THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

19 June 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

June 16, U.S. Attorney's Office, Northern District of Illinois – (International) **Alleged associate of NullCrew arrested on federal hacking charge.** The FBI arrested a Tennessee man June 11 and charged him with federal computer hacking for allegedly conspiring to launch cyberattacks on two universities and three companies, and releasing information from previously hacked computers causing significant financial damage to the institutions. The suspect is believed to be an associate of the NullCrew hacking group. Source: http://www.fbi.gov/chicago/press-releases/2014/alleged-associate-of-nullcrew-arrested-on-federal-hacking-charge-involving-cyber-attacks-on-companies-and-universities

June 18, Softpedia – (International) **Zbot variant poorly detected by AV engines.** An AppRiver researcher discovered a variant of the Zeus/Zbot trojan being distributed in spam emails inside a password-protected .zip file, allowing it to evade many security programs and filters. The researcher reported that the malware was identified by 5 of 52 antivirus engines. Source: http://news.softpedia.com/news/Password-Protected-Zbot-Variant-Poorly-Detected-by-AV-Engines-447373.shtml

June 18, Help Net Security – (International) **Microsoft patches DoS flaw in its Malware Protection Engine.** Microsoft released an update for its Malware Protection Engine that closes a vulnerability that could allow an attacker to use a specially-created file to trigger a denial of service (DoS) attack. Source: http://www.net-security.org/secworld.php?id=17022

June 18, Threatpost – (International) **Belkin patches directory traversal bug in wireless router.** Belkin released a firmware update for its N150 wireless home routers in order to close a serious directory traversal vulnerability that could allow a remote, unauthenticated attacker to read system files on the router. Users were advised to update their firmware as soon as possible. Source: http://threatpost.com/blekin-patches-directory-traversal-bug-in-wireless-router

June 18, Softpedia – (International) **Symantec Web Gateway 5.2 susceptible to SQL injection and XSS attacks.** Symantec advised users of its Symantec Web Gateway product running version 5.2 of its appliance management console to update to the newest 5.2.1 build after a SQL injection and a cross-site scripting (XSS) vulnerability were found in 5.2. The vulnerabilities could enable unauthorized privileged access to databases and the hijacking of user sessions. Source: http://news.softpedia.com/news/Symantec-Web-Gateway-5-2-Susceptible-to-SQL-Injection-and-XSS-Attacks-447241.shtml

June 18, Softpedia – (International) **Tumblr blogs compromised to redirect to diet pill spam.** A Symantec researcher found that several Tumblr blogs and Pinterest accounts have been hijacked in order to redirect visitors to a spam Web site promoting diet pills. Source: http://news.softpedia.com/news/Tumblr-Blogs-Compromised-to-Redirect-to-Diet-Pill-Spam-447395.shtml

June 17, SC Magazine – (International) **Researchers detect spike in "snowshoe" spam attacks using .club gTLD.** Researchers with Symantec reported an increase in spam attacks utilizing multiple IP addresses and generic top-level domains (gTLD) to attempt to prevent detection by spam filters, known as "snowshoe" attacks. The increase was first observed June 12, with the attacks using .club domains. Source: http://www.scmagazine.com/researchers-detect-spike-in-snowshoe-spam-attacks-using-club-gtld/article/356258/

June 17, Securityweek – (International) **TowelRoot vulnerability could lead to attacks on Android devices.** Researchers with Lacoon Mobile Security reported that a Linux vulnerability exploited in the TowelRoot rooting tool for Android devices could also be used by attackers to gain root/administrator privileges and bypass Android security controls. Source: http://www.securityweek.com/towelroot-vulnerability-could-lead-attacks-android-devices-researcher

U.S. senators push ahead with cybersecurity legislation

The U.S. Senate Intelligence Committee is expected to consider a bill next week aimed at encouraging companies to exchange information on hacking attempts and cybersecurity threats with the government, senators said on Tuesday as they released a draft of the legislation. Although the politically polarized Congress has just over seven weeks left to pass new laws, the bill's authors have expressed optimism about passing it this year. U.S. Homeland Security Secretary Jeh Johnson in May also told the Reuters Cybersecurity Summit that he expected Congress to agree on cyber legislation this summer. U.S. lawmakers have been considering legislation to help private companies better communicate about security breaches and cyber threats with the government and each other, but spats over liability and privacy protections have thwarted passage of comprehensive cyber security bills thus far. The bill by Feinstein and Chambliss would offer companies liability protections for monitoring their networks for hacking attempts and for sharing cyber data with the government through the Department of Homeland Security, which would immediately disseminate the information to relevant federal agencies. The legislation would also require companies to remove personally identifiable information before sharing cyber data. The U.S. attorney general would establish procedures to limit the government's use of cyber data, and the Privacy and Civil Liberties Oversight Board and federal inspectors general would monitor application of the law. Chambliss earlier this month said he was confident he and Feinstein could "pretty quickly" combine their bill with the one passed last year in the House of Representatives, which he said differed from the Senate bill on liability protections offered to companies. The Republican-controlled House of Representatives last year for the second time passed legislation addressing cyber information sharing, but efforts fizzled in the Senate, where many Democrats had sought a broader bill. Privacy advocates have opposed giving company's liability protections, worried about abuses of consumer data both by the private sector and the government. To read more click HERE

Obvious scam Android app installed over 1 million times in under a month

BGR, 17 Jun 2014: An obvious scam Android app has been installed over 1 million times in under a month. Reddit's Android community has flagged an obvious scam app called Subway Train Game in the Google Play store that has been installed more than 1 million times in less than a month. What makes this game such an obvious scam? Start with the excessive permissions it requests — a game that purportedly is centered on running through subway tunnels for some reason needs to have access to your device's microphone to record audio, to your device's camera to snap pictures and to know your precise location through GPS. What's more, as Redditor Androidclean points out, the game violates Google's in-app ad policy by having banner ads on both the top and bottom of the game and that clicking on the supposed link to the developers' homepage redirects you to Facebook's main page. You can flag this app as inappropriate by finding it on an Android device through the Google Play store and clicking the "Flag as inappropriate" at the bottom of the game's page. You can only do this through an Android device, however, and you won't be able to flag it if you're trying to do so from your PC. To read more click HERE

Incredibly sneaky piece of malware finally removed from Google Play

BGR, 17 Jun 2014: An incredibly sneaky piece of malware has finally been pulled from Google Play. Even various legit Android apps have been found to have additional hidden powers, which is why it shouldn't surprise us that one more piece of malware has apparently made it to the Google Play Store. FireEye, the security firm that discovered the malicious app, worked with Google to have the app removed from the store after finding that it was able to steal user data including SMS messages, certificates and even banking details. Titled "Google Play Stoy," the app pretended to be the official Google Play Store app once installed featuring the same app icon, albeit it did have a weird "google app stoy" name. Apparently the app was able to evade detection – with only three out of 51 antivirus apps being able to detect it – by encrypting the malware part behind a fake user interface. Once installed, the malware app can't be uninstalled. Instead, it fools the user into believing it malfunctions and is automatically uninstalled by providing fake error messages. However, while the app disappears from the screen after showing an error message, it still runs in the background, from where it's able to collect data and send it via email to Gmail accounts – the FireEye team has worked with the Gmail team to also terminate the Gmail accounts that received data from this app. To read more click HERE

7 Million+ Cards Likely to Have Been Stolen in P.F. Chang's Breach

SoftPedia, 19 Jun 2014: The computation took into consideration the possibility that the company's restaurants had in fact been leaking credit card data for a period of nine months, since September 2013. According to KrebOnSecurity, Visa released a CAMS (Compromised Account Management System) alert on June 17 informing that hundreds of cards had been exposed in a recent breach that actually started on September 18. CAMS alerts are generally circulated privately by card associations to banks that issue their cards, in order to inform them that certain cards have been involved in a data breach incident. The banks can then take the necessary steps for mitigating the damage. Although the CAMS notification did not mention that the breach had occurred at P.F. Chang's, one of the banks that contributed to breaking the news of the incident "purchased more than a dozen cards sold from an underground store that's been exclusively selling cards stolen in the P.F. Chang's break-in, and every one of those cards was listed on the June 17 CAMS alert from Visa," says KrebOnSecurity. At the moment, there is no clear information about the number of cards that were stolen, but Brian Krebs made some computations that included the income statement of the company for the first quarter of 2012, an estimate of the average customer's bill and the number of P.F. Chang's locations affected. The estimation is that the restaurants processed about 800,000 credit and debit cards per month. Multiplied by the number of months provided by the Visa CAMS alert, this gives a total of 7,200,000 cards. Of course, these are just estimates, but they are based on old information and rough calculations. The number could be much higher, or it can very well not reach this figure. The results of the initial investigation revealed that the batch of stolen cards that were for sale on the underground forum have been used in locations in the US only, like Florida, Maryland, New Jersey, Pennsylvania, Nevada and North Carolina. Also it appears that the seller is Russian because he instructed customers not to transfer the money for the items during the days of a Russian national holiday. The price for the cards varies between $18 (13EUR) and $140 (104 EUR). As a precaution to future customers, P.F. Chang's switched to charging the cards through a manual credit card imprinting system. This has been implemented in all their locations in the continental US. To read more click HERE

Simplocker Changes Attack Vectors

SoftPedia, 19 Jun 2014: Despite the simplicity publicized by various security researchers and the fact that there are solutions to reverse its malicious activity, Simplocker has seen an increase in distribution. Robert Lipovky, malware researcher at ESET, warns that several variants of the Trojan have been detected, a fact also confirmed at the beginning of last week by Kaspersky. However, the researcher points out that the new modifications have integrated the command for file decryption, which indicates that the ransom was paid by the victim. Also, different sums of money are demanded, in both Ukrainian hryvnias and Russian rubles. Only Russians and Ukrainians seem to be targeted by the Trojan right now, and there is no indication of extortion attempts in other currencies than the ones mentioned above; but the trend could change since the distribution in the rest of the world has reached 10%, according to ESET metrics. The threat is most prevalent in Russia, where 48% of the infections have been recorded, while Ukraine accounts for 42%. As far as the attack vectors are concerned, the threat is still distributed using social engineering tactics that lure the victim with incentives ranging from adult video content to apps purporting to be popular games. Apart from this, the ESET team noticed a new strategy from the cybercriminals, which involves a Trojan downloader, identified by the products of the security firm as Android/TrojanDownloader.FakeApp. Lipovky says that the analyzed sample tempted the victim to download the malware masqueraded as a video player via an external link. This way, the downloader has slimmer chances of being detected by security mechanisms that verify the items published on Google Play. This is possible because there are no signs of malicious behavior; opening a link outside the app is common to many other programs and "the downloader has practically no 'potentially harmful' application permissions – so even a user who scrutinizes app permissions at installation may allow this one," writes Lipovsky. Additionally, in the sample checked by the ESET team "the URL contained within the app didn't point to the malicious Simplocker APK package directly. Instead, the trojan was served after a redirect from the server under the attacker's control. This technique is something to watch out for." This week, Avast released a tool that can scan Android devices for signs of Simplocker infection and remove it. Moreover, it provides file decryption services if the data has already been taken hostage. The tool is free and can be installed remotely from Google Play on the affected device. To read more click HERE

Microsoft Issues New Windows 8.1 Update Patch for Windows 8.1 Users

SoftPedia, 19 Jun 2014: Windows 8.1 Update is mandatory for Windows 8.1 users, but due to a number of issues experienced when trying to install the new OS version, many users are yet to upgrade, which means that theirs computers no longer receive updates and security patches released by Microsoft. Redmond is aware of the fact that some users had problems installing Windows 8.1 Update and recently issued a new patch that's supposed to resolve some, if not most, of these issues. No specifics have been provided on what's new in this revised version of KB2919355, but Windows 8.1 computers started receiving it last week when the company began shipping new Patch Tuesday fixes. Others, however, are only getting it these days, as their computers are yet to be upgraded to Windows 8.1 Update. Microsoft announced a deadline of June 10 for Windows 8.1 users to install Windows 8.1 Update, admitting that some experienced errors when trying to deploy it. "While we believe the majority of people have received the update, we recognize that not all have. Having our customers running their devices with the latest updates is super important to us. And we're committed to helping ensure their safety. As a result, we've decided to extend the requirement for our consumer customers to update their devices to the Windows 8.1 Update in order to receive security updates another 30 days to June 10th," Microsoft said in a statement published in May. Basically, computers that aren't updated to the new OS version won't receive any other patches and security fixes until users deploy the KB2919355 pack, which means that they could easily become hackable if someone finds a vulnerability in the operating system. "Consumer customers who do not update their Windows 8.1 devices to the Windows 8.1 Update by this new deadline will no longer receive updates. We're confident that within the next month, the majority of the remaining customers who haven't updated their devices to the Windows 8.1 Update will be able to do so," the company explained. Right now, it appears that some users are still having trouble installing Windows 8.1 Update, but it's not yet clear whether their machines received the new patch or not. We've reached out to Microsoft for more information on this and to find out what exactly is new in the updated build, so we'll update the article when we receive an answer. To read more click HERE

Windows 8.1 Update 2 to be 3GB in Size, No Start Menu Included – Rumor

SoftPedia, 19 Jun 2014: Windows 8.1 Update was officially launched in April, but Microsoft is already working on a second update that's expected to arrive in either August or September. A post on the Windows Eight Forums claims that Windows 8.1 Update 2, if Microsoft indeed plans to name the second update this way, could arrive in August or September and be 3GB in size. While we already knew that Windows 8.1 Update 2 is very likely to arrive in August or September, this new post also suggests that the whole pack might have 3GB in size, which could be an indication that several important new features are very likely to be included. And still, it appears that the Start menu will be missing from Windows 8.1 Update 2, as Microsoft continues work on this particular feature and doesn't plan to bring it to the market sooner than early 2015. This pretty much means that the Start menu is very likely to debut in Windows 9, the next full version of the operating system that could be released in April 2015. According to the same forum post, all these details have been provided by a company support engineer, so we should really take all of them with a pinch of salt because Microsoft is very unlikely to share so important plans with workers and even allow them to disclose them to customers. Here's the full forum posting along with the new Windows 8.1 Update 2 details: “Spoke to a helpful rep and he sorted out my issue with the phone activation application. I asked him about Windows 9 and he said it was about a year away but they were being trained on update 2 for August or September time frame which will be served up by the store apparently and it is another 3Gb download. That is what I was told, now whether to believe them I don't know but what the heck would they be doing with a 3Gb download to update the OS? “ Windows 8.1 Update 2 will obviously be offered free of charge to everyone running Windows 8.1 and Windows 8.1 Update, and although the parent company hasn't disclosed such details until now, it's very likely to be offered through Windows Update for a much faster installation process. People familiar with the matter have said that the second Windows 8.1 update is expected to debut in August or September, so more details on this should be provided soon. To read more click HERE