The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

16 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

REMINDER – HACKERS CONSISTENTLY TARGET ORACLE AND ADOBE PRODUCTS – MAKE SURE YOU APPLY THESE PATCHES AS SOON AS POSSIBLE!

January 15, Softpedia – (International) **Oracle fixes 144 vulnerabilities, including 36 Java flaws, with January 2014 CPU.** Oracle released its January Critical Patch Update (CPU) January 14 which includes fixes for 144 vulnerabilities in several products, including 36 vulnerabilities affecting Java SE components. Source: http://news.softpedia.com/news/Oracle-Fixes-144-Vulnerabilities-Including-36-Java-Flaws-with-January-2014-CPU-417058.shtml

January 15, Softpedia – (International) **Adobe Flash Player 12 addresses critical vulnerabilities.** Adobe released the latest version of its Flash Player 12, closing two serious vulnerabilities that could allow an attacker to run malicious native code and take control of a system. Source: http://news.softpedia.com/news/Adobe-Flash-Player-12-Addresses-Critical-Vulnerabilities-417086.shtml

January 15, Softpedia – (International) **Adobe Reader and Acrobat 11.0.06 hold critical security improvements.** Adobe released updates for its Reader and Acrobat products which close three critical security vulnerabilities which could allow an attacker to crash the application and gain control over affected systems. Source: http://news.softpedia.com/news/Adobe-Reader-and-Acrobat-11-0-06-Hold-Critical-Security-Improvements-417178.shtml

January 15, Softpedia – (International) **Google Chrome 32.0.1700.77 security fixes.** Google released a new version of its Chrome browser January 14, closing several vulnerabilities and implementing new security features. Source: http://news.softpedia.com/news/Google-Chrome-32-0-1700-77-Security-Fixes-417267.shtml

January 15, IDG News Service – (International) **Spammers target Google hospitality listings.** Google worked to fix hospitality-related listings on its services January 14 after receiving a report that spammers had replaced direct links to several hotel Web sites with links that redirect to other sites in order to receive payment through an affiliate marketing network. Source: http://www.computerworld.com/s/article/9245428/Spammers_target_Google_hospitality_listings

January 15, Softpedia – (International) **Android gamers targeted with trojanized version of Minecraft PE.** Researchers at F-Secure identified a malicious Android version of the game Minecraft available on some third-party application marketplaces which could be used by cybercriminals to send SMS messages to premium rate numbers. Source: http://news.softpedia.com/news/Android-Gamers-Targeted-with-Trojanized-Version-of-Minecraft-PE-417176.shtml

January 14, SC Magazine – (International) **Light Patch Tuesday addresses 6 bugs, including XP zero-day, with 4 bulletins.** Microsoft released its monthly Patch Tuesday round of patches January 14, addressing six vulnerabilities in its products, including a zero-day vulnerability in Windows XP and Server 2003. Source: http://www.scmagazine.com/light-patch-tuesday-addresses-6-bugs-including-xp-zero-day-with-4-bulletins/article/329325/

16 Saudi Arabian Government Websites Hacked by Syrian Electronic Army

SoftPedia, 16 Jan 2014: Hackers of the Syrian Electronic Army have breached and defaced a total of 16 Saudi Arabian government websites. The targeted sites are the ones of various administrative regions, also known as principalities. The attacks have been launched under the banner #ActAgainstSaudiArabiaTerrorism. On the defaced pages, the hackers posted a message in which they condemn the Al Saud regime, which they accuse of using terrorist groups for its dirty work. At the time of writing, the impacted websites have been taken offline. However, this doesn't mean that the hackers have stopped targeting Microsoft. They say that more attacks will follow in the upcoming period. Recently, hackers of the Turkish group Turkguvenligi have breached the SEA's website through its hosting provider. The Syrian hackers say their website will remain offline until they can find another hosting company that will accept their site. "While that our operations and hacks will continue normally, we will keep you updated on our social media sites," they noted. To read more click **HERE**

Class Action Filed Against Neiman Marcus Following Data Breach

SoftPedia, 16 Jan 2014: A class action has been filed against Neiman Marcus, the high-end retailer that suffered a data breach in which customer payment card information has been compromised. SC Magazine reports that the lawsuit has been filed in the Eastern District of New York on Monday. Equitable relief is sought for impacted customers. However, one woman, Melissa Frank, is the lead plaintiff because her credit card has already been used by fraudsters. She believes the unauthorized transactions are a result of the breach suffered by Neiman Marcus. The plaintiffs say the damages in the incident exceed $5 million (€3.67 million). The company is accused of failing to implement proper security measures to protect its customers' personal information. A number of US retailers suffered data breaches over the past holiday season, including Target and three smaller ones that haven't been named yet. Target has admitted that 40 million payment cards have been compromised. In the case of Neiman Marcus, the number of impacted individuals has not been made public. To read more click **HERE**

RedHack Leaks Phone Numbers of Turkcell Employees

SoftPedia, 16 Jan 2014: Hackers of the RedHack collective have leaked the phone numbers of over 4,000 people who work for Turkcell, the leading mobile phone operator of Turkey. Lawmakers in Turkey have recently drafted a bill that allows authorities to block access to certain websites and it will force ISPs to keep detailed records of Internet users' online activities for one or two years. As expected, the bill sparked a lot of controversy and hackers of the RedHack group almost immediately stepped into play. The hacktivists leaked the phone numbers of deputies and ministers just as the bill was being debated in Parliament. They also published the phone number of Prime Minister Recep Tayyip Erdogan's son. Shortly after the information was published, Turkcell changed the phone numbers of impacted officials. In response to Turkcell's actions, the hacktivists have now leaked the phone numbers of the company's own employees. "We are warning these thieves and those GSM operators protecting them: Censorship is a crime against humanity and those who defend this crime are our targets," the hackers said, cited by Hurriyet Daily News. "We exonerate those Turkcell workers who are not involved in the incident. Here are the numbers of the 4,164 people who work at the Turkcell call center," they added. The supporters of the Internet censorship legislation argue that the bill will line up Turkey with other, more developed countries. However, critics say the law would actually turn Turkey into a country like China, where Internet users have many restrictions. This latest leak from RedHack comes shortly after the group

hacked into the systems of the Ankara transport department. The files found on the organization's networks allegedly demonstrate the wrongdoings of Melih Gökçek, the capital city's mayor. To read more click **HERE**

Microsoft Admits That Syrian Hackers Also Hijacked Its Email Accounts

SoftPedia, 16 Jan 2014: Microsoft had two really tough weeks in the beginning of 2014, as several of its social accounts and blogs got hijacked by Syrian hackers who used them to post anti-Microsoft messages. The Syrian Electronic Army is the group behind the recent attacks, and even though Redmond has taken the necessary steps to make sure that no similar security breaches would be discovered in the near future, more similar hack attempts would follow soon, according to a recent tweet. Redmond, on the other hand, decided to break the news with more information on what actually happened in early 2014, admitting that Facebook, Twitter, and blog accounts were not the only ones affected by the recent hacks. It turns out that the SEA also managed to break into company email accounts and even posted some conversations between Steve Clayton, who is in charge of the social accounts, and Frank Shaw. But according to a statement released by Microsoft for ITProPortal, no user data was compromised following these attacks, and the company still works to make its accounts more secure. "A social engineering cyberattack method known as phishing resulted in a small number of Microsoft employee social media and email accounts being impacted. These accounts were reset and no customer information was compromised," the company noted in a statement. But what's worse is that Microsoft's employees don't seem to have a well-developed sense of security when it comes to protecting their email accounts. According to the Syrian Electronic Hackers, a Microsoft employee was using the phrase "Microsoft2" as password for his account and, after he got hacked, he changed it to… "Microsoft3." "A Microsoft employee wanted to make his password more stronger, so he changed it from 'Microsoft2' to 'Microsoft3' #happened," the hackers said in tweet whose legitimacy cannot be verified. To read more click **HERE**

Twitter Account of Indian Minister Shashi Tharoor Hacked

Softpedia, 16 Jan 2014: The official Twitter account of the Indian Minister of State for Human Resource Development, Shashi Tharoor, has been hacked this week. The hacker posted some tweets from the hijacked account that made it look like Tharoor had an "affair" with a Pakistani writer. "I'm not crying any more. I'm not falling to pieces. I'm more lucid than ever. How little I knew you became visible to me," the "official" wrote in a tweet addressed to Palkistani writer Mehr Tarar. "You unfollowed me. You don't RT me and you don't answer me on twitter. I can live with your facourites. I have your personal validation," another tweet read. Mehr was confused about the tweets at first, but she soon realized something was amiss, DNA India reported. Later, Tharoor confirmed that his Twitter had been hacked, and deactivated the account. It later turned out that the Twitter account of Tharoor's wife, Shashi Tharoor, was also hijacked. The following joint statement was published on Tharoor's Facebook account to clarify that they are happily married. "We are distressed by the unseemly controversy that has arisen about some unauthorised tweets from our Twitter accounts," the couple noted. "Various distorted accounts of comments allegedly made by Sunanda have appeared in the press. It appears that some personal and private comments responding to these unauthorised tweets -- comments that were not intended for publication -- have been misrepresented and led to some erroneous conclusions," they added in the statement on Facebook. "We wish to stress that we are happily married and intend to remain that way. Sunanda has been ill and hospitalised this week and is seeking to rest. We would be grateful if the media respects our privacy." To read more click **HERE**

Windows XP: Three More Patch Tuesdays to Go

SoftPedia, 16 Jan 2014: Windows XP remains a very popular operating system, but despite the big market share it has right now, Microsoft plans to discontinue it on April 8 this year. If the company doesn't change its plans, this means that only three more Patch Tuesdays will see Windows XP on the market and, just like WindowsITPro reports, the operating system would then become fully vulnerable to attacks. This month, Windows XP got its zero-day flaw patched, while we're hearing that Microsoft has also silently fixed the SVCHOST error that caused CPU usage to skyrocket when

launching Windows Update. Microsoft hopes that Windows XP's 28 percent market share would drop to 13 percent by April and even though that seems to very unlikely, it's still a sign that Redmond should delay the end of support a little bit, just to make sure that everyone is ready for the big moment. To read more click **HERE**

Healthcare.gov Could Suffer an Insider Breach, Experts Predict

SoftPedia, 16 Jan 2014 SpectorSoft, a company that specializes in user activity monitoring and analysis software, has published its predictions for 2014. The predictions are interesting because they're from the perspective of insider threats. Ever since it was launched in the autumn of 2013, Healthcare.gov has experienced numerous problems, including security and privacy-related issues. SpectorSoft believes the healthcare service might experience an insider-driven breach carried out by someone who has access to sensitive information. Why would someone do that? They might do it to make a political statement, to embarrass those who support the program, to gain fame, or stall progress. Experts also believe that C-level executives whose companies suffer data breaches will get involved more, not only for public relations reasons, but also to approve payments to mitigation services providers. They will also become more involved with security operations, and they'll support investments for security solutions that protect the company against both insider and external threats. Organizations have always been concerned about the access rights of privileged users, but after the Edward Snowden incident, it's likely that they'll focus even more on this area. Up until now, enterprises haven't been too keen on publicly disclosing details of their IT security programs, in many cases because they didn't want potential threat actors to think they had large volumes of valuable data that might be worth targeting. However, as consumers and business customers start demanding increased levels of privacy and data security, organizations will start publicizing their IT security programs to win their customers' trust. In 2014, more value will be placed on threat intelligence systems that can detect threats and provide alerts in real time. This initiative will be driven by the increasing number of news headlines about data breaches carried out by both insiders and external actors. To read more click **HERE**

UK Government Reportedly Bans Videoconferencing Devices from Huawei

SoftPedia, 16 Jan 2014: The British Home Office, Ministry of Justice, the Crown Prosecution Service and other government departments have allegedly stopped using videoconferencing equipment from Huawei due to concerns that the devices might be plagued by security vulnerabilities that could be exploited for spying. The Sunday Mirror reported that Whitehall became concerned that top level discussions might be intercepted. Huawei representatives have told The Telegraph that their products are secure and that the claims are "misleading." The company has told the South China Morning Post that the reports are inaccurate, but they're taken seriously. The company is investigating the possibility that the equipment in question was sold to the UK government departments through a third party. In mid-December 2013, the British National Security Adviser concluded its investigation into the activities of the Huawei Cyber Security Evaluation Center. The organization recommended that future senior appointments at the cyber security center should be overseen by the GCHQ. To read more click **HERE**

World's greatest hacker calls Healthcare.gov security 'shameful'

Fox News, 16 Jan 2014: Security expert -- and once the world's most-wanted cyber criminal -- Kevin Mitnick submitted a scathing criticism to a House panel Thursday of ObamaCare's Healthcare.gov website, calling the protections built into the site "shameful" and "minimal." In a letter submitted as testimony to the House Science, Space and Technology Committee, Mitnick wrote: "It's shameful the team that built the Healthcare.gov site implemented minimal, if any, security best practices to mitigate the significant risk of a system compromise." Mitnick's letter, submitted to panel Chairman Lamar Smith, R-Texas, and ranking member Eddie Bernice Johnson, D-Texas, held comments from several leading security experts. Mitnick concluded that, "After reading the documents provided by David Kennedy that detailed numerous security vulnerabilities associated with the Healthcare.gov Website, it's clear that the management team did not consider security as a priority." His comments were backed up by testimony by Kennedy, who is CEO and

founder of TrustedSec LLC and a self-described "white hat hacker," meaning someone who hacks in order to fix security flaws and not commit cybercrime. In November, Kennedy and other experts testified before the same panel about security issues on Healthcare.gov. Kennedy testified that most of the flaws they identified at the time still exist on the site, and said "indeed, it's getting worse," telling the panel that he and other experts have seen little improvement in the past two months. Only one-half of a vulnerability has been found and plugged since then, he told the committee. "They did a little bit of work on it and it's still vulnerable today." Also speaking at the panel were Michael Gregg, chief executive officer of Superior Solutions, Waylon Krush, co-founder and CEO of Lunarline, and Dr. Lawrence Ponemon, chairman and founder of the Ponemon Institute. There have been no confirmed security breaches or hacks of the site yet, despite the alarming current and past testimony from the panel. (At the November panel, Kennedy said the website "may have already been hacked.") The flaws that have been found are mere speculation, pointed out Krush, whose firm has done security work for the Department of Health and Human Services. "Nobody here at this table can tell you there is a vulnerability," he said during testimony. To actually test the flaws would require hacking the website itself, which would mean breaking the law, he noted. To read more click **HERE**