THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

24 October 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

October 22, Securityweek – (International) **Windows zero-day exploited in targeted attacks through PowerPoint.** Microsoft reported that it has observed limited targeted attacks exploiting a zero-day vulnerability in the company's Object Linking and Embedding (OLE) technology which could allow an attacker to perform remote code execution if a user opens a specially-crafted Microsoft Office file. The vulnerability affects all current Microsoft Windows releases except Windows Server 2003 and Microsoft advised users to apply a series of workarounds until a patch can be released. Source: http://www.securityweek.com/windows-zero-day-exploited-targeted-attacks-through-powerpoint

October 22, Help Net Security – (International) **Koler worm spreads via SMS, holds phones for ransom.** Researchers at AdaptiveMobile identified a new variant of the Koler worm for Android that spreads via a bitly link that directs users to a Dropbox page where the malware is disguised as an app. The malware then blocks infected devices' screens with a fake law enforcement page and demands a ransom to be paid via Money Pak Voucher. Source: http://www.net-security.org/malware_news.php?id=2890

October 22, Help Net Security – (International) **Attackers change home routers' DNS settings via malicious code injected in ads.** Sucuri Security researchers identified a malvertising campaign that embeds malicious code into an ad hosted on the googlesyndication.com network and attempts to change the DNS settings on users' home routers in order to lead them to potentially malicious Web sites. Source: http://www.net-security.org/malware_news.php?id=2891

October 22, Help Net Security – (International) **Malware directs stolen documents to Google Drive.** Researchers with Trend Micro identified a new piece of information-stealing malware dubbed Drigo that uploads any .PDF, text, and Microsoft Word, Excel, and PowerPoint files to a Google Drive account. The researchers reported that the malware appears to be targeting government agencies and reported the Google Drive account associated with the malware to Google. Source: http://www.net-security.org/malware_news.php?id=2888

October 21, Securityweek – (International) **Apple fixes security flaws with release of iOS 8.1.** Apple released an update to its iOS 8 mobile operating system, closing several vulnerabilities and adding new features. Source: http://www.securityweek.com/apple-fixes-security-flaws-release-ios-81

October 22, Securityweek – (International) **'Operation Pawn Storm' cyber-espionage campaign hits organizations.** Trend Micro researchers identified a cyberespionage operation dubbed "Operation Pawn Storm" that uses targeted emails and compromised Web sites to infect users in government, military, and media organizations with the SEDNIT (also known as Sofacy) malware. Source: http://www.securityweek.com/operation-pawn-storm-cyber-espionage-campaign-hits-organizations

October 21, Dayton Daily News – (National) **FBI arrests Weather Service employee for alleged cyber hacking.** The FBI arrested and charged a National Weather Service employee working out of the Wilmington, Ohio office October 21 for allegedly hacking into the restricted U.S. Army Corps of Engineers' National Inventory of Dams, which contains detailed information about dams nationwide, in May 2012 and downloading sensitive files from the inventory. Source: http://www.daytondailynews.com/news/news/fbi-arrests-weather-service-employee-for-alleged-c/nhpKt/

October 23, Softpedia – (International) **CryptoWall 2.0 delivered through malvertising on Yahoo and other large sites.** Proofpoint researchers observed a recent campaign using malicious advertisements on Yahoo, 9gag, and other popular Web sites to deliver the CryptoWall 2.0 ransomware via the FlashPack Exploit Kit. The exploit kit exploits vulnerabilities in Adobe Flash Player to deliver the ransomware that encrypts users' files and demands a ransom to decrypt them. Source: http://news.softpedia.com/news/CryptoWall-2-0-Delivered-Through-Malvertising-On-Yahoo-and-Other-Large-Sites-462970.shtml

October 23, Securityweek – (International) **1.2 million networking devices vulnerable due to NAT-PMP issues.** A security researcher with Rapid7 reported October 21 that the company identified around 1.2 million Internet-connected devices that are vulnerable to various attacks due to poor implementation or configuration of the Network Address Translation – Port Mapping Protocol (NAT-PMP). The vulnerabilities could allow attackers to perform denial of service (DoS) attacks, intercept traffic, or perform other malicious actions. Source: http://www.securityweek.com/12-million-networking-devices-vulnerable-due-nat-pmp-issues

October 22, Softpedia – (International) **Apple warns users of attack targeting iCloud site.** Apple confirmed reports of man-in-the-middle (MitM) attacks against its iCloud service that employed an insecure certificate and advised users not to dismiss browser warnings regarding the security of content. The attacks trigger warnings in the Chrome and Firefox browsers but not in Qihoo, the most popular Web browser in China. Source: http://news.softpedia.com/news/Apple-Warns-Users-of-Attack-Targeting-iCloud-Site-462846.shtml

Navy stands up cybersecurity task force

Fox News, 23 Oct 2014: The Navy has established a special new unit designed to protect computer networks and improve cyber security across the service called Task Force Cyber Awakening, or TFCA, service officials said. Created in August of this year, TFCA is a 100-person force dedicated to establishing protocols, identifying vulnerabilities, increasing cyber awareness and shoring up security and access with the Navy's computer networks, service leaders explained. "The genesis of this started several years ago when we started to see that the risk calculus associated with cyber was changing. If you look at risk and how we characterize risk with things like vulnerabilities, the consequences of exploiting those vulnerabilities and the actors, you'll see that consequences are continuing to grow in cyber," Matt Swartz, lead for Task Force Cyber Awakening, told Military.com. The consequences associated with cyber-attacks are growing in part because weapons systems are increasingly relying on networks, creating a much larger cyber component to platforms and operations, he added. "Combat and control systems are integrated. Years ago things were stand alone. Through modernization we've connected things like weapons systems and engineering systems to a network. A risk to one now is a risk to all," Capt. Kathy Creighton added. According to a Wall Street Journal report in September 2013, Iranian hackers succeeded in penetrating into the Navy Marine Corps Intranet, an internal network used by the services for email and internal intranet functions. Although Swartz, Creighton and other Pentagon officials have not publicly confirmed that the hacking was done by Iranians, the WSJ report cites U.S. officials saying that Iranian hackers did penetrate into NMCI. The report also says U.S. officials do not think any significant information was stolen from the unclassified NMCI network. The NMCI network has more than 700,000 users at more than 2,000 different locations. The hackers were able to penetrate deep into the network through some of the Navy's publicly accessible websites, the WSJ report said. Swartz

acknowledged the intrusion, without specifying any perpetrators, and said the new task force is looking at implementing lessons learned from the U.S. military response to the incident – an effort called Operation Rolling Tide. "Over the last several years we have seen a lot more aggressive actions on the part of adversaries. We responded to that NMCI incident and when we looked at that we realized we could not just piecemeal our response. We started doing assessments across our enterprise," Swartz said. Operation Rolling Tide involved a vigorous effort to secure government databases and improve the overall security protocols for Navy computer networks. "Operation Rolling Tide was broad. We wanted to make sure we could respond rapidly to those types of incidents in the future, not only to detect them but to respond to them. We took the lessons that we learned and looked across business and tactical networks, applying those principles to all those enterprises within the Navy," Swartz added. The TFCA is interested in establishing integrated cyber policies and procedures governing access and use of Navy networks. At the same time, the special task force is hoping to prioritize protections and identify which parts of the Navy's many networks are most crucial to operational functioning and missions – in the event of crisis. "The realization came to us that you can't protect the entire enterprise at the same level. Ultimately, there are hard trade-offs that you are going to have to make. There is probably a subset of our enterprise that is no-kidding critical to the warfighter," Swartz explained. At the same time, the TFCA is working to better understand and protect network and combat system connectivity in light of rapid cyber-related technological progress. Some of the anticipated measures sought after by the task force include improving what's called "cyber-hygiene," effort to create secure passwords and better user practices. "We're not just talking about firewalls, routers and sensors but we are talking about taking our traditional navy cyber apparatus – operations, defense, inspections and all the different parts. We're saying this is not just going to be the traditional C4ISR networks and SIPRNet (Secret Internet Protocol Router Network). We want to extend that apparatus to the whole of Navy's networks. This includes combat systems, control systems and platform IT," Creighton said. Creighton said representatives from all five naval systems commands are participating in the TFCA such as Naval Air Command and Naval Sea Systems Command. There is also involvement from Fleet Forces Command as well as the Pacific Fleet and other areas of the Navy, she said. Improving cyber situational awareness and better understanding how networks share information with one another is an essential element of the task force's agenda, Creighton added. These efforts can include a number of hardware-related technical solutions designed to protect or better fortify boundaries between systems. To read more click **HERE**

Promote Windows Users to Admins with the Debian-Based Rescatux 0.32 Beta 2

SoftPedia, 22 Oct 2014: Rescatux, a Linux distribution that allows users to perform all kinds of rescue operations with the help of an easy to use wizard called Rescapp, is now at version 0.32 Beta 2 and is ready for testing. Rescatux works like a regular Live CD distro, but it has a very specific purpose. Despite the name, this is not really a recovery tool, or at least not for data. It's designed to help in the recovery of entire operating systems by repairing the boot process, the Grub, the MBR for Windows OS, and so on. It also comes with some nice features related to the users of a particular system, but we'll get to that in a minute. Rescatux is based on Debian, so the GUI should not be too alien for regular users. It has very low hardware requirements and it should be able to run on basically any system from the past decade. This tool is already full of very interesting options, but the developers are refining it constantly. Some of the new options are still in the Beta stages and they might remain that way for some time. Other features, like the ability to upgrade a Windows user to admin in the system with just a single mouse click, are working flawlessly. "As you might imagine the biggest improvement in this release is that resetting windows password, promoting a windows user to Administrador and unlocking a windows user uses the latest version of chntpw which makes easier and more safe to add users to the admin group. It also fixes a bug that prevented a promoted admin user to be demoted from windows." "Finally you can boot Rescatux from Super Grub2 Disk thanks to its loopback.cfg file which I hope will be accepted upstream in Debian Live soon although they seem to be busy with Jessie freeze. In the development arena I have removed old scripts and add new build folders so that everything is easier to understand when developing Rescatux," says the developer. Other improvements that have been made in this release include Btrfs

support, much better CPU detection, and the ability to fix MBR entries for Windows 7 operating systems. To read more click **HERE**

CryptoWall 2.0 Rampage: 84 New Variants Spotted in Less than a Month

SoftPedia, 23 Oct 2014: The new version of the CryptoWall ransomware was first noticed at the beginning of October, and since then, no less than 84 variations have been detected by security researchers. Recently, this piece of malware with file encryption capabilities has been used in a massive malvertising campaign on prominent websites such as Yahoo, AOL, 9Gag and major news publications in Australia. In a blog post on Wednesday, Ryan Olson from Palo Alto Networks says that, although starting September 30 telemetry from their systems showed increased activity for CryptoWall 2.0, more and more variants are popping up on a daily basis. F-Secure was the first to observe the official 2.0 version of the malware, which included capabilities that had been tested in version 1.0. One of the modifications includes communication with the command and control (C&C) server over ToR (The Onion Router) anonymization network, which is now built into the crypto-malware. This allows the attackers to hide the C&C servers and avoid them being taken down by law enforcement. On the same note, only Bitcoin digital currency is accepted as ransom. Olson says that since CryptoWall 2.0 was first detected by Palo Alto Networks, more than 85,000 attacks have been recorded to try to deliver the malware. "The majority of these have come through e-mails with executable attachments, sometimes contained in .zip files," he says. CryptoWall expands rapidly, victimizes hundreds of thousands This crypto-malware in particular appears to have been adopted at a large scale, as it has been seen to be delivered through multiple exploit kits (EK). French vulnerability researcher Kafeine saw it in Nuclear Pack EK, while in the recent malvertising campaign, it was funneled in by FlashPack EK. In August, Dell SecureWorks published a report saying that over 625,000 victims had been recorded in a period of five and a half months, with an estimated $1.1 million / €835,000 being collected by the cybercriminals. In a different malvertising campaign in September, a version of CryptoWall signed with a digital certificate from Comodo was seen to be delivered to victims. One of the latest attacks observed by Palo Alto Networks had the malware connect to four domains registered on Wednesday, all resorting to a Russian IP address associated with an email that has been used with other two payment domains registered earlier this month. "If these domains are confiscated or otherwise shut down, CryptoWall instructs the user to download the Tor Browser and access a website (paytordmbdekmizq.onion) that is only accessible over the Tor network," said Ryan Olson. Bottom line is that the number of attacks involving CryptoWall has increased lately and the trend does not appear to slow down, especially with the shopping season coming up, when people are more likely to land on dodgy websites in search of bargains. To read more click **HERE**

Recently Patched Flash Player Glitches Leveraged by another Exploit Kit

Softpedia, 23 Oct 2014: Other security flaws in Flash Player, patched by Adobe about a week ago, may have been integrated in Angler exploit kit (EK). Earlier this week, French vulnerability researcher Kafeine announced that an exploit for the Flash Player vulnerability CVE-2014-0569 had been integrated in Fiesta EK. This is a quick step for cybercriminals, since the details of the glitch had been reported privately to Adobe through the Zero-Day Initiative group and were not exposed to the public. With no proof-of-concept being released, it generally passes more time until an exploit for the vulnerability is created, but as Jerome Segura of Malwarebytes says, as soon as the fix is out, "skilled reverse engineers will start looking at the patch to be able to reconstruct the exploit." It is not known how the cybercriminals managed to obtain the necessary details; one theory is that they received a heads-up, another is that they have an extraordinary reverse engineer, the researcher added. The sooner an exploit is created, the larger the number of users that have not applied the update. This obviously ensures a higher rate of success for the bad actors in their endeavors to compromise computers. "That means we have less and less time to deploy and test security patches. Perhaps this is not too much of a deal for individuals, but it can be more difficult for businesses which need to roll out patches on dozens of machines, hoping doing so will not cause malfunctions in existing applications," Segura said. Although there is no certainty at the moment, Kafeine suspects that the new Angler EK includes an exploit for a different weakness that has

been addressed by Adobe with last week's Flash Player update. The payload delivered to the affected computer is a variant of Zeus, which at the beginning had a low detection rate on VirusTotal; more recent scans show an improvement. However, Kafeine has also detected that Bedep, a piece of malware that resides in the memory of the system and is not saved to disk, is also added to the compromised computer. Initially, Kafeine believed that CVE-2014-0569 extended to other malicious tools; now he waits for input from other sources to determine which vulnerability is leveraged. Regardless of the glitch the crooks try to profit from, one thing is certain: users need to update Flash to its latest version in order to reduce security risks. "Browsing the net on an unpatched computer is like playing Russian roulette with a handful of loaded guns," Segura said via email. For cybercriminals, patched software translates to fewer infections, which is a heavy blow for their business. To read more click **HERE**