The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

19 March 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

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, Sandia 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 open source data

March 18, Softpedia – (International) **Two Ukrainians and one American charged for role in global cybercrime operation.** Two Ukrainians and one American were charged by federal authorities with hacking into the systems of several U.S. banks, government agencies, payroll processing companies, and brokerage firms in an attempt to steal at least $15 million between 2012 and 2013. Source: http://news.softpedia.com/news/Two-Ukrainians-and-One-American-Charged-for-Role-in-Global-Cybercrime-Operation-432716.shtml

March 17, Help Net Security – (International) **Mt. Gox CEO doxing was a ploy to spread Bitcoin-stealing malware.** A researcher at Kaspersky Lab reported that an archive file purporting to contain financial and personal information relating to the Mt. Gox Bitcoin service also contains a Windows and a Mac trojan designed to steal users Bitcoin virtual currency. Source: http://www.net-security.org/malware_news.php?id=2733

March 17, Associated Press – (Maryland) **Md. nonprofit serving disabled reports data breach.** Frederick, Maryland-based Service Coordination Inc., notified about 9,700 clients March 14 after an individual hacked the computers of the provider and stole Social Security numbers and medical information. Authorities are continuing to investigate the breach. Source: http://www.miamiherald.com/2014/03/17/4000908/md-nonprofit-serving-disabled.html

March 18, Softpedia – (International) **ESET uncovers server botnet that infected over 25,000 UNIX machines.** Security researchers with ESET, CERT-Bund, and other organizations identified a cybercrime operation dubbed Windigo that has infected around 25,000 UNIX servers over the past 2 years. The infected servers are being used to send around 35 million spam emails daily. Source: http://news.softpedia.com/news/ESET-Uncovers-Server-Botnet-That-Infected-over-25-000-UNIX-Machines-432801.shtml

Fake Google Drive Phishing Scam Steals Login Info

Yahoo, 17 Mar 2014: Usually, you can tell a legitimate Google notification from a phishing scam by reading the URL's domain name — a message that redirects you to a non-Google address is sure to be a scam. However, a sophisticated phisher has come up with a method of stealing Google login information by using the company's own servers against it. Sunnyvale, Calif.-based security firm Symantec discovered the phishing attempt and reported the incident on its blog. The scam comes in an email titled "Documents," and encourages users to click on an included link to check out an important message on Google Drive. This link leads to a login page hosted on a bona fide Google URL, complete with secure sockets layer (SSL) authentication. The login prompt is identical to that of a real Google site, inviting users to sign in for "One account. All of Google." Those who log in get access to a Google Drive document which says nothing of great import. Of course, the document isn't the point; the point is that the phishers now have access to a user's Google account. This gives them access to Google Drive documents, private email and, perhaps most damning, payment information for Google Play. The trick works because the lure document is actually hosted on Google Drive. Combined with the convincing login page, this trick could theoretically fool the tech-savvy as well as the

uninformed. Still, cautious users would still spot a few red flags in this otherwise-clever scam. First of all, the email itself does not come from an official Google email address, even if it's preferred display name indicates otherwise. Clicking on links embedded in emails is also generally a bad practice, although in this case, even copying and pasting it would still bring a user to a "verified" Google page. If you get an email message purporting to come from a big organization such as Google, it's generally a good idea to check the content of the email against the company's official blog or Twitter feed. A company will rarely institute policy changes without informing its users on a grand scale. To read more click **HERE**

Drop-Dead Date Looms for Microsoft's Windows XP

Minyanville, 18 Mar 2014: A handy countdown clock on the Microsoft site is ticking through the minutes until April 8, when the venerable and very outdated Windows XP operating system will no longer be supported by the company that created it way back in 2001. Nobody can say the company didn't warn us, but that might not cushion the blow. Somewhere between 30% and 40% of the world's computers are still running on XP. The lower number would translate to nearly 500 million computers. All of those computers are at least six years old, since that's when Microsoft stopped installing the operating system in new computers. It's not like those personal computers are going to blow up in anybody's face on April 8, but some of their users might wish they had. The absence of support will mean that Microsoft will no longer track or fix newly discovered problems, security flaws, malware, and viruses in XP. Users of XP will no longer receive the famous "Patch Tuesday" download, in which the company automatically sends updates and fixes to its software, on the first Tuesday of each month. In short, those computers are vulnerable to hackers, who are widely assumed to be eagerly watching that clock countdown, too. This is not a nefarious plot by Microsoft to goose personal computer sales. Its XP operating system has lasted for some years beyond the normal life cycle of a computer program, and it has been replaced by a more modern operating system, not once but three times. Each generation -- Windows 7, Vista, and Windows 8 -- has added significant levels of security designed to prevent viruses from spreading from an individual computer through the Internet. It is having an effect on sales, though. Hewlett-Packard (NYSE:HPQ) credited replacements for computers running XP for helping it beat sales expectations for the last quarter of 2013. Nevertheless, Microsoft might wind up with a public-relations nightmare on its hands. Apparently, 95% of the world's ATMs are running on Windows XP. So are many medical systems, retail credit card systems -- you name it. The company has a perfectly rational explanation for its decision to cut off XP support, and it seems likely that nobody is going to want to hear it once the security breaches start occurring. "Abandoning Windows XP is a big mistake, especially since Microsoft has not been very successful in transitioning XP users to newer systems," an executive of Avast, an antivirus software company, warns in a blog post. Consumers have non-Microsoft choices, some of which weren't available back when XP was introduced. Notably, there are Google (NASDAQ:GOOG) Chrome devices, which are cheap, light, and suitable for tasks like Web browsing and emailing, if not for heavy-duty office tasks. And, nobody knows how many of those XP machines are actually gathering dust in the closets of their owners, who are now walking around with pocket-sized devices that do the trick most of the time. Some percentage of Windows XP computers may not be hooked up to the Internet, in which case their owners can keep using them until their machines literally do blow up. The real problem is in business and government, and some of those folks are going to be in a lot of trouble next month. Businesses have been dragging their feet since 2008 because of the significant cost involved, and not only for new hardware. Many are using customized software that will have to be totally reworked, and even basics like word-processing software will have to be replaced. And then there's the federal government. The government has purchased hundreds of thousands of new computers over the past two years, as the drop-dead date for XP approaches. But according to a new report in the Washington Post, hundreds of thousands of XP-equipped computers are still rattling around in the federal system, including many that handle sensitive classified military and diplomatic materials. The Department of Homeland Security claims it should have no XP machines in place by April 8. The departments of Defense and State claim "nearly all" will be gone, the Post reports. To read more click **HERE**

Fake Walt Disney World Pages on Facebook Trick Thousands of Users

Minyanville, 18 Mar 2014: There are a number of fake Walt Disney World pages on Facebook that attempt to trick users into thinking that they can win tickets if they share and like some posts. One of these pages was first spotted by Hoax Slayer. Currently, there seem to be at least four such scam pages. The following message is posted on them every few hours: "Good news were giving you and 50 other people a chance to win an all paid for Florida, Disney World vacation with passes to every park. Each winner will receive 4 tickets each for a date of your choice with $2,000 spending money. To enter just share & like this photo. (Comment to double your chances). Good luck, competition ends in 48 hours. Winners will be posted." Each of the scam Walt Disney World pages has been liked by thousands of users. The bogus posts have been liked and shared by tens of thousands of unsuspecting Facebook customers. In reality, no one gets the tickets, no matter how many times they share the photos, or how many comments they publish. So what are the scammers after? In this case, their goal is to harvest as many likes as possible for their Facebook pages. Once a page has tens of thousands of likes, it can be repurposed by its owners or sold to others on the underground market. A Facebook page with a large number of likes can be worth a lot because it can be successfully utilized to advertise all sorts of shady products, services or websites. These like-farming scams have been making the rounds for quite some time now. The scammers leverage the names of various world-renowned companies in an effort to trick users. The reputation of Disney has been leveraged by scammers on a number of occasions in the past. In addition to Disney, other fake pages claim to represent BMW, Chevrolet and other major car makers. Users who come across such Facebook pages are advised not to like or share any of the posts. Instead, report the pages to Facebook. Although it might seem that there's no harm in liking a picture on Facebook, users who interact with the scammers' pages are actually contributing to the success of the campaign. After the scam page is repurposed, those who liked it might end up with all sorts of malicious links in their feed. To read more click **HERE**

Mozilla Releases Firefox 28, Fixes Vulnerabilities Presented at Pwn2Own

SoftPedia, 19 Mar 2014: Firefox 28 is available for download. In addition to some new features and bug fixes, Mozilla has also addressed a number of security holes, including the ones disclosed by researchers at Pwn2Own 2014. A total of 18 security issues have been fixed. Five of them are critical, three of them are high-impact, seven are moderate-impact, and three are minor security vulnerabilities. All of the flaws presented at Pwn2Own are considered critical. They've been identified by Mariusz Mlynski, VUPEN, George Hotz (geohot) and Jüri Aedla. Mlynski managed to execute arbitrary code in Firefox by loading a JavaScript URL executed with full privileges of the web browser. For this, he leveraged a couple of bugs: one that allowed for untrusted web content to load a chrome-privileged page by getting JavaScript-implemented WebIDL to callwindow.open(), and one that allowed the bypassing of the pop-up blocker without any user interaction. Aedla has managed to execute code by exploiting security holes leading to out-of-bounds reads and writes into the JavaScript heap. He accomplished this after discovering that "TypedArrayObject does not handle the case where ArrayBuffer objects are neutered, setting their length to zero while still in use." An exploitable use-after-free issue was identified by VUPEN. Experts found that memory pressure during Garbage Collection could lead to memory corruption of TypeObjects in the JS engine. Hotz has executed arbitrary code by causing an exploitable crash after leveraging an issue where values are copied from an array into a second, neutered array, which allows an out-of-bounds write into memory. These vulnerabilities impact not only Firefox, but also Seamonkey and Thunderbird. The fifth critical vulnerability fixed with the release of Firefox 28 is described as "miscellaneous memory safety hazards." The high-impact security holes refer to SVG filters information disclosure through feDisplacementMap, an information disclosure through polygon rendering in MathML, and out-of-bounds read during WAV file decoding. Google fixed the vulnerabilities presented at Pwn2Own 2014 shortly after the hacking competition ended. It appears that Mozilla didn't want to wait too much either. It remains to be seen when Microsoft will address the Internet Explorer security holes exploited by experts at Pwn2Own. Firefox users are advised to update their installations as soon as possible to protect their computers against potential cyberattacks. To read more click **HERE**

Notorious Hacker Diabl0 Arrested in Thailand

SoftPedia, 18 Mar 2014: Farid Essebar, a 27-year-old Moroccan with Russian citizenship known on the hacking scene as Diabl0, has been arrested by Thai authorities on suspicion of being involved in cyberattacks against Swiss financial organizations. According to the Bangkok Post, Essebar was arrested after Swiss police alerted Thai authorities through the embassy in Bangkok about the hacker and three other members of his gang being in Thailand. In Switzerland, Essebar is accused of hacking into the computer systems of several banks, causing damage estimated at around $4 billion (€2.87 billion). Police in Thailand have been tracking Diabl0 for the past two years. Apparently, they wanted to make sure he's the man wanted by Swiss authorities before arresting him. Essebar is said to have visited Thailand, Hong Kong and other neighboring countries several times in the past years. Police Colonel Songsak Raksaksakul, chief of the International Cases and International Crime Division of the Department of Special Investigation, said Essebar never gambled and never purchased any assets in Thailand, despite visiting a number of tourist destinations. Diabl0 was first arrested in 2005 by Moroccan authorities. He was accused and sentenced for being involved in the creation of Zotob, a notorious worm that infected a lot of computers, including the ones of organizations like CNN, ABC News, NYT, Boeing and the US Department of Homeland Security. He was sentenced to two years, but he was released after one. To read more click **HERE**

Man Who Hacked and Blackmailed Miss Teen USA Sentenced to 18 Months in Prison

SoftPedia, 18 Mar 2014: Jared James Abrahams, the 20-year-old who hacked into the computers of several women, including Miss Teen USA Cassidy Wolf, has been sentenced to 18 months in a federal prison. Abrahams pleaded guilty on November 12, 2013, to one count of computer hacking and three counts of extortion. The US Attorney's Office for the Central District of California revealed that Abrahams hacked into as many as 150 accounts with the purpose of obtaining information and content that he could use to extort his victims. The man targeted both women that he knew personally, such as Wolf, and ones that he identified after hacking into Facebook pages. He used malicious software to break into email and social media accounts, and to hijack computers. By taking control of his victims' computers, Abrahams was able to remotely turn on their webcams and take intimate pictures of them. The photos were later used to extort the women. They were told that the compromising photos or videos would be posted online unless they sent more intimate photos or videos, or accepted to engage in a live 5-minute session on Skype. At least two women accepted to take part in Skype sessions. Several victims, mostly teens and women in their early 20s, refused to give in to extortion so the hacker posted their private photos on their social media accounts. "As digital devices, email accounts, and social media accounts now contain the most intimate details of the public's daily lives, the impact of this type of hacking and extortion becomes more pronounced, troubling, and far-reaching," prosecutors noted. "In some cases, this type of criminal behavior can be life-changing for the victims – especially for vulnerable victims who may feel it is impossible to rebuild their tarnished reputations. Stated differently, individuals like defendant have the ability to affect a person's life in frightening ways by using the broad reach of the Internet." Authorities started to investigate Abrahams' activities after Wolf and others filed complaints with the police. Wolf was the first to make her story public. The FBI identified the hacker after one of the victims reported his extortion attempts. Back in December 2013, a 27-year-old from Glendale, California, was sentenced to five years in prison for hacking into the online accounts of at least 350 women. The man, Karen "Gary" Kazaryan, stole embarrassing or explicit photos which he used to blackmail the victims. He blamed his actions on depression and the use of marijuana. To read more click **HERE**