THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

22 July 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

July 17, Bloomberg News – (International) **Tesla Model S hacked in Chinese security contest.** Researchers with Qihoo 360 Technology Co., reported identifying security vulnerabilities in the Tesla Model S vehicle that could allow an attacker to remotely operate the door locks, horn, skylight, and headlights of the vehicle while in motion. Tesla Motors stated that the company will investigate and address any issues identified by Qihoo 360 Technology or others during the SyScan +360 conference. Source: http://www.chicagotribune.com/classified/automotive/chi-tesla-model-s-hacked,0,7108232.story

July 21, The Register – (International) **Secondhand Point-o-Sale terminal was horrific security midden.** A researcher with HP found that a second-hand Aloha point-of-sale (PoS) terminal purchased from eBay still held a database of employee names, Social Security numbers, and addresses, as well as default passwords that could be used by an attacker if the previous owners did not change passwords in new equipment. Source: http://www.theregister.co.uk/2014/07/21/ebayed_point_of_sale_terminal_leak_peril/

July 21, Help Net Security – (International) **Unpatched OpenSSL holes found on Siemens ICSs.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) stated July 17 that six Siemens industrial control products contained vulnerabilities in their OpenSSL implementation that could lead to man-in-the-middle (MitM) attacks or the crashing of Web servers. Four of the vulnerabilities remain unpatched and are present in industrial control products used by the manufacturing, chemical, energy, agriculture, and water industries and utilities. Source: http://www.net-security.org/secworld.php?id=17146

July 19, Softpedia – (International) **Kelihos trojan delivered through Askmen.com.** Researchers with Malwarebytes reported that the online publication Askmen.com was compromised by attackers and used to redirect users to a malicious page serving the Nuclear Pack exploit kit for the purpose of infecting users with the Kelihos malware. The compromise was achieved by injecting malicious code into the Askmen.com server, and the site's administrators were notified. Source: http://news.softpedia.com/news/Kelihos-Trojan-Delivered-Through-Askmen-com-451345.shtml

July 18, Help Net Security – (International) **Fake Flash Player steals credit card information.** Dr. Web researchers reported finding a new piece of Android malware dubbed BankBot that is disguised as Adobe Flash Player and persistently asks users for administrator privileges in order to display a fake credit card information form and steal any entered information. The malware is currently targeting users in Russia but can be repurposed to attack other targets. Source: http://www.net-security.org/malware_news.php?id=2812

July 18, Securityweek – (International) **Researchers analyze multipurpose malware targeting Linux/Unix Web servers.** Virus Bulletin published an analysis of a recently discovered piece of malware that infects Linux and Unix Web servers known as Mayhem, which has infected around 1,400 servers. The malware relies on several plugins for various capabilities, including information stealing and brute-force attacks. Source: http://www.securityweek.com/researchers-analyze-multipurpose-malware-targeting-linuxunix-web-servers

July 18, Network World – (International) **Cisco counterfeiter gets 37 months in prison, forfeits $700,000.** The CEO of ConnectZone.com was sentenced for his role in conspiring with a Chinese company to produce counterfeit Cisco Systems network products and then sell them as genuine products. Four people and two companies were charged in the case, with two others found guilty and a Chinese co-conspirator remaining at large. Source: http://www.networkworld.com/article/2455477/cisco-subnet/cisco-counterfeiter-gets-37-month-prison-forfeits-700-000.html

July 18, Threatpost – (International) **Critroni crypto ransomware seen using TOR for command and control.** Security researchers found that a new piece of ransomware known as Critroni has been spotted in use by various attackers using the Angler exploit kit to infect users with it and other malware. The ransomware encrypts victims' files and demands a ransom, and uses the TOR network to contact its command and control servers. Source: http://threatpost.com/critroni-crypto-ransomware-seen-using-tor-for-command-and-control/107306

Your iPhone May Be Rigged to Spy on You

Tom's Guide, 22 Jul 2014: iOS forensic examiner Jonathan Zdziarski may know more about iPhones than any other non-Apple employee. Yet even he can't find a reason for some of the mystery features buried within the iOS operating system, which look an awful lot like security backdoors that bypass user-designated data protections. The features could be there to let Apple — or even the National Security Agency or the FBI — get access to most of your iOS device's data without you knowing it. In a presentation Friday (July 18) at the HOPE X hacker conference here, Zdziarksi detailed his discoveries about the data-collection tools hidden on iOS devices. Some tools are listed by name, yet not explained, in the Apple developer manual and do far more than advertised. Others are undocumented and buried deep within the iOS code. The hidden features may partly explain allegations, based on documents leaked in the Snowden archive, in the German newsmagazine Der Spiegel that the NSA has had the ability to access data on BlackBerrys and Android and iOS devices. Der Spiegel did not detail how the NSA would do so. The undocumented features can be accessed by any PC or Mac to which a targeted iOS device has been connected via USB, Zdziarski says. Some hidden features can also be accessed via Wi-Fi while the phone is at rest, or even while the owner is using it. Zdziarksi is certain that these mechanisms, whatever their purpose, are no accident. He has seen them become more complex, and they seem to get as much maintenance and attention as iOS's advertised features. Even as Apple adds new security features, the company may be adding ways to circumvent them. "I am not suggesting some grand conspiracy," Zdziarski clarified in a blog post after his HOPE X talk. "There are, however, some services running in iOS that shouldn't be there, that were intentionally added by Apple as part of the firmware and that bypass backup encryption while copying more of your personal data than ever should come off the phone for the average consumer." How would someone connect to these mechanisms on an iPhone? Zdziarski explained the trick has to do with iOS "pairing." When an iOS device connects to a PC or a Mac via USB, the mobile device and the computer exchange security certificates that establish a trusted relationship between the two, and exchange encryption keys for setting up an encrypted SSL channel. The keys and certificates are stored on the iOS device and on the desktop, and never deleted unless the iOS device is wiped (via the "Erase All Contents and Settings" feature) or the desktop is restored to factory settings. In most cases, this pairing relationship is established automatically as soon as the devices are connected. The first step in spying on an iOS device is to get that pairing data. A targeted iPhone could be covertly connected to a computer without the owner's knowledge (sort of the James Bond approach). Or spyware could be installed on the targeted person's desktop, and the pairing data copied. With the pairing data, attackers can locate the targeted iOS device on a Wi-Fi network. Because iPhones are set up to automatically join networks whose names they recognize (like "linksys" or "attwifi"), attackers can also force an iPhone to connect to an attacker-controlled network. In a research paper published in March in the journal Digital Investigation, Zdziarski writes: "It may even be possible for a government agency with privileged access to a cellular carrier's network to connect to the device over cellular (although I cannot verify this, due to the carrier's firewalls)." This is all a lot of ifs, of course. The attacker has to have the

pairing keys; the attacker must know where the targeted iOS device is; the attacker has to get on the same Wi-Fi network as the device; and the iPhone needs to have its Wi-Fi switched on. This may be more than the average criminal could pull off, but it wouldn't be difficult for the NSA, an agency with an approximately $52 billion budget, or the FBI. Once the paired connection is established, access is granted to the mystery tools. Perhaps the most serious is one that Zdziarski described as an "undocumented file-relay service that really only has relevance to purposes of spying and/or law enforcement." The feature, com.apple.mobile.file_relay, copies and relays nearly all the data stored on an iOS device, even when Backup Encryption is enabled. It is separate from iOS's documented backup and sync features. Since around 2009 iOS devices have had an optional feature called Backup Encryption. The feature encrypts all data backed up from an iOS device to a PC or Mac running iTunes, complete with a separate password. File_relay bypasses the password. Other tools are are only partly documented in official Apple publications. One is a packet sniffer, or network traffic analyzer, called com.apple.pcapd that views all network traffic and HTTP header data going to and from the iOS device. (Some packet sniffers can also analyze traffic to and from other devices on the same Wi-Fi network.) Packet sniffers can be useful for iOS developers testing their apps, but Zdziarksi said the feature enabled on all iOS devices, even those not in developer mode. "Why do we need a packet sniffer running on 600 million personal iOS devices?" Zdziarski asked during his presentation. No visual indication is given when com.apple.pcapd is running; it could be triggered and run without the user's knowledge. "It remains a mystery why Apple decided that every single recent device needed to come with a packet sniffer," Zdziarksi wrote in his research paper. Why do these features exist? Zdziarski can't prove that they were created as backdoors for law enforcement, and isn't even sure they were. But in his talk, he eliminated some of the other possibilities. Could the features be there for developers? No, said Zdziarski: Most of the mechanisms he identified are not in the official Apple developer manual. Are they there for Apple's engineers? No: Engineering tools don't need to be installed on every single iPhone. Is it simply forgotten code? No: Zdziarksi has seen these tools grow more capable with each iteration of iOS. When Apple added the Backup Encryption feature, he said, it also added the means to circumvent it. Clearly, Zdziarski feels, Apple is keeping these secret abilities alive. "They're maintaining this code," Zdziarski said at the HOPE X talk. "Over the years, year after year, there are new data sources in file_relay ... nobody has forgotten about [these mechanisms]." "I think at the very least, this warrants an explanation and disclosure to the some 600 million customers out there running iOS devices," Zdziarksi wrote on his blog. "At the same time, this is NOT a zero day and NOT some widespread security emergency. My paranoia level is tweaked, but not going crazy." To read more click **HERE**

Apple iOS Laced with Undocumented Data Exfiltration Services

SoftPedia, 22 Jul 2014: Apple's iOS being targeted by the NSA is a fact, but in a talk last week at the Hackers On Planet Earth (HOPE X) conference in New York, data forensics expert Jonathan Zdziarski revealed the existence of certain services in iOS that offer a backdoor for surveillance. According to the expert, this is a feature that has been available in the operating system for years and has evolved in time, constant updates being applied in each version of the mobile OS. Although present in about 600 million devices, Zdziarski says that the feature "is not a zero day and not some widespread security emergency." The services discovered to offer the possibility to extract data from Apple devices function separately from regular backup encryption, and are low-level components that can be handled through methods and mechanisms that are not publicly available, more appropriate for corporations and government agencies. Zdziarski notes that "every single device has these features enabled and there's no way to turn them off, nor are users prompted for consent to send this kind of personal data off the device." Among the components that can be used for data acquisition is the "mobile.file_relay" service, which can also be accessed remotely (WiFi) and bypasses the backup encryption of the iOS. It can be used for exfiltrating information available in the address book, photos, voicemail, audio data, keystrokes, clipboard details, accounts (Twitter, iCloud, Facebook, etc.) configured on the device, as well as GPS logs. On iOS 7, "mobile.file_relay" can provide a complete metadata disk sparse image of the file system, meaning that no actual content is available, only the details about each item: time stamp, file name, size, creation date,

time of the last activation or wipe of the device, list of apps installed and their files, names of email attachments or phone numbers related to short text messages. It appears that the services allow extraction of the data in raw format, which makes it impossible to put it back in an altered state, or to restore the original data of the phone. This eliminates diagnostics and enterprise as reasons for their presence and suggests that they may be of use to spying agencies, especially since "the data they leak is of an extreme personal nature," and no notification is sent to the user. Among the components is a packet sniffer, called "com.apple.pcapd," that can start capturing in/out traffic immediately. It is active on every iOS device, about 600 millions of them, and can be targeted via WiFi for remote monitoring; obviously, all activity is hidden from the user. A set of slides from Jonathan Zdziarski explain the purpose of some of the features and why they couldn't have been created specifically for the good of the user. It is worth noting that most of these data acquisition features are documented by Apple, and that Zdziarski contacted both Steve Jobs and Tim Cook for an explanation about them, but received no reply from either of them. To read more click **HERE**

Russia Ready to Dump Microsoft Software after Sanctions

SoftPedia, 22 Jul 2014: Russia is planning to launch a new rule that would help the country move away from software and hardware products developed by hardware companies, trying instead to focus on solutions created by local firms. Microsoft, HP, IBM, Cisco and Oracle are among the companies to be affected by the new law, which could come following new sanctions imposed by the United States to Russia due to the military conflict in Ukraine. Even though this hasn't been yet confirmed, it appears that this new law is Russia's answer to the sanctions is received, with the aforementioned companies very likely to be severely impacted by the restriction. "This all has to do with sanctions," Andrey Chernogorov, executive secretary of the commission, was quoted as saying by BusinessWeek. "Given the current international tensions, substituting imports with local software and hardware becomes the key to ensuring self sufficiency." According to the same publication, HP, IBM, Microsoft, Cisco, Oracle and Germany's SAP reported combined revenues of 285 billion rubles ($8.1 billion) from Russia last year, mostly thanks to contracts with the government and other state-controlled companies. Russia is not the first country where Microsoft might have to face the government's decision to step away from its software, as authorities in China are also planning to switch from Windows and Microsoft Office to alternative solutions, including an open-source platform. Microsoft itself said that in most cases it's willing to continue talks with government officials to get its products unbanned, but it's not yet clear if company officials can really do anything in the Russian crisis. As far as China is concerned, the country banned Windows 8 on security claims, but Microsoft said that Windows 7 would continue to be offered as a replacement until discussions come to an end. "Microsoft has been working proactively with the Central Government Procurement Center and other government agencies through the evaluation process to ensure that our products and services meet all government procurement requirements. We have been and will continue to provide Windows 7 to government customers. At the same time we are working on the Window 8 evaluation with relevant government agencies," the company said in a statement a couple of months ago. We've also contacted Microsoft for a word on the new law proposed by the Russian government, so we will update the article when and if we receive an official statement from a company spokesperson. To read more click **HERE**

Alleged Stormbot Source Code Advertised for Sale on YouTube

SoftPedia, 22 Jul 2014: A video advertising the selling of the source code for the Stormbot malware and providing a list of features for the threat was posted on YouTube on July 20. The poster also provides a link to a website where the purchase can be made by those trying to start a criminal business. The price has been set to $200 / €148. At the moment, there is no confirmation that the post is really pointing to the real source code of the malware, but this is not the first time Google's video repository is used to promote alleged illegal activities. The YouTube entry contains details about each of the modules included in the package: UDP DNS, SYN, Abuse, DNS Scanner, and SYN Scanner. The video shows a complete demonstration of the damage that can be delivered from the command and control server, which offers

various options, from adding new servers to upgrading or rebooting the remote machine. The clip has been seen before on YouTube, in January, the same details about the modules being shared with the viewers. However, this time, a link to a purchase page is also available. Storm bot in its original form is believed to be extinct and to have evolved into other malicious tools. Even so, such videos may not be considered YouTube-worthy because they could give ideas to the wrong individuals. Code for threats that are now defunct is publicly available on the Internet for research purposes, but selling it may not be exactly legal. To read more click **HERE**