The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

21 May 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

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

May 19, The Register – (International) **LifeLock snaps shut Wallet mobile app over credit card leak fears.** LifeLock removed its Wallet app from application markets and deleted user data as a precaution due to undisclosed elements of the app being incompatible with the payment card industry's Data Security Standard (PCI DSS), according to a company statement. Source: http://www.theregister.co.uk/2014/05/19/lifelock_yanks_mobile_app/

May 16, SC Magazine – (Pennsylvania) **Hackers exploit vulnerability to breach Pennsylvania payroll company.** Pennsylvania-based payroll processing company Paytime Inc., stated that an undisclosed number of clients may have had their personal and payment information exposed when attackers exploited a vulnerability in the company's Client Service Center. Paytime learned of the breach April 30 and found that the breach began April 7. Source: http://www.scmagazine.com/hackers-exploit-vulnerability-to-breach-pennsylvania-payroll-company/article/347371/

May 19, NBC News; Reuters – (International) **U.S. charges China with cyber-spying on American firms.** The U.S. Department of Justice announced criminal charges May 19 against five members of the Chinese military's Unit 61398 for allegedly conducting cyberespionage against U.S. solar power, nuclear power, and metals manufacturing companies for the purpose of stealing trade secrets. Source: http://www.nbcnews.com/news/us-news/u-s-charges-china-cyber-spying-american-firms-n108706

May 19, Softpedia – (International) **81 people arrested in international operation against BlackShades RAT users.** Law enforcement agencies in 13 countries arrested 81 people the week of May 12 for allegedly being involved in the creation, sale, or use of the BlackShades remote access trojan (RAT). The BlackShades RAT can be used to hijack webcams, log keystrokes, steal files, and launch denial of service (DoS) attacks and is sold on underweb markets. Source: http://news.softpedia.com/news/81-People-Arrested-in-International-Operation-Against-BlackShades-RAT-Users-442833.shtml

May 19, Help Net Security – (International) **Record month for Linux trojans.** Researchers at Dr. Web identified a record-high number of trojans for the Linux operating system thus far in the month of May, with variants of three separate trojans appearing to be created by the same author. The majority of the trojans are designed to carry out distributed denial of service (DDoS) attacks and can infect Linux desktop, server, and ARM distributions. Source: http://www.net-security.org/malware_news.php?id=2768

May 20, Help Net Security – (International) **Fascinating MiniDuke backdoor hits again.** ESET researchers identified a new variant of the MiniDuke Assembler-based backdoor. The new variant uses a Word RTF memory corruption vulnerability to deliver the backdoor, and contains new features including a Jscript component that contacts a command and control server via Twitter. Source: http://www.net-security.org/malware_news.php?id=2769

May 19, Softpedia – (International) **XSS vulnerability affected comments section of hundreds of Yahoo pages.** A researcher identified and reported a cross-site scripting (XSS) vulnerability affecting hundreds of Yahoo pages via the pages' comment sections that could be used to perform a persistent XSS attack that would affect all visitors or a self-XSS attack that would only affect users if the comment with the malicious code was a popular or recent comment. Yahoo closed the vulnerability after being notified. Source: http://news.softpedia.com/news/XSS-Vulnerability-Affected-Comments-Section-of-Hundreds-of-Yahoo-Pages-442754.shtml

May 19, Softpedia – (International) **Yahoo, Microsoft and Orange domains affected by same remote code injection flaw.** A researcher identified and reported a remote code injection vulnerability affecting several subdomains belonging to Yahoo, Microsoft, Orange, and others that could allow an attacker to access an administrator panel without login credentials. The vulnerability appears to be connected to an astrology content delivery network, and Yahoo, Orange, and Microsoft closed the vulnerabilities once informed. Source: http://news.softpedia.com/news/Yahoo-Microsoft-and-Orange-Domains-Affected-by-Same-Remote-Code-Injection-Flaw-442776.shtml

May 16, SC Magazine – (International) **Critical info on modems, load balancer, exposed via SNMP community string.** Researchers at Rapid7 reported that information disclosure vulnerabilities were identified in Brocade ServerIron ADX 1016-2-PREM TrafficWork application load balancers and Ambit U10C019, Ubee DDW3611, and Netopia 3347 modems. The vulnerability can be exploited by the Simple Network Management Protocol (SNMP) public community string and can disclose Management Information Base (MIB) tables that contain device and configuration information. Source: http://www.scmagazine.com/critical-info-on-modems-load-balancer-exposed-via-snmp-community-string/article/347393/

May 19, Help Net Security – (International) **Researchers discover critical flaws in the Chip and PIN system.** Researchers at Cambridge University identified two vulnerabilities in the Europay, MasterCard, and Visa (EMV) 'chip and PIN' payment card system that could allow attackers to carry out "pre-play" attacks in order to commit ATM or point of sale (POS) fraud. One vulnerability involves poor random number generation that could be predicted and used for ATM withdrawal, while the second is a protocol failure that could enable malware or a man-in-the-middle (MitM) attack to replace randomly generated numbers with ones chosen by the attacker. Source: http://www.net-security.org/secworld.php?id=16881

May 20, Help Net Security – (International) **Angler exploit kit starts wielding Silverlight exploits.** Researchers at Cisco reported an increase in the number of exploit kits adding Silverlight vulnerabilities to their capabilities, with a large increase in traffic being directed to sites hosting the Angler exploit, which then attempt to exploit a Silverlight memory disclosure vulnerability. Source: http://www.net-security.org/malware_news.php?id=2770

May 19, SC Magazine – (International) **'Infinity' exploit kit targets IE, Firefox, Opera to deliver malware.** Researchers at IntelCrawler identified a new exploit kit known as Infinity being sold on underweb markets which targets vulnerabilities in the Internet Explorer (IE), Firefox, and Opera browsers, as well as plug-ins such as Adobe Flash, in order to upload malware. Source: http://www.scmagazine.com/infinity-exploit-kit-targets-ie-firefox-opera-to-deliver-malware/article/347590/

Social media posts could get Kansas university employees fired

Fox News, 21 May 2014: The Kansas state attorney general approved a revised policy that states any employee at a public university in the state can be fired over improperly using social media, raising questions that their First Amendment rights are being infringed upon. "It's too broad; it's too vague, and it's already causing people to chill themselves in the way that they use social media," Doug Bonney, the legal director for the ALCU of Kansas, told Think Progress. The Kansas Board of Regents approved last week an amended version of the new social media policy. The Wichita Eagle reported that the new policy allows a university's chief executive to fire any faculty member who uses social media and posts a comment that could incite violence, disclose confidential information or otherwise damage the university. One of the elements of the new policy that has legal experts confused is the part that says a faculty member can face disciplinary action for "speech contrary to the interests of the university." "Unless you had access to every piece of information pertaining to the university, you would never know what affects its interests," Ken Paulson, the president of the First Amendment Center, told Think Progress. The regents developed the social media policy after an anti-NRA tweet in September 2013 by David Guth, a University of Kansas journalism professor. He reportedly tweeted, "blood is on the hands of the #NRA. Next time, let it be YOUR sons and daughters." Under the policy, social media covers blogs and social networking sites. Kirk McClure, a professor in the Department of Urban Planning at Kansas University, said the social media policy would hamper the ability for Kansas schools to compete for top faculty. "The social media policy makes it even harder to sell KU to top faculty candidates. A new faculty member can be disciplined, even terminated for a tweet," McClure said. To read more click **HERE**

Filipino hackers wage cyberwar on Chinese Web sites

Washington Post, 20 May 2014: Attention this week has centered on the covert cyberwar taking place between the United States and China. Chinese authorities pointed to the supposed hypocrisy of Washington leveling cyberspying charges against China, even while the United States maintains its own vast network of clandestine surveillance and monitoring. There are myriad other stealth attacks launched from the dark ravines and hideaways of the Internet that governments have to monitor and protect against. And the Chinese aren't just facing the United States. On Tuesday, the Philippine branch of the hacker collective Anonymous announced on its Facebook page that it had hacked and defaced nearly 200 Chinese government sites. The raid on the Chinese state Web sites comes amid heightened tensions between Beijing and Manila. The two countries have locked horns in a heated maritime territorial dispute over islands in the South China Sea, initially provoked, Philippine authorities argue, by illegal Chinese poaching of endangered species in islands not far from the archipelago nation's coast. Those provocations have escalated into dangerous standoffs between Chinese and Philippine naval vessels. Fear over China's increasingly expansionist behavior spurred the government in Manila to tie up a new security deal with Washington last month. The Anonymous hackers from the Philippines are clearly riled up by this state of events. "China's alleged claim on maritime territories and oppressive poaching can no longer be tolerated," read one message posted on a hacked Chinese Web site. Previously, though, Anonymous Philippines targeted Web sites of its own country's government, following the passage of a controversial cybercrime law. The Philippines has a considerable pool of Internet-savvy people, some of whom end up dabbling in the Web's dark arts. Recently, with the aid of Interpol, Philippine authorities arrested dozens in the country involved in global "sextortion" syndicates that would trick gullible netizens around the world into exposing themselves in lewd ways online and then blackmail them. They claimed more than 530 victims in the Chinese special administrative region of Hong Kong alone. To read more click **HERE**

Security Breach at eBay – Change Your Passwords Now

SoftPedia, 21 May 2014: Global commerce and payments giant eBay has released an alarming memo that its servers have been breached and user data has been compromised, urging everyone who uses its services to change their passwords immediately. The announcement hit the wires just minutes ago, with eBay noting that it will be asking users via email "to change their passwords because of a cyberattack that compromised a database containing encrypted

passwords and other non-financial data." Although the company has no evidence of the compromise causing unauthorized activity for customers, or any unauthorized access to credit card information, "which is stored separately in encrypted formats," after conducting extensive tests on its networks the commerce giant decided that "changing passwords is a best practice and will help enhance security for eBay users." Users can go ahead and change their passwords now if they are aware of how the system works, or they can wait for the email from eBay to arrive with the necessary instructions. Our winning advice is to change that password ASAP. eBay reveals in its press release that cyberattackers compromised a small number of employee log-in credentials between late February and early March. The breach resulted in unauthorized access to eBay's corporate network, but also "included eBay customers' name, encrypted password, email address, physical address, phone number and date of birth." "However, the database did not contain financial information or other confidential personal information," eBay clarifies, and that it has seen "no indication of increased fraudulent account activity on eBay." Sister company PayPal also shows "no evidence of unauthorized access or compromises to personal or financial information for users [as] PayPal data is stored separately on a secure network, and all PayPal financial information is encrypted." Customers who know they are using the same password across various other payment services or networks that might compromise their security are advised to carry out the procedure across all these services. "Beginning later today, eBay users will be notified via email, site communications and other marketing channels to change their password. In addition to asking users to change their eBay password, the company said it also is encouraging any eBay user who utilized the same password on other sites to change those passwords, too. The same password should never be used across multiple sites or accounts," eBay said. Earlier today, eBay rushed out the headline "eBay Inc. To Ask eBay Users To Change Passwords" but failed to produce the actual text body included in this announcement. Now the news is official. To read more click **HERE**

Security Warning: Microsoft Silverlight Attacks Skyrocketing

SoftPedia, 21 May 2014: Users who are running Microsoft Silverlight right now are strongly recommended to update the software to the newest version as security companies are experiencing an increase in the number of attacks supposed to exploit old vulnerabilities. Cisco has issued a statement this week to warn that there is evidence that Angler, an exploit kit previously developed to take advantage of some old vulnerabilities in Silverlight, is again being used in a new wave of attacks. According to Cisco Information Security Researcher Levi Gundert, Angler is based on a malicious tactic called malvertising which comes down to dangerous code injected into ads displayed on legitimate websites. "Silverlight exploits are the drive-by flavor of the month. In this particular Angler campaign, the attack is more specifically targeted at Flash and Silverlight vulnerabilities, and though Java is available and an included reference in the original attack landing pages, it's never triggered," he said. It appears that only older versions of Silverlight are being exploited right now, so users who are running the newest version are perfectly secure. Of course, those who are still using outdated builds should update as soon as possible, Gundert recommended. "Unfortunately, we observe extensive global DNS requests for the Angler landing pages, indicating that this campaign is largely succeeding... due to [each victim's] failure to upgrade their system's applications." Security company Trustwave has also confirmed that Silverlight attacks have also skyrocketed recently and has warned that the same exploit kits that have been spotted in previous waves are being used right now as well. "Within a month, Silverlight became the most popular target for exploitation. To make matters worse, integrating this exploit into a kit was so simple that developers could use the same .dll file across all versions. They merely added their own methods of obfuscation and evasion to the code," the company warned according to Dark Reading. The latest version of Silverlight is 5.1.30214.0 and was released by Microsoft on March 11, as part of the company's Patch Tuesday rollout that month. Of course, the new build has brought several security improvements, including support for Internet Explorer 11 Enhanced Protected Mode (EPM) and reporting of unavailable features. At the same time, it fixed an issue that could allow the bypass of the protection systems implemented in the app and thus expose users' data to online attacks. Obviously, everyone is recommended to update to this new version as soon as possible, so download Microsoft Silverlight 5.1.30214.0 right now to make sure that you're entirely secure. To read more click **HERE**

U.S. utility's control system was hacked, says Homeland Security

Chicago Tribune, 21 May 2014 A sophisticated hacking group recently attacked a U.S. public utility and compromised its control system network, but there was no evidence that the utility's operations were affected, according to the Department of Homeland Security. DHS did not identify the utility in a report that was issued this week by the agency's Industrial Control Systems Cyber Emergency Response Team, or ICS-CERT. "While unauthorized access was identified, ICS-CERT was able to work with the affected entity to put in place mitigation strategies and ensure the security of their control systems before there was any impact to operations," a DHS official told Reuters on Tuesday. Such cyber attacks are rarely disclosed by ICS-CERT, which typically keeps details about its investigations secret to encourage businesses to share information with the government. ICS-CERT said in the report posted on its website that investigators had determined the utility had likely been the victim of previous intrusions. It did not elaborate. The agency said the hackers may have launched the latest attack through an Internet portal that enabled workers to access the utility's control systems. It said the system used a simple password mechanism that could be compromised using a technique known as "brute forcing," where hackers digitally force their way in by trying various password combinations. Justin W. Clarke, an industrial control security consultant with security firm Cylance Inc, said it is rare for such breaches to be identified by utilities and even more rare for the government to disclose them. "In most cases, systems that are so antiquated to be susceptible to such brute forcing technologies would not have the detailed logging required to aid in an investigation like this," Clarke said. DHS also reported another hacking incident involving a control system server connected to "a mechanical device." The agency provided few details about that case, except to say the attacker had access over an extended period of time, though no attempts were made to manipulate the system. "Internet facing devices have become a serious concern over the past few years," the agency said in the report. Last year ICS-CERT responded to 256 cyber incident reports, more than half of them in the energy sector. While that is nearly double the agency's 2012 case load, there was not a single incident that caused a major disruption. Those incidents include hacking into systems through Internet portals exposed over the Web, injecting malicious software through thumb drives, and exploitation of software vulnerabilities. To read more click **HERE**

Hacking victims fell prey to China's mundane ruses

AP, 21 May 2014: The hacking techniques the U.S. government says China used against American companies turned out to be disappointingly mundane, tricking employees into opening email attachments or clicking on innocent-looking website links. The scariest part might be how successfully the ruses worked. With a mouse click or two, employees at big-name American makers of nuclear and solar technology gave away the keys to their computer networks. In a 31-count indictment announced Monday, the Justice Department said five Chinese military officials operating under hacker aliases such as "Ugly Gorilla," "KandyGoo" and "Jack Sun" stole confidential business information, sensitive trade secrets and internal communications for competitive advantage. The U.S. identified the alleged victims as Alcoa World Alumina, Westinghouse, Allegheny Technologies, U.S. Steel, the United Steelworkers Union and SolarWorld. China denied it all on Tuesday. "The Chinese government and Chinese military as well as relevant personnel have never engaged and never participated in so-called cybertheft of trade secrets," Foreign Ministry spokesman Hong Lei said in Beijing. "What the United States should do now is withdraw its indictment." That's unlikely. What the Justice Department is doing is spelling out exactly how it says China pulled it off. The U.S. says the break-ins were more Austin Powers than James Bond. In some cases, the government says, the hackers used "spear-phishing" -- a well-known scam to trick specific companies or employees into infecting their own computers. The hackers are said to have created a fake email account under the misspelled name of a then-Alcoa director and fooled an employee into opening an email attachment called "agenda.zip," billed as the agenda to a 2008 shareholders' meeting. It exposed the company's network. At another time, a hacker allegedly emailed company employees with a link to what appeared to be a report about industry observations, but the link instead installed malicious software that created a back door into the company's network. "We are so used to solving problems by clicking an email link, looking at the information and forwarding it on," said Chris Wysopal, a computer security expert and chief technology officer of the software-security firm Veracode. "And if hackers know

about you and your company, they can create really realistic-looking messages." And use of the rudimentary efforts the Justice Department described doesn't mean foreign governments and others won't use more sophisticated and harder-to-detect techniques, said Joshua Corman, the chief technology officer for Sonatype, which helps businesses make their software development secure. Determined hackers escalate their attacks when necessary, he said, but in the cases cited in the federal indictment announced Monday, they didn't have to escalate very far. Security layers failed in the hackings blamed on China, too. More-effective antivirus or security software could have blocked the malicious attachments or prevented users from visiting risky web links. Back-end server filters could have prevented dangerous emails from reaching employees. Intrusion-detection systems on corporate networks could have more quickly raised red flags internally after a successful break-in. "The problem is the technology hasn't advanced enough to detect malicious code," said Kevin Mitnick, the famous hacker who now works as a corporate security consultant. Tricking someone to let you into the system is far easier than identifying hidden vulnerabilities that can be exploited. Even worse: Employees, by their nature, are socially conditioned to want to open and respond to an email that purports to be from the boss -- never mind that the message may actually be a trick. "If you start with an incorrect assumption that every email that comes in is a real email," said Hossein Eslambolchi, chief executive at security company CyberFlow Analytics, "you're putting yourself and your corporation at a major risk." To read more click **HERE**