The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

24 February 2014

Purpose
Educate recipients of cyber events to aid in the protection of electronically stored corporate proprietary, DoD and/or Personally Identifiable Information from theft, compromise, espionage, and / or insider threat

Source
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
To receive this newsletter please send an email to scott.daughtry@dtra.mil

NMCIWG Members
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, Sandia Labs

Banking Malware Distributed via YouTube Ads

SoftPedia, 24 Feb 2014: Malvertising attacks are becoming more and more common and it appears that not even YouTube users are safe. Security researchers from Bromium have come across a YouTube link that led users to an exploit kit website. According to experts, cybercriminals compromised an ad network that's used to serve advertisements on YouTube. The ad network in question hosted the Styx exploit kit. This particular exploit kit is designed to leverage Java vulnerabilities in order to push malware onto infected devices. In this case, the malware that's being distributed is Caphaw, a threat that's designed to harvest banking information from victims. The command and control server used by the cybercriminals appears to be hosted in Europe and it relies on a domain generation algorithm (DGA). Bromium has notified Google of the attack, but so far, there are no details on how the cybercriminals have pulled this off. To read more click **HERE**

SQL Injection Vulnerability on Tesla Motors' Website Exposed Customer Records

SoftPedia, 24 Feb 2014: A security researcher known as Bitquark has identified an SQL Injection vulnerability on the official website of Tesla Motors. Fortunately, the electric car maker addressed the security hole shortly after being notified of its existence. Initially, the expert only found some cross-site scripting (XSS) vulnerabilities on Tesla's website. However, after a while, he found the SQL injection bug in the Tesla Motors design studio, which allows customers to customize their car before placing an order. The flaw plagued a URL shortener that can be used by customers to share the configuration they've created with others. The vulnerability exposed the backend database, including customer records and administrator credentials. Tesla fixed the problem after being provided with some technical details and a Python script that exploited the security hole. Additional details are available on Bitquark's **blog**. To read more click **HERE**

Phishing Alert: PayPal Is Launching a New Survey Program

SoftPedia, 24 Feb 2014: Cybercriminals are trying to trick unsuspecting Internet users into handing over their personal and financial information with the aid of fake PayPal emails, which claim that the payment processor has launched a new survey program. It starts with an email that reads something like this: "As today 23 February 2014, PayPal is launching a new survey program. All customers can participate in the survey. The survey will take 5 minutes and for your effort and understanding PayPal will select most of the customers that takes this survey and reward them with £25.00 GBP. It would be helpful if you fill it out right now. If that is not possible, please do it soon. We plan to close the survey on 23 February 2014, so do not delay. Please note that all responses will be confidential. To start completing the Survey please download the attachement form and follow the steps to open a secure browser window." Security experts from Malwarebytes have analyzed this scheme. They warn that the archive file attached to the emails, online_form.zip, contains an HTM page that instructs users to answer a few questions. The answers to these questions are not important. What is important, at least for the cybercriminals running this scam, is that users enter the information in the second part of the form. Victims are asked to hand over their name, address, city, postal code, date of birth, payment card number, expiration date, CVV, sort code, and password. The submitted information is transmitted to a server controlled by the cybercriminals. These details can be more than enough for the crooks to perform fraudulent transactions with victims' credit cards. To read more click **HERE**

Neiman Marcus Says 350,000 Cards Are Impacted by Breach, Not 1.1 Million

SoftPedia, 24 Feb 2014: Shortly after learning that it had suffered a data breach, high-end retailer Neiman Marcus revealed that a piece of malware might have captured the data of as many as 1.1 million payment cards. After further analysis, the company has now determined that only around 350,000 cards are affected. In a letter published last week on the company's website, Neiman Marcus CEO and President Karen Katz noted that the number decreased because experts determined that the malware was not operating at all stores, and it wasn't operating every day. "Of the 350,000 payment cards that may have been affected by the malware in our system, Visa, MasterCard and Discover have notified us to date that approximately 9,200 of those were subsequently used fraudulently elsewhere," Katz explained. "Regardless of whether or not your card was affected, we have notified customers for whom we have mailing and/or e-mail addresses who shopped with us either in-store or online in 2013. Additionally, we are offering one free year of credit monitoring and identity-theft protection," she added. So far, there's no evidence that Social Security numbers and dates of birth have been compromised. There's also no indication that Neiman Marcus cards have been used fraudulently, or that online customers are impacted by the breach. Furthermore, PINs are not at risk because the retailer doesn't use PIN pads in its stores. Although the Neiman Marcus breach was announced shortly after Target admitted being hacked, experts say there doesn't appear to be any connection between the incidents. In the case of Neiman Marcus, the attackers had access to the company's systems for around eight months, but card data was stolen only between July 16 and October 30, 2013. To read more click **HERE**

Backdoor.AndroidOS.Torec.a: First Tor-Based Trojan for Android

SoftPedia, 24 Feb 2014: Security researchers from Kaspersky say they've identified the first Tor-based Android Trojan. The threat, dubbed Backdoor.AndroidOS.Torec.a, uses the anonymization network to hide its communications. According to experts, Torec.a relies on Orbot, an open source Tor client for Android mobile devices. Orbot functionality is leveraged to send commands from the C&C server to the Trojan. The list of commands includes intercepting incoming SMSs, stealing incoming SMSs, retrieving information on the phone and the installed applications, and sending SMSs to a specified number. Using Tor for C&C has some advantages, mainly the fact that the communications infrastructure is more difficult to disrupt. On the other hand, experts highlight that the malware developers have used more code to implement the use of Tor than they have for the Trojan's own functionality. Additional details on Backdoor.AndroidOS.Torec.a are available on Kaspersky's **blog** (report in Russian). To read more click **HERE**

Apple Confirms OS X Update Is Rolling Out "Very Soon"

SoftPedia, 23 Feb 2014: Following the discovery of a bug which leaves Apple's SSL/TLS library vulnerable to outside attacks, the Cupertino company has issued a statement confirming that a software fix is on the way. Discovered in iOS for iPhone, iPod touch, iPad, and Apple TV, and subsequently found in OS X as well, the flaw would allow an attacker with a privileged network position to "capture or modify data in sessions protected by SSL/TLS." Confirming that the vulnerability affects both of Apple's OSes, spokeswoman Trudy Muller now tells Reuters, "We are aware of this issue and already have a software fix that will be released very soon." Dmitri Alperovitch, chief technology officer at security firm CrowdStrike Inc., describes the flaw as "fundamental bug in Apple's SSL implementation." In other words, expect a patch to be released next week. The severity of the flaw became immediately visible when Apple released not only an unexpected iOS 7.0.6 update, but also iOS 6.1.6 for older-generation devices that don't normally receive updates anymore. Even the Apple TV software got a similar patch, in what became apparent that Apple's entire software ecosystem was affected by the flaw. Software researchers then quickly confirmed their hunches, namely that OS X was vulnerable too. Apple could either cook up a standalone fix or include the patch in the upcoming OS X 10.9.2 update for Mavericks users and additional security updates for older OS X versions. The company is just about done developing this imminent Mavericks update, so there's no reason not to believe that Apple is launching it next week, especially given the urgency of the matter. OS X 10.9.2 will be a free update for all Mavericks users, and any standalone updates designed to deal with this security flaw will be deployed in tandem. To read more click **HERE**

Cybercriminals Are Adapting Ransomware Tactics to Local Markets

SoftPedia, 22 Feb 2014: Security researchers from Trend Micro say they've identified a couple of ransomware attacks which suggest that cybercriminals are adapting their tactics to target local markets. A couple of attacks have been spotted – one aimed at users in Turkey and one at Hungarian internauts. The Turkish variant doesn't have a fancy interface. Instead, users are notified via a pop-up and the desktop wallpaper that they must pay a certain amount of money within three days to recover their files. Victims are told that their most important files have been encrypted using a technique that makes them impossible to recover without the proper key. The attacker in this case uses an email address that belongs to a provider in Ukraine. The malware is detected by Trend Micro as TROJ_RANSOM.ZD. The second piece of ransomware, TROJ_RANSOM.HUN, targets users in Hungary. Victims are told to pay 20,000 Forints ($88 / €64) to recover their files. Payment can be made via SMS or paysafecard codes. "While the attacks may have very similar behavior, our analysis indicates that the malware files themselves are not related. This indicates that multiple cybercrime gangs have 'gone local' and are adapting ransomware tactics to their local 'markets'; they may have been inspired by the success of CryptoLocker in recent months," experts noted. To read more click **HERE**

Apple Hires 17-Year-Old Jailbreaker "Winocm"

SoftPedia, 22 Feb 2014: Apple has hired jailbreaker "winocm," a teenager who was able to port the entire iPhone operating system over to Nokia N900. Of course, winocm's resume doesn't just include this single feat. He says he's been able to do some "insane" things with both iOS and OS X on a core level, and he's responsible for some iOS jailbreaks (for iOS 6.1.5, more recently). "I had to basically do exactly what Apple did when they were making iPhone OS originally," winocm tells Cult of Mac which points out that "By rewriting the iPhone OS from the ground up, he was essentially able to create an open source version of the operating system." Winocm added, "It's really complex and hellish stuff. Usually they have a team of people working on this type of thing, but I'm just one person, not a team." Hence the reason why Apple could really use a guy like him. Winocm himself broke the news about his hiring on Twitter yesterday, when he relayed to his 44K followers, "I figured now is the right time to say this, I will be working at Apple starting later this year." The Cupertino, California-based Apple Inc. will most likely use winocm's skill set to strengthen the security of iOS and OS X. As always, Apple hiring an iOS jailbreaker is somewhat ironical, having indulged in a fierce cat and mouse game before shaking hands. On the other hand, jailbreaking is getting less and less necessary these days, as Apple is offering more features and flexibility in its mobile software. But where there's room for tweaks that Apple doesn't allow, you can bet lots of people will still want to jailbreak their devices. In related news, Apple has discovered and subsequently patched a serious vulnerability in iOS 7 where "An attacker with a privileged network position may capture or modify data in sessions protected by SSL/TLS." The issue affects most iPhones and iPads currently in circulation today and has been addressed with the release of iOS 7.0.6 for new-generation hardware, and iOS 6.1.6 for old devices, such as the iPhone 3GS. Apple TV Software 6.0.2, released in tandem with these two updates, also includes the security patch. To read more click **HERE**

The Tricks LinkedIn Uses to Attract New Users

SoftPedia, 22 Feb 2014: LinkedIn has some 277 million users in the entire world, which is great for a professional social network, but apparently not nearly enough to appease the company that has resorted to some questionable techniques to appear larger. Countless users are complaining about one big issue that the service has – the fact that people in their contacts list appear as members of the platform, when, in fact, they're not. One user complained on Google+ that he had sent a connection request to an old acquaintance, but that he later found out that he didn't actually have a LinkedIn account. A quick investigation of the issue revealed that, most likely, the network went through this individual's email contacts and displayed the aforementioned person as active member. There's no more evidence to this than the fact that one of the contacts that LinkedIn was suggesting he add to his network was, in fact, his aunt, who had passed away and who was not an Internet user in any way, let alone LinkedIn. Basically, he points out, as he's backed by many other users, that LinkedIn is misrepresenting people who have an account to entice users. The system is quite simple. You are

made to believe that your high school friend has an account, so you send a connection request. In turn, that person receives an email saying you're looking for them on LinkedIn. This may end up with LinkedIn boosting its user base, which, in the end, seems to be the company's desire. Of course, LinkedIn isn't the only network to use this little trick, so you may want to be more careful about which tools you let in to your email address book. To read more click **HERE**

Holder calls for Congress to pass national data breach alert requirement for retailers

Fox News, 24 Feb 2014: Attorney General Eric Holder has called on Congress to require retailers to immediately report data breaches to customers and law enforcement. Holder's push comes in the wake of a massive data breach suffered by Target during the holiday shopping season late last year. The retailer and investigators estimated that approximately 40 million people had their debit and credit card information stolen, while as many as 70 million people had their personal information accessed. As we've seen – especially in recent years – these crimes are becoming all too common," Holder said in a video message posted on the Justice Department's website Monday. "And they have the potential to impact millions of Americans every year. Target was criticized for not informing customers of the issue sooner. The retailer disclosed the breach on December 23, but the data was accessed and stolen between November 27 and December 15. This [standard] would empower the American people to protect themselves if they are at risk of identity theft," Holder said. "It would enable law enforcement to better investigate these crimes – and hold compromised entities accountable when they fail to keep sensitive information safe." Executives from Target and Neiman Marcus were called before the Senate Judiciary Committee earlier this month to give testimony on their response to the data breaches. To read more click **HERE**

Details about Neiman Marcus breach revealed

Heise Security, 24 Feb 2014: The Neiman Marcus breach is not as bad as previously believed, as the number of potentially affected cards dropped from 1.1 million to approximately 350,000. "The number has decreased because the investigation has established that the malware was not operating at all our stores, nor was it operating every day in those affected stores, during the July 16 -October 30 period," shared Neiman Marcus CEO Karen Katz. The forensic investigation has determined that the malware was operating at 77 out of 85 of the retailer's stores, but not at every register or every day during the aforementioned period. "Of the 350,000 payment cards that may have been affected by the malware in our system, Visa, MasterCard and Discover have notified us to date that approximately 9,200 of those were subsequently used fraudulently elsewhere," she added, and also made sure to reiterate that Social Security numbers, birth dates and PIN numbers were not compromised, and that online customers were not impacted on by the breach. Consulting firm Protiviti's 157 page report revealed:

- The attackers are probably not the ones who breached Target, as they wrote specific code to compromise the Neiman Marcus network
- They had given the malware a name similar to the company's payment software, so that when the endpoint protection logs would be reviewed, entries tied to it wouldn't stand out
- The malware triggered the company's security systems on nearly 60,000 occasions, but it wasn't flagged as such and removed, and the system didn't automatically block suspicious activity as that particular feature had been turned off as not to hamper system maintenance
- The design of the retailer's POS system allowed attackers to reload the malware on a number of registers quickly after it was deleted at the end of each day
- The attackers compromised the POS system by way of an Internet-facing vulnerable server connected to it
- The company was in compliance with transaction data protection standards.

To read more click **HERE**

February 21, Softpedia – (International) **Mistake made by BitCrypt developers allows experts to recover encrypted files.** Airbus researchers discovered a new type of ransomware named BitCrypt and found a way to restore infected, encrypted files after discovering the developers made a mistakenly generated a 128-digit number instead of a 128-byte key. Source: http://news.softpedia.com/news/Mistake-Made-by-BitCrypt-Developers-Allows-Experts-to-Recover-Encrypted-Files-428605.shtml

February 21, Softpedia – (International) **Operation GreedyWonk: Flash zero-day used in attack on visitors of foreign policy sites.** Adobe released an out-of-band update to patch three vulnerabilities including a zero-day, and researchers from FireEye released a report stating that the zero-day was used in an attack dubbed "GreedyWonk" which targeted visitors of multiple economic and foreign policy sites. Source: http://news.softpedia.com/news/Operation-GreedyWonk-Flash-Zero-Day-Used-in-Attack-on-Visitors-of-Foreign-Policy-Sites-428544.shtml

February 21, Softpedia – (International) **Leak of iBanking bot source code opens up new opportunities for cybercriminals.** RSA researchers found that the source code for the server-side software of the iBanking mobile bot was leaked on a cybercrime forum, as well as a builder that can be used to unpack the existing APK file and repack it with different configurations. Source: http://news.softpedia.com/news/Leak-of-iBanking-Mobile-Bot-Source-Code-Opens-Up-New-Opportunities-for-Cybercriminals-428648.shtml

February 21, Softpedia – (International) **Massive DDoS attack launched against Namecheap's DNS platform.** Namecheap announced that it suffered of a massive distributed denial-of-service (DDoS) attack, targeting around 300 domains in its DNS platform. The company mitigated the attack and restored services about 11 hours later. Source: http://news.softpedia.com/news/Massive-DDOS-Attack-Launched-Against-Namechap-s-DNS-Platform-428467.shtml

February 20, Threatpost – (International) **Google fixes 28 security flaws in Chrome 33.** Google released Chrome 33 which included fixes for 28 security vulnerabilities and a number of high-severity bugs. Source: http://threatpost.com/google-fixes-28-security-flaws-in-chrome-33/104391