The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
13 February 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

February 12, Softpedia – (International) **Bitstamp suspends Bitcoin withdrawals due to DOS attack.** Bitcoin exchange service Bitstamp began suspending withdrawals while dealing with a denial of service (DoS) attack exploiting a transaction malleability issue. Source: http://news.softpedia.com/news/Bitstamp-Suspends-Bitcoin-Withdrawals-Due-to-DOS-Attack-426249.shtml

February 11, Softpedia – (International) **Corkow trojan targets bank customers, Bitcoin owners and Android developers.** Researchers at ESET have monitored the use of a modular banking trojan known as Corkow that can be fitted with additional capabilities and is able to steal keystrokes, screenshots, and inject phishing pages. The malware also appears to be targeting Android developers and the login credentials for Bitcoin Web sites. Source: http://news.softpedia.com/news/Corkow-Trojan-Targets-Bank-Customers-Bitcoin-Owners-and-Android-Developers-426056.shtml

February 12, Help Net Security – (International) **400Gbps NTP-based DDoS attack hits Cloudflare.** Cloudflare confirmed February 10 that one of its customers was being targeted by a massive distributed denial of service (DDoS) attack that utilized Network Time Protocol (NTP) reflection. The attack reached over 400 gigabits per second and misused over 4,500 NTP servers. Source: http://www.net-security.org/secworld.php?id=16350

February 12, Softpedia – (International) **Bitcoin-stealing Mac malware distributed via Download.com and MacUpdate.** Researchers from SecureMac analyzed the CoinThief Bitcoin-stealing malware for OS X and found that it is being distributed under various names on several legitimate Web sites, including MacUpdate and Download.com. Source: http://news.softpedia.com/news/Bitcoin-Stealing-Mac-Malware-Distributed-via-Download-com-and-MacUpdate-426284.shtml

February 11, IDG News Service – (International) **Microsoft addresses critical IE vulnerabilities for Patch Tuesday.** Microsoft released its monthly Patch Tuesday round of patches February 11, including 7 bulletins, 4 of which were rated critical, closing a total of 31 vulnerabilities. Source: http://www.networkworld.com/news/2014/021114-microsoft-addresses-critical-ie-vulnerabilities-278672.html

February 11, Threatpost – (International) **Adobe patches critical vulnerabilities in Shockwave.** Adobe released a patch February 11 for its Shockwave Player, closing a critical vulnerability in the platform that could allow an attacker to remotely take control of an affected system. Source: http://threatpost.com/adobe-patches-critical-vulnerabilities-in-shockwave/104207

February 11, Computerworld – (International) **Windows XP isn't the only software getting the knife in 8 weeks.** Microsoft will cease support and no longer issue security updates for its Office 2003 and Exchange Server 2003 after April 8, the same date it will cease support for the Windows XP operating system. Source: http://www.networkworld.com/news/2014/021114-windows-xp-isn39t-the-only-278675.html

February 11, Help Net Security – (International) **Older Flash Player vulnerability exploited in the wild.** Researchers at Microsoft discovered several recent attacks exploiting a Flash Player vulnerability that was patched in November 2013, which attempts to install a trojan downloader on vulnerable computers. Source: http://www.net-security.org/secworld.php?id=16343

Experts warn of coming wave of serious cybercrime

Washington Post, 13 Feb 2014: Nearly two dozen companies have been hacked in cases similar to the Target breach and more almost certainly will fall victim in the months ahead, the FBI recently warned retailers, according to an official who was not authorized to speak publicly. Not all of the compromised firms have been publicly identified, nor is it clear how many shoppers' credit card numbers and other personal data have been stolen. Banks, retailers and policymakers have been slow to address the growing sophistication of cybercriminals. Only 11 percent of businesses have adopted -industry-standard security measures, said a recent report by Verizon Enterprise Solutions, and outside experts say even these "best practices" fall short of what's needed to defeat aggressive hackers lured by the prospect of a multimillion-dollar heist. "You're going to see more and more people trying this," said Nicolas Christin, a security researcher at Carnegie Mellon University. "If you just saw your neighbor win the lottery, even if you weren't interested in the lottery before, you may go out and buy a ticket." Cybercrime cost U.S. companies an average of $11.5 million in 2012, according to a study by the Ponemon Institute, up 26 percent compared with the previous year. The effect on consumers can last for years, as they are left vulnerable to bogus charges and potential identity theft. Experts say that reversing the rise in major data breaches would require expensive upgrades, including the adoption of end-to-end encryption, the walling-off of the most sensitive data on separate networks, and the adoption of newer credit card technology that holds customer information on an embedded chip rather than the familiar black magnetic strip now on most American cards. Credit card chips can communicate with banks in a way that better protects a user's private information, often requiring a personal identification number to verify a purchase. Such systems are widespread in most of the developed world but are appearing in the United States only gradually. "Our decades-old payment system was not designed with cybersecurity in mind," said Christopher Soghoian, principal technologist at the American Civil Liberties Union. "Times have changed. Data breaches now occur on a weekly basis, the result of which is that consumers become victims of fraud and identity theft." An industry group including the major American credit card issuers are pushing for widespread adoption of chip cards by October 2015. Consumer groups want Washington to mandate a faster and more complete shift, but federal regulators have balked at forcing the politically influential banking industry to invest in new technology, especially if there is a chance that it might not thwart future attacks. In a sign of the growing concern over credit card security, Congress held four hearings last week to examine whether the industry and the government are doing enough to protect consumers. Tuesday's meeting featured officials from the largest retailers at the center of the recent run of data breaches. "The unfortunate reality is that we suffered a breach, and all businesses — and their customers — are facing increasingly sophisticated threats from cybercriminals," John J. Mulligan, Target's chief financial officer, told lawmakers. Hackers lifted 40 million debit and credit card numbers from Target customers during the holiday season. The company later said thieves also grabbed personal information, including names, home addresses and telephone numbers, of an additional 70 million customers in that attack. Other companies, including craft store Michael's and hotel-management firm White Lodging Services, have since reported breaches of their computer systems. "I think we're going to hear a lot about these breaches over the next year," said Brian Krebs, a cybersecurity journalist who blogs at KrebsOnSecurity.com. "It just looks like some of the guys involved in this activity have compromised a ridiculous number of companies." Krebs reported that the Target breach happened after criminals gained access to the company networks through a contractor that was servicing heating and air-conditioning systems at several stores. Department store Neiman Marcus also was attacked recently. Its senior vice president, Michael Kingston, told lawmakers Tuesday that the company's antivirus software was virtually useless in defending its computers. The retailer didn't detect that its credit card systems were being hacked, and the company did not learn of the intrusion until the beginning of January, many months after it began. His reference to antivirus software drew scoffs from security experts, who compare the protections offered by such programs to a flu shot — capable of staving off infection from wide and unfocused threats but of little value against a serious attacker determined to breach a specific network. Security experts say companies must install systems that detect and halt intrusions quickly, before massive amounts of personal data can be lost. "Companies need to be hunting on their networks constantly .?.?. looking for signs of compromise," said Shawn Henry, former head of cybercrime for the FBI and now president of Crowdstrike Services, a security company. "If you give people unfettered access for weeks and months and years, they can do a lot of damage." The recent conviction of Russian national Aleksandr Andreevich Panin in federal court offers a window into the robust market for malicious software. Panin, the architect of SpyEye malware, sold his virus for as little as $1,000 online through invitation-only forums, prosecutors said. At least 150 hackers snagged versions of SpyEye between 2009 and 2011, using the virus to set up servers designed to steal money from bank accounts. One customer made more than $3.2 million in six months using the virus. Panin's code, which automates the theft of user names, passwords and PINs, infected more than 1.4 million computers worldwide. To read more click **HERE**

Only 17% of UK Business Leaders Consider Cybersecurity a Top Priority, Study Finds
SoftPedia, 13 Feb 2014: Telecoms company BT has published a report that analyzes the cybersecurity readiness of UK companies. Compared to organizations in the United States, ones in the United Kingdom are lagging behind. For instance, 41% of US business leaders consider cybersecurity a top priority. In the UK, only 17% do so. And it's not only the US that's better than the UK in this category. Brazil, Singapore, France, Hong Kong and Germany also top it. Furthermore, only 21% of IT decision makers in Britain are capable of measuring the return on investment (ROI) of their cyber security systems. In the US, 90% of firms can do it. As far as IT security training is concerned, only 37% of Britain's senior decision makers and directors benefit from it. In the United States, on the other hand, the percentage is 86. So what are decision makers most afraid of? On a global scale, non-malicious insider threats are currently cited by most as the number one concern. In Britain, the most commonly cited security concerns are non-malicious insider threats (60%), malicious insider threats (51%), hacktivism (37%) organized crime (32%), state-sponsored actors (15%) and terrorism (12%). "The research provides a fascinating insight into the changing threat landscape and the challenge this poses for organisations globally," said Mark Hughes, CEO of BT Security. "The massive expansion of employee-owned devices, cloud computing and extranets, have multiplied the risk of abuse and attack, leaving organisations exposed to a myriad of internal and external threats – malicious and accidental," he added. "US businesses should be celebrated for putting cyber security on the front foot. The risks to business are moving too fast for a purely reactive security approach to be successful. Nor should cyber security be seen as an issue for the IT department alone." The complete report is available on BT's website [**LINK**]. To read more click **HERE**

Fake "Track Shipments/FedEx" Emails Used to Distribute Malware
SoftPedia, 13 Feb 2014: In case you've shipped a parcel via FedEx, you should be careful if you receive a legitimate-looking email that informs you of the fact that it has been delivered. Cybercriminals are using such notifications to spread malware. The emails carry the subject line "Track shipments/FedEx" and they contain information on the alleged shipment. Dynamoo's Blog reports that the links in these emails point to a website that's set up to serve an archive file called "track_shipments_FedEx.zip." The ZIP contains an executable that has a very long name: "Track_shipments_ FedEx_Office_orders_summary_ results_Delivered_tracking_ number_9384758293431234834312 _idju2f83f9hjv78fh78.doc.exe". Although it looks like a harmless Word document, in reality, the file is a piece of

malware that's currently detected by 28 of the antivirus engines on VirusTotal. The threat appears to be a Trojan downloader. To read more click **HERE**

Oracle Confirms Existence of 30 Security Holes in Java Cloud Service
SoftPedia, 13 Feb 2014: Security Explorations has informed me that Oracle has confirmed the existence of the 30 Java Cloud Service security issues reported to the company in late January. All of the 30 flaws have been confirmed by Oracle. Over half of them can be exploited to completely bypass the Java security sandbox. Security Explorations CEO Adam Gowdiak says that Oracle has not informed them of any specific plans regarding the security fixes. However, Oracle will provide the security research firm status updates on the 24th of each month. According to Gowdiak, the nature of these vulnerabilities shows that Oracle hasn't put too much effort into making sure that the Java Cloud Service is secured properly. "They illustrate known and widely discussed security risks related to Java. They also expose weak understanding of Java security model and attack techniques by Oracle engineers," he said. To read more click **HERE**

Obama Administration Announces Final Version of Cybersecurity Framework
SoftPedia, 13 Feb 2014: The final version of the Cybersecurity Framework has been released [**LINK**]. Work on the framework, which aims at helping organizations in the critical infrastructure sector, started one year ago, when US President Barack Obama signed an executive order on "Improving Critical Infrastructure Cybersecurity." During this year, organizations and individuals from the United States and other countries have contributed with guidelines, best practices and standards. The best ideas have been incorporated into the voluntary Cybersecurity Framework by the National Institute of Standards and Technology (NIST). The framework provides a road map to show organizations the steps they need to take in order to secure their systems. It has three main components, designed so that they reinforce the connection between cybersecurity and business drivers. The first component is the core, which represents a set of activities and informative references that are common for all sectors. The cybersecurity activities are grouped into five categories: identify, protect, detect, respond and recover. The second component is "Profiles." This enables organizations to align their cybersecurity with business requirements, resources and risk tolerance. The profiles can be used not only to determine a company's current posture, but also to measure progress. The last component, called Tiers, is designed to help organizations in managing cyber risk. The tiers are numbered from 1 to 4 (1 being "partial" and 4 being "adaptive"). They're used to describe various factors, such as the degree of rigor in risk management practices, and the integration of cybersecurity risk management into the organization's overall risk management practices. Critical infrastructure organizations are not forced to adopt the Cybersecurity Framework. So, in order to encourage them to do so, the DHS has established the Critical Infrastructure Cyber Community (C3) Voluntary Program to encourage its adoption. It's worth noting that critical infrastructure organizations from all over the world can use the Cybersecurity Framework, not just ones from the US. To read more click **HERE**

Microsoft Rolls out Updated Malicious Software Removal Tool for Windows
SoftPedia, 12 Feb 2014: Redmond released a new version of the Microsoft Malicious Software Removal Tool on Patch Tuesday, thus lending a hand to users who are trying to get rid of specific infections from their computers. While the company is yet to disclose some official release notes for version 5.9, the fresh build most likely comes with detection and cleaning capabilities for new forms of malware, which means that you can remove even more infections from your computer. Of course, the application continues to provide support for all Windows versions still on the market right now, starting with the old XP and ending with the newly-launched 8.1. The program will continue to support Windows XP after April 8, the date when the ancient operating system will go dark, so it might be a good idea to download Microsoft Malicious Software Removal Tool 5.9 [**LINK**] right now to stay on the safe side. To read more click **HERE**

RedHack Leaks Contact Information of US Embassy Staff
Softpedia, 12 Feb 2014: Hackers of the RedHack group have leaked the contact information for 36 staff members of the US Embassy in Turkey. The hacktivists have published a list of names, email addresses, job titles and phone numbers. A RedHack representative has told me that the information has been leaked in memory of Sinan Cemgil, one of the founders of Turkish People's Liberation Army. The slogan accompanying the leaked information, "We have learned only three words of English at METU: Go home Yankee," was used by Sinan in the 1960s in protest against the United States' politicians and military. Now, the hacktivists send a message to the United States, telling it not to interfere in Turkey and other Middle Eastern countries. RedHack says it protests against the US government, but it doesn't have anything against the American people. The hackers accuse the US, China and Russia of occupying other countries with their military under a slogan of "peace," after which they engage in "economical occupation." To read more click **HERE**