THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

26 June 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

June 25, Dark Reading – (International) **PayPal two-factor authentication broken.** PayPal disabled its two-factor authentication option for mobile users after Duo Security researchers confirmed an independent researcher's findings showing that it was possible to bypass the feature. The vulnerability exists in a PayPal API and affects mobile users but not PayPal's Web application. Source: http://www.darkreading.com/mobile/paypal-two-factor-authentication-broken/d/d-id/1278840

June 25, Softpedia – (International) **GameOver trojan is still in the game.** Researchers with Arbor Networks reported that a Citadel campaign that evaded takedown attempts has been retrofitted with the GameOver trojan in order to continue its bank fraud operations as well as to distribute the CryptoLocker ransomware. Source: http://news.softpedia.com/news/GameOver-Trojan-Is-Still-In-the-Game-448305.shtml

June 25, Softpedia – (International) **Cybercriminals lift over $680,000/500,000 EUR in one week.** Researchers with Kaspersky reported finding a command and control (C&C) server for a man-in-the-browser (MitB) campaign that targeted an undisclosed large European bank and stole around $680,000 within 1 week from customers' accounts. The C&C server was identified in January but the cybercriminals running it took it offline after 2 days, which prevented further analysis. Source: http://news.softpedia.com/news/Cybercriminals-Lift-Over-680-000-500-000-EUR-In-One-Week-448325.shtml

June 25, Reuters – (Montana) **Montana health record hackers compromise 1.3 million people.** The Montana Department of Public Health and Human Services reported June 24 that a May data security breach compromised about 1.3 million individuals' State health records including Social Security numbers when hackers gained access to the department's computer server. Officials continue to investigate the incident and the full extent of damage. Source: http://news.msn.com/science-technology/montana-health-record-hackers-compromise-13-million-people

June 24, Long Island Newsday – (New York) **Long Island radiology practice NRAD informs 97,000 patients of data breach.** Garden City-based Nassau Radiologic Group Medical Associates (NRAD) informed 97,000 patients that a former employee had unauthorized access to their personal information after learning the former radiologist accessed and acquired protected health and personal information from NRAD's billing system in April. Source: http://www.newsday.com/news/health/long-island-radiology-practice-nrad-informs-97-000-patients-of-data-breach-1.8553832

June 24, Securityweek – (International) **AskMen compromised to distribute financial malware: Report.** Researchers at Websense reported June 23 that the AskMen online magazine was compromised and used to redirect visitors to a malicious Web site hosting exploits for Java and Adobe Reader. Source: http://www.securityweek.com/askmen-compromised-distribute-financial-malware-report

June 23, WCBS 2 New York City – (New Jersey) **Orange High School student accused of hacking into computer system, changing grades.** Essex County prosecutors charged a 16-year-old Orange High School student with hacking into the New Jersey school's computer system to change grades and attendance records using a staff member's password. Source: http://newyork.cbslocal.com/2014/06/23/orange-high-school-student-accused-of-hacking-into-computer-system-changing-grades/

June 24, IDG News Service – (International) **Researchers expect large wave of rootkits targeting 64-bit systems.** McAfee released a report June 24 that found that the number of new rootkit samples in the first quarter of 2014 increased to the highest levels seen since 2011, with more rootkits designed for 64-bit operating systems expected in the future. Source: http://www.networkworld.com/article/2367401/researchers-expect-large-wave-of-rootkits-targeting-64bit-systems.html

Passwords Stored in Plain Text during OkCupid Breach, Investigation Reveals
SoftPedia, 26 Jun 2014: The investigation of last year's OkCupid security incident is over and the findings showed that there were no encryption mechanisms in place to protect the sensitive information of the 254,000 users whose info was stolen. The Australian Privacy Commissioner, Timothy Pilgrim, concluded that Cupid Media, the company administrating the OkCupid dating site, did not comply with the Privacy Act 1988 that compelled it to secure the personal information stored on its systems. Back in January 2013, the administrators at Cupid Media took notice that a hacker had attempted to gain access to a table in its databases. The immediate response actions included patching the exploited vulnerability to prevent future unauthorized access. When the company determined that the vulnerability had been in ColdFusion, it obtained the patch and applied it immediately to all its servers. An external ColdFusion security contractor was also engaged in making sure that the security flaw had been fixed and that the respective ColdFusion installation complied with the best practice standards. The information the hacker stole included full name, date of birth, email addresses, and passwords. This would allow an attacker to find more details about the victim, like racial or ethnic origin, religious beliefs or affiliations, or sexual preferences or practices. "Personal information includes 'sensitive information.' The Privacy Act's definition of 'sensitive information' prior to 12 March 2014 included information or an opinion about an individual's racial or ethnic origin religious beliefs or affiliations or sexual preferences or practices," says the report. Cupid Media runs a total of 35 dating websites that are categorized "African dating," "Asian dating," "Latin dating," "gay and lesbian dating," "special interest," and "religion." At that time, the password protection measures in effect consisted of an account lockout policy and enforcement of strong password policies on all servers. However, none of the passwords benefited from encryption and all were available in plain text. Hashing and salting sensitive information such as passwords is an effective measure to secure storage of the data and mitigating the risk for users in case of a security breach. The report says that the actions taken by CupidMedia to contain the data breach included notification of the affected users that the password had been reset and analysis of the server logs to determine the hack method used by the attacker. As a security measure, the Commissioner advises users of dating sites to update privacy settings and change passwords on a regular basis, as well as to be careful about the personal information they share so as to avoid becoming victim of identity theft or online scams. To read more click **HERE**

Steam Phishing Attacks Use Typosquatting and Trojan to Bypass 2FA
SoftPedia, 26 Jun 2014: The Steam gaming community is a constant target for phishing, and new attacks are perpetrated through the chat client, giving the fraudsters the possibility to focus on accounts with valuable items. Active gamers with trusted accounts are in the cross-hair because these allow trading of the items immediately. According to Steam Trading support page, "any account that has made any valid purchase from the Steam Store more than 30 days ago is considered trusted." Paul Mutton of Netcraft says that the victims are contacted on the chat and offered to access a link to a profile with virtual items that can be exchanged. The profile is actually fake, but it looks like a legitimate one. To

reduce the risk of detecting the deceit by looking at the profile URL, the fraudsters appeal to typosquatting, a method that relies on using an address similar to the original but with a letter changed in the domain name, making the fraud more difficult to recognize at first glance. Trading virtual Steam items can be done with friends, so the victim has to add the fake profile to the list of friends. This is when the victim is asked for their Steam login credentials, which are automatically sent to the crook. However, the security measures imposed by Steam require two-factor authentication (2FA), a feature that is automatically enabled for users with verified email addresses. One way to bypass 2FA is to use a "ssfn" file that acts as an authentication key and is available in the Steam folder. Simply asking the user to upload it would raise suspicions, so the attacker resorts to another deceit that consists in downloading an executable named SteamGuard.exe. In fact, this is a piece of malware designed to search for the "ssfn" file and send it to the fraudster by uploading it to a hardcoded address. The pop-up serving the malware also looks as if created by the Steam developers and covers the trickery by informing the user that it is an added security measure required to grant access to the account. Login credential in hand and the two-factor authentication bypassed, the fraudster has free access to the victim's account and the coveted virtual items. Albrecht Neumann, a mathematics student in Germany, told Netcraft that keys and earbuds are relatively stable currency on the Steam market, and some gamers accumulate this sort of goods, increasing the value of their accounts to thousands of dollars. To read more click HERE

1.3 Million Records Exposed in Data Breach

SoftPedia, 26 Jun 2014: Hackers accessed a server of the Department of Public Health and Human Services (DPHHS) in Montana, U.S., and reached sensitive information of 1.3 million individuals. The details that were accessed without authorization include names, addresses, dates of birth, and Social Security numbers. Information about clients may be related to health assessments, diagnoses, treatment, health condition, prescriptions, and insurance. Also, it seems that details about the DPHHS services that clients applied for or received were present on the affected machine, too. The breach was discovered on May 22, a week after the public health department ordered a forensic investigation because signs of suspicious activity had been detected. In the case of contractors and current and former employees, it is possible that the data on the server included names, addresses, dates of birth, Social Security numbers, bank account information and dates of service. The immediate response of the DPHHS officials was to shut down the server and contact the law enforcement. At the moment, there is no clear information on the exact records that have been accessed as a result of the incident, and the DPHHS Director, Richard Opper, says that "out of an abundance of caution, we are notifying those whose personal information could have been on the server." According to a news release, the activity of the DPHHS services has not been affected in any way thanks to the backup systems that have created a safe copy of the data. State of Montana officials say that all parties that could be affected will be notified about the breach and they will be offered free credit monitoring and identity protection insurance. They are to receive an official letter explaining the nature of the incident and the instructions for contacting the recommended services if fraudulent credit activities are detected. "I encourage Montanans who are notified to sign up for the free credit monitoring and insurance that is being provided," Opper said. State of Montana Chief Information Officer Ron Baldwin says that the state changed the property insurance last year, so now it covers cyber security incidents of this nature. The policy covers the costs for toll-free Help Line, mailing notification letters, free credit monitoring and other services up to $2 million/1,465 million EUR. In the wake of the incident, the security of the DPHHS server system has been upgraded for better protection of the sensitive details. A similar incident affected NRAD systems, the culprit being identified as a company employee, who accessed without authorization the files of 97,000 patients, containing personally identifying information, including social security numbers. To read more click HERE

Hospital Networks Are Leaking Data, Leaving Critical Devices Vulnerable

Wired, 25 Jun 2014: Two researchers examining the security of hospital networks have found many of them leak valuable information to the internet, leaving critical systems and equipment vulnerable to hacking. The data, which in some cases enumerates every computer and device on a hospital's internal network, would allow hackers to easily locate and map systems to conduct targeted attacks. In at least one case, a large health care organization was spilling info about 68,000 systems connected to its network. At this and every other facility that was leaking data, the problem was an internet-connected computer that was not configured securely. Quite often, the researchers found, these systems also were using unpatched versions of Windows XP still vulnerable to an exploit used by the Conficker worm six years ago. "Now we know all the targeted info and we know that systems that are publicly connected to the internet are vulnerable to the exploit," says Scott Erven, one of the researchers, who plans to discuss their findings today at the Shakacon conference in Hawaii. "We can exploit them with no user interaction… [then] pivot directly at the medical devices that you want to attack." Attackers could, for example, infect one of these systems and use it as a launchpad to find and hack the control system that manages embedded pacemakers. Such systems, Erven says, generally require no authentication to administer test shocks to patients or to configure thresholds that determine when a shock is automatically administered. An attacker could therefore alter the settings that determine when a patient is going into cardiac arrest in order to administer shocks when they aren't needed or prevent life-saving shocks from occurring. The data leak is the result of network administrators enabling Server Message Block, or SMB, on computers facing the internet and configuring it in such a way that allows data to broadcast externally. SMB is a protocol commonly used by administrators to help quickly identify, locate and communicate with computers and equipment connected to an internal network. With SMB, each system is assigned an ID number or other descriptor to help distinguish, say, the PC in a doctor's office from surgical systems an operating room or testing equipment in a lab. This kind of information should only be available to network staff. But the researchers found many hospitals had misconfigured the SMB service, allowing outsiders to see it as well. "It goes to show that health care [organizations are] very sloppy in configuring their external edge networks and are not really taking security seriously," Erven says. The vulnerability was uncovered by Erven and Shawn Merdinger, an independent health care security researcher and consultant, expanding on work Erven has done identifying vulnerabilities in medical devices and hospital equipment. Erven is head of information security for Essentia Health, which operates about 100 facilities––including clinics, hospitals and pharmacies––in four states. He and his staff recently completed a two-year investigation into the security of all of Essentia's medical equipment. Among other problems, they found drug infusion pumps—for delivering morphine drips, chemotherapy and antibiotics—that could be remotely manipulated to change dosages delivered to patients; Bluetooth-enabled defibrillators that could be manipulated to deliver random shocks to a patient's heart or prevent a medically needed shock from occurring; and temperature settings on refrigerators storing blood and drugs that could be reset to cause spoilage. At the time Erven's team conducted their research, they didn't know how many vulnerable medical devices were directly connected to the internet as opposed to simply being connected to internal networks accessible via the internet. Erven and Merdinger set out to scan the internet to answer this question. They scanned for any systems using port 445—the port the SMB protocol uses to transmit data—and filtered for hospitals and other health care organizations while using keywords like "anesthesia" and "defibrillator." Within half an hour, they discovered a health care organization that was leaking information on 68,000 systems. The organization, which Erven would not identify, has more than 12,000 employees, 3,000 physicians and large cardiovascular and neuroscience institutions associated with it. Among the systems with exposed data, the researchers easily identified at least 32 pacemaker systems in the organization, 21 anesthesiology systems, 488 cardiology systems, and 323 PACS systems—radiology systems for reading X-Rays and other images. They also identified telemetry systems, high-risk systems that are often used in infant-abduction prevention systems as well as for monitoring the movement of elderly patients throughout a hospital to ensure they don't wander off. The problem went beyond this one organization. Because the health care organization's network was connected to third-party networks, data from those networks was exposed as well. Hospital networks often are connected to those of other

providers, pharmacies and laboratories. Systems belonging to these other organizations can also be exposed to SMB data leaks if the hospital doesn't configure its own systems properly. Although this organization was the largest one they identified with problems, they soon found others. "We started running organization searches to identify hospitals, clinics, and other medical facilities and we quickly realized this is a global health care organization issue," Erven says. "This is thousands of organizations [that are leaking this information] across the world." Most hacks involve multiple stages of reconnaissance and varying levels of penetration to reach critical systems and identify vulnerabilities. But in this case, the SMB data would allow an attacker to home in on vulnerable machines quickly instead of having to scan a hospital's entire network, searching for something interesting—an activity that runs the risk of getting them noticed. On some of the networks that were leaking data, the system administrators had assigned names to the systems on their network—such as "Dr. Armstrong's office," or "cardiology defibrillator in OR1? making it even easier for hackers to identify specific systems for attack. Armed with this information, as well as the research Erven had previously done to identify vulnerable hospital equipment, an attacker could craft a custom payload to target a specific brand of defibrillators or oncology equipment and send it to a hospital worker via a phishing email. The payload could then seek out the equipment on the network—using the SMB data—and execute its attack only on these specific devices. The attack could even be conducted to target a specific patient. "The doctor's name doesn't necessarily help an attacker," Erven says. "But when you know that this patient has an appointment with this doctor and I know this doctor uses this system, you could build a case for a major targeted attack and have more certainty of where you want to target." Erven says the SMB problem is just one security issue that health care organizations are facing. He says the problems exist because the security teams at these organizations are too often focused solely on HIPAA compliance—checking off boxes to meet government regulations for protecting data—while failing to conduct penetration testing and vulnerability maintenance to really test their systems and secure them the way the security teams at banks and other financial organizations do. To read more click **HERE**