THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

5 June 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

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, and Sandia National 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 this open source data

June 3, Securityweek – (International) **Soraya malware mixes capabilities of Zeus and Dexter to target payment card data.** Researchers with Arbor Networks identified a new family of point-of-sale (PoS) malware known as Soraya that is capable of performing memory scraping techniques similar to the Dexter PoS malware as well as intercepting Web browser data similar to the Zeus trojan. The researchers found that thousands of payment cards have been compromised by the malware, mostly originating from financial institutions in the U.S. and Puerto Rico. Source: http://www.securityweek.com/soraya-malware-mixes-capabilities-zeus-and-dexter-target-payment-card-data

June 4, The Register – (International) **New software nasty encrypts Android PHONE files and demands a ransom.** Researchers at ESET identified a new piece of Android ransomware known as Android/Simplocker that encrypts victims' data and demands a ransom via the MoneXy service. The malware is controlled by a command and control server hosted within the TOR network. Source: http://www.theregister.co.uk/2014/06/04/android_simplocker_file_scrambling_ransomware/

June 3, Threatpost – (International) **GnuTLS patches critical remote code execution bug.** GnuTLS released a patch for the open source cryptographic library May 28 that closes a critical remote execution vulnerability which could allow an attacker to trigger a buffer overflow and cause a server to crash or potentially execute arbitrary code. Source: http://threatpost.com/gnutls-patches-critical-remote-code-execution-bug

June 3, Securityweek – (International) **Report examines how attackers mask threat activity.** Palo Alto Networks released their latest Application Usage and Threat Report June 2, which found that attackers continue to use common sharing applications such as email and social media to initiate multi-phased attacks, among other findings. Source: http://www.securityweek.com/report-examines-how-attackers-mask-threat-activity

Windows 8.1 Update Users Getting Error Code 0x80070490 after Reboot
SoftPedia, 5 Jun 2014: Windows 8.1 Update was released to users on April 8, 2014, but many have actually experienced issues that prevented them from installing the new OS version, no matter if they tried to do it manually or via Windows Update. While Redmond actually tried to address some of these bugs with the help of new patches or fixes aimed at the error experienced during installation, it appears that a number of consumers who actually managed to deploy Windows 8.1 Update are now struggling to deal with an issue affecting Windows Store app synchronization across devices. "Windows Store failed to sync machine licenses. Result code 0x80070490" is the error that multiple users are getting after installing Windows 8.1 Update and judging by the number of posts on Microsoft's Community forums, some are still searching for a workaround on this. A message posted in April by one of the affected users perfectly describes what's happening, while also confirming that some of the common workarounds haven't made any difference in this case. Here's what the message posted by the user reads: "After a clean install of windows8.1.1 using the ISO from Technet I started getting the following error message in my event log the first time I start my

machine in the morning: Event 512 Store-Licensing 'Windows Store failed to sync machine licenses. Result code 0x80070490' I use a Microsoft account and I have synced by Modern apps many times manually. Running the scheduled task manually will also produce the same error. I disabled the Scheduled Task that runs the sync and I'll see if it shows up tomorrow. Btw, the Store seems to be working fine. I read somewhere that the MS Store will be changed for 8.1.1 so I wonder if the 'new' store will stop these messages. The Scheduled Task that kicks this off appears to be Microsoft/Windows/WS and is called WSRefreshBannedAppsListTask." At this point, it's not yet clear whether this is a widely experienced error, but there's no doubt that it clearly adds some frustration in the case of users who tried to install Windows 8.1 Update on their computers. What's worse is that Microsoft made Windows 8.1 Update mandatory for everyone running Windows 8.1, so you have basically no other option than to get it up and running, no matter what issues you are experiencing. Windows 8.1 PCs that won't be running Windows 8.1 Update until June 10 won't receive any new patches and security updates, with Microsoft explaining that this new OS version is the core of all future improvements, so everyone needs to deploy it as soon as possible. To read more click **HERE**

Skype Users Face Security Risk Due to Unencrypted Data

SoftPedia, 5 Jun 2014: Microsoft's Skype is an extremely popular VoIP/video conferencing tool that is used by both individuals and business organizations, but with over 300 million users, the security risks affecting it have an even bigger impact. According to Solutionary's May Threat Report, the fact that Skype keeps personally identifiable information, alongside chat transcripts in an unencrypted file on the local system, makes users vulnerable. What does this mean? It means that anyone that has the knowledge and skill to hack a Skype user can easily get access to personal information without actually having to hack into Microsoft's servers. The file that concerns Solutionary was named main.db, a clear indicator as to what the document holds. It can be found on:

- C:\Users\Username\AppData\Roaming\Skype\SkypeName on Windows
- /Users/user/Library/Application Support/Skype/SkypeName on Mac
- /home/user/.Skype/SkypeName on Linux.

On Windows and Linux, the locations are hidden by default, but that doesn't mean anything to someone who knows their way around a computer and it will certainly not prevent an attacker from locating the files they want. When the file is collected, it can be opened with SQLite since it is completely unencrypted. Inside, there's a long list of tables such as Accounts, Alerts, Calls, ChatMmebers, Contact, DBMeta, Messages, Participants, SMSes, VideoMEssages, Videos and Voicemails, to name just a few. Basically, it's the main database file for Skype functions, which makes it pretty easy to infer what kind of information is stored in most of the tables. Hackers can gain access to the users' full name, birth date, country, city, email address, phone numbers and even the complete chat transcript. "The details above are stored both about the direct user and any contacts that they may have in Skype. All of this could represent valuable information to an attacker. Additionally, the plain text and simple location make it an easy task for anyone, even without administrator access, to extract the database's information. Of course, this does indicate a larger issue, such as that the file system is compromised in another fashion," reads the security research. Users are advised to use an alternate, more secure program, such as Citrix. There's also the option of using full-disk encryption to make sure the data remains secure. Deleting the database each time the program is closed should work as well, but it's a process that takes time and it can be quite annoying. Furthermore, while the program is running, users are still vulnerable. To read more click **HERE**

Criminals seeking more buyers with all-in-one malware

CSO, 4 June 14: Security researchers have discovered multipurpose malware capable of stealing payment card numbers from electronic cash registers and data entered in Web forms through a browser. The authors of the malware, dubbed Soraya, are also working on adding capabilities for stealing credentials for FTP servers. However, that feature is not fully baked, so researchers at Arbor Networks Security

Engineering and Response Team (ASERT) are not sure how the credentials would be stolen. "At this point, that feature hasn't been implemented, so we don't know how it will actually work," David Loftus, research analyst for ASERT, said Tuesday. The versatility of Soraya, which means "rich" in Iranian, makes it unique, researchers said. The authors are likely trying to make their software as marketable as possible on the criminal underground. "It's sort of an all-in-one package for the malware authors," Matthew Bing, another research analyst at ASERT, said. The piece of Soraya that could be used in attacking retailers' electronic cash registers, called point-of-sale (POS) systems, scrapes debit- and credit-card numbers from memory after card holders swipe their cards at the register. The technique is similar to what was used in the Target breach that led to the theft of 10s of millions of payment card numbers during last year's holiday shopping season. A twist in Soraya's memory scraping is its use of the Luhn algorithm, a formula used to determine which numbers collected are valid payment card numbers. "Previously, RAM (random access memory) scrapers had just grabbed any 16-digit long string, but this one, Soraya, is just a little bit more sophisticated," Bing said. At least a couple of thousand valid debit- and credit-card numbers have been stolen through Soraya and posted for sale on criminal forums, the researchers said. Most of the numbers have been taken from U.S. businesses, with the remainder from companies in Costa Rica and Canada. POS malware has become popular on online criminal marketplaces, since the Target attack, Loftus said. "Since the Target breach, we've seen an explosion in the different variants of point-of-sale malware," he said. To reduce the risk of having a POS system hacked the researchers recommend using them only for transactions, do not make them accessible from a remote location and replace default passwords with strong ones. The side of Soraya that can steal data inputted into Web forms imitates capabilities used by the Zeus family of malware, which is popular among criminals for stealing online banking credentials. Soraya, like other similar malware, sends captured data to a command-and-control server used by the cybercriminals. To read more click **HERE**