The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

1+2 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

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

March 28, San Diego Union-Tribune – (California) **Data stolen from 5,000 patients.** Palomar Health notified about 5,000 patients March 28 of a potential personal data breach after a company laptop and two flash drives were stolen in February from an employee's vehicle parked in Oceanside. Police arrested an individual believed to be tied to the sale of the stolen items March 17 and authorities continue to investigate the incident. Source: http://www.utsandiego.com/news/2014/mar/28/palomar-health-data-theft-5000-patients/

March 30, Associated Press – (New Mexico) **Albuquerque police website under cyberattack.** The Albuquerque Police Department reported that its Web site was down for several hours March 30 due to a cyberattack, and the department continued to investigate the incident while IT personnel worked to resolve the disruption. Source: http://news.msn.com/crime-justice/albuquerque-police-website-under-cyberattack

March 28, Threatpost – (International) **FTC settles with Fandango, Credit Karma over SSL issues in mobile apps.** Fandango and Credit Karma agreed to a settlement with the Federal Trade Commission (FTC) after the FTC charged that both companies deliberately misrepresented the security of their mobile apps and created apps that failed to validate SSL certificates. The companies are required by the settlement to submit to independent security audits for the next 20 years and to create comprehensive security programs. Source: http://threatpost.com/ftc-settles-with-fandango-credit-karma-over-ssl-issues-in-mobile-apps/105128

March 28, IDG News Service – (International) **Philips smart TVs open to remote attacks via default wireless connection, researchers say.** Researchers at ReVuln published a demonstration video showing that the newest firmware for some Philips smart TVs opens an insecure Miracast wireless network that could allow attackers within signal range to control the TV. The Miracast feature is vulnerable to attackers due to a hard-coded password. Source: http://www.networkworld.com/news/2014/032814-philips-smart-tvs-open-to-280196.html

March 31, Tacoma News Tribune – (National) **Phishing emails net medical records, Social Security numbers at Tacoma's Franciscan Health System.** Franciscan Health System notified more than 12,000 patients nationwide that their personal information may have been accessed after Franciscan Medical Group employees were targeted in a phishing scheme in January. Staff received emails which appeared to be sent by the health system's parent company, Catholic Health Initiatives, and entered their user names and passwords. Source: http://www.then

April 1, Softpedia – (International) **Experts unhappy with Oracle's Java Cloud patching process, vulnerability details published.** Researchers at Security Explorations published details of 30 vulnerabilities in Oracle Java Cloud Service, about half of which can be used to break the Java security sandbox. The vulnerabilities were previously reported to Oracle in January. Source: http://news.softpedia.com/news/Experts-Unhappy-with-Oracle-s-Java-Cloud-Patching-Process-Vulnerability-Details-Published-435125.shtml

April 1, IDG News Service – (International) **CryptoDefense ransomware leaves decryption key accessible.** Symantec researchers analyzed the CryptoDefense encryption ransomware and found that the decryption key needed to undo the malware's file encryption is also left on the victim's computer, potentially allowing victims to decrypt the files held for ransom themselves. Source: http://www.computerworld.com/s/article/9247348/CryptoDefense_ransomware_leaves_decryption_key_accessible

April 1, V3.co.uk – (International) **Middle Eastern hackers use remote access trojan to infect 24,000 machines worldwide.** Researchers at Symantec reported finding 487 groups actively using the njRAT remote access trojan (RAT) for malicious uses, with around 24,000 machines infected worldwide. Symantec reported that most attacks using njRAT originate in the Middle East and that the majority of the RAT's command and control servers are located in the Middle East and North Africa. Source: http://www.v3.co.uk/v3-uk/news/2337382/middle-eastern-hackers-use-remote-access-trojan-to-infect-24-000-machines-worldwide

March 31, SC Magazine – (International) **Smartphones at risk of malicious code injection through HTML5-based apps.** Researchers at Syracuse University published a paper detailing how HTML5-based smartphone apps could allow for devices to be targeted with a new Cross-Device Scripting (XDS) attack that could inject malicious code via WiFi scanning, SMS messaging, or other means. Source: http://www.scmagazine.com/smartphones-at-risk-of-malicious-code-injection-through-html5-based-apps/article/340513/

Anonymous Hackers Publish List of Demands for Operation Albuquerque
SoftPedia, 2 Apr 2014: Anonymous hacktivists involved in Operation Albuquerque, the campaign initiated after Albuquerque Police Department (APD) officers shot and killed a homeless camper, have published a new statement with a list of demands. "We are here in solidarity with the Albuquerque's citizens and to help bring justice that is long overdue. Members of the Albuquerque community, families of APD victims, and community organizations formulated the following fourteen demands for Albuquerque City Council and Albuquerque Police Department," the hackers said in a statement published on YouTube. "We call upon you to hold the appropriate authorities accountable, informing them that they must incorporate these demands into the US DOJ's comprehensive plan for APD'S sustainable reform." The hacktivists want the US Department of Justice to take over the APD to prevent further abuses, they demand "authentic and verified citizen oversight of APD," the immediate arrest of the officers involved in the killing of the homeless man James Boyd, the termination of the Police chief, and the indictment of all officers who have violated citizen rights. They also demand the "demilitarization of ADP," an increase of funding for social services, an investigation into the ADP's hiring practices, that the access of ADP officers to deadly weapons be "dramatically reduced," the introduction of community-based policing to enhance the relationships between authorities and citizens, and an evaluation of all police officers to see if they're mentally fit to carry weapons. The list of demands comes just as US Marshals shot a man on the run in southwest Albuquerque. This is the third shooting in the past few weeks, but in this case, the suspect wasn't killed. The attention of America turned to Albuquerque after the shooting of Boyd. To make matters worse, a second man was killed by APD officers shortly after. Both are controversial cases that are being investigated by the Department of Justice. So far, hacktivists have launched distributed denial-of-service attacks against the websites of the APD and the City of Albuquerque. Albuquerque officials knew that the city's websites would be targeted by Anonymous hackers and claimed to have taken measures. However, the websites were disrupted for hours over the weekend. Twitter and Facebook pages were shut down as a precaution. The initiators of the OpAlbuquerque campaign are planning a Twitter storm for today, April 2. Check out the video statement they've published on YouTube. A full transcript is available on Pastebin (**link**). To read more click **HERE**

iWork "View-Only" Is Broken, Documents Are Actually Editable

SoftPedia, 2 Apr 2014: Apple has deployed a major new ability to lock up iWork documents for viewing only, in an attempt to prevent edits when you share a text document, spreadsheet, or presentation. As it turns out, documents created with the view-only setting are, in fact, quite editable. Pages, Keynote and Numbers all received big updates with improvements and tweaks across every aspect, including one major new addition to set documents as view-only. Apple explained that the "New 'view only' setting lets you share documents you want others to view but not edit." We were skeptical when we first heard this. How could a Pages document be locked up to prevent edits yet still be offered up for viewing in your application of choice? So we put Apple's claim to the test and, sure enough, any Pages document shared with the view-only setting can indeed be tampered with. Below is a screenshot of the view-only file I sent to a friend. He returned it with a modified headline. In my friend's native tongue, it means "Stay hungry, stay foolish, and don't troll." The Pages file can be opened, viewed and modified in regular text editors, then whisked away anywhere carrying said edits. You can convert it into your preferred format, so there's really no restriction whatsoever. Simply put, "view-only" is (at best) just a handy tool for people looking to collaborate on a project and not make edits by mistake. To read more click **HERE**

MiniDuke Malware Used in Targeted Attacks against Ukraine

SoftPedia, 2 Apr 2014: Since the Ukraine crisis started, security experts have revealed spotting cyberattacks aimed at the country's networks. Now, researchers from F-Secure say they've uncovered a number of Ukraine-related documents that appear to have been used last year as a decoy to distribute MiniDuke malware. The existence of the MiniDuke cyber espionage campaign, which targeted European governments, was revealed in February 2013 by Kaspersky. At the time, experts said that cybercriminals had been using a PDF zero-day to trick targets into installing malware. For their investigation of MiniDuke attacks, F-Secure researchers have developed a tool that extracts the payloads from the decoy PFD documents in an effort to find similar cases. They've uncovered a series of documents referencing Ukraine. Many of the decoy documents have been taken from public sources. However, there's one file that doesn't appear to be publicly available. It's a letter from the First Deputy Minister for Foreign Affairs of Ukraine, Ruslan Demchenko, to the heads of foreign diplomatic institutions in the country regarding the 100th anniversary of World War I. The fact that the document is not publicly available could indicate that the MiniDuke attackers had or still have access to the systems of Ukraine's Ministry of Foreign Affairs. However, for the time being, F-Secure doesn't want to jump to any conclusions. "We don't know where the attacker got this decoy file from. We don't know who was targeted by these attacks. We don't know who's behind these attacks," noted F-Secure's Mikko Hypponen in a blog post. "What we do know is that all these attacks used the CVE-2013-0640 vulnerability and dropped the same backdoor (compilation date 2013-02-21)." To read more click **HERE**

"This Drive Has a Hardware Problem That Can't Be Repaired"

SoftPedia, 2 Apr 2014: Between October 2009 and July 2011, Apple sold a bunch of iMacs with faulty 1TB drives. The company only found out about the failing hardware when complaints began cropping up on its forums, so Apple opened up the iMac 1TB Seagate Hard Drive Replacement Program to offer free repairs for affected customers. To this day iMacs with 1TB Seagate drives continue to fail, but there's just one problem. The program in question isn't running anymore. If you suspect your drive is acting up (i.e. Mac fails to boot sometimes, freezes, hangs, strange sounds come out of the chassis), do a check using Disk Utility's "Verify Disk" function. If the utility displays an error saying "This drive has a hardware problem that can't be repaired," you're pretty much stuck with having to cover the replacement costs on your own. Apple also says, "Back up as much of the data as possible and replace the disk. See an authorized Apple dealer for more information." Which is the sensible thing to do considering that it's not exactly easy to pry open one of these things and reach the hard drive behind the display. But if you're tech savvy and all, grab a suction cup, a screwdriver, and watch this YouTube guide to see how it's done. If you choose to go at it alone, you will do so at your own risk. To read more click **HERE**

Hackers Had Access to Systems of Liquor Store Chain Spec's for 17 Months
SoftPedia, 2 Apr 2014: Spec's, a liquor store chain based in Houston, Texas, has suffered a data breach. Cybercriminals had access to the computer systems of 34 stores for a total of 17 months, during which they might have stolen the details of as many as 550,000 customers and employees. In a statement published on its website last week, Spec's revealed that the attack started on October 31, 2012. The attackers had access to the company's systems until March 20, 2014. The attackers had access to payment card and check information. The payment card data includes names, credit and debit card numbers, expiration dates and security codes. The check information includes bank account numbers, bank routing numbers, dates of birth and, in some cases, driver's license numbers. The 34 affected stores (Spec's has a total of 165 stores) are said to be small neighborhood stores in College Station, Corpus Christi, El Paso, and the Greater Houston area. The list of impacted establishments includes Copperfield Liquors, JJ's Liquors, Cowtown Discount Liquors, Restaurant & Bar Supply, Warehouse Liquors (in Corpus Christi), The Beverage Shoppe, Richard's Fine Wines & Spirits. The company says that Rio Grande Valley stores, the Houston superstore and shops in North and Central Texas are not affected. "Thankfully, most of our customers were not affected. While it is a relief that fewer than 5% of our total transactions may have been impacted, that in no way diminishes our great concern for those affected," Spec's said in a statement published on its website. The company's representatives have told the Houston Chronicle that fewer than 550,000 customers and Spec's employees are impacted. They've clarified that the security hole exploited by the cybercriminals was patched. The malware used to exfiltrate data has been removed and cash registers at affected locations have been replaced. Spec's spokeswoman Jenifer Sarver told the Houston Chronicle that it was a sophisticated cyberattack by a group that went to great lengths to ensure that it could not be identified. "It took professional forensics investigators considerable time to find and understand the problem then make recommendations for Spec's to fully address and fix them," Sarver said. Evidence has been provided to the US Secret Service. There's no indication that this was an insider breach. Spec's advises customers to place a fraud alert on their files with the major credit bureaus. In addition, all those who have made purchases at one of the 34 locations between October 2012 and March 2014 are being offered one year of free fraud resolution services with AllClear ID. Starting today, April 2, the firm is launching a hotline at 1-855-731-6017 for those who might have any additional questions. To read more click **HERE**

Over 10,000 Romanian Websites Compromised in 2013, CERT-RO Reports
SoftPedia, 2 Apr 2014: CERT-RO, Romania's National Computer Security Incident Response Team, has published a cyber-security alerts report for 2013. The study details malware infections, compromised websites, phishing, spam and even advanced persistent threats (APTs). The organization says it has collected a total of 43,231,149 alerts from automated systems, involving a total of 2,213,426 unique IP addresses. The number of manually collected alerts is 450. The figures show that a total of 10,239 .ro domains were compromised in 2013. This number represents around 1.4% of the total number of domains. There are around 710,000 domains registered in Romania. CERT-RO's report reveals that 60% of the compromised domains were infected with some sort of malware. 27% of the affected sites were defaced and 13% were used to host phishing sites. Over 33.6 million of the alerts recorded by the agency were related to botnets (botnet drone), over 6.7 million to vulnerabilities (open resolvers), close to 2 million to abusive content (spam) and half a million to information harvesting. There are around 13.5 million IP addresses allocated to Romania. More than 16% of them were involved in at least one cyber security alert in 2013. It turns out that Conficker (Downup) infections are still highly common in Romania. Over 12.5% of the IPs allocated to Romania are said to have been infected with the worm. In fact, 40% of the alerts collected last year refer to Conficker worm infections. In addition to Conficker, which accounts for 53% of infections, the list of common malware infections also includes Sality (11%), Citadel (8%), Pushdo (7%) and ZeroAccess (3%). As expected, most of the computers involved in cyber security incidents are running Windows, followed by Solaris and Linux. When it comes to APTs, Romanian organizations were targeted in two major operations last year: MiniDuke, with 6 infected victims, and Red October, with 55 unique IPs targeted. "It is worth noting that Romanian entities are becoming more frequent targets for APT threats, respectively cyber-attacks with a high degree of complexity, launched by groups that have the capacity and motivation to persistently attack a target in order to obtain certain benefits

(usually sensitive information),” CERT-RO noted in its report. Experts believe a growth in the number and severity of APT attacks should be expected in 2014. An important conclusion of the report is that computer systems in Romania are used by foreign attackers as a proxy, and the country shouldn’t be viewed as a “generator of cyber security incidents.” The full cyber security alerts report (**LINK**) from CERT-RO is available on the organization’s website. To read more click **HERE**

$34,000 / €25,000: Amount of Money Cybercriminals Make Each Month with CryptoDefense
SoftPedia, 1 Apr 2014: Security researchers from Symantec have been monitoring CryptoDefense, a piece of ransomware that’s similar to the notorious CryptoLocker. Based on the Bitcoin addresses and blockchain information, experts estimate that CryptoDefense earns cybercriminals as much as $34,000 / €25,000 per month. CryptoDefense is a relatively new piece of ransomware. It appeared in late February 2014, but Symantec’s products have already blocked over 11,000 unique infections. Infections have been spotted in more than 100 countries. Most are in the United States, the United Kingdom, Canada, Australia, Japan, India, Italy and the Netherlands. Similar to CryptoLocker, CryptoDefense encrypts the most important files on compromised computers and holds them that way until a ransom is paid by the victim. In order to secure its communications, the malware uses Tor. To make sure encrypted files cannot be recovered without paying the ransom, RSA 2048 encryption is used. Symantec experts say the threat is being distributed with the aid of spam emails that purport to carry a scanned copy of a document. When it’s executed, CryptoDefense connects to four remote domains to which it sends basic information on the infected device. Then, the files on the computer are encrypted and the private key is sent back to the server. Next, a screenshot of the compromised desktop is taken and uploaded to the cybercriminals’ server. Instructions with the ransom demands are added to every folder containing encrypted files. Victims are told how to make the payment and how to recover their files. The attackers demand the payment of 500 USD/EUR. The cost doubles if the payment is not made within four days. Fortunately for victims, there is a way to recover their files without paying the ransom. Although they’ve implemented RSA 2048 encryption, the developers have neglected one important aspect: the decryption key is not removed after being sent to the server. “As advertised by the malware authors in the ransom demand, the files were encrypted with an RSA-2048 key generated on the victim’s computer. This was done using Microsoft’s own cryptographic infrastructure and Windows APIs to perform the key generation before sending it back in plain text to the attacker’s server,” Symantec experts explained. “However, using this method means that the decryption key the attackers are holding for ransom, actually still remains on the infected computer after transmission to the attackers server,” they added. “Due to the attackers poor implementation of the cryptographic functionality they have, quite literally, left their hostages a key to escape.” Additional details on the CryptoDefense ransomware are available on Symantec’s blog (**LINK**). To read more click **HERE**

CyberTab: Free Tool That Helps Organizations Calculate Cost of Cyberattacks
SoftPedia, 1 Apr 2014: If your company has become the target of a cybercriminal operation, or if you fear that it might soon be targeted in a certain type of attack, it could be very useful to understand and evaluate the damage and the costs. CyberTab is a free tool that does just that. Released by The Economist Intelligence Unit and sponsored by Booz Allen Hamilton, CyberTab is an easy-to-use tool that can estimate the financial impact of a cyberattack. Users have to specify their industry, their revenue, number of employees, number of customers, the type of attack, details on how it was detected, and attack-related expenses, and they get a detailed report explaining total costs. This enables a cost-benefit analysis of security strategies. CyberTab can be useful to information security, risk, financial and other types of senior executives. CyberTab doesn’t collect any data without permission and it doesn’t ask for any information that could identify users. “Executives can gain new insight into their own company’s risks by using CyberTab, and can do so anonymously and leave no trace of their data,” said Riva Richmond, editor at The Economist Intelligence Unit. “But we want people to be part of the solution and take part in our research programme. By submitting data anonymously, they will be taking a step towards a broader understanding this complex problem.” CyberTab is available on Booz Allen Hamilton’s website (**LINK**). To read more click **HERE**

FireEye Analyzes the 11 Zero-Day Vulnerabilities It Uncovered in 2013
SoftPedia, 31 Mar 2014: IT security company FireEye has published a new report detailing the eleven zero-day vulnerabilities the company discovered last year. The same technology that was used to analyze these security holes was leveraged earlier this year to uncover two more zero-days. “Advanced threats against enterprises today thrive on exploiting the unknown and evading blocking techniques thanks to a growing, global marketplace for selling software vulnerabilities,” explained Zheng Bu, vice president of security research at FireEye. “The old security model of tracking known threats and relying on signature-based solutions are simply powerless to stop zero-day threats. The number of zero-day attacks profiled in the paper highlight why organizations need to take a new approach to security by combining next-generation technology with human expertise.” FireEye discovered the following vulnerabilities in 2013: CVE-2012-4792, CVE-2013-0422, CVE-2013-0634, CVE-2013-0640, CVE-2013-0641, CVE-2013-1493, CVE-2013-1347, CVE-2013-3893, CVE-2013-5065, CVE-2013-3918 and CVE-2014-0266. These zero-days have been used in the attacks that involved the websites of the Council on Foreign Relations, the LadyBoyle cyber espionage campaign, Tobfy ransomware attacks, an operation against Japanese organizations, the Sunshop campaign, the US Department of Labor watering hole attack, the Deputy Dog operation, and Operation Ephemeral Hydra. “While FireEye's ‘Less Than Zero’ paper is a must-read for security professionals, it is equally important for business executives as a means for understanding what they are up against,” noted Jon Oltsik, senior principal analyst at the Enterprise Strategy Group. “Today's sophisticated cyber adversaries can easily circumvent existing security controls, penetrate corporate networks, and may ultimately be used to steal extremely valuable data. CEOs must come to terms with these threats and make sure to align them with their overall risk management, business planning, and fiduciary responsibilities.” The report highlights the fact that system-level protections set in place by many organizations are becoming less and less effective against zero-day attacks. Although DEP and ASLR systems are a step in the right direction, cybercriminals have started finding ways to bypass them. Watering hole attacks are becoming more common because they can be highly efficient in targeting a certain industry. In such attacks, the victims come to the traps (compromised websites) set up by the cybercriminals, which means that they no longer have to worry about findings ways to penetrate the targeted organization’s systems. The complete report on the zero-days identified by FireEye in 2013 is available on the company’s website. The whitepaper also contains some recommendations for organizations on how to protect their networks against cyberattacks that rely on zero-days. To read more click **HERE**