The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
17 - 21 April 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

April 16, Softpedia – (International) **POS malware, RATs and banking trojans used by cybercrime group.** FireEye researchers reported on the activities of a cybercrime group that is targeting financial services companies, banks, and businesses with a variety of malware, including the Netwire and DarkComet remote access trojans (RATs), JackPOS point of sale malware, and the Zeus trojan. The researchers found that the group uses spam emails to begin their attacks and that over 9 percent of targets opened the emails' malicious attachments. Source: http://news.softpedia.com/news/POS-Malware-RATs-and-Banking-Trojans-Used-by-Cybercrime-Group-437880.shtml

April 16, Softpedia – (International) **Oracle fixes 104 security holes with April 2014 CPU.** Oracle released its April Critical Patch Update (CPU), containing patches for 104 vulnerabilities in various Oracle products, 37 of which affect Java SE. Source: http://news.softpedia.com/news/Oracle-Fixes-104-Security-Holes-with-April-2014-CPU-437964.shtml

April 16, V3.co.uk – (International) **Samsung Galaxy S5 fingerprint scanner hacked.** Researchers at Security Research Labs demonstrated a method to defeat the Samsung Galaxy S5's fingerprint scanner, which could allow an attacker to unlock the device by using a print of the owner's fingerprint. Source: http://www.v3.co.uk/v3-uk/news/2340156/samsung-galaxy-s5-fingerprint-scanner-hacked

April 16, Softpedia – (International) **Adobe Reader for Android 11 updated to fix remote code execution vulnerability.** Adobe released an update for its Adobe Reader for Android, closing a vulnerability that could be used to remotely execute arbitrary code when a user opens a malicious .PDF document. Source: http://news.softpedia.com/news/Adobe-Reader-for-Android-11-Updated-to-Fix-Remote-Code-Execution-Vulnerability-437978.shtml

April 17, Softpedia – (International) **Java RAT UNRECOM mines for Litecoins, infects Android devices.** Researchers at Trend Micro analyzed a new version of the UNRECOM remote access trojan (RAT) and found that it is being distributed via spam emails in order to compromise Android and other devices. The RAT contains the ability to take screenshots, mine for the Litecoin virtual currency, and can add additional plugins to itself, among other functions. Source: http://news.softpedia.com/news/Java-RAT-UNRECOM-Mines-for-Litecoins-Infects-Android-Devices-438191.shtml3

April 17, Help Net Security – (International) **Tor relays vulnerable to Heartbleed dropped from anonymity network.** The leader of the Tor Project stated that the Tor anonymity network could temporarily lose around 12 percent of exit capacity and guard capacity after the network began rejecting relays and bridges that are still vulnerable to the Heartbleed vulnerability in OpenSSL. Source: http://www.net-security.org/secworld.php?id=16708

April 17, Help Net Security – (International) **Attackers use reflection techniques for larger DDoS attacks.** Akamai released a global distributed denial of service (DDoS) attack report, which found that attackers in the first quarter of 2014 favored using reflection and amplification techniques to conduct DDoS attacks, rather than relying on traditional botnets. The report found that the most abused protocols were Character Generator (CHARGEN), Network Time Protocol (NTP), and Domain Name System (DNS.) Source: http://www.net-security.org/secworld.php?id=16707

April 16, Softpedia – (International) **65% of US organizations experienced SQL injection attacks, study finds.** A report by the Ponemon Institute for DB Networks found that 65 percent of 595 U.S. security professionals surveyed reported experiencing SQL injection attacks during the past 12 months. The study also found that it took an average of 140 days to discover a breach and another 68 days to remediate the issue, among other findings. Source: http://news.softpedia.com/news/65-of-US-Organizations-Experienced-SQL-Injection-Attacks-Study-Finds-438048.shtml

April 17, Reuters – (National) **Retailer Michaels Stores confirms payment card data breach.** Craft retailer Michaels Stores confirmed April 17 that it was the victim of a data breach that may have exposed information on around 2.6 million payment cards used at Michaels and Aaron Brothers stores. The breach was initially reported in January, and after investigation was found to have taken place between May 8, 2013 and January 27, 2014. Source: http://www.reuters.com/article/2014/04/17/us-michaelsstores-cybercrime-idUSBREA3G27N20140417

April 17, Reuters – (National) **SEC's information technology at risk of hacking: report.** A report by the Government Accountability Office found that the U.S. Securities and Exchange Commission failed to take steps to protect its data networks from breaches, including failing to encrypt sensitive information and failing to physically secure some systems. Source: http://www.reuters.com/article/2014/04/17/us-sec-cybercrime-security-idUKBREA3G25720140417

April 17, Pittsburgh Post-Gazette – (Pennsylvania) **UPMC data breach may affect as many as 27,000 employees.** The University of Pittsburgh Medical Center (UPMC) reported April 17 that as many as 27,000 employees may have had their personal information exposed in a February data breach, with at least 788 employees becoming victims of tax fraud since the breach was discovered. UPMC assured their patients that none of their information was breached. Source: http://www.post-gazette.com/business/finance/2014/04/17/UPMC-data-breach-may-affect-as-many-as-27-000-employees/stories/201404170277

April 18, Softpedia – (International) **Cybercriminals can hijack Steam accounts with Steam Guard enabled.** Researchers at Malwarebytes found that attackers have been able to compromise Steam accounts with the Steam Guard verification service enabled by using phishing pages that ask users to upload the .ssfn file from their Steam folder, allowing the Steam Guard security feature to be bypassed. Source: http://news.softpedia.com/news/Cybercriminals-Can-Hijack-Steam-Accounts-with-Steam-Guard-Enabled-438488.shtml

April 18, Softpedia – (International) **Trojan-SMS.AndroidOS.Stealer.a is one of the most widespread mobile trojans.** Kaspersky Labs researchers found that the Trojan-SMS.AndroidOS.Stealer.a trojan accounted for almost a quarter of attempted infections of Android devices running the company's security software during the first quarter of 2014, with the highest amount of infections found in Russia. The trojan is capable of opening Web

pages, sending SMS messages, installing applications, and other functions. Source: http://news.softpedia.com/news/Trojan-SMS-AndroidOS-Stealer-a-Is-One-of-the-Most-Widespread-Mobile-Trojans-438270.shtml

VMware Fusion 6.0.3 Released with Bevy of Fixes and Enhancements

SoftPedia, 21 Apr 2014: Virtualization company VMware Inc. is offering a new and improved version of its Fusion software that emulates a PC environment on a Mac, allowing customers to have both OS X and Windows running side by side. One of the hottest-selling virtualization solutions on the Mac, VMware Fusion gets constantly updated with new features, tweaks, and fixes, and this update is no exception to the rule. VMware Fusion 6.0.3 build 1747349 fixes an issue where connecting USB devices while Fusion is running would cause the Connect to Mac prompt to appear. USB devices can now connect to a virtual machine, and performance with USB audio and video devices has been improved. Same goes for compatibility with various types of hardware. For customers where the virtual machine crashes when the Mac comes out of sleep mode, these instances "have been reduced," but not completely eliminated. Don't expect a flawless experience, in other words. The black-screen issue incurred when locking the system then returning to the Mac OS X 10.9 desktop while the virtual machine is running should no longer occur. An issue that could cause the default web browser to be reset in a Windows 8 virtual machine has been addressed, and resizing a Windows XP VM window will no longer cause it to go dark. Full-screen virtual machines no longer display a black bar at the top, Winlogon.exe now works properly with Windows XP in Boot Camp, virtual machines no longer show a black screen when using Apple TV as an external display, and Fusion no longer stalls when using a restricted VM without Internet. The release notes also state that "single mouse clicks are interpreted as double-clicks when running Windows XP virtual machines on OS X Mavericks." It isn't clear if this was an issue for some, or what changes have been made in this department. The ability to use two monitors with the same virtual machine is improved. When VMware Fusion is not open, VMs can be started and shut down from the VMware Fusion menu now. Any compatibility issues between shared folders and QuickTime for Windows have been resolved as of version 6.0.3 Build 1747349, and the graphics for Solidworks and JavaFX applications have been improved, according to the developer. To read more click **HERE**

Secret Service: It Could Take Years to Identify Cybercriminals Behind Target Breach

SoftPedia, 21 Apr 2014: Secret Service representatives say they're close to determining exactly how cybercriminals managed to breach the systems of retailer Target and steal the details for 40 million payment cards. However, they're not very optimistic about identifying the perpetrators. Ari Baranoff, assistant special agent in charge with the Secret Service's criminal investigative division, says that it could take years to identify the cybercriminals. Furthermore, since they're likely from overseas, extraditing them and prosecuting them could also turn out to be problematic, Baranoff said, cited by The Associated Press. However, the Secret Service hopes that by keeping a close eye on suspects, the agency could arrest them when the time is right. While it might take years, Baranoff says that the agency is very patient when it comes to these things. It doesn't have a problem in prosecuting criminals even 10 years after the crime was committed. While he hasn't said anything about the attacker's identity or location, US Senator Mark Warner (D-VA) has told 13News that evidence suggests that the cybercriminals are from Ukraine. Furthermore, the senator claims that the former Ukrainian government knew about their activities, but turned a blind eye because they "saw this as a money making way." Warner has urged President Barack Obama to leverage the US's aid to Ukraine to ask the government to crack down on organized cybercrime. To read more click **HERE**

Spammers Hijack Facebook Accounts with the Aid of Fake Chat Verification Posts

SoftPedia, 21 Apr 2014: If you come across an announcement from the "Facebook Chat Team," you should know that it's part of a scam designed to trick users into giving spammers access to their accounts. "All Chat Box must be verified before 24th May 2014 to avoid Chat Blocking under SOPA and PIPA Act. The unverified Chat will be terminated," the scammy announcements read. According to Trend Micro, users who click on the links are taken to a Pastebin post that

contains instructions on how to allegedly "verify the chat." Victims are provided with pieces of code which they're told to paste in their web browser's JavaScript console. Once the code is executed, the scammers gain access to the victim's account. While their actions are limited, they can re-post the scam on the hijacked timeline, tag other users, and subscribe the victim to certain pages. "From the get-go, users should know that there is no product called 'Facebook Chat,' let alone a team that sends out a supposed 'advisory' to its users," Trend Micro experts warn. Facebook is aware of these types of scams and the social media platform has taken steps to block them. "There is a popular scam going around that claims the user will gain some benefit (illicit access to someone else's account, some new Facebook feature, etc) by pasting some piece of JavaScript into the browser's console," Facebook explained on a page about self-XSS attacks and the way the JavaScript console works on the website. "This is a variant on the self-XSS attack. By pasting the code in the browser console, the user gives the code access to their account. The code usually posts the same scam on other people's walls, and subscribes the user to pages controlled by the attacker – but it could do much worse things," the company added. "To avoid this, the console is now gently disabled in some browsers. If you want to use the console, turn the following setting on; you'll need to reload the page for it to take effect." Users who fall victim to such attacks should check their timelines and remove all the posts published on their behalf. It might also be wise to check the Activity Log to see what other actions have been performed without their knowledge. In general, if you want to avoid falling victim to such scams, don't trust any posts claiming that your account or certain features will be deactivated unless you perform some actions. To read more click **HERE**

Windows Phone 8.1 Update Installation Fails with Error 80188309, Microsoft Issuing Fix Soon

SoftPedia, 21 Apr 2014: Since Microsoft released the hotly anticipated Windows Phone 8.1 Developer Preview earlier this week, all owners of compatible devices could install it as long as they also owned a developer account or an App Studio one. According to the Redmond-based company, all Windows Phone 8 smartphones are fully compatible with the new version of the operating system, so there is not reason for why one owner of such device could not upgrade to Windows Phone 8.1, assuming it has an App Studio or Dev Center account. Unfortunately things did not work quite well for some Windows Phone fans, especially for those who own Huawei smartphones powered by Windows Phone 8. Basically, Windows Phone 8.1 can't be installed on any compatible Huawei smartphone, or at least on the majority of the devices branded with the Chinese company's logo. Moreover, some other smartphones that should have been compatible with the new version of the operating system were not able to cope with the installation of Windows Phone 8.1. As WMPoweruser points out, all Windows Phone 8.1 installation attempts on these devices were met with error code 80188309, which became (in)famous soon after the Developer Preview was released online and made available for download. Well, it took Microsoft several days to acknowledge the issue and according to the company a fix is already in the works. There's also an official statement issued by Microsoft, in which the company promises to continued to work on getting this update to the people affected by this error, but that it cannot commit to specific timeline for the release. Nevertheless, a Microsoft official did promise to update Windows Phone fans hit by the 80188309 error code with additional news on how the work on the fix is progressing. Here is the full statement posted on Microsoft's support site:

> "Hello Everyone,
> Here is the Friday update on how things are moving forward. Without further delay, here is the news for today:
>
> 1. A little clarification on the update notification. The notification has stopped for all devices that have not yet taken the first update, however those that have taken the first update and are waiting for the second update to the current 8.1 build will continue to occur. At this point, I would recommend ignoring the update notification and wait for further updates from us.
>
> 2. The update itself is not going to be available today, or likely early next week. We will continue to work on getting you this update but it will not be as fast as you would like. I know a lot of you would like a better timeline

on when it will be available, and at this time I cannot commit to a date. I will however, commit to updating you next Thursday April 24th, 2014 with any additional news. If I have any news or details before then, I will of course update you at that time.

We appreciate you being eager to participate in the Windows Phone Developer Preview Program, and look forward to getting it to you as soon as possible."

To read more click **HERE**

Heartbleed Bug Shows Which Companies Really Care About Security

SoftPedia, 21 Apr 2014: The critical OpenSSL vulnerability, known as the Heartbleed bug, is said to have impacted two thirds of the websites that use SSL to secure their customers' communications. While many organizations have patched their installations by now, a lot of users' data has been at risk because of the flaw. The HeartIbleed bug was discovered by a Google security expert sometime in March. Its existence was made public on April 7. Some companies, such as CloudFlare, Facebook and some Linux distributions, learned of its existence before that, and they quickly rolled out fixes. On April 7, OpenSSL released version 1.0.1g allowing all companies to secure their websites. However, it took some of them a lot of time to apply the fix. Considering that Heartbleed made a lot of headlines all over the world, you'd expect every company to install the latest version of OpenSSL quickly, if not to protect users, at least to brag about it in an effort to boost their reputation. Shortly after the world learned of the vulnerability, experts started publishing lists of the affected services. Exploits were also published online soon after. While initially some doubted that private SSL keys could be obtained by exploiting Heartbleed, researchers quickly demonstrated that it was possible. Unsurprisingly, some organizations have started admitting to their customers that their information might have been stolen by cybercriminals exploiting the Heartbleed bug. There are rumors that some entities might have known about the existence of Heartbleed for a long time, including the National Security Agency (NSA), which is said to have known about it for two years. The NSA has denied the accusations, but there could be some who really knew about the OpenSSL flaw for a long time. Even if no one knew about it, it was clear that as soon as its existence came to light, cybercriminals would start exploiting it to take advantage of the relatively small window of opportunity they had before website owners started updating their OpenSSL installations. However, while there were a few companies that acted quickly, there were some that took their time, giving potential attackers the opportunity to strike. Of course, it's true that in some cases, it's a bit trickier to mitigate Heartbleed attacks. There are some reports about companies that experienced some serious issues updating OpenSSL. On the other hand, if Yahoo managed to fix the issue within around 48 hours (which, by the way, was considered by many a slow response), others should have been able to update sooner, not in 5 days or more, as many have. This just goes to show that "We take security very seriously" is just a sentence that companies include in their notifications to customers after they get hacked, not something they actually mean. The fact that it has taken some organizations a lot of time to fix the Heartbleed vulnerability has also caused some confusion. The first piece of advice that everyone gave was "change your password!" However, as experts have highlighted, this recommendation is only good if the website you're changing your password for has updated OpenSSL. To read more click **HERE**

Microsoft Fixes Security Essentials Bug on Windows XP

SoftPedia, 21 Apr 2014: An update released by Microsoft for its own Security Essentials anti-virus and other anti-malware solutions caused a number of Windows XP computers to freeze after boot, with some reports pointing to thousands of machines that got affected by the issue. Redmond has however shipped another update that comes to address all these problems, so consumers who were experiencing problems on Windows XP, Windows Server 2003, and other platforms after deploying anti-malware signature updates should get the new one as soon as possible. Antimalware Engine 1.1.10502.0 was shipped to computers running Microsoft Security Essentials, Forefront Client

Security, Forefront Endpoint Protection, Windows Intune Endpoint Protection, and System Center Endpoint Protection customers and contains signature package 1.173.0.0 that fixes the aforementioned bug. "This is due to an update that was shipped on April 15, 2014 that may have caused interrupted service for some customers using Microsoft security products. This was corrected via signature update, which automatically resolved the issue, and customers who have deployed the most recent signatures do not need to take any action," Microsoft says. The company also noted that while the problems were initially experienced on Windows XP and Windows Server 2003, some other platforms might have been impacted as well. Customers who disabled Behavior Monitoring or applied other workarounds are recommended to revert the changes as soon as possible and deploy this new update. To read more click **HERE**

SATCOM Vulnerabilities: Insecure Protocols, Backdoors and Hardcoded Credentials

SoftPedia, 18 Apr 2014: Ruben Santamarta, a principal security consultant with IOActive, has published a whitepaper on the security issues that plague some of the most widely deployed satellite communications (SATCOM) systems. This isn't the first time someone reports that satellite communications are vulnerable to cyberattacks. Earlier this year, we had an interview with security expert Nicholas Lemonias on this topic. However, Santamarta's research is more specific since it targets Inmarsat and Iridium SATCOM terminals. The security expert has found backdoors, insecure protocols, weak encryption algorithms and hardcoded credentials that expose satellite communications to cyberattacks. The vulnerabilities affect ships, aircraft, the military, media and emergency services, and even industrial facilities that rely on this equipment. The study describes possible attack scenarios against Inmarsat-C, Very Small Aperture Terminal (VSAT), Broadband Global Area Network (BGAN), BGAN machine-to-machine (M2M), FleetBroadband (FB), SwiftBroadband and Classic Aero Service systems. It's worth noting that the researcher hasn't had physical access to the devices. Instead, static firmware analysis has been conducted by reverse engineering the terminals. "IOActive found that all devices within the scope of this research could be abused by a malicious actor," the researcher noted in his report. "These vulnerabilities allow remote, unauthenticated attackers to compromise the affected products. In certain cases no user interaction is required to exploit the vulnerability; just sending a simple SMS or specially crafted message from one ship to another ship would be successful for some of the SATCOM systems." For instance, the attack scenario against Harris BGAN terminals, which are used by NATO, describes vulnerabilities that can be exploited to install malicious firmware or execute arbitrary code. In the documentation for the equipment, the vendor describes a real scenario in which a military convoy that's attacked by the enemy uses the system to launch and coordinate a response. However, the attacker can leverage vulnerabilities in the equipment to inject malicious code that can be designed to transmit the location of the target and even completely disable communications. The Hughes BGAN M2M terminals are used in various industries for Smart Grids, SCADA (utilities), pipeline monitoring (oil and gas), remote ATM (retail banking), and environmental monitoring. These devices can be controlled via SMS or AT commands. Due to the vulnerabilities that plague the equipment, an attacker could, depending on the targeted industry, commit fraud, launch denial-of-service (DOS) attacks, cause physical damage and leverage the flaws for data spoofing. IOActive is working with the CERT Coordination Center and SATCOM vendors to address the highlighted security issues. Check out the "A Wake-up Call for SATCOM Security" whitepaper for more details (**link**). Technical information will be made available in the upcoming months. To read more click **HERE**

South Africa Sentences Its First Online Pirate

SoftPedia, 17 Apr 2014: A court from South Africa sentenced the first digital pirate in the country. Majedien Norton is the name of the offender who pleaded guilty of copyright infringement for sharing a media file over the Internet. The judges gave him a five-year suspended sentence and he won't even have to pay a fine for his deeds. "It's a huge relief for me and my wife. I'm just glad we can put this behind us now and move on," Norton said, reports htxt.africa. Norton is guilty of uploading a torrent file and seeding the file, which was a digital version of "Four Corners," a movie about the gangster life in Cape Flats. The film was uploaded to The Pirate Bay in November 2013 after Norton ripped a DVD purchased from a street vendor. The South African Federation Against Copyright Theft said in the charges that the

torrent was generated from a file acquired directly from the film studio. As expected, the trial received quite a bit of coverage since it was a first time for South Africa to host such a case. Given the suspended sentence, it remains to be seen whether it will deter others from following in the same footsteps. To read more click **HERE**

Cybercriminals Combine Phishing with Tech Support Scams

SoftPedia, 17 Apr 2014: Back in February, experts warned Internet users of a campaign in which cybercriminals not only tricked people into handing over their login credentials, but also lured them to bogus tech support services. More variations of the scam have surfaced. According to Malwarebytes researchers, scammers are using various methods to trick people into calling fake tech support services. In some cases, they advertise their sites via sponsored ads on search engines. In other cases, they first lure victims to a phishing page. The phishing sites target the customers of various services, including Netflix, AT&T, AOL, online gaming site Pogo, Comcast and CenturyLink. After unsuspecting internauts enter their username and password on the phishing site, they're informed that their accounts have been temporarily suspended. Victims are instructed to call a certain number to regain access to their accounts. The phishing sites also host pages containing a live chat that's also used to lure victims. The so-called support technicians ask for various amounts of money for allegedly fixing some non-existent security issues. The phishing sites are hosted on legitimate-looking domains. The list includes aolrisk.com, aolfix.com, affiliatedhelp.com, myscreenname.com and login-emails.com. Experts highlight the fact that targeted advertising is much more efficient than random cold calls. To read more click **HERE**