The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

6 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, Newport News Daily Press – (Virginia) **Riverside reports health records breach.** Riverside Health System attempted to notify 919 Riverside Medical Group patients of an electronic health records breach discovered in November 2013. The company discovered a former employee inappropriately accessed the medical records over a 4-year period during an audit. Source: http://articles.dailypress.com/2013-12-31/health/dp-nws-riverside-breach-0101-20131231_1_patients-bon-secours-sentara-healthcare

January 2, Portsmouth Herald – (New Hampshire) **Virus attacks Greenland Town Hall computers.** Greenland Town Hall computers became infected with the ransomware virus CryptoLocker after an employee inadvertently opened an email containing the malware December 26. Officials missed the deadline for paying the ransom and lost 8 years of electronic data. Source: http://www.seacoastonline.com/articles/20140102-NEWS-401020387

December 30, Lafayette Journal & Courier – (Indiana) **2 involved in Purdue grade changing-scheme plead guilty.** Two former students at Purdue University in Indiana pleaded guilty December 30 to hacking into the university's computer systems and changing their grades from May 2008 to May 2012 by installing key logging devices and breaking into professors' offices. Authorities believe a third student, still wanted, was also part of the scheme. Source: http://www.jconline.com/article/20131230/NEWS03/312300022/2-involved-in-Purdue-grade-changing-scheme-plead-guilty?nclick_check=1

January 3, Help Net Security – (International) **Critical backdoor in Linksys and Netgear routers found.** A security researcher identified a backdoor in certain Netgear and Linksys routers' firmware that can be used to reset the devices to default settings, including default administrator passwords. Other brands of routers manufactured by the same company may also be affected. Source: http://www.net-security.org/secworld.php?id=16155

January 3, The Register – (International) **Slovenian jailed for creating code behind 12 MILLION strong 'Mariposa' botnet army.** The creator of the Mariposa botnet malware and the Rimecud malware pack was sentenced by a court in Slovenia to almost 5 years in prison for creating the malware which infected around 12 million computers. Source: http://www.theregister.co.uk/2014/01/03/mariposa_botnet_mastermind_jailed/

January 3, Softpedia – (International) **Facebook fixes open redirect vulnerability on "How are you feeling?" page.** A security researcher found and reported an open redirect vulnerability in the mobile version of Facebook's "How are you feeling?" page which could have allowed an attacker to redirect users to malicious Web sites. Facebook confirmed that the vulnerability was closed December 31. Source: http://news.softpedia.com/news/Facebook-Fixes-Open-Redirect-Vulnerability-on-How-Are-You-Feeling-Page-Video-413243.shtml

January 3, Softpedia – (International) **OpenSSL website hacked through insecure password at hosting provider.** The OpenSSL Foundation reported January 1 that a recent attack on its Web site was carried out by attackers exploiting an insecure password at the site's hosting provider, which allowed the attackers to take control of the hypervisor management console. Source: http://news.softpedia.com/news/OpenSSL-Website-Hacked-Through-Insecure-Password-at-Hosting-Provider-413377.shtml

January 3, Softpedia – (International) **3 vulnerabilities fixed in Elgg 1.8.17.** The developers of open source social networking platform Elgg released new versions of the platform, which address three critical security issues as well as several functionality issues. Source: http://news.softpedia.com/news/3-Vulnerabilities-Fixed-in-Elgg-1-8-17-413314.shtml

Phishing Alert: Unauthorized Activity on Your Amazon Account
SoftPedia, 6 Jan 2014: Amazon customers should be on the lookout for fake emails that inform them of unauthorized activity on their accounts. According to Dynamoo's Blog, the emails read something like this: "We recently confirmed that you had unauthorized activity on your Amazon account. Please be assured that because your card includes 'zero-liability fraud protection', you are not responsible for unauthorized use of your card. Unfortunately, we have not confirmed your complete information, please follow the instructions below. Click the link below to validate your account information using our secure server." The link from the email doesn't point to Amazon.com, but to a website that hosts an Amazon phishing page. First, victims are asked to enter their email addresses and their passwords. Then, they're instructed to provide even more information, including name, contact information, and payment card data. Once the information is entered on the phishing site, victims are taken to the legitimate Amazon website in an effort to avoid raising any suspicion. If you're a victim of this scam, change your Amazon password as soon as possible. If you've handed over payment card information, it might be wise to contact your bank. To read more click **HERE**

Microsoft Absolutely Tight-Lipped on Windows 8.1 Installation Problems
SoftPedia, 6 Jan 2014: Back in October, Microsoft rolled out the Windows 8.1 OS update with much fanfare, giving Windows 8 adopters the chance to quickly and easily install it from the store. Many users, on the other hand, experienced issues with the installation process, mostly due to incompatible drivers. Redmond recommended users to check for the latest drivers and compatible software. Fast forward to January 2014 and people are still struggling to cope with the same installation errors, with the Microsoft Community forums still assaulted by posts revealing a number of errors returned when trying to download the update. Error messages 0xC1900101-0x40019 and 0x80070652 are still among the common problems encountered by users and no workaround is available at this point, aside from driver updates and the installation of some patches released by Microsoft. Here's what one user posted recently on the forums: "Turns out this issue was easily resolved for me. I had a couple of updates available and after applying them, I attempted another upgrade to 8.1 and it was successful. "Another thing which might have contributed, although I'm not at all sure; I set power options to maximum performance and enabled 100% brightness on both sliders." Windows 8.1 was officially launched in October and was supposed to be available as a free update that could be quickly installed on all devices running the new Windows 8. The update, on the other hand, caused quite a lot of issues to many users, pretty much because installation failed completely and got stuck before deploying all files. Most of the instructions provided by Microsoft made almost no difference, so users are still struggling to diagnose the bugs and find the cause of the problems that prevent them from deploying Windows 8.1 on either desktop PCs or tablets. To read more click **HERE**

Unknown Cybercriminals Launch DDOS Attacks against 3 Popular BitTorrent Sites
SoftPedia, 6 Jan 2014: For the past few days, private BitTorrent websites What.cd, PassthePopcorn.me and Broadcasthe.net have been offline due to distributed denial-of-service (DDOS) attacks being launched against their

systems. No one has taken credit for the attacks. The representatives of the targeted trackers have told TorrentFreak that they have no idea who is behind the cyberattacks. What.cd operators have decided to null-route all the site's IP addresses to avoid wasting bandwidth. This isn't the first time popular BitTorrent websites are targeted with DDOS attacks. In 2012, a hacker called Zeiko Anonymous disrupted most of the popular trackers after What.cd refused to give him an invitation. On this particular occasion, it's difficult to determine who is behind the attacks. It could very well be an anti-piracy group, but it could also be the competition, or someone with a personal agenda. To read more click **HERE**

Hackers Steal Financial Data of over 93,000 Staysure Customers

SoftPedia, 6 Jan 2014: Staysure, a British company that provides travel insurance, has suffered a data breach. The company said that hackers broke into its servers in the second half of October 2013, but the breach was detected only in mid-November. In a notice posted on its website, Staysure reveals that the attackers stole names, addresses, encrypted payment card details, and CVVs. The information belongs to customers who had purchased insurance before May 2012. After this date, Staysure stopped storing this type of data. Around 93,000 people (less than 7% of the customer base) might be impacted. The insurer has started sending out notification letters to affected individuals. The police, the ICO and the Financial Conduct Authority have also been notified. The company is confident that the vulnerabilities exploited by the cybercriminals have been patched. Customers are being offered free access to Experian's identity fraud monitoring service Data Patrol. To read more click **HERE**

More Brazilian Government Sites Hacked in Protest against 2014 FIFA World Cup

SoftPedia, 6 Jan 2014: Anonymous hackers continue to target Brazilian government websites in protest against the upcoming 2014 FIFA World Cup. Over the past days, they've hacked and defaced subdomains on the websites of various Brazilian states, including Ceará (barro.ce.gov.br), Santa Catarina (indaial.sc.gov.br), Bahia (dommacedocosta.ba.gov.br) and São Paulo. At the beginning of the campaign, in late-December 2013, they hacked the website of the Igarapé do Meio municipality in Maranhão (igarapedomeio.ma.gov.br). Various hacker groups are behind the #OpWorldCup attacks, including DK Brazil HackTeam and Insanity HackTeam. The hacktivists are protesting against the World Cup because they say the sporting event has a negative impact on Brazil and its people. At the time of writing, some of the websites have been restored. However, many of them have been taken offline or they're still defaced. To read more click **HERE**

Yahoo servers hit in malware attack

USA Today, January 5, 2014: Visitors to Yahoo Web pages who click on ads were at Visitors to Yahoo's Web pages who viewed ads the past few days are potentially at risk of having their computers infected by malware, according to published reports Sunday. Fox IT -- an Internet security firm that discovered the alleged malware infection -- says 300,000 users were visiting the infected ads every hour. That means roughly 27,000 computers and devices were being infected every hour since typically 9% of computers are actually infected after visiting the site. Most computer users either use software that combats such infections or may have configured their computers to be resistant to the attacks. Malware, short for malicious software, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Computers connected to a network can spread the malware onto many more computers. The malware may have started spreading on Dec. 30. This is just the latest technical problem to hit the struggling Yahoo as it attempts to become more relevant as online services proliferate. The company's e-mail service experienced widespread outages and problems in late December. Consumers should know that this Yahoo malware attack works by redirecting visitors on Yahoo's pages to an infected site, which then uses security holes in Oracle's Java to install malware. Java is a commonly used "plug in" designed to add additional computational capability to Internet browsers. The infected site proceeds to install a variety of malware to the user's device including those called ZeuS, Andromeda, Dorkbot, Tinba or Necurs, Fox IT says. Most of the users affected have been in Great Britain, France and Romania. In a statement, Yahoo said it is aware of the security issues. "On Friday, January 3 on our European sites, we

served some advertisements that did not meet our editorial guidelines, specifically they spread malware. We promptly removed these advertisements. Users in North America, Asia Pacific and Latin America were not served these advertisements and were not affected," according to an updated Yahoo statement released Sunday evening. The infection rate has declined significantly, indicating that Yahoo is making adjustments to fix the problem, Fox IT says. Computer users can protect themselves from this and other similar attacks. Perhaps the easiest form of defense is turning off the Java plug in, which is commonly installed in most browsers including Internet Explorer, Chrome, Firefox and Safari. Internet Explorer users can easily turn off Java by clicking on the icon that looks like a gear in the upper right-hand corner of the screen and selecting "Manage add-ons." Under the "Add-on Types," look for a section titled Oracle America, Inc. Right-click on any entry that starts with the word Java, and choose Disable. To read more click **HERE**

Cryptolocker 2.0 turns into worm that spreads via USB drives

ComputerWorld, 6 Jan 2014: Security researchers have discovered what looks like a copycat version of the Cryptolocker ransom Trojan that drops some of the malware's sophistication in favor of the single innovation of being able to spread via USB drives. According to security firms Trend Micro and ESET, the recently discovered worm-like Crilock. A variant (which calls itself 'Cryptolocker 2.0) poses as an updater for Adobe Photoshop and Microsoft Office on sites frequented by P2P file sharers. Trend Micro believes that Crilock.A is the work of copycats rather than the original Cryptolocker gang. Targeting file sharers is a strange choice because it while it increases the chance that the malware will be downloaded the potential list of victims is still far smaller than with previous 'official' version. A similar point could be made about the abandonment of DGA for hard-coding, which is much easier to block; security firms simply have to reverse engineer the list and the malware becomes useless. However, there are advantages to these changes. Using hard-coding is simpler while spreading from P2P sites is a way of remaining less visible than would be the case when using a flood of phishing emails. Most interesting and perhaps revealing of all, Crilock.A adds the ability to infect removable drives. This worm technique is as old as the hills and although slowing its spread it does ensure a degree of longevity. On the other hand, while it can hide on drives for years to come, by the time it activates it will probably detected by every security program in existence. This whole strategy speaks of an opportunist gang that has hijacked (i.e. reverse engineered) the malware to hit a small but global target that has something valuable to protect - files shared illegally via P2P. This group is for obvious reasons also less likely to raise a complaint with police. Just for added spice, the variant adds other sneaky abilities, including launching a component to launch DDoS attacks, steal Bitcoin wallets and even launch a Bitcoin-mining tool. ESET has published a full list of the differences between Cryptolocker and Crilock.A/Cryptolocker 2.0 on its website, including noting the eccentric use of the more compute-intensive 3DES encryption format rather than more conventional AES. In the same week Cryptolocker 2.0 was detected before Christmas, Dell SecureWorks published its estimate that the original version of the program had infected around 200,000-300,000 PCs in 100 days. Around 0.4 percent of these victims probably paid the demanded ransom of around $300 in Bitcoins or via MoneyPak. To read more click **HERE**

Healthcare Data Breaches to Surge in 2014

Program Business, 3 Jan 2014: Healthcare will be a hotbed of consumer data breaches in 2014, according to an Experian report, "2014 Data Breach Industry Forecast." "The healthcare industry, by far, will be the most susceptible to publicly disclosed and widely scrutinized data breaches in 2014," according to the report (registration required), which addressed healthcare risks as one of six major trends. "The sheer size of the industry makes it vulnerable when you consider that as Americans, we will spend more than $9,210 per capita on healthcare system refers to the parts that pose the greatest opportunity for attack or error. Best known as a credit bureau and consumer data tracking service, Experian also has a business helping companies recover from personal data breaches. The company has had its own data security problems this year. Michael Bruemmer, vice president of its breach resolution service, Data Breach Resolution, and author of the report, said healthcare accounted for about 46% of the breaches his division serviced in 2013 -- and he expects that to rise significantly in 2014. Bruemmer said he is basing this prediction at least partly on reports of security

risks posted by the HealthCare.gov website and the health insurance exchanges established by various states. The web infrastructure to support health insurance reform was "put together too quickly and haphazardly." The most glaring problem for these sites has been their inability to keep up with consumer demand. The organizational infrastructure behind the implementation of Obamacare is also complex, meaning that many parties have access to the personal data and could misuse or mishandle it. "So we have volume issues, security issues, multiple data handling points -- all generally not good things for protecting protected health information and personal identity information." Another factor: In 2014, the industry will feel the full force of tightened rules that that went into effect in September for protecting health information and disclosing breaches. Part of the problem is that many participants in the healthcare industry, such as individual doctor's offices, don't think of themselves as being in the data management business, so they are inadequately prepared to protect data against the threats that exist today, according to Bruemmer. In most cases, data breaches have less to do with advanced hacking techniques than with lost laptops, failing to shred paper records, and other employee errors. Though the threat from malicious insiders is significant, a bigger threat is "people doing dumb things." In the IT realm, there are stories of people installing anti-malware software but forgetting to turn it on. "And then there's my favorite: where the people in the network operations center actually left the door unlocked, and another employee came in, sat at a console, and played around with the system to see what he could get." Overall, Experian's remediation group worked on more than 2,200 breaches in 2013, versus 1,700 in 2012. In three of the top 10 breaches, the error was traced to a system administrator's sloppy password practices, such as neglecting to change a default password or carelessly sharing the password. Whether stolen or accidentally disclosed, healthcare data is valuable, and that makes it a target. On the black market, personal records suitable for use in identity theft are worth $10-$12 each at the low end or maybe $25-$28 for a particularly attractive identity, he said. When enriched with health data, the value of an identity data set jumps to about $50 per record, because then it can be used for medical and insurance fraud. To read more click **HERE**