THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

10 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 7, The Register – (International) **Belkin flings out patch after Metasploit module turns guests to admins.** Belkin recently released a patch for its N750 dual-band router to close a vulnerability demonstrated in a Metasploit module that could allow attackers on guest networks to gain root access. Users were advised to update their firmware to close the vulnerability. Source: http://www.theregister.co.uk/2014/11/07/belkin_flings_patch_after_metasploit_module_turns_guests_to_admins/

November 7, Help Net Security – (International) **WireLurker: Apple blocks Trojanized apps, revokes certificate.** Apple stated that it blocked apps identified as containing the WireLurker malware for OS X and iOS and revoked the certificate used to sign the malware. Source: http://www.net-security.org/malware_news.php?id=2911

November 7, Securityweek – (International) **Metasploit module released for new UXSS vulnerability in Android browser.** An independent researcher in coordination with Rapid7 identified and reported a universal cross-site scripting (UXSS) vulnerability in the default Android browser that could allow an attacker to scrape page contents and cookie data. A Metasploit module for the vulnerability was released, and although Google fixed the issue September 30 many Android users may not receive the fix due to lack of Android version updates. Source: http://www.securityweek.com/metasploit-module-released-new-uxss-vulnerability-android-browser

November 6, Softpedia – (International) **Cisco patches three out of four buggy small business RV series routers.** Cisco posted an advisory November 5 stating that three vulnerabilities in four routers intended for small business use could allow attackers to execute arbitrary commands and upload files to the devices. The company issued patches for the RV120W Wireless-N VPN Firewall, RV180 VPN Router, and RV 180W Wireless-N Multifunction VPN Router, while a patch for the RV220W Wireless Network Security Firewall is expected by the end of November. Source: http://news.softpedia.com/news/Cisco-Patches-Three-Out-Of-Four-Small-Business-RV-Series-Routers-464341.shtml

November 5, Lafayette Daily Advertiser – (Louisiana) **LUS Fiber victim of Internet attack.** The director of Lafayette Utilities System (LUS Fiber) stated that disruptions to customers' Internet access November 4 and November 5 in Lafayette were the result of an attacker intentionally overwhelming the system. LUS Fiber had also experienced an unrelated email server malfunction the week of October 27 that left customers without email service for several days. Source: http://www.theadvertiser.com/story/news/local/2014/11/05/lus-fiber-victim-internet-attack/18547439/

November 7, Help Net Security – (International) **53M customer email addresses were also stolen in Home Depot breach.** Home Depot officials disclosed November 6 that an investigation into a previously reported breach of the company's payment data systems revealed that 53 million email addresses of customers in the U.S. and Canada were also compromised during the attack and officials urged consumers to be on guard against phishing scams. The company also reported that hackers used

the stolen credentials of a third-party vendor to access the company's point-of-sale (PoS) devices, then acquired administrator rights that enabled them to deploy custom-built malware on self-checkout systems at the company's stores in the U.S. and Canada. Source: http://www.net-security.org/secworld.php?id=17606

RI Dem: Cyberattacks against US a 'real threat'

ABQ News, 9 Nov 2014: Rep. Jim Langevin (D-R.I.) on Sunday called the risk of terrorists launching cyberattacks against critical U.S. infrastructure "a real threat." "Right now, these … worst weapons and cyber weapons are in the hands of nation states who have the capability but not necessarily the will to use them," Langevin, a member of the Armed Services Committee, said on ABC's "This Week." "But then you have groups like ISIL or al Qaeda, that certainly would have the intent, but not the weapons. Langevin said he's been trying to "raise the alarm" and try to close an "aperture of vulnerability" since he chaired the Homeland Security subcommittee on cybersecurity. "We did a deep dive on this, looking at how vulnerable critical infrastructure is, in particular, how vulnerable our electric grid is. And we found that it's very vulnerable." Langevin said a study by Idaho National Labs showed that an attack could cause a number of generators "to blow themselves up." "And you could see a whole sector of the country without electricity for a period of not just days or weeks, but potentially months, because these generators are -- are large. They're not just like batteries that are sitting on a shelf that you can, you know, take one out and plug another one in. "These generators take months to build, ship and install," he added. Langevin called on the Congress to pass an information-sharing bill. "That bill passed and was unanimous out of the House Intelligence Committee, on which I sit. It passed the House with strong bipartisan support. And now we're waiting for the Senate to take it up." "That would allow classified threat information to be passed to the private sector and for the private sector to pass the -- the threats or the -- the attacks that they're experiencing back to the government so that information could be more widely shared." "This is not a problem … that we're ever going to solve," Langevin said. "It's one that we need to manage." To read more click **HERE**

Cyber crime targets feds

Martinsville Bulletin, 10 Nov 2014: A $10 billion-a-year effort to protect sensitive government data, from military secrets to Social Security numbers, is struggling to keep pace with an increasing number of cyberattacks and is unwittingly being undermined by federal employees and contractors. Workers scattered across more than a dozen agencies, from the Defense and Education departments to the National Weather Service, are responsible for at least half of the federal cyberincidents reported each year since 2010, according to an Associated Press analysis of records. They have clicked links in bogus phishing emails, opened malware-laden websites and been tricked by scammers into sharing information. One was redirected to a hostile site after connecting to a video of tennis star Serena Williams. A few act intentionally, most famously former National Security Agency contractor Edward Snowden, who downloaded and leaked documents revealing the government's collection of phone and email records. Then there was the contract worker who lost equipment containing the confidential information of millions of Americans, including Robert Curtis, of Monument, Colorado. "I was angry, because we as citizens trust the government to act on our behalf," he said. Curtis, according to court records, was besieged by identity thieves after someone stole data tapes that the contractor left in a car, exposing the health records of about 5 million current and former Pentagon employees and their families. At a time when intelligence officials say cybersecurity trumps terrorism as the No. 1 threat to the U.S. — and when breaches at businesses such as Home Depot and Target focus attention on data security — the federal government isn't required to publicize its own data losses. Last month, a breach of unclassified White House computers by hackers thought to be working for Russia was reported not by officials but The Washington Post. Congressional Republicans complained even they weren't alerted to the hack. To determine the extent of federal cyberincidents, the AP filed dozens of Freedom of Information Act requests, interviewed hackers, cybersecurity experts and government officials, and obtained documents describing digital cracks in the system. That review shows that 40 years and more than $100 billion after the first federal data

protection law was enacted, the government is struggling to close holes without the knowledge, staff or systems to outwit an ever-evolving foe. To read more click **HERE**

Keeping EU cybersecurity focused on critical infrastructure

Reuters, 10 Nov 2014: There is an uneven landscape when it comes to cybersecurity readiness in Europe, writes Thomas Eboué. To build a foundation for cyber protections, the European Union needs to start with the most critical infrastructure, he argues. Thomas Boué is public policy manager at BSA | The Software Alliance, an advocacy organisation for the global software industry. Improving Europe's ability to defend against cyber threats is vital to the safety and security of European citizens and the economy. Stronger safeguards, faster and better detection, and more effective response and remediation – that's the goal. To build a foundation for cyber protections in Europe we need to start with Europe's most critical infrastructure, ensuring from the outset that EU laws are helping to secure that which needs protecting the most. Earlier this year, the European Commission took its first foray into the cybersecurity space by introducing a draft directive to ensure a high common level of network and information security across the union (the "NIS Directive") with the intent to improve harmonisation of cybersecurity across the EU. That's a worthwhile objective, as there is an uneven landscape when it comes to cybersecurity readiness in Europe. A report due out from BSA early next year will show the patchwork effect that exists across the 28 EU Member States. Bolstering cybersecurity has been of paramount concern for the software industry for decades. Software companies monitor networks and information systems constantly, looking for threats and responding with updates and tools. But the cyberthreat landscape is vast, and ever-changing. Those who invest significant time and resources in cybersecurity will tell you the importance of viewing cyber threats through a lens of risk; focusing protections on those areas where the potential for harm is greatest. While the Commission's initiative is positive, the proposal tries to tackle too much from the outset by casting the scope of the Directive so wide as to include everything from critical infrastructure to online games and music services. The NIS Directive should start with Europe's most critical networks and infrastructure, such as transport, energy and banking, in order to establish a foundation for cybersecurity readiness first and foremost in those areas where disruption would have major security and public safety impacts. It should build on the regulatory infrastructures already in place that support critical systems and infrastructure. Keeping the Directive's reporting requirements focused on critical infrastructure and excluding information society services would eliminate conflicts or redundancies in process. Consider this example: If business-to-business services like cloud services are included in the scope directly, it would create a situation where a single incident would be reported by both an IT service provider and the operator of the infrastructure. There would then be two (or more) reports for what is ultimately one problem, wherein only one entity has an clear and complete understanding of the impact of the incident on the critical network or service. This would create a confusing and burdensome situation for operators, service providers and competent authorities. It also puts service providers in the untenable position of having to circumvent their customer (the critical infrastructure provider) and provide sensitive and confidential information – that may be imprecise – to a third party. A better solution would be to have one consolidated report from the critical infrastructure operator outlining the problem and its implications, no matter where it occurred within the value chain. This would ensure clear, first-hand information is provided to the competent authority about how to reduce the threat risk in the future. The European Parliament wisely recognised the value of a narrow focus in the Directive. MEP Andreas Schwab said in his report, "at the beginning of the project, we need to talk specifically and first and foremost about protecting critical infrastructure in the EU," which of course doesn't exclude expanding its scope in the future. The consequence of casting the net too wide at the outset will be inefficiency and compliance challenges, and a false sense of security that important protections have been achieved when, perhaps, they have not. Focusing on critical infrastructure and creating reasonably harmonized reporting structures are, by far, the best ways to improve cybersecurity protections in Europe. We very much hope that the next round of trilogue discussions on 11 November will reflect this approach. To read more click **HERE**

Windows Version of WireLurker Also Used to Compromise iOS Devices

Softpedia, 10 Nov 2014: Malicious software for both OS X and Windows has been used in China to infect iOS devices with WireLurker Trojan when connected to the desktop system via a USB connection. Researchers at Palo Alto Networks announced on Wednesday that they found a piece of malware that can compromise an iOS device regardless if it is jailbroken or not (enterprise certificates used for signing the rogue apps). They dubbed the threat WireLurker because it would be installed on a Mac computer and then wait for an USB connection with a targeted device. Initially, it was reported that 467 programs in a third-party app store (Maiyadi) hosting premium pirated content included WireLurker, and they were downloaded more than 356,104 times in the last six months. Immediately after publishing this information, Palo Alto Networks (PAN) researchers received news that a Windows version of WireLurker existed, with the same modus operandi and targeting iOS devices. Claud Xiao and Royce Lu of PAN inform that it is an older variant of the malware that can only affect jailbroken devices. It was found embedded in 180 Windows executables and 67 OS X applications, all hosted in an account in the public cloud storage service of Baidu. The files have been downloaded 65,213 times, and in 97.7% of the cases, the user retrieved a Windows executable; this included two iOS app installation bundles, one of them being malicious, the other being a pirated iOS app. Infecting the iPhone or iPad is done through iTunes, when the mobile device is connected to the desktop. If iTunes is not present on the system, the victim is provided with a download link and instructed to install it. The malware is added to the iOS device together with the pirated app. According to the researchers, the iOS malware contains code for three CPU types: 32-bit ARMv7, 32-bit ARMv7s and 64-bit ARM64. "As far as we know, this is the first iOS malware that attacks the ARM64 architecture," they said in a blog post on Thursday. There aren't any differences in terms of functionality between the OS X and the Windows versions of WireLurker. The same behavior has been observed in both cases and the same command and control server (comeinbaby.com) has been used. The mystery around the purpose of the malware remains, since the end-game could not be determined based on the amount of information it extracts (product serial and model numbers, phone number, Apple ID, Wi-Fi address, disk usage, and the unique device identifier – UDID). A Windows variant of WireLurker shows that the operating system is not an obstacle for cybercriminals to spread their malware. Any platform can be used to spread rogue apps to a targeted device. To read more click **HERE**

Who Is the Silk Road 2.0 Mastermind?

Softpedia, 10 Nov 2014: It was about a year ago that the original Silk Road was taken down by the Feds, when the alleged Dread Pirate Roberts was arrested. Now, the second Silk Road platform was taken down, along with yet another mastermind. The alleged Silk Road 2 mastermind is 26-year-old Blake Benthall, who is a contractor for a series of companies, including Close, a secretive startup that was founded by a group of former Google employees, Wired reports. Federal prosecutors claim Benthall worked alone, however, or at the very least, his colleagues didn't know about his side business of running Silk Road 2, the illegal online drug marketplace. The young tech worker drove a Tesla Model S, worth some $127,000, and spent his days working with various startups. Nothing about him gave out what the police say he was doing behind closed doors, nothing hinted to the fact that he was running a drug empire. Other than having spent a fortune on a Tesla car, Benthall didn't seem to be extremely rich. Therefore, it's surprising that he had some $100,000 in cash in his home, as prosecutors claim. On Twitter, Benthall describes himself as a "rocket scientist, bitcoin dreamer." He's a fan of Edward Snowden, Radiohead and he's an active GitHub user, as well as a fan of hackathons. He is described by others as a passionate coder that's been busy with various projects. For instance, a while back, he wrote TweetCall, a tool letting you call an 800 number and convert the words into a tweet. People who know him say he was focused on his work and tended to take control of projects. Aside from being an obvious Tesla fan, Benthall also worked for Elon Musk's SpaceX, as his LinkedIn profile reveals. He also worked as a software engineer for Carbon Five, RPX Corporation, and Momentum Design Lab, to name a few. The authorities claim he was hosting the Silk Road 2 server on a subdomain of the Close.co Internet address. Back in late May, after Benthall left SpaceX, the feds managed to get a hold of the Silk Road 2 server, even though it was placed well beyond the jurisdiction of US authorities. For a few hours, the site went down as they copied its contents

for forensic investigation. "Defcon," as the site's admin went by, was notified by the service provider about the downtime. As a result, he immediately contacted them and asked them not to reboot the machine, due to the critical process rolling on it. The Googlers running the Close startup had no idea that the server running Silk Road 2 was on the company's Close.co domain and the arrest took them by surprise. The FBI claims that there were some 150,000 active users of Silk Road 2 prior to the takedown and they generated a money flow of at least $8 million (€6.45 million), while the operators earned some $400,000 (€323,000) in commissions. Silk Road 2.0 was taken down by a group of cybercrime fighting units, coordinated by Europol. The operation saw the joined forces of law enforcement from Bulgaria, the Czech Re public, Finland, France, Germany, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Romania, Spain, Sweden, Switzerland, and the United Kingdom. It wasn't just Silk Road 2.0 that was taken down, but other Darknet marketplaces, including Cloud 9, Hydra, Pandora, Topix, Cannabis Road, and Black Market, to name just a few. To read more click **HERE**

iOS and OS X Are Beginning to Be as Targeted as Windows

Softpedia, 9 Nov 2014: Whether Apple products were ever immune to malware is arguable, but reports from the security industry in the past few months are clearly showing an increased interest from cybercriminals in OS X and iOS users. "OS X and iOS users have been relatively shielded from malware compared to Windows users. However, as both the mobile and desktop operating systems from Apple gain popularity amongst users, they become viable targets for cyber-crime," says Bogdan Botezatu, senior malware analyst at Bitdefender. Lately, it has been observed that these platforms have become more appealing for different types of attacks, not just the financially motivated ones. In August, a research on an older discovery revealed that a threat dubbed AdThief infected about 75,000 iOS devices, managing to steal the revenue from 22 million advertisements. The user would not be directly impacted by this, but iOS app makers would no longer receive the monetary rewards. According to the analysis, AdThief had been in use since at least December 10, 2013, and it caught the attention of security researchers in March 2014, when about 22,000 daily activations were observed. In this case, the malware worked on jailbroken devices, which do not benefit from the inherent security restrictions from Apple. In September, researchers from FireEye announced that a piece of malware called XSLCmd had been ported from Windows to OS X. Stealing data from the affected computer seemed to be the main purpose of the threat. All evidence pointed at cyber-espionage activity from a group they named GREF, which, based on historical information, is believed to operate since 2009. Another Trojan was revealed by the experts at Lacoon Mobile Security at the end of September. The malware, named Xsser mRAT, is designed for the iOS platform and is allegedly the work of the Chinese government. It was found on a server hosting its Android counterpart that was flung at Hong Kong pro-democracy protesters under the guise of an app that would help with better coordination of the manifestation. Like AdThief, Xsser mRAT also works on jailbroken devices only, and it would send to its command and control server information about the infected phone, from version of the OS, MAC address, IMSI and IMEI codes, to the phone number of the SIM card. The month of September was unusually prolific in reports about malware for Apple products, as news about another threat came from antivirus vendor Doctor Web, this time alerting of a botnet of OS X systems caused by iWorm. According to telemetry data at the time, connections from more than 17,000 unique IP addresses were recorded; this does not reflect the real number of infected computers, since dynamic IPs are generally assigned by ISPs to customers, and as such, an infected computer could connect to the command and control server under different IPs. In October, we saw another report about an OS X threat called Ventir put together by researchers at Kaspersky. They said that one of the modules was actually an open source tool built to intercept keystrokes. However, in more recent news in November, Palo Alto Networks found WireLurker, an impressive piece of malware aimed at users in China that jumps from OS X to iOS via a USB connection and it can compromise even non-jailbroken devices. The amount of victims is estimated at hundreds of thousands, while the attack vector consisted in Trojanized apps downloaded from a third-party marketplace that offered premium pirated content. The move from OS X to iOS was possible through malicious apps signed with enterprise certificates, which can be installed without restriction on non-jailbroken devices. Researchers expect more malware to be

discovered It is clear that there is a real interest in compromising products from Apple in order to spy or steal from the owners. "Most of the cyber-criminals are focused on making money, so the more potential victims, the lower the overall cost of the attack is, which in turn makes developing Mac or iOS malware a profitable business. We expect to see more of these threats in the wild during the next year," said Botezatu via email. Other researchers agree that malware has become a real threat for Apple products, WireLurker being the perfect example in the argument, according to Christian Funk, senior security researcher at Kaspersky. He says that the chances of an unprotected Mac system to become infected has grown by three percent in the first eight months of 2014, as 25 different malware families for Apple's platform have been discovered. A 3% security risk increase may not seem like much, but these numbers come from devices protected by a security solution from Kaspersky, the researcher warns; the total amount of threats is likely to be much higher. "Compared to the malware situation on PCs and even Android devices the threat landscape in the Mac world is pretty calm, but nevertheless threats do exist. Macs can also be carriers of malware intended for other operating systems - the malware doesn't affect the Mac directly, but can forward an infected file to a Windows computer, or - as in this case [WireLurker] - an iPhone," Funk said. If it hasn't happened already, Apple users are about to wake up to a harsh reality where their devices have become a target, and the security measures from the developer are no longer proving to be 100% efficient, even for non-jailbroken devices. To read more click **HERE**

Healthcare Entities and Retailers Lead Data Breach Top in 2014

Softpedia, 5 Nov 2014: It comes as no surprise that medical-related organizations and retail businesses have been most impacted by data breach incidents this year, each of them recording at least 200 events and together exposing over 72 million personal records, according to a partial report. The information has been collected from public resources by the Identity Theft Resource Center (ITRC) and sums up only the numbers that have been disclosed by the affected party. In many cases, the amount of affected individuals is not disclosed, which has a direct impact on the total of records that have been put at risk. However, the report is useful in showing the sectors most affected by cyber-attacks. According to the ITRC document last updated on Monday, the business sector in the US was involved in 206 data breach incidents in 2014, which makes for 32% of all events. Probably because of more relaxed security policies, the medical and healthcare sector was hit by 273 breaches, accounting for 42.4% of the total. These figures may not be accurate, since some entities may have suffered such an incident and have not reported it yet; but it is clear that more emphasis should be put on protecting the computer systems in medical facilities and healthcare centers. Recently, Jessie Trice Community Health Center announced that records on 7,888 patients have been exposed as a result of a cyber-intrusion aiming at stealing identities. In the case of retailers, although security measures are definitely higher, the information stored on the systems is a prize valuable enough for cybercriminals to devise ways of compromise. The difference in that the amount of data revealed to unauthorized individuals is not too relevant, since it is based on incomplete data. Furthermore, the report from ITRC counts as a data breach only incidents risking the exposure of social security numbers, credit or debit card numbers, credentials or medical records. In some cases, such as the attack on JP Morgan Chase systems, only names, addresses, phone numbers and emails have been exposed, which are not taken into consideration by ITRC as data breach. If it did, this incident alone would have increased the number of leaked records by 83 million. The report for 2013 from ITRC shows that nearly 92 million records have been compromised in 614 incidents. Again, many of the entries show zero records because the affected entities did not make the information public; also, not all entities have disclosed a cyber-attack on their network in the course of the year and attacks are often announced with a delay of a few months. On the other hand, an analysis from Risk Based Security reveals that in 2013 there have been over 546 million records exposed in the US in a total of 1054 incidents. To read more click **HERE**