THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

10 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 6, WPMT 43 York – (Pennsylvania) **Hershey Medical Center notifies patients of potential health information breach.** Pennsylvania State University's Milton S. Hershey Medical Center is notifying 1,801 patients that their health information may have been accessed after an employee entered protected health information at home on a personal device outside the secured network. An investigation determined that the employee did not misuse the information, which consisted of material related to a test ordered by the medical center's women's health or family medicine clinicians between August 2013 and March 2014. Source: http://fox43.com/2014/06/06/hershey-medical-center-notifies-patients-of-potential-health-information-breach

June 9, Bloomberg News – (International) **Cybercrime remains growth industry with $445 billion lost.** A McAfee and Center for Strategic and International Studies (CSIS) report estimated that various forms of cybercrime globally caused losses of $445 billion a year to various industries, including financial institutions, energy companies, and retailers. The report pointed to stolen trade secrets and intellectual property as the largest source of losses to legitimate companies, as well as the potential for market manipulation and insider trading, among other findings. Source: http://www.bloomberg.com/news/2014-06-09/cybercrime-remains-growth-industry-with-445-billion-lost.html

June 6, Threatpost – (International) **Debian urging users patch Linux kernel flaw.** Debian published a security update June 5 that closes several vulnerabilities in the Linux kernel that could allow attackers to perform privilege escalation or denial of service (DoS) attacks. Users were advised to apply the patch as soon as possible. Source: http://threatpost.com/debian-urging-users-patch-linux-kernel-flaw

June 6, The Register – (International) **Redmond is patching Windows 8 but NOT Windows 7, say security bods.** Two security researchers created a tool known as DiffRay which scans Windows libraries and found that several security functions were updated by Microsoft in Windows 8 but not in Windows 7. The researchers warned that the differences in patching could lead to the discovery of zero day vulnerabilities. Source: http://www.theregister.co.uk/2014/06/06/patch_piker_redmond_means_win_8_fixes_skip_7_researchers_say/

June 6, Dark Reading – (International) **TweetDeck scammers steal Twitter IDs via OAuth.** Researchers at Bitdefender found that scammers are luring users into authorizing TweetDeck as part of a free or paid followers scheme, allowing the scammers to obtain users' authentication tokens. The scammers can then take actions on behalf of users, such as posting tweets and following other users. Source: http://www.darkreading.com/attacks-breaches/tweetdeck-scammers-steal-twitter-ids-via-oauth/d/d-id/1269503

Ransom-taking iPhone hackers busted by Russian authorities
Naked Security, 10 Jun 2014: The mystery of the ransom messages from "Oleg Pliss," and the iDevice locking attack that popped up in Australia and the US last month, appears to have been solved. Authorities in Russia said they detained two criminals behind ransom attacks on Apple users that locked their devices remotely and demanded payment to unlock them. I say "seems to have been solved" because Russian

police said the hackers were responsible for the same scam on users in Russia, without mentioning victims in other countries. The two Russian hackers - a 23-year-old and a 17-year-old from Moscow - reportedly confessed to scamming users into giving away their Apple IDs and using the Find My iPhone feature to lock the devices until the victims paid a ransom of up to $100 USD. According to The Sydney Morning Herald, Russian media reported the pair of hackers were caught on CCTV when they withdrew victims' payments from an ATM. Russia's Ministry of Internal Affairs stated on its website that agents searched the hackers' apartments and seized computers, phones, SIM cards and "literature" on hacking. Russian authorities said the hackers used "two well-known schemes" to perpetrate their attacks, which affected Apple users in Russia. It seems the two hackers tricked Apple users into giving away their Apple IDs with a phishing scam that asked them to sign up for an online video service that required their Apple IDs. If a hacker gets hold of your Apple ID they can create an iCloud account which they can then use then lock your iPhone, iPad, iPod or iMac device remotely. The Sydney Morning Herald reports that victims who locked their phones with passcodes could simply enter it, change their iCloud password and avoid having to pay a ransom. Users who didn't set passcodes were less fortunate and had to resort to wiping their devices and restoring them from backups. If you've been hacked by 'Oleg Pliss' then we recommend you follow the advice in our earlier article Apple ransomware strikes Australia. In the security industry we call cyber attacks that take over your computer and demand payment "ransomware". The most famous ransomware is the notorious CryptoLocker, which authorities recently knocked out by taking over the cybercriminals' command and control servers. Only recently, however, have crooks figured out how to turn the success of ransomware for PCs into a lucrative racket on mobile devices. Technically, since the "Oleg Pliss" hackers didn't drop any malware onto the devices of their victims, the iDevice-locking attack isn't a real example of ransomware, but it has the same devious purpose - to extort victims for money. It's a much different story for Android, which is more susceptible to mobile malware. A file-encrypting ransomware for Android called Simplelocker was recently discovered, and another kind of ransomware known as a "police locker" has hit Android users who download an infected file claiming to be a video player. Securing iDevices and Androids As a security precaution, you should make sure you lock your phone with a secure passcode. Your Apple ID is the key to your iDevices, so make sure you hold onto it tight (don't use your Apple ID for a suspicious media-download website, for example). You should also make sure your iDevices are up to date with the latest iOS software version to stay safe from known exploits. To read more click **HERE**

Patch Tuesday for June 2014 - 7 bulletins, 3 RCEs, 2 critical, and 1 funky sort of hole

Naked Security, 8 Jun 2014: The elevator pitch for this month's Microsoft Patch Tuesday is as follows:

- Seven bulletins.
- Three remote code execution (RCE) holes, of which two are deemed Critical.
- Patches apply to Windows, Internet Explorer (IE), Office, Live Meeting and Lync.
- All supported versions of IE get patches.
- All Windows versions, including Server Core and RT, get at least one Critical RCE patch.
- All patched systems need a reboot.

Even more briefly: you'll need to patch and reboot every Windows system on your network. OK, except for your Windows XP computers. But why not reboot them all in solidarity, anyway? Some of them might not come back up, and then you'll have an excuse to tell your boss that you can't put off updating them anymore. One of the patches, number seven, is a security hole of a type you don't see announced very often in Microsoft bulletins: Tampering. You're probably used to seeing vulnerability tags like RCE (remote code execution), EoP (elevation of privilege, where a regular user can get unauthorized administrative or system powers), DoS (denial of service, where an outsider can crash software that you rely on), and Information Disclosure (where data that should stay private can be accessed without authorization). If you've listened to our Understanding Vulnerabilities podcast, you'll know that RCE bugs usually get the most attention, because they offer a break-and-enter path to attackers who are outside your network. But

the other sorts of vulnerability can be combined with RCE into a much more dangerous cocktail. For example, a Disclosure bug might allow crooks to steal authentication data that makes it much easier for them to pull off an RCE; a cunningly timed DoS might knock out intrusion detection software that would otherwise trigger an alert; and an EoP might add system administrator powers to a user-level compromise. → Here's an analogy: a Disclosure bug tells a crook where you live and when you won't be home; the RCE lets him pick your front door lock and get inside; the DoS means he knows how to turn off your burglar alarm; and the EoP gets him into your safe as well, once he's in the house. Tampering is another sort of security hole that may help crooks, either by allowing them to initiate their attack more easily, or by making things worse for you once they have broken in. Very loosely, tampering means that you can make a security-related change that should raise an alarm, but doesn't. For example, you might be able to add malware to someone else's digitally signed software and have the system still accept it as trusted. You might be able to make your own digital certificate, for example for a fake web page, but pass it off as someone else's. Or you might be able to tamper with a protected configuration file, thus altering the settings and behavior of software such as a web server, without being noticed. One well-known example of a tampering exploit is last year's MasterKey malware for Android, which bypassed Google's Android Package (APK) cryptographic verifier, making the malware look legitimate. This didn't just allow the malware to get the blessing of Google's compulsory install-time security check, but also allowed the crooks to put the blame on a innocent vendor, whose digitally signed package they started with. Another famous tampering exploit is the announcement by security researchers in 2008 that they had succeeded in creating a fake Certification Authority web certificate by finding a collision in the MD5 hashing algorithm. Their home-made certificate appeared to have been signed by one of the top-level "root authorities" that almost every browser trusts by default, and would have allowed them to sign apparently-trusted certificates for any website they liked. We can't yet say exactly what form this latest Windows tampering vulnerability takes, but it affects Windows 7; 8 and 8.1; Server 2008 R2 (not Itanium, and not Server Core); and all supported flavors of Server 2012, including Server Core. The final item of interest about the June 2014 Patch Tuesday is that the update to IE fixes a security hole known as CVE-2014-1770. Technically, this became a zero-day in IE 8 when it was disclosed by HP's Zero Day Initiative during May 2014, after Microsoft hadn't managed to come up with a fix for six months. (More precisely, after 180 days.) The discoverer of the bug, who sold it to HP for an undisclosed sum, was careful to point out that all that was published last month was an advisory, not a proof of concept; indeed, he said that "it won't be easy reproduce the vulnerability based on the advisory alone." Even after you have uncovered a vulnerability, there is almost always a lot of work (and sometimes it proves as good as impossible) to weaponize the vulnerability by actually coming up with a way to exploit it. According to Microsoft, writing on its Security Response Center blog, no in-the-wild exploit using CVE-2014-1770 was ever seen, and thankfully the issue becomes moot on 10 June 2014, when the latest IE patches come out. To read more click **HERE**

Retail breaches and the SQL injection threat

Heise Security, 10 Jun 2014: Continuous monitoring of database networks is the best approach to avoid breaches such as the high-profile attacks against major U.S. retailers, according to a Ponemon Institute and DB Networks study. More than half (57 percent) of respondents believed that the attacks against the U.S. retailers involved SQL injection as one of the components of the attacks. The research was conducted to gain a deeper insight into the recent U.S. retailers breaches, including to better understand why these retailers were so vulnerable, what security countermeasures could have been employed, and who was likely responsible for the attacks. The study analyzed responses from 595 IT security experts in the United States working across a broad spectrum of industries and also the public sector. Study respondents are very familiar with the security compliance requirements for retailers who accept payment cards, and 69 percent of the respondents indicated their organization must comply with PCI DSS. Additional key findings of the study include:

- Fifty-three percent of respondents in total indicated that breach notification should occur within a month
- Initial reports were that a Russian teenager was the perpetrator of the Target breach, however half the respondents felt that it was actually the work of a cyber-criminal syndicate. Only 15 percent responded that a lone wolf hacker was the likely culprit, while 11 percent responded that nation-state actors were likely responsible.
- While most respondents believed that the attacks against the retailer's databases involved SQL injection, almost half of the respondents said the SQL injection threat also facing their own organization is very significant.
- Nearly two-thirds of respondents (64 percent) felt that their organization presently does not have the technology or tools to quickly detect SQL injection database attacks.
- Only one-third of respondents either scan continuously or daily for active databases. However, 25 percent reported they scan irregularly and 22 percent do not scan at all.
- Only 48 percent of respondents indicated that they test or validate third party software to ensure it's not vulnerable to SQL injection.
- Forty-four percent utilize professional penetration testers to identify vulnerabilities in their IT systems; but 65 percent of those penetration tests do not include testing for SQL injection vulnerabilities.

To read more click HERE

Adobe Flash Player 14.0.0.125 Released

SoftPedia, 10 Jun 2014: Adobe has just rolled out a brand new version of the Flash Player software that comes to address many of the security issues and bugs found in the previous builds. At this point, Adobe hasn't provided any specifics regarding this update, but it's safe to assume that this particular build is specifically focused on fixing the bugs that existed in older releases, so everyone using Flash Player should update as soon as possible. Adobe Flash Player 14.0.0.125 is obviously available on all supported platforms, including Windows, Mac OS X, and Linux, and brings basically the same pack of improvements on all of them. Adobe decided in November 2012 to synchronize its Flash Player updates with Microsoft's Patch Tuesday rollout, thus promising to work with the Redmond-based company on improving its software and also fixing the application that's now implemented in Internet Explorer by default. As a result, Microsoft is delivering Flash Player updates for Internet Explorer users via Windows Update, so users of this particular browser will get the same fixes later today via the official update channel. "The alignment of the release cycle to Patch Tuesdays will make updates more predictable for customers, in particular for customers running the Flash Player bundled with Internet Explorer 10 on Windows 8," Adobe said in November 2012. Basically, Adobe's change of security rollouts also allowed Microsoft to deliver more frequent security updates for its own Internet Explorer browser, with the software giant promising to release new patches at least as often as the Flash Player owner. Microsoft thus said that Internet Explorer updates comprising Flash Player updates would be released "on a quarterly basis when Adobe normally issues Flash Player updates, we will coordinate on disclosure and release timing," but also when "the threat landscape requires action outside of Adobe's normal update cadence, we will also work to align our release schedules. For example, this may mean that in some cases we will issue updates outside of our regular monthly security bulletin release." To read more click HERE

Notorious Hacker Who Leaked George Bush's Self-Portraits Sentenced To 4 Years in Prison

The Guardian, 10 Jun 2014: A Romanian court has sentenced the hacker known as Guccifer, famed for posting nude self-portraits of former U.S. President George W. Bush on the internet, to four years in jail on Friday. Marcel Lazar Lehel, 42, a former cab driver in Arad near the Romanian border with Hungary, was better known by his aliases Guccifer and Small Fume, which he used while hacking into various high-profile people's email accounts. Victims also included Jeremy Paxman, three members of the House of Lords and the head of the Romanian secret service. Guccifer was arrested by agents from Romania's

Directorate for Investigating Organized Crime and Terrorism in January this year, but shot to fame in 2013 when he hacked into Bush's AOL email account and those of his family. The hacker stole private photos, artwork, and correspondence, including self-portraits depicting Bush in the shower and bath and photos of George H.W. Bush in hospital, which he posted online. Lehel gained access to a confidential list of home addresses, phone numbers, and emails of dozens of members of the Bush family, including both former U.S. presidents and their children. The hacker also leaked personal emails sent between the former U.S. Secretary of State Colin Powell and the Romanian European parliament member Corina Cretu — prompting Powell to deny allegations of an affair in 2013. Guccifer also hacked into the private Yahoo email account of George Maior, head of Romania's secret service, which the agency said had been used in the past for academic correspondence, not secret-service business. The long list of Guccifer's high-profile victims allegedly covered entertainers, industrialists, academics, diplomats, financiers, government and military officials, and journalists, including Obama administration officials, three members of the House of Lords, and Jeremy Paxman, according to documents sent to news site the Smoking Gun. Lehel employed several methods to break into the email but found success simply guessing answers to security questions using publicly available information, including Wikipedia, to gain access to online accounts with Facebook, BT Internet, AOl, Yahoo, and others. Guccifer's simple attacks display the importance of securing private information and ensuring that personal data linked to security and password reset questions is not publicly available following several high-profile break-ins where personal data was stolen including eBay and Office shoes. Lehel was also convicted of hacking into the email accounts of Romanian public figures in 2012 but was given a three-year suspended sentence. The court ordered the defendant to pay 11000 Romanian Leu (£2,020) in legal costs to the state and confiscated a silver NEC laptop owned by the Lehel. The FBI and other U.S. law enforcement agencies have reportedly been investigating Lehel since 2013, but the Romanian court did not publish any details of Lehel's actions or whether the U.S. had sort extradition. To read more click **HERE**

NIST Updating Mobile Forensics Guidance

GovInfoSecurity, 10 Jun 2014: Apple unveiled the iPhone in June 2007, a month after the National Institute of Standards and Technology issued "Guidelines on Cell Phone Forensics." Seven years later, NIST is revising its guidance and giving it a new moniker, "Guidelines on Mobile Device Forensics" (**link**). The latest version of the guide is known as the second draft of Special Publication 800-101 Revision 1. The final version of Revision 1 should be published later this year. The revised guidance has two objectives, says Rick Ayers, who co-authored the 2007 and 2014 versions of the guidance: To help organizations develop appropriate policies and procedures for dealing with mobile devices and to prepare forensic specialists to conduct forensically sound examinations. "The technology has changed so much within the past seven years; it was time to update the document to best meet the needs of mobile forensic examiners," Ayers says. "The older document, while technically correct, did not cover many of the more recent technologies in use today." Ayers identified the recent technologies to include micro SIM cards and flasher box extraction methods. Forensic experts use flasher box devices to recover user data from dead or faulty mobile phones. Since 2007, changes have occurred in mobile device memory, identity modules and cellular network technology. In addition, mobile device tool classification systems, methods for handling obstructed devices and certain data preservation techniques didn't exist seven years ago. Back then, about a dozen tools existed to help forensic experts recover and investigate data on cell phones. Today, the marketplace offers hundreds of tools, many designed for specific models of specific mobile devices. "In the past, there were enough tools that you could hold them in your hands and say, 'I'm the master of all the mobile forensic tools,'" says guidance co-author Sam Brothers, a digital forensic specialist at U.S. Customs and Border Protection, part of the Department of Homeland Security. "We laugh at that now. But we've come to a point where that's virtually impossible. You have at least 100 different tools that are out there. For someone to try to know all of them would be very difficult." The revised guidance provides on-site triage processing, illustrated with a flow chart outlining common situations encountered by forensic examiners. "There are so many different kinds of phones that are being used to support so many different kinds of cases in so many different kinds of situations," says Barbara Guttman,

NIST software quality group manager. The new guidance also furnishes updated acquisition and preservation techniques for handling current mobile devices. "The publication is not intended to be used as a step-by-step guide for executing a proper forensic investigation when dealing with mobile devices nor construed as legal advice," Ayers says. "Its purpose is to inform readers of the various technologies involved and potential ways to approach them from a forensic perspective." The draft publication discusses procedures for the preservation, acquisition, examination, analysis and reporting of digital evidence. The publication also addresses the ever increasing backlogs for most digital forensics labs and provides guidance on handling on-site triage casework. To read more click **HERE**