THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

23 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

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

The world's most secure OS may have a serious problem

The Verge, 22 Jul 2014: The Tails operating system is one of the most trusted platforms in cryptography, favored by Edward Snowden and booted up more than 11,000 times per day in May. But according to the security firm Exodus Intelligence, the program may not be as secure as many thought. The company says they've discovered an undisclosed vulnerability that will let attackers deanonymize Tails computers and even execute code remotely, potentially exposing users to malware attacks. Exodus is currently working with Tails to patch the bug, and expects to hand over a full report on the exploit next week. "We're hesitant to release any technical details because we don't want anyone to be able to reproduce [the exploit]," Exodus co-founder Aaron Portnoy told The Verge. After announcing the discovery in a tweet yesterday, the company has promised to withhold the details of the bug until it is successfully patched, a process that could take months. Exodus sells undisclosed vulnerabilities as part of its business, but because of Tails' activist user base and the extreme privacy concerns, Portnoy says they disclosed the bug to Tails developers free of charge. "We were just trying to let everyone know, you can't trust any of these systems 100 percent," Portnoy says. In response, the Tails developers stressed the constantly updating nature of the project, and the abruptness of Exodus's disclosure. "We were not contacted by Exodus Intel prior to their tweet," the development team said in a blog post. "In fact, a more irritated version of this text was ready when we finally received an email from them." It's still unclear which aspect of the software is vulnerable, and it may prove to be a plug-in application like Claws Mail or Pidgin that was developed separately from Tails itself. But until the bug is patched and published, it will be hard to say for sure. "We're really looking forward to reading this report," the developers said. To read more click **HERE**

July 22, Securityweek – (International) **Attackers bypass 2FA systems used by banks in 'Operation Emmental'.** Researchers with Trend Micro released a report July 22 detailing a cybercrime campaign targeting banks in Europe and Japan dubbed "Operation Emmental" that uses computer and Android mobile device malware to steal users' banking credentials and two-factor authentication (2FA) tokens. The malware used in the campaign can install fake Secure Sockets Layer (SSL) certificates, delete itself after use, and perform other actions to trick users. Source: http://www.securityweek.com/attackers-bypass-2fa-systems-used-banks-operation-emmental

July 21, Krebs on Security – (National) **Banks: Card breach at Goodwill Industries.** Goodwill Industries stated that it is working with the U.S. Secret Service to investigate a possible breach of payment card data from some of its U.S. stores. The company stated that it became aware of a possible breach July 18 after they were contacted by a payment card industry fraud investigation unit and federal authorities. Source: http://krebsonsecurity.com/2014/07/banks-card-breach-at-goodwill-industries/

July 21, NextGov – (National) **Significant deficiencies found in Treasury's computer security.** Two reports by the Government Accountability Office released the week of July 14 found new computer security vulnerabilities at the U.S. Department of the Treasury's Bureau of Fiscal Service and existing security issues at the Federal Deposit Insurance Corporation that remain unaddressed from 2012 which could compromise reporting efficiency or the security of data. Source: http://www.nextgov.com/cybersecurity/2014/07/significant-deficiencies-found-treasurys-computer-security/89144/

July 21, SC Magazine – (California) **Thousands had data on computers stolen from California medical office.** The California office of the Bay Area Pain Medical Associates notified about 2,780 patients July 10 that their personal information may have been accessed after three desktop computers were stolen May 19. The computers held spreadsheets containing patients' personal information. Source: http://www.scmagazine.com/thousands-had-data-on-computers-stolen-from-california-medical-office/article/361852/

July 22, Securityweek – (International) **iOS backdoors expose personal data: Researcher.** A security researcher presenting at a security conference reported that Apple's iOS mobile operating system contains several undocumented services which could be used in some circumstances to access email, location data, media, and other personal data. Apple stated that the services are used for diagnostic purposes and can only be used to access data with user approval. Source: http://www.securityweek.com/ios-backdoors-expose-personal-data-researcher

July 21, V3.co.uk – (International) **Fresh threat to critical infrastructure found in Havex malware.** Researchers at FireEye analyzed a variant of the Havex malware (also known as Fertger or Peacepipe) and found that it contained an open-platform communication (OPC) scanner that could be used to target supervisory control and data acquisition (SCADA) systems used by several industries, including power plants and water utilities. Source: http://www.v3.co.uk/v3-uk/news/2356410/fresh-threat-to-critical-infrastructure-found-in-havex-malware

Vladimir Putin Signs Law Forcing Internet Companies to Store Russian Data Locally
SoftPedia, 23 Jul 2014: The Russian president has just signed a law that will make things extremely difficult for all foreign companies that hope to reach users in the country. Putin has validated a law that requires Internet companies to store personal data of Russian users within the country's borders. This means that all companies that don't even have offices in Russia, need to store user data into local data centers, ZDNet reports. Despite this being veiled as an effort to keep people's data safe inside Russia and away from the watchful eye of the NSA and the GCHQ and any other foreign intelligence service, there's more to the decision. The most important part is that using Russian data centers makes companies subject to Russian laws on government access to information. Basically, the government gave itself the right to get whatever data it wants from these companies. Even so, lawmakers continue to claim that it's all about minimizing the risk of Russian citizens' data being hacked and stolen by criminals, as if keeping things locked inside the country will automatically fend off those with ill intent. If they managed to refuse this type of access before, now the entire opposition has been crushed and the companies will have to comply or risk being blocked in the country entirely. The Russian Association of Electronic Communications, which is essentially a group that lobbies in the name of Internet companies, believes that the law will make it impossible for many global Internet services to operate. Furthermore, the two-year deadline included in the law to have companies comply with the new regulations isn't nearly enough. While some smaller companies would likely just try to find some data center to store the data, companies such as Facebook, Google, and many others would need to build data centers. The process is obviously a lengthy one since companies need to find a location, to create a project, to build the center, bring in the necessary equipment, test it out and so on. The new law is part of a larger effort in Russia to control the Internet through various measures and, perhaps more importantly, to compel foreign

companies to abide by Russian laws and requests of data without question. The idea of having big companies store data within a country's borders isn't exactly new since in the past year the notion has come up more than once, mostly following the NSA scandal and the international implications of the mass surveillance effort. To read more click **HERE**

Apple Denies Backdoor Data Allegations, Calls Them "Diagnostic Capabilities"

SoftPedia, 23 Jul 2014: A known iOS Jailbreaker, currently iOS security expert, Jonathan Zdziarski has published a report about the way iOS devices may have a backdoor access to important user data. His allegations were detailed in an almost 60-page report complete with questions for Apple officials. The Cupertino-based company responded with a new page on iOS Diagnostic capabilities. Jonathan Zdziarski, also known as NerveGas, was a member of the dev-team, the jailbreak stars who made iOS Jailbreaking possible until iOS 4. He then published five iOS-related books and went on designing iOS forensics techniques used in law enforcement and commercial products. Zdziarski believes Apple has worked hard to make iOS devices reasonably secure against typical attackers so now iPhone 5 or newer devices and iOS 7 is a more secure combination for everybody except Apple and the government. According to him, "Apple can extract certain categories of active data from passcode locked iOS devices. Specifically, the user generated active files on an iOS device that are contained in Apple's native apps and for which the data is not encrypted using the passcode ('user generated active files'), can be extracted and provided to law enforcement on external media." He says that Apple can do that even on newer iOS versions and the files can be SMS, photos, videos, contacts, audio recordings, and call history. Apple cannot provide emails, calendar entries or any third-party App data. Zdziarski is worried about a packet sniffer that runs on 600 million iOS devices. He says the data obtained from these devices is too raw to be used for tech support and can't be put back onto the phone so it's not just a way to back-up the settings. Moreover, the fingerprint reader doesn't add any additional encryption beyond the basic PIN. He does not accuse Apple of working with the NSA or other agencies, but makes the point that the technical possibility exists. Apple has responded to the allegations presenting the list of iOS diagnostic capabilities that can help IT Departments, developers and AppleCare troubleshoot issues. However, the Tech Giant says that, in order for someone to access them, the user has to unlock his device and agree to trust another computer. All data transmitted between an iOS device and a trusted computer is not shared with or sent to Apple. To read more click **HERE**

Cybercriminals Deliver Exploits through Facebook

SoftPedia, 23 Jul 2014: A recent malicious campaign that lured users into clicking on a link to news about easy making of large amounts of money from home would use multiple redirects, some of the pages delivering the Nuclear Pack exploit kit. It seems that the crooks are becoming more sophisticated in their attacks, making the scam as profitable as possible, as potential victims did not have to actually infect their computers to fill the scammers' pockets; simply sharing one of the URLs provided by the crooks would be sufficient. Security researchers from Symantec say that the lure is an article purporting to reveal how a woman makes $8,000 / €5,900 per month without having to leave her home. Users interested in finding out more details click on the link and end up on another page that runs redirects to different online malicious locations. In some cases, these deliver the Nuclear Pack exploit kit, known to leverage vulnerabilities in older versions of Java, Adobe Acrobat, and Adobe Reader. However, in this example, the researchers say that the exploits used take advantage of security glitches in Microsoft Internet Explorer (CVE-2013-2551) and Java (CVE-2012-1723). "After successfully exploiting the vulnerability, the Nuclear exploit kit drops Trojan.Ascesso.A. Trojan.Ascesso.A is known for sending spam emails and downloading other files from a remote location," says Symantec's Ankit Singh. Telemetry from the systems of the security firm shows that the most affected regions are North America and Europe. By enticing the potential victim to first share the malicious link, the crooks make sure that the scam perpetuates to other users. A similar strategy that relies on multiple redirects to pages specially created to ensure the scammers make money in one way or another has been seen in the recent Facebook malicious campaign that purported to show the shooting down of the MH17 Malaysian airliner. Users were blasted with all

sorts of malicious actions, from being pushed software downloads, very likely as part of an affiliate marketing scheme, to being prompted to install fake updates for Adobe Flash in order to be able to watch the alleged footage. By attempting different scams while the user accesses a single link, the success of the scam increases, especially since efforts are made to keep the user on the page that fires the redirects. Users are warned to refrain from accessing links that appear suspicious, even if they are sent from a familiar individual, because they might have inadvertently participated in distributing the lure. To read more click **HERE**

Nigerian 419 Scammers Move Up the Cybercrime Ladder

SoftPedia, 23 Jul 2014: After running 419 scams, a group of Nigerians changed their activity and now target victims in Taiwan and South Korea, using cheap software designed to take control over their computer systems. Palo Alto Networks, a Santa Clara-based network security firm, released a report showing that Nigerian cybercrooks started to employ remote access tools (RATs) in order to gain access to the victim's system, be it Windows, Mac or Linux. They managed to track the origin of a malware campaign to IP addresses in Nigeria and also found evidence of 419 scammers learning the tricks of the trade for using malware in order to steal from their victims. Researchers found that the crooks relied mainly on two pieces of malware to render their attacks undetectable. One is called NetWire and its purpose is to provide access to the remote machine via a graphical interface. The second, dubbed DataScrambler, is used for encrypting the RAT in order to avoid antivirus detection; the malware is delivered via email, as an attachment. In some of the email samples discovered by Palo Alto Networks, the malicious executable file was called "Quatation For Iran May Order.exe," and it appears that at that time it was detected by only two of the 51 antivirus engines that scanned it on VirusTotal. During the investigation of this type of attack, the security researchers identified additional ones, with similar traits. The tracking of this malicious campaign was called "Silver Spaniel." The Californian security firm is not aware how the former 419 Nigerian scammers choose their victims, but they noticed that targets were companies in Taiwan and South Korea. It appears that despite their remarkable social engineering skills, these cybercriminals have still a lot to learn about malware. They purchase ready-made tools from underground forums, do not have experience with coding, and no software vulnerability is leveraged to infect the computer. Instead, they rely on social engineering for tricking the victim into installing the malware. According to the results of the investigation, the scammers set up the remote access tools to connect to a dynamic DNS domain from NoIP.com. They also use a VPN service to route the traffic through a different IP address than the one provided by the ISP. "Silver Spaniel actors' objective appears to be stealing passwords and other data they can use to further compromise their victim. Thus far we have not observed any secondary payloads installed or any lateral movement between systems, but cannot rule out this activity," says the Palo Alto Networks report. To read more click **HERE**

Simplocker Crypto-Malware Now Locks Backup Files, Targets Larger Audience

SoftPedia, 23 Jul 2014: A new variant of the Android ransomware Simplocker has been detected and it comes with encryption capabilities for archives, which is the preferred format of many backup apps for mobile devices. Security researchers at ESET, who uncovered the first trace of the crypto-malware for mobile in the first place, warn that the fresh strain has been prepared for targeting a larger audience, as the ransom message is now in English and the demanded fee increased to $300 / €222. Cybercriminals seem to have learned their lessons during the test run on the Russian-speaking victims and included 7z, ZIP and RAR compression formats on the list of files the malware should be encrypting. These types of archives are the most popular when creating safety copies of the Android device with a backup app. As such, when the device is infected, the victim can no longer restore the information from the backup because it is also encrypted and its contents cannot be accessed; thus, the crooks increase the chances of getting paid. However, ESET's Robert Lipovky says that there is no significant modification as far as the encryption function is concerned, as it uses a different key for carrying out file locking. So, he mentions that there are solutions for decrypting the locked data and provides an ESET tool for the job. The researcher noticed that the revised Simplocker asks for administrator privileges, which increases its

resistance against removal, because not many users know that stripping an app of admin advantages can be easily done from Settings>Security>Device Administrators, in order to be able to remove it. Simplocker is the first file-encrypting ransomware for Android operating system, and samples appeared on the security industry's radar at the beginning of June. At that time, the malware was more of a proof of concept rather than a full-fledged money making tool. It created some confusion, because while the ransom message was in Russian, the fee was expressed in Ukrainian hryvnia. Security researchers at Kaspersky spotted the malware for sale on underground forums in May, for the price of $5,000 / €3,680. After that date, the Simplocker infections took off and spread to non-Russian speaking countries. Multiple strains have been seen since then, as researchers observed different working methods. One of the variants would show the victim the ransom message with their picture on the screen, taken with the built-in camera; this also seems to be the case with the fresh strain. The current version does not seem to propagate differently than its predecessors and social engineering is still employed for the trickery. Crooks lure the potential victim with legitimate looking apps, such as Flash video player, but others can be promoted, too; the downloads are from unverified app stores. To read more click **HERE**

Mozilla Firefox 31 Fixes Three Critical Vulnerabilities

SoftPedia, 23 Jul 2014: On July 22, Mozilla officially released the stable version of Firefox 31 for all supported platforms, integrating 11 security fixes, three of them being marked as critical. One of the major vulnerabilities corrected would allow exploitation of a WebGL crash with Cesium JavaScript library. Details about this glitch are not available at the moment, but Mozilla notes that it cannot be leveraged through email in the Thunderbird client because scripting is disabled. Another flaw refers to a use-after-free vulnerability when handling DirectWrite font. Exploiting it would be possible on Windows platform only, OS X and Linux remaining unaffected. The potential risk would occur when rendering MathML content with certain fonts, an error in handling font resources and tables causing DirectWrite to crash; the result would be a use-after-free of a DirectWrite font-face object an attacker might be able to exploit. Last on the list of critical fixes are multiple memory safety hazards that affected version 30 of the web browser. According to Mozilla, memory corruption would be evident in specific scenarios and a motivated attacker might find a way to take advantage and run arbitrary code. Additional security vulnerabilities repaired by Mozilla in the latest revision of Firefox refer mostly to use-after-free flaws identified in Web Audio, with the FireOnStateChange event and when manipulating certificates in the trusted cache. Security improvements do not stop at this, though, as the company announced that Firefox 31 has been added a protection mechanism against malicious downloads. The feature relies on the Safe Browsing API from Google and leverages application reputation information to detect malware in file downloads. The mechanism consists in verifying the metadata, such as download URL, SHA-256 hash, details about the certificate, belonging to the item requested by the user, and comparing it to a given block list. The verification is carried out both based on a local list of files as well as a remote one. If a match is found, the file is not saved to disk. Alternatively, when files are signed, they are checked against a given whitelist, the binary is marked as trusted, and the remote check is no longer performed. A new SSL/TLS certificate verification is now present in Firefox 31 and uses the more robust and easier to maintain "mozilla::pkix" library. This should not be something noticeable by the regular user, but compatibility issues may arise for websites that do not use a certificate issued by an authority accepted in the Mozilla CA Program. A more comprehensive overview is available in an April post from Mozilla. To read more click **HERE**