startup when the malicious BIOS payload would overwrite the MBR code again," ethical hacker Marco Giuliani wrote in 2011, when he was a threat research analyst at Webroot Software. MBR, or master boot record, is a special type of boot sector at the very beginning of partitioned computer mass storage devices, such as fixed disks or removable drives, intended for use with IBM PC-compatible systems "Developing an anti-virus utility able to clean the BIOS code is a challenge, because it needs to be totally error-proof, to avoid rendering the system unbootable at all," Giuliani said. This isn't NIST's first guidance regarding BIOS. In 2011, NIST issued SP 800-147, BIOS Protection Guidelines (LINK), primarily aimed at desktops and laptops, not servers. To read more click HERE

Malicious Kindle Ebooks Can Give Hackers Access to Your Amazon Account

SoftPedia, 16 Sep 2014: There’s an ever-growing feud between book lovers – the choice between paper and electronic seems to split people into groups. These days, however, you should probably be a little more careful if you’ve adopted the latter. It seems that there’s a bug going around, making rounds attached to e-books that can hack people’s Amazon accounts. A security researcher has discovered a security hole in the “Manage your Kindle page” on Amazon’s website that provides hackers with the needed data – users’ credentials. This happens when you upload a malicious e-book to your account and move it through Amazon’s system to store it on your device. The Send to Kindle plugin for Windows and Mac can be used to send personal documents to Kindle, including e-books from other sources than Amazon. These end up archived in the Kindle Library in the cloud and they can be downloaded to the connected devices at any time, be them Kindles or mobile devices with the Kindle app, or even the desktop app. If one of the e-books you put on your device has been hacked to include a script in the title, then you could easily see your Amazon account in trouble, along with all your data. The code is executed once the book that was added to the library is opened in a web page. Hackers can then access the cookies related to Amazon and take over the account. The bug was fixed nearly a year ago, but has made a comeback Researcher Benjamin Mussler states that he first discovered the flaw nearly a year ago and reported it to Amazon. While the issue was fixed at the time, it seems that the problem is still very much present and that it has made its way into the new “Manage Your Kindle” page. “When I first reported this vulnerability to Amazon in November 2013, my initial Proof of Concept, a MOBI e-book with a title similar to the one mentioned above, contained code to collect cookies and send them to me. Interestingly, Amazon's Information Security team continued to use this PoC on internal preproduction systems for months after the vulnerability had been fixed. This made it even more surprising that, when rolling out a new version of the ’Manage your Kindle’ web application, Amazon reintroduced this very vulnerability,” he wrote on the issue. He adds that the issue goes farther than Amazon though. Calibre was also affected by the same bug last year, but seems to have fixed it in the meantime. To read more click HERE

Mozilla Officially Releases Firefox 32.0.1

Softpedia, 14 Sep 2014: Mozilla developers have announced that a new version of the Firefox browser is now available for download and testing. This is just a maintenance upgrade for the recently released 32.x branch of Firefox, so the number of changes is not that impressive. The Firefox developers usually offer a few point releases for each new major update that's being pushed from time to time, and the new 32.0.1 version is just such a release. Interestingly enough, this update is not very consistent, which isn't something that happens very often. The 32.0.1 update for Firefox features just a few changes that will be noticed by the users, and most of the modifications are under the hood. In any case, it would be a great idea to get the update as soon as the application becomes available in the repos. According to the changelog, a number of stability issues for computers with multiple graphics cards have been fixed, mixed content icon is no longer incorrectly displayed instead of the lock icon for SSL sites, and the setRemoteDescription() no longer silently fails if no success callback has been specified. Some of the bigger changes that have been made to the Firefox 32.x branch include a few pretty interesting ones, like the ability to display the number of found items in the find toolbar, Password Manager and the Add-on Manager performance improvements, and lots of HTML 5-related modifications. To read more click HERE