THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

11 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

September 9, Securityweek – (International) **Vendor fixes vulnerabilities in wireless traffic sensors.** Sensys Networks, a company that manufactures sensor devices used in wireless traffic control systems, announced September 5 that it released software updates for its products to address security vulnerabilities and protect systems against attacks caused by lack of encryption or sufficient authentication methods. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an advisory stating that the issues affect Sensys Networks VSN240-F and VSN240-T systems and advised operators to update their software installations. Source: http://www.securityweek.com/vendor-fixes-vulnerabilities-wireless-traffic-sensors

September 9, Softpedia – (International) **Compromised Web server exposes personal info at California State University, East Bay.** California State University, East Bay officials notified over 6,000 employees and former students that a security breach was detected during a routine inspection August 11 and that an attacker used malware to access a Web server and extract files containing personal information, including full names and Social Security numbers. The university removed the malware from its systems and mitigated server vulnerabilities. Source: http://news.softpedia.com/news/Compromised-Web-Server-Exposes-Personal-Info-At-California-State-University-East-Bay-458268.shtml

September 9, IDG News Service – (International) **Adobe fixes critical flaws in Flash Player, delays Reader and Acrobat updates.** Adobe Systems released a critical security update for its Flash Player software, closing 12 security issues, 9 of which could lead to remote code execution. The company also delayed planned patches for Reader and Acrobat by 1 week due to issues identified during testing. Source: http://www.networkworld.com/article/2604961/adobe-fixes-critical-flaws-in-flash-player-delays-reader-and-acrobat-updates.html

September 9, Network World – (International) **September Patch Tuesday: Microsoft closes door on IE zero day attacks.** Microsoft released its monthly Patch Tuesday round of updates for September, with 4 bulletins closing 42 vulnerabilities in various Microsoft products. One bulletin for the Internet Explorer browser closes 37 vulnerabilities, 1 of which was a critical Internet Explorer zero-day vulnerability. Source: http://www.networkworld.com/article/2604465/microsoft-subnet/september-patch-tuesday-microsoft-closes-door-on-ie-zero-day-attacks.html

September 9, The Register – (International) **Use home networking kit? DDoS bot is BACK…and it has EVOLVED.** A researcher identified a new variant of the Lightaidra router-to-router malware that targets consumer-grade cable and DSL modems using default passwords in order to use them in distributed denial of service (DDoS) attacks. The new variant is able to reconfigure victims' firewalls and requires Linux to be running on targeted devices in order to infect them. Source: http://www.theregister.co.uk/2014/09/09/linux_modem_bot/

September 9, Softpedia – (International) **Apple beefs up security, sends iCloud access alert.** Apple announced September 5 that within 2 weeks it would implement new security policies for its iCloud service following attacks that leaked personal photos belonging to celebrities. Some features have already been implemented, such as a notification when an iCloud account is accessed via a Web browser. Source: http://news.softpedia.com/news/Apple-Beefs-Up-Security-Sends-iCloud-Access-Alert-458282.shtml

September 9, The Register – (International) **Phishing miscreants are THWARTING secure-sleuths with AES crypto.** Researchers with Symantec identified what they believe was the first use of AES encryption to disguise fraudulent Web sites designed to steal users' login credentials. The use of AES encryption allows attackers to make the analysis of phishing sites more difficult without affecting how the sites appear and function to users. Source: http://www.theregister.co.uk/2014/09/09/phishing_scam_uses_aes_crypto_to_hide/

September 9, WTVT 13 Tampa – (Florida) **Police: Beef O' Brady's electronic payment network hacked.** Police reported that the electronic payment network of four Beef O' Brady's restaurants in Florida was breached and customers' payment card information was stolen. The company has taken steps to ensure the security of the systems since the issue was identified. Source: http://www.myfoxtampabay.com/story/26486959/police-beef-o-bradys-electronic-payment-network-hacked

September 9, Softpedia – (International) **Yandy.com hacked, financial information exposed.** Yandy.com notified its customers that a Web-based database hosting customers' information, including payment card data, was accessed by an unknown party at least four times between May 28 and August 18. The online retailer detected the breach August 18 and has implemented additional measures to secure its systems. Source: http://news.softpedia.com/news/Yandy-com-Hacked-Financial-Information-Exposed-458255.shtml

Microsoft Patches Information Disclosure Bug in Internet Explorer

SoftPedia, 11 Sep 2014: In this month's cumulative set of updates for Internet Explorer, Microsoft patched the browser against a flaw that allowed attackers to glean information about Enhanced Mitigation Experience Toolkit (EMET) and other security products that were active on the affected system. The vulnerability was exploited during a cyber-espionage campaign, dubbed Operation SnowMan by FireEye and carried out at the beginning of the year against American military personnel. Available in Internet Explorer 10, the flaw offered the possibility to check the protection solutions available on the compromised system. If EMET was detected, exploitation would be aborted. The same would happen if the user browsed with a different version of Internet Explorer. Switching to a newer IE build or having EMET enabled was the recommendation of the experts for protecting against the attack. Microsoft explained the risk of the bug in the security bulletin and said that "an information disclosure vulnerability exists in Internet Explorer which allows resources loaded into memory to be queried. This vulnerability could allow an attacker to detect anti-malware applications in use on a target and use the information to avoid detection." Attackers leveraged Microsoft.XMLDOM ActiveX control to enumerate local resources and determine the existence of local pathnames, intranet hostnames and IP addresses through scrutiny of error codes generated by loading of a one-line XML string pointing to EMET DLL. In the security bulletin, Microsoft says that a perpetrator could gain the same rights as the logged-in user. As such, users with limited privileges would be less impacted than those with administrative rights. An attack scenario provided by the company includes a compromised website rigged to exploit the vulnerability. "In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit this vulnerability through Internet Explorer, and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit this vulnerability," Microsoft says. Most of the glitches fixed with the cumulative updates eliminated the risk of

remote code execution through different methods. Potential attackers could exploit weaknesses to modify the way IE handled objects in memory, as well as add new permission validations to the web browser. A good deal of the vulnerabilities were reported by Bo Qu of Palo Alto Networks, who disclosed to the company a total of 15 critical glitches, for all browser versions. To read more click **HERE**

Users Should Start Preparing for Windows Server 2003's Deadline, Experts Warn

Softpedia, 10 Sep 2014: Windows Server 2003 will officially go dark on July 14, 2015, and Microsoft is preparing for another Windows XP moment, as most of the companies running it might actually delay the transition to a newer platform more than recommended. That's why experts across the world have already started recommending customers to step away from Windows Server 2003, explaining that the transition to a newer platform usually takes more than 200 days. "Many companies are unaware of the workload, let alone the deadline," reseller ITC Infotech was quoted as saying by ChannelWeb. "Once support ends next year, there will be no further patches or security updates, exposing companies to major security and compliance issues." Obviously, expect Microsoft itself to step up its game and start issuing upgrade warnings in order to make more users aware that Windows Server 2003 support is coming to an end. "The end of Windows 2003 is a great opportunity for enterprises looking at optimising and driving efficiencies. They should see it as the chance to tighten the slack that has crept in over the years, and end sunset services and applications that are no longer required," the reseller added. Windows Server 2003 is the Windows XP of server platforms, and it's currently one of the top software solutions in its own category. Of course, Microsoft again hopes that everyone will switch to Windows Server 2012, but it remains to be seen how many are actually willing to upgrade their hardware configurations and invest in a totally new platform. To read more click **HERE**

Mobile Malware Infection Rate in H1 2014 Almost as High as in the Entire 2013

SoftPedia, 9 Sep 2014: In the first half of 2014, the infection rate for mobile devices grew by 17%, which is almost as much as the increase for the entire year 2013, when 20% was recorded. According to a study from Kindsight Security Labs of Alcatel-Lucent, with data pulled from their sensors, 60% of the infected devices run Android operating system, and less than 1% rely on iOS, Blackberry, Symbian and Windows. Based on telemetric information, the researchers estimate that about 15 million devices are currently infected worldwide. However, this number could be conservative because it does not include data from areas where infection rates are known to be higher, such as China and Russia, where Alcatel-Lucent sensors are not available. Furthermore, information from the International Telecommunication Union (ITU) says that there are 2.3 billion smartphones in the world. The study shows that the most prevalent form of malware is spyware, with four new entries being added to the top 20 list of malware. This type of threat is used for tracking device location, spying on incoming and outgoing calls and text messages, as well as tracking web browsing activity. On Android, at the top of the list is a variant of a Trojan called Coogos, affecting more than 35% of the devices monitored by the security firm. It appears that it sends information from the phone to a server located in China. Researchers say that, in the beginning, it was distributed as a wallpaper, but a newer version is packaged as a game. In second place, accounting for little over 30% of the infections, is Uapush Trojan, which displays advertisements on the device but also includes functions for stealing information such as call history and contacts, and for sending text messages (probably to premium-rate services); its command and control server has also been traced to China. The company also included information about residential infection rate in fixed broadband networks, which doubled since December 2013 (9%) to 18% at the end of June 2014; the increase is attributed to moderate-threat-level "adware" infections. According to Kindsight's three-month detection period, the most prevalent threats on users' home devices are adware programs that generally install toolbars and display advertisements on the affected system. However, the top threats are in a different class of malware and pose a much greater risk as they are equipped with functions that can lead to identity theft. At the top of the list is ZeroAccess Trojan (11.13% of infections), mostly used to funnel in other threats that are generally used for large scale ad-click fraud. Carberp, the infamous banking

Trojan, is also on the list. It accounts for 6.33% of the infections and is designed specifically for stealing banking information that is uploaded to a remote server. To read more click **HERE**

About 5 Million Google Account Credentials Dumped Online

Softpedia, 10 Sep 2014: A database containing usernames and passwords for almost five million Google accounts emerged on a Russian forum late on September 9. The user dumping the information on Bitcoin Security board uses the online alias "tvskit" and says that although not all the entries are valid, more than 60% of them should be working; all passwords are provided in plain text. It is unclear how the information was collected, but the most plausible theory is that the attacker(s) gathered the details through phishing and different forms of data exfiltration, such as the use of infostealing malware. Users who want to verify if their address is included in this database can do it through the isleaked.com website, which parsed the information and offers search capabilities. The total number of entries in the database is 4,929,090, and it appears that most of the accounts belong to speakers of Russian, English and Spanish. Any individual impacted by this leak should immediately change the access password. Turning on two-factor authentication (2FA) for extra security against fraudulent account access is also a good measure, regardless if the account has been compromised or not. The collection of data also includes addresses from Yandex and Mail.ru email services, and according to Russian publication CNews, there are several thousands of them. The publication also says that this leak is the third one this week, 4.6 million credentials of Mail.ru users and 1.26 Yandex accounts having been dumped in a public online location prior to this incident. "tvskit" is either the one gathering these details or is acquainted with the perpetrator and has been involved in all three leaks, to an unknown degree. To read more click **HERE**

DOE to investigate possible security breach

AP, 5 Sep 2014: The Department of Energy says it plans a probe into a possible security breach at the Y-12 nuclear plant in Oak Ridge. According to the Knoxville News Sentinel, a Sept. 3 letter from the DOE says the incident was discovered in June and concerns "the potential mishandling and unauthorized access to classified information." Further details weren't immediately available. The plant spokesman declined to comment. The newspaper cited a Sept. 3 letter to Jim Haynes, the president of Consolidated Nuclear Security, the contractor that took over management at Y-12 in July. Security has been a hot topic at the plant since a breach in 2012 when three protesters broke in to a secure area. The letter says DOE officials will visit the plant in October as part of the investigation. To read more click **HERE**