THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

29 July 2014

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

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, and Sandia National Labs

July 25, U.S. Securities and Exchange Commission – (National) **Citigroup business unit charged with failing to protect confidential subscriber data while operating alternative trading system.** New York-based LavaFlow Inc., agreed July 25 to pay $5 million to settle U.S. Securities and Exchange Commission charges that the Citigroup business unit failed to safeguard the confidential trading data of its subscribers when it allowed an affiliate to access the LavaFlow-operated alternative trading system (ATS). Source: http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370542371114#.U9Zy6fldVKI

July 27, Softpedia – (International) **Englishman indicted for stealing thousands of U.S. government employee records.** A man from England was indicted July 24 in the Eastern District of Virginia for offenses that enabled him to access sensitive information belonging to more than 100,000 federal government employees by breaching the systems of the U.S. Department of Energy, the U.S. Sentencing Commission, FBI's Regional Computer Forensics Laboratory, and Deltek, Inc., among several others. The man was able to exploit a security vulnerability in Adobe ColdFusion gaining administrator-level access to the networks using custom file managers. Source: http://news.softpedia.com/news/Englishman-Indicted-for-Stealing-Thousands-of-US-Government-Employee-Records-452280.shtml

July 28, Softpedia – (International) **XSS flaw fixed in Barracuda Spam and Virus Firewall.** Vulnerability Laboratory researchers discovered a non-persistent cross-site scripting (XSS) vulnerability in the Barracuda Spam and Virus Firewall web application affecting versions 5.1.3 and earlier that allowed a potential attacker to hijack session information or execute a non-persistent code. The vulnerability was patched July 15 after researchers notified the developer. Source: http://news.softpedia.com/news/XSS-Flaw-Fixed-in-Barracuda-Spam-and-Virus-Firewall-452377.shtml

July 26, Softpedia – (International) **Remotely exploitable flaws fixed in Siemens SCADA system.** Siemens patched 5 vulnerabilities discovered in its SIMATIC industrial automation system, four of them presenting remote exploitation risk, after an advisory by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) which explained that the flaws resided in the SIMATIC WinCC product which is a supervisory control and data acquisition (SCADA) system. Source: http://news.softpedia.com/news/Remotely-Exploitable-Flaws-Fixed-in-Siemens-SCADA-System-452219.shtml

July 25, Softpedia – (International) **XML-RPC abused in brute-force attacks against WordPress sites.** Sucuri researchers found new brute-force attacks delivered against WordPress Web sites leverage the XML-RPC protocol and the wp.getUersBlogs function have increased since July 4 with 2 million attempts originating from 17,000 different IP addresses. Source: http://news.softpedia.com/news/XML-RPC-Abused-In-Brute-Force-Attacks-Against-WordPress-Sites-452143.shtml

Linux DDoS Bot Found in Amazon Cloud

SoftPedia, 29 Jul 2014: Logged events may suggest a compromise of the server Threat actors are actively exploiting a vulnerability in an older version of Elasticsearch software in order to add distributed denial-of-service (DDoS) malware in Amazon Elastic Compute Cloud (EC2) services. Elasticsearch is an open source search server that can be used to look for various types of documents; its advantages include scalability, almost real-time search and support for multi-latency. The security flaw, CVE-2014-3120, exists in the scripting capability of the software, which can be exploited to execute arbitrary code remotely on the server it is installed on. One solution for administrators that cannot perform an update would be to turn off this functionality, if possible. Because vulnerable versions of Elasticsearch (1.1.x) are still active in the EC2 instances of some organizations, the attackers rely on a modified version of the proof-of-concept exploit code to fit their needs; they have added a Perl-based web shell, which allows execution of Linux shell commands from a remote machine. This is used to deliver a variant of the Backdoor.Linux.Mayday.g DDoS malware, as is identified by Kaspersky, to the Amazon cloud. It appears that despite its DNS amplification capabilities, the current Mayday variant floods the targeted sites with UDP traffic only, Kaspersky researcher Kurt Baumgartner said in a blog post. An UDP flood attack can be started by delivering UDP packets to different, random ports of the intended victims. If the flow of packets is too large, the target becomes unreachable by other clients. DNS amplification attacks are more powerful, as the returned amount of information is much larger than the initial query. But even so, "the flow is strong enough that the DDoS'd victims were forced to move from their normal hosting operations IP addresses to those of an anti-DDoS solution. The flow is also strong enough that Amazon is now notifying their customers, probably because of potential for unexpected accumulation of excessive resource charges for their customers," writes the researcher. Elasticsearch can be installed in the cloud solutions of other services than Amazon, too, and they may be facing a similar situation. According to Baumgartner, among the victims of DDoS attacks using Mayday there is a large regional bank in the United States and a notorious electronics maker and service provider in Japan. Elasticsearch was patched against the vulnerability that is used to compromise the cloud machines back in May. Version 1.2 of the software no longer has dynamic scripting turned on by default. Also, a new release, 1.3, became available on July 23. To read more click **HERE**

Stolen Self Regional Healthcare Laptop Exposes Patients' Details

SoftPedia, 29 Jul 2014: A burglary to one of the Self Regional Healthcare facilities that resulted in the theft of a laptop puts sensitive information about patients at risk. The incident occurred on May 25, and the employees of the organization learned about it two days later, on May 27. Two individuals responsible of the breach, who have since been arrested, confessed to the crime and said that the computer was destroyed and thrown into a lake. The device, which was protected by a password but not encrypted, has not been found, and because of this, there is the assumption that the data on it could have been accessed by unauthorized persons. As such, Self Regional must notify the individuals whose data may have been exposed. According to the executives, at least 500 patients may be affected by the data breach. The data available on the computer device included patients' names, Social Security numbers, driver's license numbers, treating physician names, insurance policy numbers, patient account numbers, service dates, diagnosis/procedure information, payment card information, financial account information, and possibly their addresses. "In an abundance of caution, Self Regional is providing written notice of this incident to affected individuals, to the U.S. Department of Health and Human Services, as well as to certain state regulators," said Craig White, vice president, corporate compliance and integrity. All impacted parties have been offered complimentary one-year membership to a service providing identity theft mitigation so that any misuse of the information is detected early on and dealt with according to protocols. To read more click **HERE**

Chinese Officials Raid Microsoft Offices as Part of New Anti-Trust Investigation

SoftPedia, 29 Jul 2014: Chinese government officials yesterday paid an unexpected visit to local Microsoft offices without providing a clear reason for this, making everyone wonder if this was related to the growing tension between China and the United States. Now new reports are emerging, pointing out that Microsoft offices in Beijing, Shanghai, Guangzhou and Chengdu have been visited by Chinese officials as part of a new anti-trust investigation that could be started against the Redmond-based tech giant. Little is known at this point, but it appears that the Chinese government is taking more steps to protect local companies, as they fight against the domination of firms based overseas. In China, the National Development and Reform Commission is investigating anti-trust cases involving pricing violations, while the Ministry of Commerce is the one giving the green light to acquisitions. At this point, it's not yet clear which one is investigating Microsoft. In May, the Chinese government decided to ban Windows 8 on their computers, in a move that became one of the biggest hits received by the Redmond-based software giant in this particular market. Microsoft was quick to respond to this ban, explaining that it's willing to discuss with the Chinese government to address any complaints and bring Windows 8 back on their computers. "We were surprised to learn about the reference to Windows 8 in this notice. Microsoft has been working proactively with the Central Government Procurement Center and other government agencies through the evaluation process to ensure that our products and services meet all government procurement requirements. We have been and will continue to provide Windows 7 to government customers. At the same time we are working on the Window 8 evaluation with relevant government agencies," a company spokesperson told us soon after China announced the Windows 8 ban. At the same time, China is developing its very own Linux-based operating system, so the new anti-trust investigation could be part of a broader plan to push users off Microsoft software. Earlier this month, reports coming from China indicated that the central government blocked access to a number of online services, including Microsoft OneDrive, in order to prevent news of local pro-democracy protests from spreading across the web. Qualcomm is already facing anti-trust trouble in China, as the local government is ready to issue a fine of more than $1 billion (€730 million) on claims of overcharging and monopoly on the Chinese market with a number of products. To read more click **HERE**

Botched Patch Tuesday Update Breaks Down Office 2013

SoftPedia, 29 Jul 2014: Microsoft rolled out six different security updates as part of this month's Patch Tuesday, but it turns out that one of the optional fixes is breaking down Office 2013 once and for all. A number of users turned to Microsoft's Community forums to complain about the issues, explaining that since Patch Tuesday, Office 2013 fails to start, with a simple "Something went wrong" error displayed on the screen. The same issue has been confirmed by several users who also tried the common workarounds, but none seem to work at this point. "As of Saturday, July 12, I have been unable to use Microsoft Office 2013. It has disappeared from my Start Menu. I have installed the new update that was in my toolbox this afternoon, restarted my computer, but still no luck. I do not have the option to 'Repair' Office, as is suggested in the Error Message. With the number of questions to this forum noted, something globally has happened. Please help," one user explained. While at first nobody knew what was causing the issue, another affected user claims that it's all due to optional updates KB2973488, KB2967917 and KB2962409, which seem to be causing the Microsoft Office 2013 launch errors on Windows 8.1. Microsoft has already confirmed the issue and promised a patch, but some users complain that an updated build of the fix has yet to be shipped to their computers. "Shortly after the release of the July Public Update, we received notification of a potential issue affecting a subset of Office 365 ProPlus users. In some cases, users running Office may not be able to launch Office products after the July 2014 updates are installed," a company support engineer said. One of the users whose Office 2013 installation has been broken down by the botched bulletin claims to have found a solution, even though many complained that uninstalling and reinstalling the productivity suite didn't make any difference. He claims that using Microsoft's dedicated tool for uninstalling Microsoft Office 2013 is the right way to do it, with a manual reinstallation of the application dealing with the issues. "I then re-installed and it works fine now, even with the new Windows updates applied," he pointed out. Unsurprisingly, some users expressed their frustration on the

forums, calling for Microsoft to provide a fix as soon as possible because Office is in most of the cases the key productivity suite for many businesses. "This is not good enough. This is a disaster. To force people to uninstall and reinstall is a shameful disaster. You had better come up with a better solution or I will move my entire organization to Google Docs," one user posted. To read more click HERE

Venafi: 97% of Global 2000 External Servers Are Still Vulnerable After Heartbleed

Softpedia, 29 Jul 2014: It's been months since Heartbleed was discovered, and yet, the world's servers are largely unprotected against the vulnerability. According to a research from security solutions developer Venafi, 97 percent of the Global 2000 organizations' externally facing servers continue to be vulnerable to cyber attacks due to incomplete Heartbleed remediation. That's a staggering number that should make us all think twice about what companies we deal with because our very own personal data may be on the line. The fact that all these servers continue to not be properly patched leaves the door open for attackers to spoof legitimate websites, to decrypt private communications and to steal sensitive data sent over SSL. As a reminder, Heartbleed is an OpenSSL vulnerability that went undiscovered for more than two years. The security problem appears because attacks exploiting Heartbleed don't leave any traces behind, which means it is almost impossible to know when and what type of data got picked up by the hackers. Successful exploits show that there's plenty of sensitive data that can be picked up by the attackers, including passwords, SSL/TLS keys, as well as X.509 digital certificates. Venafi points out that on top of applying the OpenSSL patch, organizations must assume that all keys and certificates were compromised, given the extent and duration of the vulnerability. They should not only issue new certificates, but also revoke the old ones. For the Threat Research Analysis, Venafi Labs looked at 1,639 Global 2000 organizations across more than 550,000 public-facing servers and found critical security flaws. Only 387 Global 2000 organizations have fully remediated Heartbleed, which accounts for 3 percent of the total public-facing servers scanned. The remaining 97 percent continue to be exposed to ongoing cyber attacks and malicious activity. "Enterprises must also assume, just as many did with user IDs and passwords, that all keys and certificates were compromised—not just the keys and certificates that secured the systems hosting the Heartbleed vulnerability—and must be revoked and replaced. Thousands of applications behind the firewall, including those of Cisco, Juniper, HP, IBM, Oracle, McAfee, Symantec and many others, remain exposed," the report reads. Kevin Bocek, vice president for security strategy and threat intelligence at Venafi, says that IT security teams are under the false impression that they've remediated Heartbleed by just applying the available patch. "But if someone walks into your house through an open door and steals your house keys, you don't then rely on the same locks once you've closed the door," he points out, urging organizations to find and replace all of their keys and certificates. As for the future, Venafi's experts believe it's difficult to predict things. The company has told Softpedia that they hope that, with the help of this report, more organizations will become aware of the continued security exposure and seek to remediate the situation with market-available technology capabilities. "The more sophisticated attacks become, the more extensive the remediation process will have to be. CISOs should not and cannot tolerate this situation. Some IT security leaders may be told by incident response teams that a full-scale rekey, reissue, and revoke is not necessary. Others may be told that it's too complicated or time consuming. And there has been a false assumption that patching is all that's required. Some may be misinformed, possibly by websites that show remediation is complete, but have no awareness of changes to keys and certificates, only to basic patching," Venafi told Softpedia. To read more click HERE

Koler Ransomware Had Complex Distribution Infrastructure

SoftPedia, 29 Jul 2014: Researchers took apart the Koler designed for Google's mobile platform and found an intricate distribution infrastructure that relies on a traffic distribution system (TDS), which aims at any other visitor, not just those using mobile devices. The ransomware, detected by Kaspersky as Android.OS.Koler.a, is believed to have been operated by the same team behind Reveton, which is based on Citadel Trojan. Based on the discoveries made by researchers from Kaspersky, the malicious file propagated to desktop and mobile device users through a well-thought distribution network, which

allowed the threat actors to launch new campaigns automatically. The entire process of infecting a device relies on a redirection chain that would end with the user being diverted to a location serving the malicious app installer (APK), which the security experts determined to resolve to an IP address from the Netherlands. Victims would be steered to the rogue locations after landing on one of the 49 adult websites (all linking to external resources) identified by Kaspersky to be involved in the distribution of Koler. They would all point to videosartex.us, the controller domain of the campaign, and from here, the victim would be steered towards the server of the malware appropriate for the operating system and device they ran. According to Kaspersky, throughout the campaign (April 2014 – June 2014), most of the infected devices have been from the US (about 146,000), although infections have been seen in the United Kingdom (13,692), Australia (6,223), and Canada (5,573) as well. The crooks created localized ransomware template messages for a total of 30 countries, so these are just the top four. The entire scheme is quite complex compared to what researchers have seen in other malicious campaigns, since the crooks target both desktop and mobile device users. "However, the distribution network used in this campaign is the most interesting part. Dozens of automatically generated websites redirect traffic to a central hub where users are redirected again according to several conditions. This second redirection could be to a malicious Android application, browser-based ransomware or to a website with the Angler exploit kit," states the analysis report from Kaspersky. Android.OS.Koler.a does not do any damage on an infected system because it does not feature encryption capabilities, such as the latest emerging threats. It simply locks the device and displays a message claiming to be from a law enforcement agency from the victim's country. Unlocking the Android can be done by paying the ransom fee, which is generally between $100 / €75 and $300 / €223. Getting rid of the annoying message and gaining control of the device is not too difficult and Malwarebytes provides specific details to get the job done. To read more click **HERE**