The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

14 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

April 10, Seattle Times – (Washington) **Audit: State sold computers with Social Security numbers, tax info still on them.** Washington officials quarantined computers, stopped sales, and established new guidelines after an audit released April 10 determined several State agencies likely gave away or sold roughly 1,800 computers out of 20,000 over the last 2 years containing confidential information, including Social Security numbers, medical records, and tax reforms. The auditors noted about 9 percent of all computers given away or sold held confidential information. Source: http://blogs.seattletimes.com/today/2014/04/audit-state-sold-computers-with-social-security-numbers-tax-info-still-on-them/

April 11, SC Magazine – (International) **Cyber attacks are targeting Heartbleed flaw, says US CERT.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued a warning April 10 stating that attackers have begun exploiting the Heartbleed vulnerability in OpenSSL and advised affected entities to report any incidents involving the vulnerability. Source: http://www.scmagazineuk.com/cyber-attacks-are-targeting-heartbleed-flaw-says-us-cert/article/342274/

April 11, Softpedia – (International) **Expert shows that hackers can abuse Chrome speech recognition API flaw.** A security researcher identified a vulnerability in an older version of Chrome's speech recognition API that could be leveraged to obtain the transcript generated by the browser. The API was introduced in Chrome 11 but may still be used by some Web sites. Source: http://news.softpedia.com/news/Expert-Shows-That-Hackers-Can-Abuse-Chrome-Speech-Recognition-API-Flaw-437237.shtml

April 11, Threatpost – (International) **BlackBerry, Cisco products vulnerable to OpenSSL bug.** BlackBerry reported that several of its software products are vulnerable to the Heartbleed OpenSSL vulnerability, though its phones were unaffected. Cisco also reported that many of its products, including video communications and phone systems, were also vulnerable. Source: http://threatpost.com/blackberry-cisco-products-vulnerable-to-openssl-bug/105406

Jetpack Wordpress plugin vendor pushes update to close critical security hole
Heise Security, 14 Apr 2014: The developers of Jetpack, one of the most widely used WordPress plugins, are urging users to download and implement the latests versions that fix a critical security bug. "During an internal security audit, we found a bug that allows an attacker to bypass a site's access controls and publish posts. This vulnerability could be combined with other attacks to escalate access," George Stephanis, WordPress core contributor and leader of the Jetpack team shared last week, adding that the vulnerability was introduced with Jetpack 1.9, which was released in October 2012. "Fortunately, we have no evidence of this being used in the wild. However, now that this update is public, it's just a matter of time before exploits occur. To avoid a breach, you should update your site as soon as possible," he warned. The team is also been sending out the warning via emails to users. They are taking this very seriously: the WordPress security team was asked to push updates to every version of the

plugin since 1.9 through core's auto-update system, and the Jetpack team has asked hosts and network providers for help and force upgrades on the users they host. Users who fail to update the plugin on their site run the danger of being disconnected from the Jetpack service until they move to fix the problem. The updated versions can be downloaded directly from the plugin's official site, or one can use the plugin's dashboard to update it (go to Plugins > Installed Plugins > Jetpack). "Finding and fixing bugs is a key part of software development," Stephanis noted at the end. "I can't promise there will never be another issue like this, but I can promise that when a problem is found we will do everything in our power to protect as many people as possible, as quickly as possible." To read more click **HERE**

Windows XP Users Already Under Attack

SoftPedia, 12 Apr 2014: Windows XP reached the end of its life on April 8, so it was only a matter of time until cybercriminals across the world started trying to capitalize on this critical moment for millions of users. No less than 300 million computers are believed to be running Windows XP right now, so hackers put in place several dangerous tactics to trick users into downloading fake software updates and malicious applications. The Telegraph is reporting that users are now targeted via YouTube links and Facebook posts that are encouraging them to download fake software updates, anti-virus applications, and programs that still work on Windows XP. Once these apps reach a Windows XP computer, users are assaulted with advertising deals, banners, and pop-ups asking them to purchase other programs, usually priced at only a few bucks, in order to remove infections which allegedly exist on their PCs. Even though their computers are not infected, some users might actually buy the advertised products which, in return, do nothing good to their PCs, but instead could be used to deploy more malicious software. The same source reports that in some cases users are directed to online surveys that need to be filled with personal information, such as name, address, and phone numbers, in order to download the application that promises to clean an infected computer. Microsoft issued plenty of warnings that such a thing could happen, but in many cases, malicious applications could be blocked by legitimate anti-virus solutions that still receive updates on Windows XP computers. Avoiding clicking on suspicious links and downloading tools coming from untrusted sources are also a thing that needs to be done these days. According to the latest set of figures provided by market researcher Net Applications, Windows XP continues to be used by 28 percent of the desktop machines worldwide, despite the fact that Microsoft had warned that end of support was coming for more than 12 months. The majority of security vendors worldwide announced that security updates would continue to be delivered to their applications for 12 to 24 more months in order to keep Windows XP users protected until they manage to move to a newer operating system that could help them stay safe while browsing the web. To read more click **HERE**

Nine People Accused of Stealing Millions of Dollars with ZeuS Malware

SoftPedia, 12 Apr 2014: US authorities have unsealed an indictment charging nine individuals with being involved in a criminal organization that relied on the ZeuS banking Trojan to infect computers and steal millions of dollars from their owners' bank accounts. Two of the suspects – Yuriy Konovalenko, 31, and Yevhen Kulibaba, 36 – have been apprehended. The Ukrainians were arrested in the United Kingdom and have recently been extradited to the United States. Three other Ukrainians and a Russian have also been charged, but they remain at large. The Ukrainians are Vyacheslav Igorevich Penchukov, Ivan Viktorvich Klepikov and Alexey Dmitrievich Bron. The Russian suspect is Alexey Tikonov. The rest of the charged individuals have not been identified so they're named as John Does in the indictment. All of the suspects have been charged with conspiracy to commit computer fraud and identity theft, conspiracy to participate in racketeering activity, multiple counts of bank fraud, and aggravated identity theft. Authorities say the suspects infected the computers of unsuspecting individuals with ZeuS. "The 'Zeus' malware is one of the most damaging pieces of financial malware that has ever been used," said Acting Assistant Attorney General David A. O'Neil of the Justice Department's Criminal Division. "As the charges unsealed today demonstrate, we are committed to making the Internet more secure and protecting the personal information and bank accounts of American consumers. With the invaluable cooperation of our foreign law enforcement partners, we will continue to bring to justice cyber criminals who steal the money of U.S. citizens," O'Neil added. According to the indictment, the cybercriminals used the malicious

software to capture bank account numbers, passwords, and other information they needed to breach bank accounts. They transferred money from the victims' accounts into the accounts of money mules, individuals who withdrew the criminal proceeds and sent it to the overseas members of the conspiracy. Kulibaba operated the money-laundering network, whereas Konovalenko was responsible for obtaining stolen banking credentials and forwarding the information to Kulibaba. The other members of the conspiracy were responsible for developing malicious software, financial management, and administrating the technical aspects of the scheme. "This case illustrates the vigorous cooperation between national and global law enforcement agencies and sends a strong message to cyber thieves," said Special Agent in Charge Thomas R. Metz of the FBI's Omaha Division. "The FBI and our international partners will continue to devote resources to finding better ways to safeguard our systems, fortify our cyber defenses and stop those who do us harm." To read more click **HERE**

How to Fix Errors 80070020, 80073712, and 0x800f081f on Windows 8.1 Update

SoftPedia, 12 Apr 2014: Some users cannot install Windows 8.1 Update due to a number of issues, with some uncanny error codes provided during the deployment process. 80070020, 80073712, and 0x800f081f are the errors popping up when Windows 8.1 Update fails to install, according to a number of users who have confirmed this on Microsoft's support forums, but the software giant is yet to provide a fix for them. It turns out, however, that a workaround actually exists, and Microsoft forum user Andrew B has published a few simple steps that need to be followed in order to successfully deploy Windows 8.1 Update. According to his post, when Windows 8.1 Update first fails to install, the original patch does not clean all leftovers, so all your attempts to manually deploy the new release will obviously fail as well. Andrew B recommends users to follow the next steps and then try to install Windows 8.1 Update manually. Here are the steps

1. Launch Command Prompt with administrator privileges
2. Run the following command:

dism /online /remove-package /packagename:Package_for_KB2919355~31bf3856ad364e35~amd64~~6.3.1.14

3. When step 2 is completed, run this command:

dism /online /cleanup-image /startcomponentcleanup

4. Try to install Windows 8.1 Update manually

This solution might not work for everyone affected by the aforementioned errors, but it's still worth a try if you can't deploy Windows 8.1 Update. To read more click **HERE**

Microsoft Acknowledges Windows 8.1 Update 0x80071a91 Error, Releases Fix

SoftPedia, 14 Apr 2014: Windows 8.1 Update is still causing lots of problems to a number of users attempting to install it from Windows Update, but a few days of complete silence, Microsoft has finally acknowledged the issue and provided a fix to address it. An advisory intuitively called "Error 0x80071a91 when installing update 2919355 in Windows" reveals that in some cases, "when you install update 2919355 by using Windows Update in Windows RT 8.1, Windows 8.1, or Windows Server 2012 R2, the installation fails with error code 0x80071a91," so consumers are recommended to download a small patch to fix the issues. Microsoft clearly states that this update does not replace a previously-released update, so you need to install it only after you install the original KB2919355 released by the company. According to information included in this advisory, the following Windows 8.1 Update versions are being affected by the 0x80071a91 error: Windows RT 8.1, Windows Server 2012 R2 Datacenter, Windows Server 2012 R2 Standard, Windows Server 2012

R2 Foundation, Windows Server 2012 R2 Essentials, Windows 8.1, Windows 8.1 Pro, and Windows 8.1 Enterprise. Keep in mind, however, that some users are experiencing different problems when trying to install Windows 8.1 Update, so this particular fix only comes to address error code 0x80071a91, so do not download it unless you are experiencing this problem. One of the users who posted on Microsoft's Community forums, a different workaround could actually help users get Windows 8.1 Update running on their computers. Here's what he says in a very short post on the forums: "After numerous failed attempts to install Windows 8.1 Update 1, I did a System Restore to bring my system back to a time before I installed any of the other Patch Tuesday updates. After that, I went into Windows Update, and clicked 'Check for updates' and unselected all the other updates and then I selected Windows 8.1 Update 1 by itself. It installed successfully! Then, after a reboot, I installed the remaining updates and those installations were also successful," he wrote. Nobody can guarantee if this workaround could also work for you too, but in case you're experiencing issues with Windows 8.1 Update, it won't hurt to give it a try. At the same time, you might also want to have a look at the other fix found by users who were trying to deal with Windows 8.1 Update installation issues, but again, it appears that it only works for a limited number of computers. To read more click **HERE**

Malware Found on Computers of Germany's Space Center, Evidence Points to China

SoftPedia, 14 Apr 2014: The German Aerospace Center (DLR), the country's national center for aerospace, energy and transportation research, has been reportedly targeted in a cyberattack apparently launched by a foreign intelligence agency. However, not many details are available at this point. According to Der Spiegel, computers used by administrators and scientists have been found to be infected with Trojans and spyware. The cyberattacks appear to be sophisticated. In some cases, the forensic investigators who have analyzed the infections haven't found the actual malware because it was programmed to self-destroy as soon as it was discovered. The attacks are said to impact all operating systems used by the DLR. Evidence indicates that the attacks have been launched from China. The country's Federal Office for Online Security (BSI) has found Chinese characters in the code of some Trojans. Typos in the code also suggest that the attacker is from the Far East. However, someone familiar with the investigation has told Der Spiegel that the real attackers might have planted these clues to hide their identity. The United States National Security Agency (NSA) is among the suspects. Because the center stores information on armament and rocket technologies, the attacks have been catalogued as being extremely serious. To read more click **HERE**

Fake Driver Downloads Offered to Windows XP Users

SoftPedia, 14 Apr 2014: Windows XP no longer receives support and security patches, so cybercriminals worldwide have started a very aggressive campaign that tries to exploit computers still running the ancient platform. As I told you during the weekend, Windows XP users are now assaulted with all kinds of fake software updates and applications, but it turns out that some malicious drivers are also involved in the scheme. Christopher Boyd of Malwarebytes warns that a fake application called YourFileDownloader promises to help Windows XP users download and install the latest drivers for their computers, but after deployment, you need to pay to register and unlock the program. "Take care with the last minute surge of XP themed downloads and offers – whether on social networks, forums or video sharing sites a lot of what you're going to see over the coming weeks will probably not do you any favours to install or sign up to," he writes. Indeed, Windows XP users are the preferred target for cybercriminals worldwide these days and since so many people are still running the unsupported operating system, up-to-date third-party software that can block such threats and protect their computers is a must-have. Plenty of security vendors have already confirmed that their apps would still work on XP, so find an anti-virus app and deploy the latest virus definitions as soon as possible if you're still running this OS version. To read more click **HERE**

Israeli Hackers Claim to Have Exposed Individuals behind OpIsrael

SoftPedia, 14 Apr 2014: A group of Israeli hacktivists called the Israeli Elite Force claim to have identified several of the people who have taken part in OpIsrael, the campaign that took place on April 7. Several hacktivist groups have taken part in Operation Israel. Some websites belonging to Israeli government agencies and financial institutions have been disrupted with distributed denial-of-service (DDOS) attacks. In addition, a large number of smaller websites have been defaced. Personal data allegedly belonging to Israelis has also been published online. However, Israeli authorities, cited by the Jerusalem Post, claimed that OpIsrael wasn't as successful as the hacktivists said it was. The country's Shin Bet security agency established a special cyber operations room to deal with the attacks, but the cyberattacks only slowed down some government websites, officials noted. Israel had plenty of time to prepare for the attacks since hacktivists announced their intentions months before the start of the campaign. Similarly to last year, Israeli hackers have responded to the attacks. Buddhax, a member of the Israeli Elite Force, has published files containing information on the identities of 16 individuals who have allegedly taken part in OpIsrael. Names, email addresses, IPs and photographs taken via their webcams have been published by Buddhax. The alleged hackers are said to be mainly from Indonesia and Malaysia, but some are from Portugal, Italy, Finland, Switzerland, Saudi Arabia, the UK and Algeria. The information has been published on Dropbox, but the account's links have been temporarily disabled because they've generated too much traffic. "I'm not a great hacker," Buddhax wrote after publishing the information. "But I'm at least good enough to expose you." He added, "next time do not take part in an offensive against Israel. We know who you are, we know where you are. Hail Israel." In addition to leaking the details of alleged OpIsrael hackers, Israeli hacktivists have also targeted a number of websites from the Arab world. "We carried out some small operations that hit the Arab world, websites and some online accounts, but this was not an official Israeli response. It was just child's play," one hacker told Israel Today. "It is really not recommended that they [Anonymous Palestine] mess with Israel, and they know this well." Judging by previous anti-Israel campaigns, hacktivists will probably soon announce something like OpIsrael Reloaded. When it comes to hacker operations initiated by actors in Asia, Israel seems to be the most targeted. Such campaigns have taken place for years, and they'll probably continue. To read more click **HERE**

BlackBerry Promises Heartbleed Vulnerability Fix for BBM for Android, iOS by April 18

SoftPedia, 14 Apr 2014: BBM users will be happy to know that BlackBerry confirmed that the level of risk for their smartphones to be vulnerable to the Heartbleed bug is minimal, but that it will offer a bug fix in the form of an update by Friday, April 18. Scott Totzke, BlackBerry senior vice president, told Reuters yesterday that most of his company's products do not use the vulnerable software, there are two apps in particular that might be affected by the Heartbleed vulnerability. BlackBerry's official named Secure Work Space corporate email and BBM for Android and iOS among the products the Canadian company plans to patch in order to remove the said vulnerability. Totzke has stated that the risk of Android and iOS users to be affected by Heartbleed is small due to the fact that the BlackBerry's security technology will make it very difficult for someone who wishes to exploit the vulnerability in order to gain data through an attack. He claims that "it's a very complex attack that has to be timed in a very small window," thus it should be safe for Android and iOS users to continue to take advantage of BBM's features without fear that their smartphones will be hacked. However, BBM users should expect a security update to arrive on their devices by Friday, which is meant to address the Heartbleed vulnerability. To read more click **HERE**

Windows 8.1 Update Apps, Malware Bytes A/V Broken By 8.1 Patch

SoftPedia, 14 Apr 2014: If you're one of the users who rushed to install Windows 8.1 Update last week, chances are that everything worked very smoothly, so you're now running the latest version of Windows. A number of users, on the other hand, experienced quite a lot of issues with the 8.1 Update, with some complaining that apps such as Internet Explorer 11 and Microsoft Office fail to start. It appears that the problem is caused by Malwarebytes Anti-Malware Enterprise, a security solution developed by Malwarebytes and which apparently has some sort of compatibility issue with the new OS version rolled out by Microsoft. The parent company has already acknowledged the issue and said that

a fix is expected to be implemented in the next full update for the application. "We are aware of a situation with Windows 8.1 Update 1 where MBAE prevents IE11 and possibly MS Office applications from opening. We are trying to fix this issue in the publicly available version of MBAE," the company said in a short post today. A fix has also been provided, but those who are experiencing similar issues are recommended to wait until a new app update is being released in order to address the compatibility problems automatically. To read more click **HERE**