THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

5 August 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

August 4, Associated Press – (National) **PF Chang's names 33 restaurants in data breach.** Restaurant chain P.F. Chang's provided the locations of 33 restaurants that were compromised in a data breach uncovered in June, which included restaurants in Baltimore; Pittsburgh; St. Louis; Austin, Texas; and Charlotte, North Carolina. An investigation into the breach is continuing. Source: http://www.cnbc.com/id/101884120

August 1, Threatpost – (International) **Citadel malware variant allows attackers remote access, even after removal.** Researchers at IBM identified a new variant of the Citadel banking malware that uses Windows shell commands to create a new local user with a non-expiring password in order to circumvent the removal of the malware and maintain remote control over the affected system. Source: http://threatpost.com/citadel-malware-variant-allows-attackers-remote-access-even-after-removal

August 4, Softpedia – (International) **Registry-residing malware creates no file for antivirus to scan.** A researcher with GData published details of a new type of malware dubbed Poweliks that can avoid detection by antivirus programs by not creating any file on the disk, performing its functions instead in the system memory, and making the registry key unavailable to the Registry Editor. Source: http://news.softpedia.com/news/Registry-Residing-Malware-Creates-No-File-for-Antivirus-To-Scan-453374.shtml

August 4, Securityweek – (International) **Remote code execution flaw patched in Samba 4.** The developers of open source software suite Samba released a patch August 1 that closes a vulnerability present in all versions of Samba 4 that could allow an attacker to generate a remote code execution vulnerability as the root superuser. Source: http://www.securityweek.com/remote-code-execution-flaw-patched-samba-4

August 4, Help Net Security – (International) **Thousands of Mozilla developers' emails, passwords exposed.** Mozilla stated August 1 that around 76,000 Mozilla Developer Network email addresses and around 4,000 hashed and salted passwords were left publicly accessible for about 30 days due to a failed data sanitation process. Developers were advised to change their passwords as a precaution. Source: http://www.net-security.org/secworld.php?id=17201

August 4, The Register – (International) **Cisco patches OSPF bug that sends traffic into black holes.** Cisco released a patch for a flaw in its Open Shortest Path First (OSPF) routing implementation that could allow an attacker to take control of the OSPF Autonomous System domain routing table, intercept traffic, or blackhole traffic. The issue affects all unpatched versions of Cisco IOS Software, IOS XE Software, ASA Software, PIX Software, and FWSM Software. Source: http://www.theregister.co.uk/2014/08/04/cisco_patches_ospf_bug/

August 4, Help Net Security – (International) **Synology NAS users hit with Cryptolocker variant.** Users of Synology's network-attached storage (NAS) devices reported having devices infected with a variant of the Cryptolocker ransomware beginning over the weekend of August 2 that encrypts files and demands a ransom to decrypt them. The method by which the malware is infecting NAS devices is currently unknown and users were advised to backup their files and unplug the devices until the infection vector is identified. Source: http://www.net-security.org/malware_news.php?id=2827

Here's How Gmail Detected the Child Abuse Photos Inside Gmail

SoftPedia, 5 Aug 2014: Google helped with the arrest of a man who, as you may have heard, was sending indecent images of children to a friend. The news made the world have contradictory feelings about Google's email scanning activities because, on the one hand, it's great that the man was captured, but on the other hand, there's a big question about everyone's privacy level while using Gmail. Google has come out and said that they are only scanning emails for advertising, and child abuse footage is the only type of content they flag while scanning. This means that other type of criminal activities remain under the radar or, at least, they're not reported by Google to the authorities. Even so, the company's assurances haven't really made people relax about the whole situation because it's long been feared that Google oversteps its boundaries when it scans emails, which is also considered a controversial practice. The company has even been sued for its email scanning habits, but since April, everything has been put in the Terms of Service to make sure that Google is no longer liable in any court for scanning emails for advertising purposes. So, how does Google detect indecent pictures but leaves everything else alone? Well, the company has been working with authorities, such as the National Center for Missing and Exploited Children, for many years. In the time that has passed since then, the Internet giant has built a database full of hashes, also known as photo fingerprints, for various child abuse images. Each one is unique and they're attached to a certain image, so it doesn't matter if someone changes the name of the file. When Google scans the email and its contents while the messages is being sent, received and stored to the cloud, as per the company's ToS, the system also detects these hashes. The company is then legally obligated to report them to the authorities, who can then obtain warrants and eventually arrest the culprits. The company is adamant about keeping its powers restricted to fighting against child abuse and has been working to take down any links from its search results that may lead to such sites, as well as actual images from the search engine, not just Gmail. Other companies have similar systems in place. Microsoft, for instance, has PhotoDNA, a piece of software that can be used to detect images of abuse. Similarly, this one too can calculate a mathematical hash for images of child sexual abuse, which immediately recognizes photos even if they were altered in one way or another. Both Facebook and Twitter use this technology. Therefore, you shouldn't worry about Google alerting the cops if you share family photos with your kids with some close family and friends. To read more click HERE

Yahoo/Gmail Used by Malware for Communication

SoftPedia, 5 Aug 2014: Security researchers discovered a new piece of malware that managed to evade detection since 2012 by relying on web platforms such as Yahoo and Gmail to communicate with the command and control servers. Dubbed IcoScript by Paul Rascagneres from the German security firm G Data, the malware is a remote access tool (RAT), modular in architecture. It leverages the Component Object Model (COM) technology in Windows that can be used to control Internet Explorer. Rascagneres says that it is "useful for malware developers because it allows them to manipulate the browser that is being used by a legitimate user." Among the advantages he points out is HTTP communication being performed by the IE's process and not the malware piece. On the same note, because the browser session is hidden, there is no evidence of additional communication through the web browser. Making use of an encrypted script, the threat actor optimizes "the manipulation of the browser and achieve a modular communication channel," a VirusBulletin report on the researcher's analysis says. By decrypting the script, Rascagneres found that it included a multi-step action, with variables and values designed to offer the attacker the possibility to access specific online locations, pointing the information to upload, control elements and IE actions in web pages, or retrieve contents of iFrames and hidden elements on the page.

In an example provided by the researcher, IcoScript can use COM to connect to Yahoo email service through Internet Explorer, fill in the username and password fields, exfiltrate data, as well as execute commands sent through emails. In the analyzed sample the malware used Yahoo email, but changing the platform, to Gmail, Facebook, or LinkedIn should not be difficult to achieve, says Rascagneres. The choice to use popular email services is what allowed the malware to escape detection, since this type of traffic is not blacklisted by companies. Also, the intrusion detection systems (ISD) do not detect the strings marking the commands in the emails "because the network flow of Yahoo webmail is compressed with gzip. The data is only uncompressed in the user's browser, so the IDS would have to uncompress on the fly." IcoScript is quite difficult to block because incident response teams generally block the bad URL on the proxy, but in this case communication occurs through legitimate channels, which cannot be blacklisted. "It demonstrates both that attackers know how incident response teams work, and that they can adapt their communication to make detection and containment both complicated and expensive," concludes the security researcher. To read more click HERE

Malware Can Evade Antivirus Code-Emulation Feature

SoftPedia, 5 Aug 2014: A researcher has found that the code emulation environments in antivirus products have weaknesses that can be leveraged by malware to bypass protection. Code-emulation is a feature designed for catching malware that still has to be identified and classified by security companies. It consists of simulating suspicious code in a virtual machine and determining whether it is malicious in nature or not. However, researcher Kyle Adams, chief software architect for Junos Webapp Secure at Juniper Networks, created a piece of malware capable of evading detection of major antivirus products, but it could not escape the code-emulation feature available in the free version of AVG. He proceeded to reverse-engineer AVG's feature and managed to find the weak spots that allowed its malware to evade detection. The researcher will present his findings, along with methods for improving code emulation environments, on Tuesday, July 5, at the BSides Las Vegas conference. "The result is a Command-and-Control (C&C) bot, in a non-obfuscated windows shell script, that AVG and many other leading AV engines will not detect," Adams said in the abstract for the conference presentation. This is not the first finding which proves that antivirus products and their components are vulnerable and can be exploited by attackers. Joxean Koret from the Singapore-based firm Coseinc made a presentation on the subject at the SysScan 360 conference in Beijing last month, revealing that multiple antivirus products had plenty of weaknesses and they could increase the attack surface on a target computer. He also talked about how the emulator in a security product could be compromised, since it is the component that unpacks files and scans them in an isolated environment. An exploitation scenario provided by the security researcher consists in sending a ZIP archive with two files inside, one forcing loading of the emulator and the other being an exploit for this feature. The purpose of Kyle Adams' presentation this week is to provide solutions that could lead to improving the security of code emulation environments and better detection of zero-days. He says that, at this moment, although code emulation technology is "a powerful step in the right direction for client security," it is far from being mature and needs to grow a lot until its true potential is fully tapped. Although he picked AVG's feature to reverse engineer, Adams says that "this is not a jab against AVG, as they get enormous credit for including such a powerful tool in a free antivirus client." To read more click HERE

Crypto-Malware Synolocker Hits Synology NAS Devices, Here's How to Defeat It

SoftPedia, 5 Aug 2014: Over the weekend, reports came in from users informing that their NAS (Network Access Storage) devices from Synology had become the target of cybercriminals, who created crypto-malware intended specifically for this type of storage. Named Synolocker, the malicious file could land on the NAS devices either through brute-forcing the login credentials or by leveraging a vulnerability in DSM (DiskStation Manager) or in the operating system. However, since Synology has not yet published a security advisory for their products, the former variant seems more plausible at the moment. Members of the Synology forum have contacted the company and received advice. Synolocker is similar in action to the infamous CryptoLocker. After infecting the device, the Trojan starts encrypting the files on the disk, one by one, at the same time displaying a ransom message asking the victim to pay a 0.6 Bitcoin fee ($350 / €262) in exchange for the decryption key. A ToR (The Onion Router) address is provided for completing the transaction, and after the money is transferred, the crook says that the file unlocking the RSA private key would be made available on the main page of the webserver. Complete instructions about what to do to recover the data are also provided. Despite the above grim scenario, there are methods to prevent the crypto-malware from infecting the NAS device, as well as for saving at least some of the data, while the encryption process begins. Users that have already been affected by Synolocker are advised to turn off the DiskStation as soon as they learn about the infection. Since the malware encrypts files one by one, there is the possibility to stop the locking process and save some of them through migration to a different, clean storage device; this method is not foolproof, though, since determining when the encryption process, which runs in the background, began is critical and in many cases it may be too late. The solution for preventing Synolocker from infecting the NAS is quite simple, and consists of several steps. The router has to be configured to stop forwarding traffic to the router (where available), the default port needs to be changed, and a strong password needs to be instated. Updating to the latest DSM version is also on the list of recommendations. As soon as these steps have been taken, it would be wise to make a backup copy of the data on the DiskStation, just to stay on the safe side. It is recommended to remove the remote access to the device. Another measure of protection is to activate the AutoBlock feature, which blocks connections from IP addresses with multiple failed login attempts. To read more click HERE

Invisible Web Infection Poses Threat to Federal Computer

NextGov, 5 Aug 2014: A surge of malicious software hit news media websites during the first half of 2014, unleashing a threat to federal agencies that rely on those sites to get information, cybersecurity researchers say. Media networks were almost four times as likely to attract malware as the average enterprise network, likely because of an increasingly popular hacking tactic called "malvertising," according to a new Cisco threat intelligence report. Web publications are magnets for online ads that harbor malware and pass it on to readers. The media industry depends on advertising for revenue, but ads are hardly ever vetted for subversive code. "Even folks in federal government-land use the Web to do their job -- they are using the same sites that we all use," Levi Gundert, a technical leader for Cisco's threat research, analysis and communications team, said in an interview. "And because of the way malvertising works, they are just as susceptible to being automatically redirected to some exploit kit site or some other malicious-type sites really seamlessly." A malvertiser who wants to target a specific population at a certain time — for example, government officials following the November elections — can pay a legitimate ad exchange to place malicious ads on news sites during that time. Sometimes, the hacker pays up and instructs the exchange to serve the ad as quickly as possible, leaving little time for vulnerability testing, Cisco researchers found. The infection is invisible to the user. "There is no user click involved -- just load the page and the next thing you know, you are redirected, and that's because of the relationship these websites have with the ad exchanges," Gundert said. During the past six months, between 5 and 10 percent of Cisco customers' malicious traffic was related to malvertising. The scheme has been around for years, but the acceleration in ad exchange abuse is pretty significant, he said. "Adversaries launching exploits and other scams around high-profile events, such as the 2014 Winter Olympic Games and the Academy Awards, and big news stories, such as the Malaysia Airlines Flight 370 mystery and the South Korean ferry disaster, are likely reasons for the increase in encounters for the media and publishing industry," states the report, which is slated for release Tuesday. Last month, malvertising apparently showed up on radio host Glenn Beck's publication TheBlaze.com, and there were reports in January of poisonous advertising on The Moscow Times newspaper . No government defense plan for malvertising really exists, said Gundert, a former Secret Service special agent. Some computer security tools prevent ads from appearing, but they are not always effective. "If you are requesting CNN.com, it is probably not going to block the request, and if the advertisement that's coming in gets served up with CNN.com, it is probably not going to block that because it's a legitimate advertisement," he said. Some departments, such as Homeland Security and Justice, impose stricter surfing restrictions

– but, again, not with the best outcomes. Access controls are put in place "so they can lower the attack surface based on what they believe is reasonable for your job function," Gundert said. "Even after all of that, they are not going to block certain news sites . . . and ultimately, those ads can end up there. It's a very tricky problem to solve without blocking legitimate content." To read more click HERE

How to recognize the cyber insider threat
Computerworld, 5 Aug 2014: Cisco Australia hosted a discussion on cyber security in Sydney this week. According to Computer Emergency Response Team (CERT) Australia's technical director, Doctor Jason Smith, many organisations CERT Australia works with become victim to an insider because their network is misconfigured or not monitored. "The ability for poorly trained or tired [IT] people to make mistakes can also have an impact," he said. "Once an adversary has code execution on your computer, they are essentially an insider. The controls you need to build need to take into account what an insider could do to your network." He added that the insider threat needs to be communicated to the company's board so that they can have input into decisions that are made to deal with the problem, in conjunction with the IT department. "Cyber security is a team sport and that team can consist of people in your organisation and service providers," said Smith. According to Cisco's information security global vice president, Steve Martino, companies need to put in place controls that can capture data and look for patterns or behavioural things that are out of the norm. For example, if a trusted staff member starts accessing systems more often, looking at data in the system or working very long hours, this can be captured via logs and the security card reader the employee uses to swipe in and out of the building. "I can look at how often a person accesses a system or data in that system. That's not violating privacy because accessing that system is part of their job," he said. "If we see a pattern, we will sit down with the [Cisco] employee and discuss what is happening and how to deal with it." However, Martino warned employers that opening up a secure email account and looking inside it could be deemed a violation of privacy. His advice when creating an insider threat plan was starting with 'who, what, why and how'. For example, who would want the data, why would they want it, what would they do with it and how would they get to the data? Edwin Cowen University's security research institute adjunct professor, Gary Blair, who previously worked as a CISO at Westpac, said that Australian banks mainly look at external threats such as organised crime, nation states and terrorist groups. "I sense that within Australia, we trust people in the work environment. That's good because it leads to harmonious working relations," he said. However, Blair said that more companies need to recognise there is a potential for an insider threat. "The Australian banking industry is starting to conduct extreme cyber scenario planning as part of their regulatory requirements. In doing so, banks are considering the worst case scenarios that could occur." For example, he said banks are conducting audit reports and risk assessments to see how secure their internal systems are. Speaking to Computerworld Australia in July, cyber forensic investigator Nick Klein from Klein & Co warned that rogue employees will do anything to get sensitive information ranging from photocopying documents to copying information into their Google Mail email account. "It's tricky because companies are using Gmail or other [cloud] email services as part of their normal business operations. It's getting harder to investigate [IP theft] because people are sending all of these services out to the cloud," he said. "The question we ask people is: If you have Google Drive, what kind of backups do you have? Executives look at their IT guys and say, `We've got backups, right?' And the IT guys will reply that they haven't implemented that yet." To read more click HERE