THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

12 September 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

September 10, SC Magazine – (Ohio) **Computer hardware containing patient data stolen from Ohio plastic surgery office.** The Beachwood-Westlake Plastic Surgery and Medical Spa in Ohio notified 6,141 patients that their personal information was on a piece of computer hardware that was stolen in a June 29 burglary. The hardware contained names and some medical information. Source: http://www.scmagazine.com/computer-hardware-containing-patient-data-stolen-from-ohio-plastic-surgery-office/article/370808/

September 9, Associated Press – (New York) **NY detective accused of leaking secret documents.** A Suffolk County police detective pleaded guilty September 9 to one charge of official misconduct for stealing confidential law enforcement documents, including police tour and intelligence reports, active criminal investigation information, and personnel information, and leaking them to a newspaper. Source: http://www.newsday.com/news/region-state/da-ny-detective-stole-leaked-confidential-papers-1.9271536

September 11, Softpedia – (International) **Zemot malware dropper strain delivered via Asprox botnet and exploit kits.** Microsoft researchers analyzed the Zemot malware dropper, a variant of Upatre, and observed that it has been distributed through the Asprox (also known as Kuluoz) spam botnet and via exploit kits including Magnitude and Nuclear Pack. Once it infects a system the dropper can then deliver click fraud malware and was recently observed to distribute information-stealing malware including Rovnix, Tesch, and Viknok. Source: http://news.softpedia.com/news/Zemot-Malware-Dropper-Strain-Delivered-Via-Asprox-Botnet-and-Exploit-Kits-458437.shtml

September 11, The Register – (International) **TorrentLocker unpicked: Crypto coding shocker defeats extortionists.** Researchers with Nixu found that the encryption used by the TorrentLocker ransomware to encrypt victims' files can be defeated if a user has an original copy of the encrypted version of a file over 2MB in size by applying XOR between the encrypted and unencrypted files. Source: http://www.theregister.co.uk/2014/09/11/torrentlocker_contains_freeunlock_crypto_shocker/

September 11, Help Net Security – (International) **Massive Gmail credential leak is not result of a breach.** Google investigated a dump of Gmail credentials posted online and found that the credentials were not the result of a breach and that less than 2 percent of the credentials might have worked. Users were advised to change their passwords, use strong passwords, and enable two-factor authentication if possible as a precaution. Source: http://www.net-security.org/secworld.php?id=17352

September 10, Threatpost – (International) **Details disclosed for critical vulnerability patched in Webmin.** A researcher with the University of Texas published details on a critical vulnerability in Webmin that was patched in May, showing that the vulnerability could have been used by unauthenticated users to delete files stored on the server. Source: http://threatpost.com/details-disclosed-for-critical-vulnerability-patched-in-webmin

September 10, Threatpost – (International) **Apache warns of Tomcat remote code execution vulnerability.** The Apache Software Foundation warned users of some older versions of Apache Tomcat that they are vulnerable under limited circumstances to a vulnerability that could allow an attacker to upload malicious JavaServer Pages (JSP) to a server, trigger the execution of the JSP, and then execute arbitrary commands on the server. The vulnerability affects versions 7.0.0 to 7.0.39 and users were advised to update their installations. Source: http://threatpost.com/apache-warns-of-tomcat-remote-code-execution-vulnerability

Home Depot and Target attackers likely not the same
Heise Security, 12 Sep 2014: More details about the malware used in the Home Depot breach have surfaced, and it seems that, after all, it wasn't the one used in the Target breach (BlackPOS). According to Trail of Bits CEO Dan Guido and another unnamed source familiar with the investigation, the malware used against Home Depot belongs to a different family of POS RAM scrapers: FrameworkPOS. The malware has been dubbed thusly because it impersonates McAfee's antivirus agent. Event though Home Depot doesn't use McAfee products, this approach was successful as Target's security team was tricked into not paying attention to the malware. There are other dissimilarities between the two malware families: the way and place they install themselves, their interaction with the OS, and the obfuscation techniques they use differ considerably. Guido noted to BusinessWeek that it's likely that the two breaches haven't been executed by the same attackers. The FrameworkPOS' code includes hidden messages denouncing United States' support to Ukraine in the latest conflict. Batches of payment card data stolen from both Target and Home Depot have been and are being sold on the infamous rescator(dot)com underground carder market, but the "dumps" of Home Depot's cards have been named "European Sanctions" and "American Sanctions," which seems to indicate that the Home Depot attackers were (partially) politically motivated. To read more click **HERE**

CryptoLocker-style ransomware booms 700 PER CENT this year
The Register, 12 Sep 2014: CryptoLocker-style ransomware is eight times more common now than in January, going a long way towards overtaking fake police warning ransomware scams, according to Symantec. The disruption of the GameOver Zeus banking trojan botnet back in late May took away one of the main distribution methods for CryptoLocker itself. Security firms have since developed a service that allows victims to recover files scrambled by CryptoLocker without caving in to the demands of extortionists. About 545,000 computers worldwide, around half of those being in the US, have been infected with CryptoLocker between September 2013 and May 2014. Victims have been defrauded to the tune of $27m (£16m) as a result of the malware, according to FBI estimates from June. While it was active CryptoLocker was extremely successful. Its legacy continues in the form of "tribute bands" even though the main scam itself has effectively been neutralised. CryptoLocker-style ransomware has seen a 700 per cent-plus increase. "These file-encrypting versions of ransomware began the year comprising 1.2 per cent of all ransomware detections, but now make up 31 per cent at the end of August," Symantec reports. "By the end of July, it made up 77 per cent of all crypto-style ransomware for the year to date," Symantec adds. The latest edition of the Symantec Intelligence Report (summary **here**) also looks at trends in spear-phishing attacks and identity theft. The full 23 page report is here (**PDF**). To read more click **HERE**

Enigmail PGP plugin forgets to encrypt mail sent as blind copies
The Register, 9 Sep 2014: Enigmail has patched a hole in the world's most popular PGP email platform that caused mail to be sent unencrypted when all security check boxes were ticked. The dangerous hole in the Mozilla Thunderbird extension affected email that was sent only to blind carbon copy recipients on all versions below 1.7.2 released last month. It could mean any Enigmail user, possibly activists and journalists, may have sent apparently encrypted emails that could be read by attackers. Enigmail dev Nicolai Josuttis explained the bug in a release note. "On previous versions of Enigmail one could send an encrypted email to a set of BCC recipients," Josuttis said. "Enigmail would ask if one wants to 'Hide BCC

recipients' and then send the email encrypted to all of them without revealing to whom the email was sent. "Such functionality is missing in version 1.7. Even when marked to be encrypted, an email with only BCC recipients is sent in plain text!" The email was sent in plaintext after users check boxes to encrypt their message. Computer Incident Response Center Luxembourg issued an alert stating "remote attackers [could] obtain sensitive information by sniffing the network." It was assigned CVE-2014-5369 by the OpenWall initiative last month. Computer scientist posting on the Enigmail support forum blasted the error and expressed dismay at having to tell journalists in an upcoming training session to use command prompt to send email. "As a serious user (dissident, whistle-blower, diplomatic or military user) I would now be waiting for the bad guys come and get me with their water-board," they wrote on the forum. The impact of the bug was mitigated by the likelihood that users would send emails using the normal address field and not by blind carbon copy. Prior to the official patch, the bug was fixed only in a nightly Enigmail build while the vulnerable stable version remained open for download without prominent warning. To read more click **HERE**

Microsoft unloads monster-sized can of bug spray on Internet Explorer, again

The Register, 9 Sep 2014 14: True to form, Microsoft has released its latest batch of monthly security fixes, although as expected, September's Patch Tuesday update is a relatively light one. As Redmond warned us, the only critical patches this time around are included in a big roll-up of fixes for Internet Explorer, which addresses one publicly disclosed vulnerability and 36 more that hadn't previously been disclosed. According to Microsoft's security bulletin on the patches, every version of IE going back to IE6 is affected, although only IE7 and later have critical bugs that need fixing. The worst of the vulnerabilities could reportedly allow remote code execution on Windows machines, where an attacker could gain the same security privileges as the current user. The issues detailed in the other three security bulletins published on Tuesday aren't as serious, although they're still ranked as "important" by Redmond's own security standards. One server-oriented bulletin discloses a flaw in the .Net Framework that could allow an attacker to carry out a denial-of-service attack against a Windows Server–hosted website that has ASP.Net installed and enabled. Similarly, a bug in Lync Server can allow an attacker to knock down the server by sending it specially crafted requests. Finally, a bug in the Windows Task Scheduler can allow an attacker to gain elevated security privileges, provided they can logon to a machine and run custom software to do it. The latter flaw only affects Windows 8, Windows 8.1, Windows RT, Windows RT 8.1, Windows Server 2012, and Windows Server 2012 R2. While Microsoft's patch batch was relatively small, however, a few other expected patches didn't arrive. Although Adobe has been timing its own security fixes to coincide with Microsoft's and it earlier said it had a few ready for Tuesday, on Monday it said those patches will be delayed until next week so it can have more time to test them. To read more click **HERE**

Comcast using JavaScript to inject advertising from Wi-Fi hotspots

The Register, 10 Sep 2014: Comcast has begun injecting adverts onto the computers of users who sign up for its public Wi-Fi network, although the company prefers to use the term "watermark" to describe its efforts. The ISP operates over 3.5 million Wi-Fi hotspots around the USA and people who sign up for home or work internet can choose to add them into their contract to get access when outside their buildings. When they take up the WiFi option, Comcast adds short pop-up messages to the data flow. "The point of the watermarking system is that it gives the user a little alert that just says 'Welcome to Comcast Xfinity," Comcast spokesman Charlie Douglas told The Register. He explained that the adverts last for a maximum of three seconds before disappearing and reassuring customers that they are using an official Comcast hotspot, although they can also advise them of apps that can be downloaded. The ad injection system was created by a third-party provider, Front Page, which calls the system a "powerful location experience." The firm sells the system to retail stores, transit terminals and sporting venues as a way of getting advertising directly onto punters' computers. Adverts are injected into the data stream using JavaScript from Comcast's hotspots. When we asked about the security aspects Douglas said that Front Page has its injection system regularly audited to make sure it can't be hijacked for nefarious purposes. This may be so, but as any visitor to the Defcon hacking conference will tell you there's nothing

on this earth that can't be hacked if someone is willing to put in the time and effort. Comcast may bill this watermarking system as a handy information feature, but El Reg is willing to bet that someone out there is working on using it for intrusive purposes. To read more click **HERE**

[NOTE: Intercepting inbound TCP/IP packets to inject messages that are displayed onscreen is something I've not seen before, but has potential for modification to become a potential hacker exploit!]

Senators ask Apple, Home Depot for information on breaches

Tech World, 11 Sep 2014: A recent data breach at retailer Home Depot and a leak of celebrity nude pictures from Apple's iCloud service raise questions about the companies' data security practices, two U.S. senators said Thursday. Senators John "Jay" Rockefeller, a West Virginia Democrat, and Claire McCaskill, a Missouri Democrat, asked Apple and Home Depot for information on their security practices. The senators, senior members of the Senate Commerce, Science and Transportation Committee, have asked the companies to provide the committee with detailed information about the causes of the breaches. "We are interested to know what security protocols Apple has adopted to maximize the safety and privacy of your customers who store information on your company's popular iCloud," the senators wrote. "We understand that the focused nature of the attack on specific iCloud accounts is very different from the massive data breaches that affected other companies, but nonetheless indicate potential vulnerabilities in your cloud security protocols that were exploited by hackers." Rockefeller and McCaskill sent a similar letter to Home Depot Chairman and CEO Francis Blake. "It has been a week since Home Depot announced its investigation ... and we expect that your security experts have had the time to examine the cause and impact of the attack and breach and will be able to provide the committee with detailed information," the two wrote. Earlier this week, two other senators called on the U.S. Federal Trade Commission to investigate the Home Depot breach, which was disclosed through media reports, not a company announcement. To read more click **HERE**