The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

24 April 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

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

April 22, SC Magazine – (New York) **Three laptops stolen from New York podiatry office, 6,475 at risk.** Three laptops containing patient data were stolen from the Sims and Associates Podiatry office in New York in January, potentially affecting 6,475 patients. Authorities do not believe any personal and medical information was misused and continue to investigate the theft. Source: http://www.scmagazine.com/three-laptops-stolen-from-new-york-podiatry-office-6475-at-risk/article/343644/

April 22, Iowa State University – (Iowa) **Iowa State IT staff discover unauthorized access to servers.** Iowa State University notified 29,780 students April 22 after the discovery of a breach affecting 5 department servers on campus. The compromised servers contained Social Security numbers and the university notified an additional 18,949 students whose university ID numbers were also located on the servers. Source: http://www.news.iastate.edu/news/2014/04/22/serverbreach

April 23, The Register – (International) **AOL Mail locks down email servers to deal with spam tsunami.** AOL confirmed that their AOL Mail email servers were under an intensive spoofing attack beginning April 20 that has sent large volumes of spam emails to users' inboxes. AOL stated that they changed their DMARC policy in order to prevent unauthorized use, but the change may affect some email-forwarding services and listservs. Source: http://www.theregister.co.uk/2014/04/23/aol_mail_locks_down_email_servers_to_deal_with_tsunami_of_spam/

April 23, Help Net Security – (International) **Amazon Cloud IaaS Service servers riddled with vulnerabilities.** Researchers at Bkav found in the course of a customer-prompted investigation that several servers for Amazon's Cloud infrastructure as a service (IaaS) Service and HP's Public Cloud service contain several vulnerabilities due to the servers' Windows Server installations not being updated for several months. Source: http://www.net-security.org/secworld.php?id=16731

April 23, Softpedia – (International) **SMS trojan FakeInst targets users in 66 countries.** Researchers at Kaspersky analyzed the FakeInst trojan for Android and found that attackers have added capabilities since it first appeared in February 2013, allowing it now to target users in 66 countries. The trojan is disguised as an app and can send SMS messages to premium rate numbers as well as intercept text messages. Source: http://news.softpedia.com/news/SMS-Trojan-FakeInst-Targets-Users-in-66-Countries-438976.shtml

April 22, The Register – (International) **Patch iOS, OS X now: PDFs, JPEGs, URLs, Web pages can pwn your kit.** Apple released updates for its OS X and iOS operating systems, closing 19 security issues including a "triple handshake" error in iOS Secure Transport that could allow an attacker to inject data into secure connections. Source: http://www.theregister.co.uk/2014/04/22/apple_ios_7_1_1_os_x_security_updates/

April 23, Softpedia – (International) **DDoS attacks increasingly used as a smokescreen for data theft.** Neustar released its DDoS Attacks and Impacts Report for 2014 which found that distributed denial of service (DDoS) attacks are increasingly used by attackers as cover for more damaging compromises. Around half of organizations that reported suffering a breach or DDoS attack in 2013 also had malware installed on their systems, with 55 percent of those hit by DDoS attacks losing data or funds, among other findings. Source: http://news.softpedia.com/news/DDOS-Attacks-Increasingly-Used-as-a-Smokescreen-for-Data-Theft-438873.shtml

Number of hacker attacks on websites has sharply risen

Fox News, 23 Apr 2014: The number of hacker attacks on websites has sharply risen, and most of them are originating from China, according to a new report on Internet activity. Akamai Technologies' Fourth Quarter, 2013 State of the Internet Report, which was released Wednesday, says reported DDoS (denial of service) attacks rose 75 percent in Q4 2013 compared to the previous year, and were up 23 percent from the previous quarter. The data was gathered from the Akamai Intelligent Platform, a cloud service for delivering and securing online content, the company said in a press release (**link**). Throughout 2013, the company says its customers reported 1,153 DDoS attacks – a 50% increase from the 768 reported attacks in 2012. In the last quarter of 2013 alone, 241 of those attacks were directed at enterprise and commerce industry websites. Slightly less than half of reported attacks in Q4 2013 were directed at American websites. In that quarter, China was the source IP for 43 percent of DDoS attacks, followed by the United States at 19 percent and Canada at 10 percent, the report states. "Akamai maintains a distributed set of unadvertised agents deployed across the Internet to log connection attempts that the company classifies as attack traffic," the company said. "Based on the data collected by these agents, Akamai is able to identify the top countries from which attack traffic originates, as well as the top ports targeted by these attacks." Despite growth in the number of hacker attacks, Akamai says the average peak Internet connection speed around the world grew 38 percent last year. Hong Kong has the fastest average speeds, while Iran has the slowest. To read more click **HERE**

Bank of England to Oversee Ethical Hacking Program to Test the Cyber Resilience of Banks

SoftPedia, 24 Apr 2014: The Bank of England will reportedly oversee an ethical hacking program that's designed to determine just how resilient banks and other financial organizations are to cyber threats. According to The Financial Times (registration required), the systems of over 20 institutions will be tested. Security experts will conduct penetration testing based on a certification scheme called Crest. The attack scenarios will rely on information from intelligence reports on terrorists, state actors and profit-driven cybercriminals. The Bank of England hasn't released any information to the public regarding its plans. However, FT reports that organizations such as the Royal Bank of Scotland (RBS) and the London Stock Exchange are likely to participate. People familiar with the initiative have told the publication that a pilot has already been conducted. Back in November 2013, the representatives of almost two dozen British banks and other financial institutions took part in a cyber security exercise dubbed Waking Shark II. In February, the Bank of England published a report on the exercise. At the time, the central bank noted that it would consider naming a single coordination body to manage communications across the financial sector. It also advised companies to remember that they had to report incidents not only to their respective regulators, but also to law enforcement. To read more click **HERE**

Google, Facebook, Microsoft, Others Join Forces to Prevent Another Heartbleed

SoftPedia, 24 Apr 2014: Heartbleed has sent the world's tech companies into frenzy, especially since so much of the web relies on OpenSSL for security. To make sure something like this never happens again, the biggest names in tech are uniting forces. Google, Facebook, Microsoft, Amazon and Cisco are just a few of the companies that have vowed to do something about it. They've each committed to donating at least $100,000 (€72,500) a year for the next three years. Dubbed the Core Infrastructure Initiative, the project was created by the Linux Foundation and it seeks to invest money into the critical software infrastructure that needs it. "After the Heartbleed crisis we asked ourselves: How did this

happen and what role can The Linux Foundation play to be sure it doesn't happen again. We decided to do what we always do: work with the industry to raise money and fund developers directly so they can do what they do best, develop, while we give them the assistance the way we do Linus Torvalds," said Amanda McPherson, marketing chief at the Linux Foundation. Overall, there are some 13 companies that have joined thus far, and the organization has already amassed a $3.6 million (€2.6 million) commitment from the backers. More companies are certainly going to join in as time goes by, so more cash will be attracted too. It's nice to see that the tech community is united in fighting security bugs that put the world and their own businesses in danger. This is exactly what the folks over at OpenSSL were hoping for when they called out to the world's governments and tech giants to help support a stable team of developers to work on the project. The Hearbleed bug was unveiled a couple of weeks ago, after staying hidden for more than two years, while affecting several versions of OpenSSL. Attacks using this vulnerability leave no traces behind, which makes it impossible to know whether or not hackers knew about it beforehand or not, whether data has been stolen and what specific data may have been exposed. Companies such as Google, Facebook and Yahoo were all affected in some way or another, although they were quick to patch things up. Governmental sites from all over the world were also affected. About two thirds of the world's secure websites use OpenSSL, which means that the number of impacted sites is huge and that it's quite likely that not all have been patched in the time that has passed since Heartbleed was made public. To read more click **HERE**

Staff at Tokyo Airport Lose Memo Containing Security Codes

SoftPedia, 24 Apr 2014: These days, you can still find a security expert or two that will say that it's OK to write down your passwords on paper if you're afraid you'll forget them. However, they will also tell you that you must never leave that piece of paper in plain sight. An incident that occurred at the Tokyo International Airport in Japan one day before the visit of US President Barack Obama demonstrates just how dangerous it is to misplace a piece of paper containing passwords. According to The Japan Times, an employee of Skymark Airlines lost a piece of paper containing airport security pass codes. The note was found half hour later, but airport officials decided to change all security codes as a precaution. It's uncertain what could have been accessed with the codes, but airport representatives decided that the information could lead to a security breach. Japanese authorities have put a lot of effort into making sure that the US president's visit goes without incidents. Security cameras have been installed, security checkpoints have been set up and around 16,000 officers have been deployed throughout Tokyo. As far as the Haneda Airport is concerned, at the beginning of April, the Tokyo police announced the launch of a counterterrorism unit that would deal with hijackings and other incidents. To read more click **HERE**

Government Employees Cause Nearly 60% of Public Sector Cyber Incidents

NextGov, 22 Apr 2014: About 58 percent of cyber incidents reported in the public sector were caused by government employees, according to an annual data breach report compiled by Verizon. The findings -- stripped of identifying information -- do not mention ex-contractor Edward Snowden's mammoth leak of national secrets. Even if Snowden's leaks had been included in the tally of results attributed to insider threats, they wouldn't have made much of a dent. "If that were recorded in here, that would be a single event," said Jay Jacobs, a Verizon senior analyst and co-author of the report. Most (34 percent) of the insider incidents in the global public sector during the past three years were miscellaneous errors such as emailing documents to the wrong person. Unapproved or malicious use of data by public servants accounted for 24 percent of reported incidents. Surprisingly, cyberspying and intrusions via security holes in websites, known to be big problems in government, represented less than 1 percent of the situations reported. The off-kilter numbers in government reflect mandatory reporting requirements for mundane incidents, Jacobs said. Small data leaks that happen every day overshadow frequent, but not daily, hacks. By contrast, cyber espionage accounted for 30 percent and 40 percent of incidents in the manufacturing and mining industries, respectively. And 41 percent of the incidents reported in the information sector involved break-ins through website weaknesses. Miscellaneous errors represented only 1 percent of reports in that industry. For the government sector, "I think that the raw numbers are

actually quite high for things like Web-based attacks and espionage as well," Jacobs said. "But it's masked because of all of this other data." "A lot of that is misdelivery -- which is either attaching the wrong thing to an email or sending the right email to the wrong people," he added. "Or another huge problem is when the mailing machine would get off by one [person] and so it was putting an address on an envelope with somebody else's personal information inside the envelope." The percentages in the Verizon study cannot be compared between sectors because they represent the proportion of incidents within each sector. Based on the raw data, cyberspying in government is comparable to cyberspying in other industries, Jacobs said. "It's just that in other industries we don't have that mandatory reporting, so we don't see that level of employee error. We don't see the misuse," he added. The raw numbers were not disclosed in the study. More than 50 organizations worldwide contributed to this year's assessment, including law enforcement agencies, government computer security incident response teams, private forensics investigators, security product vendors and public-private information sharing and analysis centers. To read more click **HERE**

Stolen Passwords Used in Most Data Breaches

Dark Reading, 22 Apr 2014: Findings from the new and much-anticipated 2014 Verizon Data Breach Investigations Report (DBIR) show that two out of three breaches involved attackers using stolen or misused credentials. "Two out of three [attacks] focus on credentials at some point in the attack. Trying to get valid credentials is part of many styles of attacks and patterns," says Jay Jacobs, senior analyst with Verizon and co-author of the report. "To go in with an authenticated credential opens a lot more avenues, obviously. You don't have to compromise every machine. You just log in." Some 422 cases last year involved the use of stolen credentials, followed by data-stealing malware (327), phishing (245), RAM scraping (223), and backdoor malware (165). Not far behind were backdoor/command & control (152), spyware (149), and downloader malware (144), as well as others. Verizon this year widened the scope of its popular annual report to include security incidents as well as data breaches, and the 2014 Verizon DBIR includes data from 50 organizations from 95 different countries, including the US Secret Service, the Poland CERT, and Latin American CERTs. That's a big jump from the 19 contributors representing 27 countries in the 2013 Verizon DBIR. The report tallied a grand total of 1,367 confirmed data breaches in 2013, up from 621 in last year's report from data compiled from a smaller number of contributing organizations. The new report looks at 63,437 total security incidents in 2013 spanning more than 95 countries. And now with a decade of reports in its portfolio, Verizon found that 92 percent of the 100,000 security incidents in its reports the past 10 years are tied to nine attack methods, some of which are more common than others in specific industries: errors such as sending an email to the wrong person; crimeware; insider/privilege misuse; physical theft/loss; web application attacks; denial-of-service attacks; cyber espionage; point-of-sale intrusions; and payment card skimmers. "With all the data we had this year, we needed to break it apart and simplify the discussion... We looked at patterns on how elements of an incident clustered," Jacobs says. Among the patterns: 75 percent of security incidents reported in the financial services industry came via web app attacks, DDoS attacks, and payment card skimming. Some 54 percent of incidents in manufacturing come via cyber espionage and DDoS. And despite conventional wisdom that retail suffers mostly card-skimming attacks, the greatest number of retail security incidents -- 33 percent -- include DDoS, and 31 percent point-of-sale system hacks. POS attacks are dropping, according to the report. Verizon tallied 198 total POS incidents in 2013, all of which included data theft. RAM scraping malware -- which lifts card or other sensitive data from memory while it's unencrypted and being processed -- rose last year, along with brute-force attacks of remote-access connections to POS systems. POS attacks were less than 20 percent last year, while web app attacks were at around 40 percent for incidents during that period. "Given recent headlines, some may be surprised to find that POS intrusions are trending down over the last several years. That's mainly because we've seen comparatively fewer attack sprees involving numerous small franchises. Brute forcing remote access connections to POS still leads as the primary intrusion vector. A resurgence of RAM scraping malware is the most prominent tactical development in 2013," the report says. The accommodations industry suffered the most POS attacks last year, with 75 percent of security incidents attributed to that methodology. Next in line was retail, with 31 percent of POS attacks and 33 percent DDoS attacks. [Verizon Data Breach Investigations Report 2014 says financial cybercrime accounting for

three-fourths of real-world breaches, followed by cyber espionage in one-fifth of breaches. See No 'One Size Fits All' In Data Breaches, New Verizon Report Finds.] Attackers are getting better and more efficient. In more than three-fourths of the cases, it takes attackers days or less to compromise their target, while only one-fourth of the time, victim organizations discover the attack in days or less, according to Verizon's findings. "Attackers are getting better and faster while we as defenders are not innovating as fast," Jacobs says. "Really, the attacker is innovating much faster and getting better and quicker." Cyber espionage is on the rise, too. Some 22 percent of breaches in 2013 were cyberspy attacks, the report says, just behind web application attacks (35 percent). Cyber espionage accounted for 15 percent of all breaches between 2011 and 2013, mostly nation-state type activity. But another trend in cyberspying is cropping up as well: "There have been a few cases where [companies] have hired organized crime type units to go after their competitors," says Jacobs. Nation-state and other cyberspies often employ a variety of tools and attack methods, he says, even within a single incident. "They are more complex attacks. What we are seeing is definitely a slower attack, more controlled and a little more complex. "The bottom line is the bad guys are still winning." To read more click **HERE**