The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

26 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

February 25, Softpedia – (International) **EC-Council says its servers haven't been hacked.** EC-Council announced that its Web site was targeted by a hacker who redirected the site's visitors via a Domain Name System (DNS) hijack to a defacement page hosted by a Finland-owned company. The organization stated that its servers were not breached and continues to investigate the incident. Source: http://news.softpedia.com/news/EC-Council-Says-Its-Servers-Haven-t-Been-Hacked-429307.shtml

February 25, USA Today; Associated Press – (International) **Bitcoin exchange Mt. Gox goes offline amid turmoil.** The Web site of Bitcoin exchange Mt. Gox was disabled February 25 and the company confirmed that it indefinitely halted withdrawals from its trading accounts earlier in February after detecting unusual activity. Source: http://www.usatoday.com/story/tech/2014/02/25/mt-gox-offline/5801093/

February 25, Softpedia – (International) **Cybercriminals use Pony botnet to steal 700,000 account credentials, virtual currencies.** Experts found that cybercriminals managed to steal more than 700,000 credentials for Web sites, email accounts, File Transfer Protocol (FTP) servers, Secure Shell (SSH), and Virtual Desktops utilizing the Pony botnet. The botnet was also used to steal $220,000 worth of virtual currencies targeting Bitcoin and other virtual currency wallets. Source: http://news.softpedia.com/news/Cybercriminals-Use-Pony-Botnet-to-Steal-700-000-Account-Credentials-Virtual-Currencies-429170.shtml

February 23, Dark Reading – (International) **Researchers bypass protections in Microsoft's EMET security tool.** Bromium Labs researchers found a flaw in Microsoft's Enhanced Mitigation Experience Toolkit (EMET) 4.1 that could potentially allow attackers to sneak malware past it through bypassing several key defenses, taking advantage of its reliance on known vectors of return-oriented programming (ROP) exploitation attack methods. Source: http://www.darkreading.com/attacks-breaches/researchers-bypass-protections-in-micros/240166227

Viruses Can Spread via Wi-Fi Access Points like the Common Cold, Researchers Show
SoftPedia, 26 Feb 2014: Researchers from the University of Liverpool have demonstrated that a computer virus can spread through Wi-Fi access points between homes and businesses just like the common cold spreads from one human to another. The researchers have performed an experiment in a laboratory setting with the aid of the Chameleon virus, which uses a WLAN attack technique to infect access points and collect the credentials of all Wi-Fi users who connect to it. Then, it seeks out other access points, connects to them and infects them. The main issue highlighted by the researchers is the fact that many Wi-Fi access points are unprotected, allowing viruses like Chameleon to spread without difficulty. In their experiment, researchers simulated an attack on the cities of Belfast and London. While the virus can't spread via access points protected by encryption and passwords, it relies on ones that are not protected, like the ones in airports and coffee shops. "WiFi connections are increasingly a target for computer hackers because of well-documented security vulnerabilities, which make it difficult to detect and defend against a virus," said Alan Marshall, professor of Network Security at the University of Liverpool and one of the authors of the research paper. "It was assumed,

however, that it wasn't possible to develop a virus that could attack WiFi networks but we demonstrated that this is possible and that it can spread quickly. We are now able to use the data generated from this study to develop a new technique to identify when an attack is likely," Marshall added. Rogues access point attacks such as the one described by the researchers can be mitigated with the aid of intrusion detection systems (IDS). These systems usually rely on receiving signal strength indicator (RSSI) values to track the location of the device. However, IDS can be bypassed by copying the expected RSSI values. This can be accomplished by placing the rogue access point within a similar radius as the target, or by editing the RSSI output to make sure it matches the victim's values. The research paper proposes a more efficient detection strategy for such viruses. The method proposed by experts relies on layer 2 management frame information and it's capable of detecting such attacks while maintaining user privacy and confidentiality. The complete research paper (**LINK**), "Detection and analysis of the Chameleon WiFi access point virus," is available on the website of the EURASIP Journal on Information Security. To read more click **HERE**

Bitcoin-Stealing Mac Malware Disguised as Angry Birds Game

SoftPedia, 26 Feb 2014: OSX/CoinThief, the malware designed to steal Bitcoins from Mac users, continues to be distributed by cybercriminals. Experts say that the threat is disguised as various applications, including the popular game Angry Birds. Initially, the threat was spotted after being posted on GitHub. Later, samples were spotted on Download.com and MacUpdate as well. Now, ESET warns that the coin thief is being distributed though torrents. The cybercriminals have disguised it as cracked versions of various popular Mac OS X apps. OSX/CoinThief has been seen as BBEdit, a text editor; Pixelmator, a graphic editor; Delicious Library, a media cataloguing app; and even as Angry Birds. "There is clearly strong evidence that the trojan was specifically designed to profit from the current Bitcoin craze and fluctuating exchange rates," security expert Graham Cluley explained on ESET's WeLiveSecurity blog. ESET's LiveGrid shows that most OSX/CoinThief victims are in the United States. OSX/CoinThief was discovered earlier this month by experts from SecureMac. Since it's designed to steal login credentials for Bitcoin wallets and other Bitcoin-related services, the malware has been mostly disguised as apps that have something to do with the virtual currency. For instance, it was first spotted under the name StealthBit, an app uploaded to GitHub. The source code for the app was clean, but a pre-compiled version hid the Mac OS X malware. A few days later, SecureMac warned that the threat had been spotted on MacUpdate and Download.com under names such as Bitcoin Ticker TTM for Mac and Litecoin Ticker. When it's executed, the coin thief installs a web browser extension, depending on what the victim is using. The first variants only had extensions for Safari and Chrome. However, a more recent version also packs a malicious extension for Firefox. In addition to the extension that monitors the victim's Web traffic, the Mac malware also installs a component that runs in the background looking for wallet login credentials. When the information is obtained, it's sent back to a server controlled by the attackers. There are a couple of clues that reveal the presence of the threat on a computer. The malicious browser extension is called "Pop-Up Blocker." If you see it, you're device is probably infected. Another way to check for the presence of this Mac malware is to open the Activity Monitor in the Utilities folder and look for a process called com.google.softwareUpdateAgent. This is a process created by OSX/CoinThief. If you've seen either of these signs, check out SecureMac's advisory on how to remove OSX/CoinThief. To read more click **HERE**

Apple Releases OS X Server 3.0.3, QuickTime 7.7.5 for Windows XP/Vista/7

SoftPedia, 26 Feb 2014: As part of the update rampage that's been going on over the past few days, Apple Inc. has released a new version of OS X Server and an updated QuickTime platform for Windows customers in particular. On the OS X front, Apple's new Server release isn't the all-new 3.1 update that the company has been testing internally for the past few months. Rather, it is an incremental (and minor) 3.0.3 update meant to fix an Xcode Server issue that prevented the addition of new users. According to a lengthier set of release notes on Apple Support, "Server v3.0.3 improves the general stability of OS X Server" and delivers specific improvements, including the aforementioned Xcode thing and all the improvements from Server v3.0.2 and v3.0.1. In other words, OS X Server 3.0.3 supersedes previous OS X Server 3.x.x releases. The Cupertino company informs customers that "OS X Server v3.0.3 is available from the Mac

App Store. It appears in the Updates pane if you have OS X Server (Mavericks) installed." Customers are instructed to click the Update button to install the new version. "To prevent the interruption of services, Server updates are not automatically installed, even if you have chosen to automatically install other updates from the Mac App Store," Apple adds. Users are also told not to panic if they see the message "Server app replacement detected" during the installation. The Mac maker says, "This is a normal part of the update process. All Server settings and data are preserved during the update." Users must open the Server app to finish setting up previously-configured services after the 3.0.3 update is done installing. Apple released QuickTime 7.7.5 with the sole purpose of improving the security of the player on Windows XP SP2 (or newer), Windows Vista, and Windows 7. Highly-recommended for all QuickTime 7 users on Windows, the update patches close to a dozen recently found vulnerabilities, some more serious than others. For example, an uninitialized pointer issue existed in the handling of track lists. According to Apple, "Playing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution." A buffer overflow was present in the handling of H.264 encoded movie files, where playing a movie file that was crafted with bad intention would lead to the same scenario. In some cases, "viewing a maliciously crafted PSD image may lead to an unexpected application termination or arbitrary code execution," Apple says. This was the case with another buffer overflow, this time in the handling of PSD images. To read more click **HERE**

Fresh Stash of 360 Million Credentials and 1.25 Billion Email Addresses Uncovered

SoftPedia, 26 Feb 2014: Security experts from Hold Security say they've identified a total of 360 million credentials and 1.25 billion email addresses stolen and misused by cybercriminals from various companies. The massive volume of data was uncovered in the first three weeks of February and it was stolen recently. The companies from which the information has been stolen have not been named. The security firm is still working on identifying some of the victims and alerting them since they might not be aware of the breach. Alex Holden, Hold Security's CISO, has told Reuters that 105 million of the credential sets are from a single attack. This information can be highly valuable for cybercriminals not only to hijack accounts, but also for targeted spam campaigns. Hold Security has gathered the data as part of its Deep Web Monitoring services. Now, the company has launched Credentials Integrity Services to help companies assert their data integrity. The firm has analyzed numerous data breaches that have resulted in tens or hundreds of millions of accounts becoming compromised. For instance, they've investigated the over 150 million credentials stolen from the systems of Adobe and the 42 million credentials taken from Cupid Media. While in many cases, cybercriminals obtain login credentials directly from the targeted organization's systems, they also use botnets to harvest large amounts of data. For example, researchers from Trustwave's SpiderLabs have analyzed credential records stolen by the Pony botnet. Over a 4-month period, the botnet has helped attackers steal over 700,000 account credentials for various services, including websites, email accounts, FTP servers, SSH and Remote Desktop services. Whenever there's a major data breach, the impacted company usually takes the necessary steps to ensure that their customers' accounts are not illegally accessed. This involves resetting passwords and locking down accounts. However, the main problem is that many people use the same credentials for multiple online accounts. This means that if the attackers obtain their credentials for a file sharing site, chances are that the same username and password can be used to access Yahoo, Gmail, Facebook, Hotmail or other accounts. Even if the breached company resets all passwords and alerts impacted customers, it will take some time until most internauts change all their passwords, and some of them probably never do. While many users consider that there's no sensitive information in their email accounts, access to such an account is usually just the first step in an attack that could have serious consequences. To read more click **HERE**

OS X Safer than Ever, Apple Deploys Fix for SSL Hole and Other Serious Flaws

SoftPedia, 26 Feb 2014: Apple is offering new software updates to the entire Mac user base, including customers running OS X Mavericks, OS X Lion, and OS X Mountain Lion. While Mavericks users are in for quite a treat, the rest of the population is receiving some boring but important security patches. High on the list of priorities for Security Update 2014-001 was the famous SSL/TSL flaw, which would allow "an attacker with a privileged network position [to] capture

or modify data in sessions protected by SSL/TLS." Apple was a bit late to address this bug, but it eventually delivered the patch in OS X 10.9.2 and Security Update 2014-001. According to the security advisory included with these two updates, a separate SSL-related flaw that would allow an attacker to decrypt data protected by SSL was also in need of fixing. However, unlike the aforementioned bug, this one resided in OS X Mountain Lion installations. Apple explains that "[In OS X 10.8.5] there were known attacks on the confidentiality of SSL 3.0 and TLS 1.0 when a cipher suite used a block cipher in CBC mode. To address these issues for applications using Secure Transport, the 1-byte fragment mitigation was enabled by default for this configuration." Even older versions of OS X, such as 10.7 (Lion), are targeted by the first security update deployed by Apple in 2014. Multiple vulnerabilities existed in Apache, ATS, Certificate Trust Policy, Date and Time, File Bookmark, ImageIO, IOSerialFamily, LaunchServices, NVIDIA Drivers, PHP, and even QuickTime, all affecting OS X Lion installations and newer versions of the Mac OS. QuickTime alone was so buggy that Apple had to deploy as many as six separate patches to secure this single application. And there's no guarantee that all holes have been completely plugged. Apple credits various security researchers and amateurs alike in the advisory. Friedrich Graeter of The Soulmen GbR reported a serious App Sandbox flaw, while Felix Groebert and Meder Kydyraliev of the Google Security Team reported ATS flaws to the Cupertino giant. Rob Ansaldo of Amherst College and Graham Bennett found a CFNetwork Cookies flaw, while Karl Smith of NCC Group sounded the alarm on CoreAnimation flaws. Lucas Apa and Carlos Mario Penagos of IOActive Labs reported a CoreText flaw. Amateurs Michal Zalewski and @dent1zt are credited in the advisory for reporting ImageIO and IOSerialFamily flaws, respectively. Other people credited come from the X.Org Foundation Nouveau project, Mozilla Corporation, and Mac security expert Intego. To read more click **HERE**

Hacktivists Target Philippines Government Sites in Protest against Cybercrime Law

SoftPedia, 26 Feb 2014: Anonymous hackers have once again targeted several websites of the Philippines government. The hacktivists are protesting against a provision of the Cybercrime Prevention Act that violates freedom of speech. The list of hacked websites includes the ones of the Office of the Vice President, the PNP Command Center, the National Telecommunications Commission, the Pilipinas Anti Piracy Team, the DOST Information Network, the Technical Education and Skills Development Authority, and the Philippine Embassy in Rome, Italy. The sites of various cities and municipalities have also been attacked. Some of the websites have been defaced. In other cases, the sites' visitors have been redirected to a third-party domain hosting the defacement page. In a message posted on the targeted sites, the hackers highlight the fact that, in 1987, President Corazon Aquino passed a bill that gave people freedom of speech and freedom of expression. However, the online libel provision of the Cybercrime Prevention Act of 2012, according to the hacktivists, "kills the right of the people to freely express their opinion and freedom of speech through the internet." "We, the citizens of the internet, fight again for this right and for this freedom. We fight not only for ourselves but also for others who stand with us against the Cyber Crime Law — bloggers, gamers or ordinary internet users," the hackers stated. "This is our way to express and oppose the bill that may destroy the future of the internet in the Philippines. We believe that together we shall achieve the goal and the purpose of this cause. We shall stand and fight for the Filipino Netizens' right to freedom of speech and expression," they added. At the time of writing, a few of the attacked government websites have been restored. However, most of them have either been taken offline or they're still defaced. The attack on government websites comes after the country's Supreme Court ruled that the online libel provision in the Cybercrime Prevention Act was constitutional. Last week, four senators called for the decriminalization of libel, PhilStar reported. Currently, those found guilty of libel face between 6 months and 4 years in prison. The Senate Bill No. 2128 filed by Senator Teofisto Guingona III aims at removing imprisonment. "This bill proposes to remove imprisonment as a penalty for libel because the threat of jail time sends a sufficient chilling effect on the freedom of expression," the senator said, cited by PhilStar. Anonymous started protesting against the Cybercrime Prevention Act back in October 2012, shortly after the law was introduced. Since then, numerous attacks have been launched by the hacktivists. To read more click **HERE**

Microsoft Officially Launches Office 2013 Service Pack 1

SoftPedia, 26 Feb 2014: Microsoft today announced the availability of Office 2013 Service Pack 1, adding quite a lot of improvements and compatibility fixes with the latest products released by the company. According to details provided by the software giant on Office 2013 Service Pack 1, the new release comes with "previously unreleased fixes that are included in this service pack; in addition to general product fixes, these fixes include improvements in stability, performance, and security," as well as with all monthly security updates released through January 2014. Among the improvements included in the service pack, it's worth mentioning improved compatibility with Windows 8.1 and Internet Explorer 11, but also better support for modern hardware, high-DPI devices and precision touchpads. Last but not least, Office 2013 Service Pack 1 provides new apps for Office capabilities and APIs for third-party developers, according to the release notes published today. Outlook 2013 SP1 also comes with support for task pane apps in the mail client, which Microsoft says should enable third-party developers to "extend the compose experience for email messages and calendar items." PowerPoint 2013 is also getting its own share of improvements in the form of new options comprising the ability to insert and use content apps in created slides. Keep in mind however that Service Pack 1 is only aimed at users running the standalone version of Office 2013 that needs to be installed on Windows computers and not the subscription-based Office 365 that's also available in multiple flavors right now. Redmond has also found some issues on Windows 8 and 8.1 computers, claiming that in some cases, if you decide to remove the Service Pack 1 from your computer, a blank live tile might stick to the Start screen. The new service pack is delivered to users via Windows Update, so the whole process should go very smooth "If the Service Pack 1 update is uninstalled on a computer that is running Windows 8 or 8.1, an Office application tile on the start screen is blank without an application name or icon if the application is pinned to the start screen," Microsoft mentioned in an advisory rolled out this morning. If you're experiencing this particular issue, Microsoft recommends users to repair the Office installation using the tool available in the Programs and Features control panel screen. Just like all the other service packs released by Microsoft for its products, Office 2013 SP1 is automatically delivered to users via Windows Update, so make sure you connect your computer to the Internet to download and install it. The process could take a while as it has approximately 650 MB in size and a reboot might be required once installation comes to an end. At the same time, you can also download Microsoft Office 2013 Service Pack 1 manually (**LINK**) and install it as long as you're running a fully up to date version of the productivity suite. To read more click **HERE**

Apple Releases OS X Mavericks 10.9.2 Update

SoftPedia, 26 Feb 2014: Apple today outed OS X 10.9.2, a highly anticipated software update that was initially tasked with adding a number of new features and small tweaks, but ended up as an urgent release because of a security flaw. OS X Mavericks v10.9.2 is highly recommended for all OS X Mavericks users, as "it improves the stability, compatibility, and security of your Mac," the company headquartered at 1 Infinite Loop, Cupertino, California, says. According to Apple's official release notes, this update adds these key features and fixes.

- the ability to make and receive FaceTime audio calls
- call waiting support for FaceTime audio and video calls
- the ability to block incoming iMessages fromindividual senders
- improves the accuracy of unread counts in Mail
- resolves an issue that prevented Mail from receiving new messages from certain providers
- improves AutoFill compatibility in Safari
- fixes an issue that may cause audio distortion on certain Macs
- improves reliability when connecting to a file server using SMB2 fixes an issue that may cause VPN connections to disconnect
- improves VoiceOver navigation in Mail and Finder

As usual, Apple throws in a link to the security advisory tied to this update. Unsurprisingly, among the numerous patches included in this release, the company mentions the widely reported SSL/TLS flaw that needed an urgent fix. Available for OS X Mavericks 10.9 and 10.9.1, the issue in question would allow an attacker with a privileged network position to "capture or modify data in sessions protected by SSL/TLS." "Secure Transport failed to validate the authenticity of the connection. This issue was addressed by restoring missing validation steps," Apple explains. OS X Mavericks 10.9.2 is also available as a Combo update, and for customers who are still on OS X Lion and OS X Mountain Lion, Apple offers Security Update 2014-001. "Security Update 2014-001 is recommended for all users and improves the security of OS X," says the Cupertino company. An SSL-related flaw is also patched in OS X 10.8.5 (Mountain Lion). The bug, allowing an attacker to decrypt data protected by SSL, is addressed through one of the aforementioned security updates. "There were known attacks on the confidentiality of SSL 3.0 and TLS 1.0 when a cipher suite used a block cipher in CBC mode," Apple's description reads. "To address these issues for applications using Secure Transport, the 1-byte fragment mitigation was enabled by default for this configuration," the company states. To read more click **HERE**

10 Years of Mobile Malware: From Symbian Worm to Tor-Based Android Backdoor

SoftPedia, 26 Feb 2014: Ten years have passed since the first piece of malware designed to target mobile devices was spotted. Mobile threats have come a long way from the SymbOS.Cabir worm that spread via Bluetooth to AndroidOS.Torec.a, the first Android threat that relies on the Tor network to protect its communications infrastructure. SymbOS.Cabir is considered the first piece of mobile malware. It targeted Symbian devices, which back in 2004 were very popular. Some Cabir versions were designed to steal data from targeted devices, while others infected files. In the same year, Trojan.Mos was spotted. Packaged with a cracked version of the popular Mosquito game, Trojan.Mos was designed to send SMSs to premium rate numbers, this being the first piece of malware that helped cybercriminals make a profit. 2004 was also the year in which a destructive piece of malware emerged. SymbOS.Skulls replaced all icons with skulls and made application files unusable. Symbian malware was king of the hill until 2006 when the first BlackBerry Trojan, Trojan.Redbrowser, was launched. This was actually the first J2ME Trojan that could infect different mobile platforms. It was designed to send text messages to premium numbers. Another BlackBerry malware that emerged in 2006 was Spyware.FlyxiSpy, a threat advertised as a spy app for spouses. SymbOS.ZeusMitmo was the first piece of malware designed to steal the verification SMSs sent by banks to customers while they performed online transactions. Actually, ZeusMitmo, which emerged in 2010, was the first mobile malware to target online banking services. In 2011, cybercriminals started targeting the Android platform. Now, most pieces of mobile malware are designed to target Google's operating system. "In the last two years, we have seen major growth from Trojans and adware targeting mobile devices, mainly focusing on Android phones. Even targeted attacks now make use of mobile threats for spying purposes," Symantec's Candid Wueest noted. "Considering this boom, mobile malware has become a real threat that needs greater attention because it isn't over yet. In fact, we are likely to see the next evolution of mobile threats soon, especially as mobile phones become identification tokens and payment solutions in the future." Android malware continues to evolve. Earlier this week, researchers from Kaspersky revealed the existence of Backdoor. AndroidOS.Torec.a, the first Android malware to rely on Tor for C&C communications. Both Symantec and Kaspersky have published reports on the evolution of mobile malware. Check out their websites for more information on this topic. To read more click **HERE**