The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

5 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

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

February 4, The Register – (International) **Gameover ZeuS adds nasty trick.** A researcher at Malcovery found that a new version of the Gameover ZeuS variant encrypts its .exe file and distributes it as a .enc file to avoid detection by security software. A phishing email with an attachment containing a new version of UPATRE is then used to decrypt and execute the file. Source: http://www.theregister.co.uk/2014/02/04/gameover_zeus_adds_nasty_trick/

February 4, Softpedia – (International) **NameChanger Fake AV has over 200 names, uses social engineering kit to spread.** A researcher at Fox-IT found that the group behind the Tritax fake antivirus malware is using three variants of the NameChanger using over 200 names to disguise the malware. The fake antivirus malware has been distributed using compromised, high-profile Websites such as DailyMotion, Business Insider, and ads on Skype. Source: http://news.softpedia.com/news/NameChanger-Fake-AV-Has-over-200-Names-Uses-Social-Engineering-Kit-to-Spread-423566.shtml

February 4, Softpedia – (International) **Experts identify 12 rogue Chrome extensions installed by 180,000 users.** Researchers at Barracuda Labs identified 12 extensions for Google's Chrome browser that injects ads on 44 popular Web sites, with the rogue ads designed to make money for the extensions' developers. Source: http://news.softpedia.com/news/Experts-Identify-12-Rogue-Chrome-Extensions-Installed-by-180-000-Users-423645.shtml

Pakistani Hacktivists Target Indian Banks, Government Websites
SoftPedia, 5 Feb 2014: Over the past couple of weeks, Pakistani hacktivists groups have targeted a large number of websites from India. Now, another series of high-profile attacks have been announced. Members of The Hackers Army have defaced the homepage of the official website of India's State Bank of Patiala, The News Informer reported. This financial institution's site has been defaced numerous times over the past period. Hackers of Team Maximizers have also been busy today. They've defaced a couple of subdomains of the state of Kerala (kerala.gov.in). The Pakistan Haxors Crew has targeted the West Bengal State Coastal Zone Management Authority (wbsczma.gov.in) and a portal of the Damodar Valley Corporation (dvc.gov.in). In the case of the West Bengal State Coastal Zone Management Authority, the hacktivists also claim to have obtained the website's database. At the time of writing, most of these websites are still defaced. To read more click **HERE**

St. Joseph Health System Hacked, Attackers Access Details of 405,000 People
SoftPedia, 5 Feb 2014: Cybercriminals operating behind IP addresses in China and other locations have targeted the St. Joseph Health System (SJHS). The organization says the hackers have gained access to a server storing the details of 405,000 patients, employees and employees' beneficiaries. According to SJHS representatives, the breached server stored a combination of names, social security numbers, dates of birth, addresses, medical information and, in some cases, bank account information. The data belongs to employees and patients of the St. Joseph Regional Health Center, the Madison St. Joseph Health Center, the Burleson St. Joseph Health Center, the Grimes St. Joseph Health Center and the St. Joseph Rehabilitation

Center. The attack took place between December 16 and December 18, 2013. The forensic investigation launched by the organization hasn't determined if the exposed data has been stolen, although it could have been. Impacted individuals are being notified. SJHS is offering them free identity protection services for a period of one year. For additional information on this incident, the organization has set up a call center at (855) 731-6011 (8:00 AM to 8:00 PM. CST, Monday – Saturday). To read more click **HERE**

Rogue GOM Player Update That Installed Malware at Japanese Nuclear Plant Analyzed

SoftPedia, 5 Feb 2014: Security researchers have analyzed the malicious GOM Player update file that was installed on a computer at the Monju fast-breeder reactor in Japan. The malware was detected after a worker installed an update for video playback software, namely GOM Player. Kaspersky researchers say the nuclear plant employee responsible for the infection downloaded a file called GoMPLAYER_JPSETUP.EXE. This is actually a self-extracting RAR archive file that contains a legitimate update for GOM Player and another executable in RAR format (GOMPLAYERBETASETUP_JP.EXE). This second archive contains five malicious files that unleash a backdoor detected by Kaspersky as Backdoor.Win32.Miancha. The investigation is ongoing, so Japanese authorities haven't provided too many details on the incident. After news of it came to light, experts noted that this probably wasn't an attack targeted at the nuclear facility, but a random infection caused by an employee's carelessness. However, they've warned that nuclear plants, even defunct ones, should focus more on cybersecurity to prevent such incidents. To read more click **HERE**

Cyber Terrorists Use DDOS Attacks to Disrupt Exchange Platforms, Influence Stock Prices

SoftPedia, 5 Feb 2014: Security experts warn that distributed denial-of-service (DDOS) attacks are increasingly used in an attempt to influence stock prices and disrupt exchange platforms. DDOS attacks are used for various reasons. Hacktivists rely on them to raise awareness, companies to disrupt the competition, and they even represent a handy "tool" for extortionists. However, DDOS protection services provider Prolexic reveals that these types of attacks are posing a significant threat to the financial services industry and trading platforms. "As part of our DDoS attack forensics, we have uncovered a disturbing trend: Many of these malicious attacks appear to be intent on lowering the target's stock price or currency values, or even temporarily preventing trades from taking place," explained Stuart Scholly, president of Prolexic. Experts say they've found a direct link between DDOS attacks and temporary changes in the valuation of companies. That's because an organization's image is closely associated with its online presence. Spreading rumors on the Web about a company or disrupting its website, particularly when it's an exchange platform or a publicly traded firm, can have a serious impact. Prolexic reveals that a small number of cyber terrorist groups are behind most of the attacks aimed at publicly traded companies, trading platforms and the financial services industry. So far, they've failed to launch an attack big enough to cause serious damage. However, experts warn that this threat should be taken seriously, especially since DDOS attacks are becoming more and more sophisticated and powerful. "What's more, the risk goes beyond the actual outage – social media chatter and media coverage can amplify the perceived effect, disruption and damage caused by a cyber-attack campaign," Scholly added. Additional details on global markets DDOS attacks are available in the white paper published by Prolexic (registration required). To read more click **HERE**

13 Security Holes Fixed with the Release of Firefox 27

SoftPedia, 5 Feb 2014: Mozilla has addressed a total of 13 security vulnerabilities with the release of Firefox 27. The list includes four critical, four high, four moderate and one low-impact flaws. The critical vulnerabilities, which can be exploited to execute arbitrary code without user interaction, are a use-after-free during image processing, an issue with image decoding in RasterImage, a crash when terminating a web worker running asm.js code, and miscellaneous memory safety hazards. The high-impact security holes are a cross-origin information leak through web workers, NSS ticket handling problems, and cloning protected XUL elements with XML Binding Language scopes. Boris Zbarsky, a Mozilla developer, has identified an inconsistency with the different JavaScript engines in the way they handle "window"

objects. For additional details on the vulnerabilities fixed in Firefox 27, check out the security advisories. You can download Firefox for all platforms from Softpedia. To read more click **HERE**

Government Websites of India's Largest State Hacked by Pakistani Group
SoftPedia, 5 Feb 2014: Two of the websites of Rajasthan, India's largest state, have been hacked and defaced by a Pakistani group called Voice of Black Hat Hackers. According to E Hacking News, the targeted sites are the ones of the Rajasthan Information and Public Relations Department (dipr.rajasthan.gov.in) and a subdomain that has been created for testing purposes (webmis.rajasthan.gov.in). This is another attack part of the ongoing "cyberwar" for the Kashmir region. "HEY INDIA!; Think again! Salute oh martyr from the land of Kashmir, your last wish to recite verses of holy Quran was not fulfilled. But the dream you lived with, will surely be fulfilled. India will taste defeat. India celebrates this day while not realising what is coming for it now, this won't end the Intifada from Kashmir, you will see more and intense revolution," the attackers said. At the time of writing, the hacktivists' defacement page has been removed from the "webmis" subdomain, but it's still live on the DIPR subdomain. To read more click **HERE**

Adobe Flash Player Receives Emergency Update
SoftPedia, 5 Feb 2014: Adobe rolled out an emergency update for Flash Player 12.0.0.43 in order to fix a vulnerability reported as having an exploit in the wild. In a security bulletin published on Tuesday, the company announced that the security glitch identified as CVE-2014-0497 had been corrected. The issue, classified as an integer underflow, can be leveraged by attackers to execute arbitrary code on the affected system and take control of them remotely and has been defined as critical. The update to version 12.0.0.44 (for Windows and Mac) and 11.2.202.336 (for Linux) of Adobe Flash Player has the highest priority level, which means that administrators are recommended to install it as soon as possible. The versions of the product for Google Chrome and Internet Explorer 10 and 11 are updated automatically to the latest build through the respective browser update mechanisms. To read more click **HERE**

Microsoft Wants Users to Dump Windows XP for a Good Reason, Expert Says
SoftPedia, 5 Feb 2014: Windows XP will be officially discontinued on April 8, but more than 29 percent of the users are still running it right now, which is quite living proof that the transition to another OS won't be completed in time. And still, Microsoft and security experts across the world warn that sticking to XP is very dangerous, especially because cybercriminals could use Windows XP machines to expand their spam networks, as no security patches and updates would be delivered. "If you keep using XP as your general operating system after the cut-off, you won't get security fixes, which of course means you are more likely to get owned and infected with malware. This means you could unintentionally become part of the spam problem," Paul Ducklin, senior security analyst at Sophos, told V3 in an interview. "I don't want to 100 percent say this is inevitable, but it is certainly a very real possibility. The lack of support is going to make XP users harder to defend and crooks know it. Think about when Microsoft issues its first series of patches for Windows 7 and Windows 8 after XP support ends. In this situation a patch for Windows 7 could very well point criminals to the magic hole in Windows XP." Windows XP is at this point the second top OS worldwide, but Microsoft still hopes that it would be able to cut its market share down to 13 percent by the time the retirement date comes. The company has already announced that while Security Essentials would continue to receive updates on Windows XP until mid-2015, no new installations would be allowed on Windows XP once end of support comes, in an attempt to show users that the security risks of staying with this OS version are too big. To read more click **HERE**

Indian Banks Association Issues Warning for Windows XP Users
SoftPedia, 4 Feb 2014: The death of Windows XP is a serious issue not only for consumers, but also for businesses across the world, as many are very likely to stay on this particular OS version many months after end of support comes. Approximately 34,000 Indian banks are very likely to stick to Windows XP after retirement, so the Indian Banks Association (IBA) has decided to issue a warning to emphasize that migration is mandatory. "We request you (banks) to

kindly arrange to take cognizance of the news item and take steps as may be necessary to mitigate the risk of disruption in banking services," IBA Deputy Chief Executive K Unnikrishnan said according to Post. Microsoft itself has added that it's working with banks across India to put transition programs in place, so many are expected to move to either Windows 7 or 8 in the next few months. "We have been in touch with most of the banks on this issue, but we not see any acceleration in their pace over this," Microsoft India GM (Windows Business) Amrish Goyal explained. To read more click **HERE**