THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

5 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

November 3, Securityweek – (International) **New version of Backoff PoS malware appears: Fortinet.** Researchers with Fortinet recently reported finding a new version of the Backoff point-of-sale (PoS) malware with the version name ROM that includes changes designed to make the malware more difficult to detect and analyze. Source: http://www.securityweek.com/new-version-backoff-pos-malware-appears-fortinet

November 4, IDG News Service – (International) **BlackEnergy cyberespionage group targets Linux systems and Cisco routers.** Researchers with Kaspersky Lab reported that the cyberespionage group that uses the BlackEnergy malware has developed several modules for the malware that can be downloaded to infected systems to add the ability to perform port scanning, disk wiping, digital certificate theft, and other actions. The malware has compromised routers, Linux systems, and Windows systems and the group behind it targets organizations in the energy, manufacturing, banking, and education sectors as well as government agencies. Source: http://www.networkworld.com/article/2843153/blackenergy-cyberespionage-group-targets-linux-systems-and-cisco-routers.html

November 4, Help Net Security – (International) **227,747 new malware samples created daily.** PandaLabs reported that around 20 million new strains of malware were created during the third quarter (Q3) of 2014, with trojans the most common type of malware at 78.08 percent, among other findings. Source: http://www.net-security.org/malware_news.php?id=2905

Free Google Tool Shows Network Security Issues
Softpedia, 4 Nov 2014: Today, Google released a network security tool, called Nogotofail, as an open source project for developers and security researchers to be able to test devices and apps for weak TLS connections and SSL certificate verification problems. Nogotofail was created by the Android Security Team and it works with any device that can connect to the Internet, regardless of the operating system it runs on, exposing network issues that could render the data insecure when in transit. Available on GitHub, the tool aims at testing apps that are more complex and override the default network configuration, which is the most secure for the average user. However, in the case of complex applications, more libraries are required and changing the initial setup is oftentimes necessary, which could lead to increased security risks for data in transit. The developers included tests for common SSL certificate verification problems, HTTPS and TLS/SSL library bugs, SSL and STARTTLS stripping issues, and clear text problems. At the core of Notgotofail is the man-in-the-middle (MitM) technique that allows intercepting the TCP traffic flowing through the tested device. Optionally, clients are available in order to determine the app or the device that made a vulnerable connection; a client offers additional information about the connection, and its purpose is only to end up with more relevant tests. "We've been using this tool ourselves for some time and have worked with many developers to improve the security of their apps. But we want the use of TLS/SSL to advance as quickly as possible," says Chad Brubaker, android security engineer, in a blog post. The attack engine included in Nogotofail can be run as a router, VPN server or proxy. This should help developers create a test environment as close as possible to a real one. The MitM component

runs on path and focuses on handlers in the connection that are responsible for making exploitation of a vulnerability possible and thus have the traffic modified. According to the description of the product, the vulnerable traffic is not detected based on port numbers, but by using DPI (deep packet inspection); this also allows it to test the TLS/SSL traffic in protocols that rely on STARTTLS. To read more click HERE

Compromised .EDU Domain Used to Send Out ZeuS-Laden Emails

Softpedia, 4 Nov 2014: ZeuS Trojan has been discovered to be distributed through a malicious attachment of an email delivered from the address of an educational organization in the United States. The message claims to be a notification for some payment confirmation (subject is "Payment has been made"), with the malicious document available in the attachment. After checking the file, researchers from PhishMe determined without a doubt that it downloaded ZeuS Trojan, also known under the name of Zbot; the undeniable evidence was the fact that the payload was retrieved from an IP address listed in ZeuS tracker. The malware includes functionality for stealing confidential information from the compromised system, including banking password and username pair. Spam campaigns are carefully monitored and automated systems manage to spot the fraudulent messages and prevent them from reaching the inbox of the user by blocking the IP address they originate from. EDU domains are generally reserved for academic institutions and their email addresses are not included on blacklists because of the elevated trust level. This is only one reason cybercriminals would want to compromise an EDU domain. Another would be the fact that universities need to accommodate the Internet needs of a high number of individuals, and for this they need very big bandwidth. According to Ronnie Tokazowski from PhishMe, "the university used in this wave of attacks currently has between 25,000-30,000 enrolled students." A trustworthy source with a very fast Internet connection is a dream come true for cybercriminals, as they can move massive amounts of email with a very high chance of reaching the recipient's inbox. "In this case, the attackers may not have directly attacked the university, but could have compromised a system which just so happened to reside at the university," says Tokazowski in a blog post. Scammers' social engineering skills are getting better, and even if no hint of deceit can be spotted in the body of the message, most of the times the best clue is in the attached file. Unless we're talking about a very large text file, an archive purporting to be a document is always suspicious, more so if only one item is compressed. Text does compress very well, but an invoice or a bill does not require this type of treatment. To read more click HERE

Palm Springs Federal Credit Union Loses Hard Drive with Customer Data

Softpedia, 5 Nov 2014: An external storage device containing personally identifiable information about the customers of Palm Springs Federal Credit Union has been lost, all data running the risk of being exposed into the wrong hands. The discovery of the lost drive has been detected as a result of a regular audit performed on the operations and records of the financial institution. The exact date the device was lost is unclear, but it is believed that the incident happened on or about October 20. Furthermore, no information is provided about the security state of the hard disk. If the information on it was encrypted, then there is really no point worrying about the data. However, if everything was accessible without any security measure in place, by simply connecting the device to a computer, then the details on it should be considered exposed. Names, addresses, social security numbers and account numbers were available on the hard drive; there are no details about how many customers have been impacted. "At this time we do not known if the external drive has been inadvertently destroyed or if it was acquired by an unauthorized person. All we know is that it is lost," says Debbie Pitigliano, CEO of the company, in a letter to the affected customers. Considering the type of data exposed, it is a good idea to take all the necessary steps to prevent identity theft, by placing a fraud alert on the credit file as well as enable the identity protection service provided for free for a period of one year by Palm Springs Federal Credit Union. To read more click HERE

Windows 8 Botched Update Fixed by User, Microsoft Confirms It Works

Softpedia, 5 Nov 2014: It's a well-known fact that Microsoft has delivered quite a lot of broken updates in the last few months and many are still yet to be fixed, even though the company released more or less complex solutions to help people address the resulting issues. As far as KB3000061 is concerned, the kernel mode driver patch failed to install for some Windows 8 and Windows Server 2012 systems, and while Microsoft said in mid-October that it was looking into the matter, users were a lot more effective in addressing the problems. As Woody Leonhard of InfoWorld writes today, the first workaround was posted by CountryKING on TechNet a couple of days after last month's Patch Tuesday rollout, explaining that deleting a registry key should be enough to solve all problems. Microsoft hasn't actually provided any information at that time, but in a post recently made by a company engineer, the user-found workaround is indeed the best way to repair the issue on the affected computer. While the reason the update actually fails to install is yet to be determined, the workaround doesn't take more than a couple of minutes and allows all systems that are impacted by the botched update to deploy the KB3000061 bulletin just fine. All you need to do is to manually delete the following registry key: [codeHKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\{e7ef96be-969f-414f-97d7-3ddb7b558ccc}] After that, simply reboot your computer and attempt to reinstall the botched update. Everything should work fine, but in case more issues are experienced, make sure that the aforementioned registry key has been successfully deleted. Once the update attempts to install, it automatically recreates it, so in case it already exists, KB3000061 deployment is automatically blocked. Even though it's a bit surprising that users actually moved faster than Microsoft, the company says that it's still investigating the issues and is working to find the root cause of the problem. "This occurs when servers have been upgraded from 2008R2 to 2012 (or WinVista to Win8). The key is being carried over in these scenarios and not being set to the proper value. We're investigating why this occurred but deleting the key and rebooting the system will resolve the problem," the company said. At the same time, it's also a bit surprising to see Microsoft confirming this workaround only two weeks after its initial release, but at least it's a good thing that the company is now collaborating closer with its users to address problems and offer an overall improved experience to everyone else. To read more click **HERE**

Hacking Planes Is Possible, Network Architecture Preventing Attacks Is in the Works

Softpedia, 5 Nov 2014 In theory, there are multiple avenues for compromising the systems of an aircraft sufficiently to lead to a crash, but researchers are developing a network architecture that would prevent "cyber-bomb" attacks. According to David Stupples, Professor at the City University in London, a cyber-attack that would meddle with the plane would be quite difficult to execute and would require an inside individual that has sufficient access to the aircraft's systems or the network it connects to. Talking to The Guardian, Stupples said that a disgruntled employee could spread the threat when the plane connects to a data port in order to update the entertainment systems. Moreover, the attack could be conducted via direct access to the aircraft's systems. The compromise mission can start with reconnaissance software and evolve to malware that impacts on the systems of the plane, ultimately leading to a crash. However, as simple as this may sound in theory, carrying out this type of mission is more difficult in reality. The knowledge an attacker needs expands to the network architecture of the flight system and should be able to move the malware from one control system to another without being detected. This is not something many individuals have access to. However, researchers have started to work on a network infrastructure that would foil malicious attempts aiming to drop "cyber bombs." Together with experts at Cranfield University, Stupples works on a system capable of identifying malware immediately after it reaches the network of the aircraft. Once the threat is spotted trying to meddle with the flight control software, the network turns off any non-essential components in order to limit access to critical parts. Basically, the end goal is to instate a known safe state of the network. A similar approach could work in the case of critical infrastructure, such as power stations or water plants. The car industry faces a similar threat, but in this case, it appears that security is more evolved, as experts have already come up with a device that would detect abnormal activity and take measures to turn off the network and the higher level functions. Charlie Miller and Chris Valasek created a $150 / €111 intrusion detection system that can be placed under the

car's dashboard and monitor for malicious activity. Normally, it records driving patterns, but in detection mode it can identify irregular commands and block them. The device was presented at the Black Hat USA security conference this year. At the time, the two experts said that the device worked fine during their tests because in "the automotive world, the traffic is so normalized that it's very obvious when something happens that's not supposed to happen." To read more click HERE

Employees Responsible for Most Record Exposure Incidents in the Healthcare Sector Since 2010

Softpedia, 5 Nov 2014: Hackers are not to blame for most of the data breach incidents in the healthcare sector since 2010 because more than half of the events occurred due to hardware containing sensitive information being lost or stolen. Starting 2010, in 68% of the cases where personal information was potentially exposed, the incident occurred as a result of thievery or because the healthcare employee was careless and lost the equipment storing the private data. A report from security company Bitglass reveals these numbers, showing not just that there are greater chances of getting robbed than hacked these days, but that inefficient security measures for mobile devices with personal health information can spell disaster for a smaller organization. Apart from locking the device with a password, encrypting the storage device is one best-practice that should be followed. Patient information should be a top priority for healthcare centers and should be protected at all times, whether in transit or on the storage unit. As far as hackers are concerned, they are responsible for 23% of the intrusions, highlighting the need for better security policies and increased network protection. Oftentimes, the intruder compromises a third party that has access to the private data. The United States Department of Health and Human Services (HHS) says that the average for the data breach incidents has remained constant for the past three years and it is of about 200 events per year. Apart from exposing the patients to the risk of having their identity stolen, each security breach has a financial impact on the organization that failed to protect the data. Bitglass says that the Ponemon Institute calculated an average of $18,660 / €15,000 being spent for each victim; this includes not just the investment in upgraded security and fines, but also in providing protection against identity theft for the affected individuals. In the report from Bitglass the incident at Fortune 500 group Community Health Services is given. For a total of 5.4 million records exposed, the estimated costs for the company were between $75 / €60 and $150 / €120 million. Medical records can be used for longer periods of time, even if the victim knows about the compromise. Unlike in the case of financial fraud, the medical data has a permanent character and cannot be changed. Because of this, medical data is more expensive on underground forums. Bitglsass says that healthcare providers have the necessary technology at their disposal to reduce the number of this type of incidents, such as Cloud Access Security Brokers (CASB), a data centric solution relying on cloud and mobile security. To read more click HERE