THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

10 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

Internet Explorer steals the Patch Tuesday spotlight again
PC World, 9 Sep 2014: Today, Microsoft released four new security bulletins, but only one of them is Critical. Guess which one? Yes. Internet Explorer. Once again Microsoft's web browser takes center stage as the most crucial of the Patch Tuesday security bulletins. Microsoft resolved a grand total of 42 separate vulnerabilities this month, but 37 of those 42 are addressed in MS14-052—the cumulative update for Internet Explorer. One of the flaws fixed by MS14-052 is publicly known and actively under attack in the wild, which is why this security bulletin is Critical. "The bulletin fixes zero day vulnerability CVE-2013-7331, which can be used to leak information about the targeted machine," says Qualys CTO Wolfgang Kandek in a blog post. "CVE-2013-7331 allows attackers to determine remotely through a webpage the existence of local pathnames, UNC share pathnames, intranet hostnames, and intranet IP addresses by examining error codes. This capability has been used in the wild by malware to check if anti-malware products or Microsoft's Enhanced Mitigation Toolkit (EMET) is installed on the target system and allows the malware to adapt its exploitation strategy." Russ Ernst, director of product management for Lumension, says that MS14-054 should be your second priority. "This is an elevation of privilege vulnerability for one privately disclosed CVE in Task Scheduler," he says. "It's rated important and Microsoft lists its deployment priority as 2." A successful exploit of this vulnerability could allow an attacker to execute code on the system with elevated privileges. An attack that can run with System privileges has the potential to do more damage than one running with standard user privileges. There is also a Critical update today for Adobe Flash. The flaw can be exploited through a malicious web page or possibly through malicious Microsoft Office files to allow the attacker to remotely execute code on the affected system. "These issues are grouped by Adobe as APSB14-21, but actually include 12 CVEs, of which most are top priority patching issues for embedded Flash in the browser," says Ross Barrett, senior manager of security engineering for Rapid7. "These issues affect Chrome on Mac, Windows and Linux, Internet Explorer 10 and 11, and any browser using the Flash Desktop Runtime. In effect this is almost everyone with a browser that has Flash support." To read more click **HERE**

September 9, Softpedia – (International) **Malvertising on YouTube and Amazon delivers sophisticated malware.** Researchers with Cisco's Talos Security Research identified a malvertising campaign dubbed Kyle & Stan that began in May and is currently affecting Windows and Mac users on popular Web sites such as Amazon and YouTube. The campaign inserts malicious ads that serve various forms of spyware, adware, and browser hijacking malware and uses unique configuration files and encryption to attempt to avoid detection. Source: http://news.softpedia.com/news/Malvertising-On-YouTube-and-Amazon-Delivers-Sophisticated-Malware-458211.shtml

September 9, Softpedia – (International) **Dyre banking trojan targets Salesforce customers.** Customer relationship management (CRM) provider Salesforce found that the Dyre banking malware (also known as Dyreza) has been used against some of its customers but found no evidence that any were impacted. The malware uses man-in-the-middle (MitM) attacks to steal credentials and Salesforce advised its users to ensure that their systems were protected against the malware. Source: http://news.softpedia.com/news/Dyre-Banking-Trojan-Targets-Salesforce-Customers-458185.shtml

September 9, V3.co.uk – (International) **Hackers going Nuclear following Blackhole takedown.** A Zscaler ThreatLabz researcher identified a campaign utilizing the Nuclear Exploit Kit and compromised sites including SocialBlade.com, AskMen.com, and Facebook survey scam pages to attempt to infect users' systems. The researcher reported that the Nuclear Exploit Kit has become increasingly popular in

in the last 3 months following the arrest of the alleged creator of the Blackhole Exploit Kit. Source: http://www.v3.co.uk/v3-uk/news/2364131/hackers-going-nuclear-following-blackhole-takedown

September 8, Threatpost – (International) **New timing attack could de-anonymize Google users.** Mavenlink identified and reported an issue in Google accounts that could be used by an attacker in specific circumstances to identify when a particular user visits a site by sharing a Google document with the user's address. Google acknowledged the issue but stated it would not address the issue because the risk presented was judged to be low and only usable in limited circumstances. Source: http://threatpost.com/new-timing-attack-could-de-anonymize-google-users

September 9, CNN Money – (International) **Home Depot confirms months-long hack.** Home Depot representatives confirmed September 8 that the company's payment systems were breached as early as April 2014 and the attack went unnoticed until September 2 when banking institutions reported unusual activity connected to debit and credit card data from the company's stores in the U.S. and Canada. The company is working with the U.S. Secret Service to determine the scope of the breach and has implemented additional security measures at its stores. Source: http://money.cnn.com/2014/09/08/technology/security/home-depot-breach/index.html

Phishers resort to AES crypto to obfuscate phishing sites
Heise Security, 10 Sep 2014: Phishers have started employing AES encryption to disguise the real nature of phishing sites from automatic phishing detection tools. This is the latest obfuscating trick in the fraudsters' bag. They have previously used - and still do - JavaScript encryption tools, data URIs and character escaping to achieve the same goal. Symantec researcher Nick Johnston analyzed the found phishing page (a online banking login page), and explained the procedure: ">The page includes a JavaScript AES implementation, which it calls with the embedded password (used to generate the key) and embedded encrypted data (ciphertext). The decrypted phishing content is then dynamically written to the page using document.write(). This process happens almost instantly, so users are unlikely to notice anything unusual." The used encryption is important for keeping the website under security researchers' radar for as long as possible and to make it more difficult to analyze. No attempt has been made to hide the key or otherwise conceal what is going on - this is the initial "version" of this obfuscation technique, and will likely not be the end one. Phishing detection will improve, and the fraudsters will have to keep pace to stay successful. To read more click **HERE**

Microsoft refuses to hand over emails stored in Ireland, held in contempt by judge
Heise Security, 10 Sep 2014 Microsoft has urged US District Judge Loretta Preska, the judge presiding over the case that sees the company refusing to hand some emails stored in its Dublin facility over to the US government, to find them in contempt. The request, made both by the company and the government, was granted and allows Microsoft to immediately appeal Judge Praska's last year's ruling. The judge didn't impose any sanctions while the case proceeds to the court of appeals. The software giant has already contested the initial decision, arguing that "the Government cannot seek and a court cannot issue a warrant allowing federal agents to break down the doors of Microsoft's Dublin facility. Likewise, the Government cannot conscript Microsoft to do what it has no authority itself to do - i.e. execute a warranted search abroad." The appeal was unsuccessful, and the ruling was confirmed on July 31, 2014. "The US has entered into many bilateral agreements establishing specific procedures for obtaining physical evidence in another country including a recently-updated agreement with Ireland. We think the same procedures should apply in the online world," the company explained in a post on its website dedicated to the case, in which they confirmed their intention to appeal the decision once more. "If the US government prevails in reaching into other countries' data centers, other governments are sure to follow. One already is. Earlier this month the British government passed a law asserting its right to require tech companies to produce emails stored anywhere in the world. This would include emails stored in the US by Americans who have never been to the UK." "The US has both a responsibility and an opportunity to show new

leadership on privacy issues," says Microsoft, who is worried that the current decision will negatively impact on its business and the competitiveness of US cloud providers, as it will erode the trust of foreign governments and companies. To read more click **HERE**

Unencrypted thumb drive containing patient data stolen from Duke University Health System
SC Magazine, 5 Sep 2014 Duke University Health System (DUHS) is notifying an undisclosed number of patients that their personal information was on an unencrypted thumb drive that was stolen from an administrative office on July 1. How many victims? Undisclosed. DUHS did not respond to SCMagazine.com requests for information. What type of personal information? Names, medical record numbers, physicians' names, and, in some instances, the names of certain Duke University Hospital locations visited. What happened? Spreadsheets containing patient data were stored on an unencrypted thumb drive that was stolen from a DUHS administrative office. What was the response? DUHS is notifying all impacted patients. DUHS is enhancing encryption processes, and furthering staff education on the use of encryption and the importance of handling patient data securely. Details: The theft occurred on July 1 and DUHS learned of it that same day. Affected patients were treated in the Duke Children's Health Center and Lenox Baker Children's Hospital between December 2013 and June 2014. The thumb drive has not been recovered. To read more click **HERE**

Access gained to California university web server storing personal information
SC Magazine, 8 Sep 2014 More than 6,000 individuals are being notified by California State University, East Bay, that their personal information – including Social Security numbers – may have been compromised by an unknown third-party. How many victims? 6,036, mostly faculty and staff, as well as 507 birth dates, according to reports. What type of personal information? Names, addresses, dates of birth and Social Security numbers. What happened? An investigation revealed that an unknown third-party broke into a University web server using an overseas IP address and a tool designed to secretly access information on the server. What was the response? Malicious files were removed from the server and vulnerabilities have been mitigated, and steps have been taken to ensure similar incidents do not occur again in the future. All impacted individuals are being notified and offered a free year of credit monitoring services. Details: The personal information was accessed on Aug 23, 2013. The affected server stored various employment transaction records and some extended learning course information. To read more click **HERE**

Goodwill announces breach, more than 800K payment cards compromised
SC Magazine, 4 Sep 2014: The investigation revealed that malware known as 'Infostealer.Rawpos' was used in the attack. In a letter to customers dated Tuesday, Jim Gibbons, president and CEO of Goodwill Industries International (GII), announced that payment card data was accessed following a malware attack on a third-party vendor used in about 10 percent of stores. The malware attack on the vendor's systems occurred sporadically from Feb. 10, 2013, to Aug. 14, 2014, Gibbons wrote, adding that the card data includes names, payment card numbers and expiration dates. He said that there is no evidence of other information, including addresses and PINs, being compromised. Roughly 868,000 payment cards were compromised and 330 stores in 19 states were impacted, Lauren Lawson, a Goodwill spokesperson, told SCMagazine.com in a Thursday email correspondence. A full list of impacted Goodwill locations and periods of exposure can be found here. "Our outside forensic expert has confirmed that the malware is known as rawpos, according to the Symantec reference," Lawson said. "This data compromise incident is not related to the ['Backoff'] malware." Lawson confirmed in a follow-up email that she was referring to the malware in this Symantec post, which states that 'Infostealer.Rawpos,' a trojan discovered in February of this year, is designed to steal confidential information from compromised computers. Goodwill has stopped using the affected third-party vendor for payment card processing and has found no evidence of infections on any of its internal systems, Gibbons wrote, adding card brands have reported "very limited" fraudulent use of cards tied to Goodwill locations. "Because this incident did not affect social security numbers, Goodwill is not offering credit monitoring services at this time," Lawson said. Actions are being

taken to ensure a similar incident does not occur again, which include launching an enterprise wide Member Security Taskforce and establishing working agreements with security organizations to ensure best security practices are used, Lawson said. "[GII] is working with the 158 independent, community-based Goodwill members across the country to launch an effort to harden their infrastructure," Lawson said. "GII has intensified its educational efforts to include seminars and peer to peer learning opportunities about data security/PCI." "Rather than attempt to control all the various entry points a hacker can use to access a network, businesses can stay one step ahead of the game by more quickly identifying suspicious user behavior on the IT network – especially when it's coming from a third-party vendor," Polak said. To read more click **HERE**

CMS administrator to testify before committee on HealthCare.gov hack

SC Magazine, 8 Sep 2014: After news that a HealthCare.gov server was broken into and injected with malware, the Centers of Medicare and Medicaid Services (CMS) Administrator Marilyn Tavenner will testify in front of the House Oversight and Government Reform Committee on September 18. The committee's chairman, Darrell Issa, had strong words regarding the testimony. "Considering this administration launched HealthCare.gov over the objections of CMS, it's unsurprising that the website has suffered a 'malicious attack'," he said in a release."The committee will continue to push for answers from the administration and Administrator Tavenner must testify on the subject of transparency, accountability, and information security…" The uploaded malware was intended to launch distributed denial-of-service (DDoS) attacks, the server compromised was one used to test new code and, according to CMS, no consumer data was exposed. To read more click **HERE**

Markey, Blumenthal pen letter to FTC over Home Depot breach

SC Magazine, 9 Sep 2014: After Home Depot confirmed a data breach, Sen. Ed Markey, D.-Mass., and Sen. Richard Blumenthal (D.-Conn.) questioned the retailer's security with Markey also highlighting a bill to protect consumer data that the two are pushing before the Senate. In a letter to FTC Chairwoman Edith Ramirez, the senators said that "given the unprecedented scope and extended duration" of the data breach, the retailer "may have failed to employ reasonable and appropriate security measures to protect sensitive personal information." If that is the case, then Home Depot "denied customers the protection that they rightly expect when a business collects such information," which would open the door for the FTC to exert its authority. To read more click **HERE**

Microsoft addresses 42 bugs in four bulletins on Patch Tuesday

SC Magazine, 9 Sep 2014: On Patch Tuesday, Microsoft addressed 42 vulnerabilities in four bulletins, one of which is deemed critical. Microsoft released four bulletins addressing 42 vulnerabilities for its Patch Tuesday release. Bulletin MS14-052 is the only one deemed critical and addresses 37 vulnerabilities in Internet Explorer that can enable remote code execution, one of which – CVE-2013-7331 – is being used in attacks, according to the Microsoft Security Bulletin Summary for September 2014. In a statement emailed to SCMagazine.com, Tyler Reguly, manager of security research with Tripwire, said that CVE-2013-7331 is a "known Internet Explorer information disclosure vulnerability that allows attackers to detect the installation of EMET or AV products. Given that there are known attacks in wild, patching is definitely the right thing to do and should ease some worries if someone in your enterprise encounters an exploit kit while surfing the net." Bulletin MS14-053 is deemed important and addresses a vulnerability in .NET Framework that enables denial-of-service if an attacker sends a small number of specially crafted requests to an affected .NET-enabled website, the bulletin summary indicates. Wolfgang Kandek, CTO of Qualys, wrote in a Tuesday post that the bulletin "should be treated as 'Critical' if you have ASP.NET framework installed with your IIS webserver. If left unpatched, remote un-authenticated attackers can send HTTP/HTTPS request to cause resource exhaustion, which will ultimately lead to denial-of-service condition on the ASP.NET webserver." Bulletin MS14-054 is deemed important and addresses a vulnerability in Windows Task Scheduler that could enable elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application, according to the bulletin summary, which

explains that the attacker must have valid logon credentials and be able to log on locally. Finally, bulletin MS14-055 is deemed important and addresses three vulnerabilities in Microsoft Lync Server that could enable denial-of-service if an attacker sends a specially crafted request to a Lync server, the bulletin summary indicates. The bulletin "fixes an issue in Lync server which provides infrastructure for instant messaging, VoIP, audio, video and web conferencing," Kandek wrote. "If left unpatched, remote unauthenticated attackers can send a malicious SIP request which will cause a denial-of-service condition on the Lync server." To read more click **HERE**

Survey: Majority of government CIOs say they don't have sufficient IT resources

Fierce Government IT, 8 Sep 2014: A recent survey found that 62 percent of government chief information officers said they don't have sufficient resources to do their jobs effectively. The revelation comes even as 60 percent of CIOs said they saw their budgets rise and 47 percent said their staffs grew over the past year, according to the survey from Consero Group, which organizes invitation-only conferences for senior-level executives across different sectors. The firm, which surveyed 47 respondents, hosted the event of federal, state and local CIOs in July and released its findings Sept. 8. In a recent survey on Federal IT Reform, Senior government IT executives laid out their vision for the coming year, detailing challenges and identifying priorities. "While there have been some budget and staff increases, which is a positive sign, government chief information officers still face resource constraints in their efforts to create long-term value," the survey said. However, the survey also found that 50 percent of CIOs said their IT infrastructure is enough to serve their constituents, a decrease from what the firm found in a 2013 survey. Still, on a broader level, 43 percent said their government's current technology infrastructure was only adequate, while 26 percent said outdated infrastructure was the biggest barrier to their agency's progress. Additionally, while only 9 percent said they experienced a data breach within the preceding 12 months, 53 percent said they felt their IT infrastructure isn't prepared for cyber attacks. "Given the potential consequences of a data breach at the government level, CIOs may want to fight more aggressively for the resources they need in order to protect their IT infrastructure against any potential cyber threats," Paul Mandell, who's Consero's founder and CEO, said in a press release. Overwhelmingly, 70 percent of CIOs -- up from 31 percent last year -- said increasing service delivery through technology has been their department's primary focus this year, while only 15 percent said they would work within their budgetary constraints. And 17 percent said cloud computing is their biggest current priority and nearly half said that will also be their biggest area of exploration down the road. Mobility and bring-your-own-device policy, desktop and/or application virtualization, and data center consolidation were tied for second for current top priorities. To read more click **HERE**

Congress turning up the screws on Healthcare.gov website breach

Fierce Government IT, 8 Sep 2014: With the revelation that the Healthcare.gov website was hacked into last week, congressional lawmakers said they're taking a closer look at what happened as well as stepping up scrutiny on cybersecurity. Rep. Darrell Issa (R-Calif.), who chairs the House Oversight and Government Reform Committee, said he will hold a hearing in mid-September regarding the Healthcare.gov website breach with Centers for Medicare and Medicaid Services Administrator Marilyn Tavenner as the main witness. "For nearly a year, the administration has dismissed concerns about the security of healthcare.gov, even as it obstructed congressional oversight of the issue," Issa, a frequent critic of the Obama administration, said in a statement last week. "The committee will continue to push for answers from the administration and Administrator Tavenner must testify on the subject of transparency, accountability, and information security alongside the Government Accountability Office at our September 18th hearing." CMS personnel found malicious files designed to launch a "denial of service" attack against other websites were uploaded on the website's test server after they noticed on Aug. 25 an anomaly through system security logs. Top HHS leaders and security officials as well as the Homeland Security Department and FBI were then notified. "Our review indicates that the server did not contain consumer personal information; data was not transmitted outside the agency, and the website was not specifically targeted. We have taken measures to further strengthen security," an HHS spokesman said in

an emailed statement. The department said it's doing a comprehensive review of security improvements and upgrades. "This report of a cyber breach on the Healthcare.gov test server is deeply troubling and underscores the scary reality of how much of a target our sensitive information has become in cyberspace," said Sen. Tom Carper (D-Del.) in a Sept. 4 statement. To read more click **HERE**