The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
15 April 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

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, Sandia 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 open source data

April 12, Softpedia – (International) **Nine people accused of stealing millions of dollars with Zeus malware.** The U.S. Department of Justice unsealed an indictment against nine individuals for allegedly being involved in a criminal organization that used the Zeus banking trojan to steal millions of dollars. The alleged scheme used Zeus to steal account information and then transfer stolen money to accounts belonging to 'mules' who withdrew and transferred the money. Source: http://news.softpedia.com/news/Nine-People-Accused-of-Stealing-Millions-of-Dollars-with-ZeuS-Malware-437311.shtml

April 11, Lubbock Avalanche-Journal – (Texas) **Lubbock Cardiology Clinic advertises security breach in electronic health records.** Lubbock Cardiology Clinic in Texas announced April 1 that more than 1,400 patients' medical records, which included personal information, were affected in a security breach of its Electronic Health Records system after an individual gained unauthorized access December 30, 2013 to January 30, 2014. Source: http://lubbockonline.com/local-news/2014-04-10/lubbock-cardiology-clinic-advertises-security-breach-electronic-health-records

April 14, IDG News Service – (International) **Akamai admits issuing faulty OpenSSL patch, reissues keys.** Akamai Technologies stated April 13 that a patch issued by the company designed to protect its customers from the Heartbleed vulnerability contained a fault, making it ineffective. The company then began reissuing all Secure Sockets Layer (SSL) certificates and security keys for affected sites. Source:http://www.computerworld.com/s/article/9247650/Akamai_admits_issuing_faulty_OpenSSL_patch_reissues_keys

April 14, Help Net Security – (International) **Jetpack pushes update to close critical security hole.** The creators of the Jetpack plugin for WordPress published an update for the popular plugin that closes a vulnerability discovered during a security audit that could allow an attacker to bypass a site's access controls. Source: http://www.net-security.org/secworld.php?id=16683

April 12, Softpedia – (International) **Google rewards experts for XXE vulnerability in Toolbar Button Gallery.** Google awarded two Detectify researchers $10,000 after they identified and reported an XML External Entity (XXE) vulnerability in the Google Toolbar Button Gallery that could have allowed an attacker to gain access to data on the company's production servers. The vulnerability was closed soon after being reported. Source: http://news.softpedia.com/news/Google-Rewards-Experts-for-XXE-Vulnerability-in-Toolbar-Button-Gallery-437290.shtml

More online Americans say they've experienced a personal data breach
Pew Research Center, 14 Apr 2014: As news of large-scale data breaches and vulnerabilities grows, new findings from the Pew Research Center suggest that growing numbers of online Americans have had important personal information stolen and many have had an account compromised. Findings from a January 2014 survey show that:

■ 18% of online adults have had important personal information stolen such as their Social Security Number, credit card, or bank account information. That's an increase from the 11% who reported personal information theft in July 2013.

■ 21% of online adults said they had an email or social networking account compromised or taken over without their permission. The same number reported this experience in a July 2013 survey.

Last week's discovery of the Heartbleed security flaw is the latest in a long string of bad news about the vulnerabilities of digital data. The bug, which affects a widely-used encryption technology that is intended to protect online transactions and accounts, went undetected for more than two years. Security researchers are unsure whether or not hackers have been exploiting the problem, but the scope of the problem is estimated to affect up to 66% of active sites on the Internet. In December, Target announced that credit and debit card information for 40 million of its customers had been compromised. Shortly thereafter, the retailer reported that an even larger share of its customers may have had personal information like email and mailing addresses stolen. In January, Nieman Marcus reported the theft of 1.1 million credit and debit cards by hackers who had invaded its systems with malware. The consequences of these flaws and breaches may add insult to injury for those who have already experienced some kind of personal information theft. And research suggests that young adults and younger baby boomers may have been especially hard hit in the second half of 2013. In our survey last year, we found that 7% of online adults ages 18-29 were aware that they had important personal information stolen such as their Social Security Number, credit card or bank account information. The latest survey finds that 15% of young adults have experienced this kind of personal information theft. Similarly, those ages 50-64 became significantly more likely to report that they had personal information stolen; while 11% said they had this experience in July, that figure jumped to 20% in January. Increases among other age groups were not statistically significant. As online Americans have become ever more engaged with online life, their concerns about the amount of personal information available about them online have shifted as well. When we look at how broad measures of concern among adults have changed over the past five years, we find that internet users have become more worried about the amount of personal information available about them online—50% reported this concern in January 2014, up from 33% in 2009. To read more click **HERE**

Heartbleed Hackers Steal Encryption Keys in Test Showing Risks
Bloomberg, 15 Apr 2014: The crown jewel of secure websites is a single string of data - a very long jumble of letters and numbers and symbols that looks like gibberish. The Heartbleed bug allows hackers to crack it. Security professionals demonstrated last weekend that the recently disclosed Heartbleed bug can be exploited to allow criminals and intelligence agencies to make off with one of the most sought-after prizes in hacking: the private keys that websites rely on to decrypt sensitive information, including passwords, banking details and health data. At least six people were able to extract the private key of a website in a test of the bug's viability organized by CloudFlare Inc., said Nick Sullivan, a security architect with the Internet security company. The results suggest hackers have stolen encryption keys using the bug and are planning attacks, he said. The company set up the competition after stating in an April 11 blog post (which was reported by the New York Times) that stealing keys appeared to be very hard or impossible using Heartbleed, one of the biggest holes in the history of the Internet. "It turns out we were wrong," CloudFlare now says. Sullivan said in an e-mail Sunday that the company was planning to replace the keys it manages for clients anyway to be safe and that the contest "made us more confident that the cost was worthwhile." The evidence that a widely used form of encryption

called OpenSSL can be undermined, giving attackers potential access to websites' future and past communications, validated fears about Heartbleed's danger and added urgency to efforts now entering their second week to fix computer systems containing it. Since its discovery, there has been much discussion about how the flaw could have gone undetected for so long and whether criminal hackers or government intelligence units might have exploited it. Bloomberg News reported April 11 that the National Security Agency knew about the bug for two years and made it part of its hacking toolkit. The NSA has since denied that it knew of the Internet hole before an April 7 report by private security researchers. Millions of smartphones and tablets running Google Inc.'s Android software are vulnerable to the bug, as are networking products from Cisco Systems Inc. and Juniper Networks Inc. Dozens of entities are conducting Internet-wide attack attempts seeking to exploit Heartbleed, including computers in China that have been associated with hacking, said J. Alex Halderman, an assistant professor of electrical engineering and computer science at the University of Michigan tracking the attacks. Sites have no way of knowing if their encryption codes have been stolen, and criminals will soon find ways to automate techniques for taking them, said Jeremiah Grossman, a Web application specialist and founder of WhiteHat Security Inc. "Exploitability matters a great deal!" Grossman wrote in an e-mail. "After that proof is done, then the black hat tool to make it scale will come next. And just because the issue is patched, doesn't mean the risk is over - far from it." Heartbleed, the result of a simple programming error, is the kind of security hole that is discovered every few years, widespread and serious enough that it sends technology companies around the world scrambling to protect their networks. Writing the code to exploit it takes creativity and patience. Good exploit code is something of an art form, and skilled hackers have signature techniques. Finding a bug and figuring out that it is exploitable are just the first steps. Intelligence agencies and criminal syndicates take what they know and create hacking packages that can be used off-the- shelf to compromise networks. Thus, a single bug can spawn multiple types of attack bundles. The goal is to maximize the ability to penetrate a target, while minimizing the chance of discovery. The Heartbleed bug could therefore have many consequences, but the ability to steal private encryption keys is the most severe. In encryption, private keys are like the keys to a house. Only you have them, and they are closely guarded. Public keys, on the other hand, are what everyone on the Internet sees when they want to communicate securely with a website. The two are paired. Stealing the private key gives an intruder unfettered access to their targets, allowing them to capture data flowing between websites' servers and users' computers. So far, efforts to fix vulnerable systems appear to be working. The majority of websites that had the bug have applied a software patch that protects them. About 12 percent have not, according to a site called istheinternetfixedyet.com tracking the progress. An urgent concern now is that they all revoke the Secure Sockets Layer, or SSL, digital certificates that handle their data encryption and contain keys that might have already been stolen by hackers. The researchers who discovered Heartbleed said the bug could exist inside hundreds of millions of websites, based on the market share of the open-source software that uses OpenSSL. The number is actually closer to 500,000, because only a fraction of sites had the vulnerable functionality turned on, according to Netcraft Ltd., a cyber-security firm based in Bath, U.K., whose data the researchers used for their original estimate. Of the vulnerable sites, just 30,000 have taken the step of revoking their encryption certificates, leaving the rest exposed to potential attack, Netcraft said. An attack would look like what Ben Murphy, a 30-year-old software developer in London, did on Saturday after his morning run. In a matter of a few hours, Murphy took a publicly available program designed to exploit Heartbleed flaws, modified it and trained it on CloudFlare's contest server using two machines from Amazon.com Inc.'s cloud-computing service. Out popped the private key before lunch. The attack required a basic understanding of encryption, information that could probably be obtained from an introductory course on the subject, Murphy said. "I don't think dumping the private key was that difficult," he wrote in an e-mail. CloudFlare's test site got 44 million hacking attempts from 2,921 unique Internet Protocol addresses, the company said. The number of contestants was smaller because some people used multiple computers. The contest was designed as a realistic simulation for an attack, and the contest server used the same software as one- seventh of all websites, Sullivan said. Ilkka Mattila, an information-security specialist with the National Cyber Security Centre in Finland, said he was preparing food and watching television while his program stole the key with relative ease. "The implications were mind-boggling," Mattila wrote in an e-mail. "Not only would anyone with a stolen key be able to impersonate any vulnerable service, but also any previous communication encrypted with the same key would be at risk. I immediately recalled the stories about large intelligence organizations storing huge amounts of encrypted traffic ‘in case they might be decrypted in the future.’ This might be that day.” Fedor Indutny, a security researcher in Moscow, said he didn’t think his straightforward approach would lead to such sensitive information. “I had no expectation of obtaining the key, because it doesn’t seem feasible at that time,” Indutny wrote in an e- mail. “Successfully extracting it was a big surprise for me!” Attackers could go after more than just encryption keys. Yahoo! Inc. found some of its data spilled onto the Internet after the Heartbleed discovery. Mark Loman, chief executive officer of software maker SurfRight BV in the Netherlands, said the bug was trivial to exploit and easily made Yahoo’s servers cough up user names, passwords and other sensitive information. Loman posted some of it online in redacted form and alerted the company. Yahoo said in an e-mailed statement yesterday that it has fixed the Heartbleed bug across all of its properties and declined to address specific questions about the gap between when the bug was disclosed and when the site was fixed. There was a silver lining: security professionals contacted Loman for advice on how to exploit the bug on websites used by criminals. “They were anxious to scrape accounts from web servers belonging to the cybercrime underground forums, to infiltrate the operations of cybercriminals,” Loman wrote in an e-mail. “Like Yahoo, the crooks hadn’t patched their Web servers.” To read more click **HERE**

Gmail does scan all emails, new Google terms clarify

theguardian.com, 15 April 2014: Google has clarified its email scanning practices in a terms of service update, informing users that incoming and outgoing emails are analysed by automated software. The revisions explicitly state that Google’s system scans the content of emails stored on Google’s servers as well as those being sent and received by any Google email account, a practice that has seen the search company face criticism from privacy action groups and lawsuits from the education sector.   “We want our policies to be simple and easy for users to understand. These changes will give people even greater clarity and are based on feedback we've received over the last few months,” said a Google spokeswoman. The automated systems scan the content of emails for spam and malware detection, as many other email providers automatically do, but also as part of Google’s “priority inbox” service and tailored advertising. “This is not the worst thing Google does,” said Jim Killock, executive director of the Open Rights Group. “But like anything like this, if people are concerned about it they should be able to completely switch it off if they want to.” Google’s ads use information gleaned from a user’s email combined with data from their Google profile as a whole, including search results, map requests and YouTube views, to display what it considers are relevant ads in the hope that the user is more likely to click on them and generate more advertising revenue for Google. The updated terms of service were clarified to specifically state: “Our automated systems analyse your content (including emails) to provide you personally relevant product features, such as customised search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.” Google’s email scanning practices stretch across consumer-facing Gmail displaying ads to support the service, as well as its products for business and education which have the option of being ad-free. Such scanning and indexing of emails, which cannot be fully turned off, could be in violation of a US law called Ferpa, the Family Educational Rights and Privacy Act, which is the main law guarding student educational records and the law being used as the basis for a lawsuit filed against Google in California. While email scanning has taken the headlines recently, leading from the revelations that Google considers that users have no “reasonable expectation” of privacy, the Open Rights Group considers other aspects of Google’s practices most troubling. “The really dangerous things that Google is doing are things like the information held in Analytics, cookies in advertising and the profiling that it is able to do on individual accounts,” said Killock. “It is the amount of information they hold on individuals that should be concerning us, both because that is attractive to government but also sometimes that information leaks out in various ways like the NSA’s use of cookies in general as a means to target users,” Killock explained. To read more click **HERE**

Zeus Malware: A Continuing Threat

BankInfoSecurity, 15 Apr 2014: The indictment of nine alleged participants in a fraud scheme that involved infecting thousands of business computers with Zeus malware to steal millions of dollars shows that the malware remains a formidable ongoing threat, financial services security experts say. The victims in the case included a Nebraska bank and a Nebraska company, according to an announcement of the indictment from federal prosecutors. The indictment was unsealed in connection with the April 11 arraignment of two Ukrainian nationals, who were recently extradited from the United Kingdom. Three other Ukrainians and a Russian have not yet been arrested; the indictment also names three other "John Doe" defendants. "These actors are only a few of those who operate Zeus botnets out of a sea of cybercriminals who use variations to commit fraud," says Ryan Sherstobitoff, a threat researcher at security vendor McAfee, a unit of Intel. "Zeus will always be a continuing threat, and cybercriminals will continue to use Zeus to steal money. We as an industry must be vigilant." Kevin Haley, security response director at security vendor Symantec, says the indictments won't put much of a dent in the use of the malware. "Zeus is not a gang; it's a toolkit, a very popular one used by many gangs," he says. "While today there is one less gang, there are still plenty of others using Zeus to attack us." Andreas Baumhof, chief technology officer at anti-fraud vendor ThreatMetrix, says that when it comes to fighting fraud, the latest indictments are "like taking a scoop of sand out of the beach. "The thing about Zeus is that the people who develop and distribute Zeus are not the same people who use Zeus to steal money," Baumhof says. "Now we have a couple less people using Zeus." Zeus is a continuing threat because many financial institutions aren't looking necessarily for the malware itself, says George Tubin, banking expert at anti-malware provider Trusteer. "What [banks] are trying to do is use different authentication means and different fraud prevention technologies to try to spot when fraud happens," he says. "But very few institutions are actually trying to identify when man-in-the-middle malware [such as Zeus] is being used." McAfee's Sherstobitoff says federal law enforcement is making progress mitigating the Zeus threat through botnet takedowns and disruption efforts. "These disruption efforts are oriented toward breaking up criminal rings who operate Zeus to steal from commercial entities," he says. Haley at Symantec notes: "Security technology continues to get better, and users become more aware of the social engineering tricks that attackers deploy. But the attackers do not stand still either." Organizations need to first identify the critical business information that must be protected and prioritize that appropriately, Haley says. Then they must implement security technology, including anti-spam technology, to mitigate the e-mail threats. "And finally, users need security awareness training," he says. ThreatMetrix's Baumhof says making progress in fighting fraud is challenging because many malware attacks are so targeted. "The trick with Zeus is that it is a very flexible toolkit that you can use in many different ways," he says. "People try to mitigate the specific attacks that they are being attacked with, not against Zeus. People are protecting against cuts and not against the Swiss Army knife." To fight attacks that use Zeus, banks need to ensure more data is available to systems that assess risk, Baumhof says. And that includes information about end users' devices. "How can a bank make a good decision regarding whether or not a particular transaction is valid if there is no visibility into the endpoint?" To read more click **HERE**