The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

2 January 2014

Purpose
Educate recipients of cyber events to aid in the protection of electronically stored corporate proprietary, DoD and/or Personally Identifiable Information from theft, compromise, espionage, and / or insider threat

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, Sandia 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 open source data

December 31, Miami Herald – (Florida) **Barry University notifies patients their records may have been hacked.** Barry University in Florida notified patients of its Foot and Ankle Institute December 30 that their medical records and personal information may have been hacked after a security breach was detected May 14 on a school-owned laptop. The university has since removed the infection from their network after discovering the malware on the laptop. Source: http://www.miamiherald.com/2013/12/31/3845178/barry-university-to-notify-patients.html

December 31, BBC News – (International) **Hackers knock League of Legends offline.** A hacktivist group claimed responsibility for using distributed denial of service (DDoS) attacks against servers belonging to popular online game League of Legends, bringing the game service down for several hours December 31. The group also caused interruptions on other gaming services and leaked a specific user's personal information, which led to a false report that summoned armed police to the user's home. Source: http://www.bbc.co.uk/news/technology-25559048

December 30, Softpedia – (International) **4 vulnerabilities fixed in MyBB 1.6.12.** The developers of MyBB released the latest version of the software which closes 4 vulnerabilities and 10 functionality issues. Source: http://news.softpedia.com/news/4-Vulnerabilities-Fixed-in-MyBB-1-6-12-412842.shtml

December 30, Threatpost – (International) **OpenSSL website defaced; code repositories untouched.** OpenSSL confirmed December 29 that a hacktivist group that defaced the organization's Web site did not gain access to its source repositories. OpenSSL is continuing to investigate the incident. Source: http://threatpost.com/openssl-website-defaced-code-repositories-untouched/103341

1 Billion PCs at Risk As Windows Error Reporting Sends Reports in Clear Text
Forbes, 1 Jan 2014: This sounds like a remarkably alarming warning: as many as 1 billion networked PCs around the world are allegedly at risk because Windows Error Reporting (aka Dr. Watson) sends its report in the clear. And those reports do include machine type, OS, version of OS, which system packs have been installed and so on. All of the information that a hacker usually is interested in to see what tools, if any, he will need to be able to access the machine. The warning comes from Websense: "Websense® Security Labs™ recently processed a sample data set from the Websense ThreatSeeker® Intelligence Network to investigate the security risk from popular applications and services. We determined enterprise and public sector networks are inadvertently leaking information, which could be used by a threat actor as intelligence to craft specific attacks and compromise networks. One troubling thing we observed is Windows Error Reporting (a.k.a. Dr. Watson) predominantly sends out its crash logs in the clear. These error logs could ultimately allow eavesdroppers to map out vulnerable endpoints and gain a foothold within the network for more advanced penetration. Here's more on why that's a concern: 80 percent of all network-connected PCs use it – that's more than one billion endpoints worldwide Dr. Watson reports information that hackers commonly use to find and

exploit weak systems such as OS, service pack and update versions Crashes are especially useful for attackers since they may pinpoint a new exploitable code flaw for a zero-day attack Information is also sent for common system events like plugging in a USB device Now it is true that this information is hugely valuable to Microsoft and also to the rest of us. For it's what is used to try and make the operating system, Windows, work better over time and given the number of us that still use it that's a highly desirable outcome. However, there are a number of problems with it being sent in clear. For a start, anyone gaining access to that flow of information obviously has a great deal of information about where Windows is currently failing. That's a great start to finding the vulnerabilities and flaws that allow the design of exploits. It's not entirely simple to gain access to that error reporting traffic but it most certainly can be done with a variety of man in the middle methods. Or, more importantly, if, just as an example of something unlikely, a hacker had fibreoptic links into the backbone it could deliberately sniff for such traffic. And this would give it a lovely database of those machines that haven't been updating their service packs and thus have known vulnerabilities. It's a rather large and gaping hole that much of this traffic is moving unencrypted. Websense don't suggest not sending the reports of course: the improvements that come from the information are too valuable for that. However, they do suggest that computers on any network should be sending their reports to a local server, within the network, there to be encrypted before being sent off to Microsoft. To read more click **HERE**

Snapchat leak reveals phone numbers, usernames of 4.6 million users

BGR, 1 Jan 2014: Snapchat users beware: someone has posted the phone numbers and usernames of more than 4.6 million accounts on the site SnapchatDB, freely available as an SQL dump or CSV text file for anyone to download. The last two digits of each phone number have been censored "in order to minimize spam and abuse," but the owner of the database says that "under certain circumstances," the site might be willing to release the uncensored records. This giant leak comes just days after Gibson Security's latest interview in which the company warns of Snapchat's vulnerabilities. According to Gibson Security, the Snapchat team had taken far too long to address some very serious issues with the coding of the software, and had left the application wide open to exploits that could compromise user information. It has been less than a week since that interview, and now an entire database of phone numbers and usernames is just a click away. Although SnapchatDB claims that the database represents "a vast majority of the Snapchat users," The Verge points us in the direction of Reddit, where one user has determined that only 76 of 322 U.S. area codes appear on the list. "This information was acquired through the recently patched Snapchat exploit and is being shared with the public to raise awareness on the issue," says the owner of SnapchatDB. "The company was too reluctant at patching the exploit until they knew it was too late and companies that we trust with our information should be more careful when dealing with it." [Note: SnapchatDB.info has been suspended and is no longer available.] To read more click **HERE**

Syrian Electronic Army says hacked into Skype's social media accounts

Reuters, 1 Jan 2014: The Syrian Electronic Army, an amorphous hacker collective that supports Syrian President Bashar al-Assad, claimed credit on Wednesday for hacking into the social media accounts of Internet calling service Skype. The group also posted the contact information of Steve Ballmer, Microsoft Corp's retiring chief executive, on its Twitter account along with the message, "You can thank Microsoft for monitoring your accounts/emails using this details. #SEA". That message was an apparent reference to revelations last year by former National Security Agency contractor Edward Snowden that Skype, which is owned by Microsoft, was part of the NSA's program to monitor communications through some of the biggest U.S. Internet companies. A message posted on Skype's official Twitter feed on Wednesday, apparently by the hacking group, read: "Don't use Microsoft emails (hotmail, outlook), They are monitoring your accounts and selling the data to the governments. More details soon. #SEA". Similar messages were posted on Skype's official Facebook pages and on a blog on its website before being taken down in late afternoon. The SEA later tweeted out copies of the message "for those who missed it." Representatives for Microsoft could not be reached for comment. Media companies, including the New York Times and the BBC, have repeatedly been targeted by the Syrian Electronic Army and other hacker activist groups that deface websites and take over Twitter accounts. To read more click **HERE**

Cyber criminals to target mobile, social in 2014

RelaxNews, 31 Dec 2013: McAfee Labs predicts that the year ahead will bring increased malware attacks and other cyber risks aimed at smartphones, tablets and social media activity. The cyber-security firm's 2014 Predictions Report gives consumers an idea of the cyber risks they could be facing as the New Year approaches. In particular, McAfee Labs believes that 2014 will be the year of "mobile malware" as hackers and other cyber criminals start turning their backs on the desktop in favor of smartphones and tablets. McAfee claims that over the past six months it has seen a 33% increase in malware attacks focused on Android and the trend is expected to continue. The easiest way to stay protected is to only ever download valid apps and to use a form of anti-virus app. It is also worth considering deactivating a handset's NFC capabilities if it supports the technology and to avoid using public Wi-Fi for anything other than web browsing. McAfee also believes that social attacks will be ubiquitous by the end of 2014. Platforms such as Facebook are hugely appealing to cyber criminals because of the wealth of personal information they carry, plus the fact that a number of other services accept Social Media log-in details to sign in to their own offerings. Facebook already has some of the most robust security in place and offers its one billion users the option of two factor authentication. However, other sites, such as Twitter, have been slower to react to the need for increased online protection and are only now just catching up. "With target audiences so large, financing mechanisms so convenient, and cyber-talent so accessible, robust innovation in criminal technology and tactics will continue its surge forward in 2014," said Vincent Weafer, senior vice president of McAfee Labs. "The activity in mobile and social is representative of an increasing 'black hat' focus on the fastest growing and most digitally active consumer audiences, in which personal information is almost as attractive as banking passwords." To read more click **HERE**

Cybercrimes will use ransomware to target businesses: McAfee

Computerworld, Jan. 2, 2014: Cybercriminals will increasingly use ransomware, malware and hacktivism over the next year to move further into the lucrative business market. McAfee has released it 2014 A/NZ threat predictions (**PDF**) which highlights the trend towards ransomware and targeted attacks over the next 12 months. In 2014, it also expects to see an increase in the new complex types of attacks on business PCs and mobiles, but it is clear that traditional tactics which have been around for years will also continue to impact businesses. Michael Sentonas, Global CTO for Security Connected at McAfee said a key trend was that ransomware attacks, which usually target consumers, such as CryptoLocker, will move further into the business space where they have the potential to severely affect operations and cost companies a lot of money. "We also expect to see an increase in mobile malware, which effectively locks the user out of his or her device or machine so the cyber criminals can access data, to have an impact on businesses via their increasingly mobile workforces," he said. "Hacktivism attacks which usually target governments are anticipated to spill over into business and enterprise markets." Understanding cyber threats and areas of vulnerability in the year ahead is vitally important as more businesses move operations into the cloud and embrace mobile technologies, providing cyber criminals with more entry points into company networks and data. But Sentonas said, unfortunately, the poor cyber security foundations of many companies will continue to create an environment of high motivation, high opportunity for the attacker in 2014. "Businesses need to understand that lax cyber security could have significant implications on their company data, operations and financial viability." The Top ten threats for 2014 are predicted as:

1. Ransomware -- Expect ransomware samples to increase given the financial success the cyber criminals have had with this type of malicious software. Ransomware such as CryptoLocker has typically targeted consumers, but now also targets enterprises.
2. Mobile Malware -- The increasing volume and complexity of malware designed to capture identity and financial information will continue to crossover from desktops to mobile devices; a significant issue for an increasingly mobile workforce.

3. Destructive Malware -- Cyber attackers are leveraging more destructive functions within their attack code. Cyber criminals will continue to drive the unprecedented rise in destructive malware, some of which are designed to damage the victim's master boot record resulting in complete computer systems being rendered inoperable.
4. Hacktivism -- Hacktivist groups based in Singapore, Malaysia, Indonesia and Australia will continue to target governments in 2014 and are expected to also spill over and target private enterprise.
5. "Next Generation" security tools will come under attack -- Attackers will continue to develop exploits that will be 'sandbox aware' aiming to bypass security systems, demonstrating that sandboxing is a feature and not a complete security solution.
6. The Internet of Things comes alive -- All devices that connect to the corporate network and the internet should be considered endpoints that come with a level of risk as they typically have less security, both by design and through poor security practices, and will be a target for attackers.
7. Bypassing Digital Signatures -- More than 1.5 million samples of malware signed with digital signatures already exist and attackers will continue to circumvent the trust mechanisms upon which our digital ecosystems rely.
8. Security vs Privacy debate will continue -- In 2014,expect to see some government and corporate organisations go dark in response to privacy issues. Consumer privacy demands will impact security architectures, the cloud, and information sharing.
9. Threat cycles will be recycled. A significant percentage of successful cyber intrusions do not rely on sophisticated techniques, rather the attackers aim to exploit lax security architecture, policy and skills shortages using tried and true methods.
10. Targeted Attacks to continue -- An increase in targeted attacks on government, large enterprise organisations and small businesses is expected as cyber criminals focus their attempts to financially exploit targets. This does not necessarily mean a correlating increase in advanced malware and advanced persistent threat samples as attackers may use sophisticated or traditional techniques to achieve their ends.

To read more click **HERE**

Even tiny microSD cards have chips that can be hacked

BGR, December 30, 2013: Andrew “bunnie” Huang and Sean “xobs” Cross have discovered a way to hack even the small microSD cards that go inside current smartphones and tablets to increase their storage, as well as other flash-based memory solutions, presenting their findings at the Chaos Computer Congress (30C3). In a detailed blog post on bunnie:studios, Huang explained how the hack works, and why many flash cards are susceptible to being hacked and used for malicious purposes by people who are aware of this particular potentially serious security vulnerability. The problem with flash memory is that it’s not flaw free, and the companies that make flash-based devices are likely to “fix” the hardware issues with the help of sophisticated software that runs on a microcontroller and is able to deal with errors and bad sectors. The firmware that makes the “fixes” possible resides in an ARM-based microcontroller that operates at speeds of up to 100MHz, and that costs only around $0.15 to $0.30 to include in each flash storage device. However, the preloaded software is not bug free, and therefore flash storage makers need to be able to update it. In some cases, the microcontroller and its firmware are not secured either, so that’s where hackers who know how to take advantage of these series of “flaws” come in. They would be able to replace the default firmware on the microcontroller with malware that is be able to deliver “man in the middle attacks” – the flash storage unit would behave in one way, but it would so something else instead. Compromised cards can’t be detected with custom security protocols, as there aren’t standard protocols in place to deal with such hacks. The only way to deal with a compromised card would be to physically destroy it. In addition to microSD cards, other type of flash memories can be affected by such hacks, including SD and MMC cards, “as the eMMC and iNAND devices typically soldered onto the mainboards of smartphones and used to store the OS and other private user data,” Huang writes. Even USB flash drives and SSDs could have similar

vulnerabilities. A recent Der Spiegel report revealed that firmware of hard drives manufactured by various companies could be altered to install spy malware. To read more click **HERE**

Database Risks Increase as Patch Frequency Decreases

Dark Reading, 27 Dec 2013: The recent report released by the Inspector General of the Department of Energy about a massive breach at the agency earlier this year detailed a number of important breakdowns in security that led to the breach [**LINK**]. Perhaps one of the biggest lessons to be learned from the report, though, was how important the patching process is to the risk posture of sensitive databases. According to Gregory H. Friedman, the author of the report, among the biggest failures that led to the breach was the fact that the management information system (MIS) breached by attackers was running on woefully out-of-date software. Critical security vulnerabilities in certain software supporting the MIS application had not been patched or otherwise hardened for a number of years," Friedman reported. In the same vein, Friedman reported that there was no sense of urgency in replacing end-of-life applications that stood up critical MIS databases. "Specifically, core support for the version of the compromised application upon which MIS was built ended in July 2012, and the department failed to purchase the extended support that would have provided limited coverage through July 2014," Friedman said. Patch management has long been a thorn in the side of database administrators, who would just as soon not deal with the performance quirks that come with security updates. "Database patches tend to introduce not only security fixes, but behavioral changes as well, which cannot be separated out of the cumulative patch," says Barry Shteiman, director of security strategy for Imperva. "For this reason, many DBAs or system admins decide to not patch, or only patch on a yearly maintenance basis, and even then, I have a strong feeling that only patches that are considered 'critical' are installed." "If an application uses a database back-end -- as they always do -- and that application is vulnerable to attacks, SQL injection, for example, then the database that it has rights to read and write from becomes vulnerable to the same attack," Shteiman says. "It is a chain reaction." Unfortunately, the basic blocking and tackling of patch and vulnerability management continues to lag at many organizations, particularly those within the public sector. A study conducted earlier this year by CentraStage that examined anonymized hardware and software data of thousands of online servers -- including those belonging to 6,000 different public sector agencies -- found that 40 percent of the machines lacked up-to-date security practices [**LINK**]. According to Dave Rosenberg, CTO at DB Networks, organizations should recognize that the patch process will be imperfect no matter how conscientiously it is pursued. "Patches are available only after significant problems occur and are detected in the field; after they are understood and addressed by beleaguered developers; knowledge of their availability and distribution to operations is unreliable and time-consuming; and they must be sequenced into production along with many other frequently conflicting priorities," Rosenberg says, explaining that it is important to complement patch management with continuous monitoring and behavioral analysis to look for exploited vulnerabilities. To read more click **HERE**