The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

4 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

February 3, InformationWeek – (National) **Hotel company investigates data breach, card fraud.** Hospitality company White Lodging Services announced that it is investigating reports of a data breach between March 2013 and late December 2013 that may have exposed customers' payment card information. The company manages 168 hotels in 21 States under franchises including Hilton, Sheraton, Marriott, and Westin. Source: http://www.informationweek.com/security/attacks-and-breaches/hotel-company-investigates-data-breach-card-fraud/d/d-id/1113671

February 3, Softpedia – (International) **PayPal and eBay websites defaced by Syrian Electronic Army.** Attackers claiming affiliation with the Syrian Electronic Army hacktivist group defaced several pages belonging to eBay and PayPal. Affected PayPal pages included pages from the service's French, British, and Indian sites. Source: http://news.softpedia.com/news/PayPal-and-eBay-Websites-Defaced-by-Syrian-Electronic-Army-423075.shtml

January 31, Threatpost – (International) **DailyMotion still infected, serving fake AV malware.** Researchers at Invincea reported that the DailyMotion video-sharing Web site continued to be compromised more than 3 weeks after malicious ads were first found on the site and reported. Source: http://threatpost.com/dailymotion-still-infected-serving-fake-av-malware/104003

Windows XP: It Still Isn't Worth the Risk of Sticking

Yahoo, 3 Feb 2014: With support of Windows XP being pulled in April, 30% of desktop computers are still yet to change to a newer operating system. Windows XP have announced pulling support in the past and have extended the date. With the recent announcement that they will extend their anti-malware support, a lot of companies are knowingly calling Microsoft's bluff and sticking with their lot or, in the face of a computer which switches on every day and does the job as necessary, aren't motivated enough to make the necessary change. Richard Thompson, Sales Director at Central Technology an IT firm based in Chesterfield, says that this time support is going to end and businesses are taking a really worrying risk by not upgrading. Microsoft were first meant to end support for XP in April 2009, but with popularity enduring they decided to extend their support another five years. Officially we're all in the "extended support" period and mainstream support died in 2009, although you'd be hard pushed to find any difference between the two. A lot of people are interpreting this as a sign that Windows can be pushed, and will have to extend the support again. This isn't something anyone should bank on, especially businesses. For those businesses sticking to their guns, hoping to force Microsoft into continuing support by sheer force of numbers, the recent announcement further updates will provided to their antimalware may appear to be a sign that Microsoft are buckling under the pressure. In truth, this will help out consumers who use Microsoft Security Essentials, but won't offer much to the majority of business users. Updates will apply to System Center Endpoint Protection, Forefront Client Security, Forefront Endpoint Protection and Windows Intune. For those businesses who don't use any of these programmes (and there are plenty of them) the announcement means very little. Moreover, the extension isn't much of a guarantee anyway. It doesn't mean that security patches will be updated and

the anti-malware will still be working on an out of date operating system. In essence, this makes a great headline, but it isn't offering as much as you might think. The most compelling reason to change is because of the extent of the risk a business takes by sticking. For those organisations still using XP when support has ended, it will be more a matter of when than if with regards to their IT systems being compromised. And don't think you'll be okay just because you're a small business, everybody is at risk. Just one PC left on Windows XP, just one door open, could be enough for something nasty to get in and take down your entire system or steal confidential information. Keep in mind that there is, on average a 156 day lapse between the time a resource is compromised and the time the compromise is detected – that gives a virus or hacker a very long time to cause damage. But making sure you have sufficient security in place (which means upgrading your OS!) can significantly reduce this time. Another massive issue is compliance. If you manage personal data there are industry regulations you must abide by. Using a non-supported OS will obviously not meet these regulations. Even if Microsoft do relent, which is unlikely, an organisation is not going to lose out by upgrading now. It is true that "Running a well-protected solution starts with using modern software and hardware designed to help protect against today's threat landscape". Windows XP is 12 years old, that's extraordinarily old in technological years and increasingly software is being developed which XP just won't have the capacity to cope with. If Microsoft do continue support for XP it can't be for that much longer and you won't have lost out by investing in an upgrade. Windows 7 has an XP compatibility mode, so if you do have software which is particularly stubborn and difficult to migrate you can always run it in this. To read more click **HERE**

Council of Europe Ransomware Blocks Users from Accessing the Internet

SoftPedia, 4 Feb 2014: Security researchers from Emsisoft have come across an interesting piece of ransomware which they've dubbed Linkup (Trojan-Ransom.Win32.Linkup). While other such Trojans lock up computers or encrypt the files stored on them, Linkup prevents users from accessing the Web. When the owners of infected devices want to visit a website, they're presented with a message that appears to come from the Council of Europe. "Internet access is temporarily blocked," reads the message on the screen. Victims are told to provide their personal and financial information to establish their identities. Internauts are informed that they only have to pay €0.01 to unlock Internet usage, but experts believe that the amount that victims end up paying is much higher. So how does this threat block Internet access? According to researchers, when it's first executed, Linkup disables Windows security features and the operating system's firewall, and makes a copy of itself under the name svchost.exe. Then, the malware contacts its command and control server. Linkup receives a command to redirect all HTTP requests to the ransomware website. It makes a number of modifications in the registries to ensure that every DNS request is redirected. However, Linkup is not designed only to block Internet access. Once it infects a computer, the threat downloads an additional component that's actually a Bitcoin miner. Devices infected with the malware actually become part of a Bitcoin mining botnet. In case your computer is infected with Linkup, here's what you need to do to clean it up. First of all, scan your device with updated antivirus software (Emsisoft recommends Malwarebytes Anti-Malware). Then you need to set DNS settings to "obtain DNS server address automatically." The malware sets the primary DNS server to 127.0.0.1. Additional technical details on the Linkup ransomware are available on Emsisoft's blog. To read more click **HERE**

Microsoft Fixed 344 Security Flaws in 2013, Windows and IE Still Vulnerable

SoftPedia, 4 Feb 2014: Microsoft struggles to make its software a little bit more secure, but a new report published by GFI Labs shows that the number of flaws found in its software more than doubled in 2013 as compared to 2012. Redmond had to fix a total of 344 vulnerabilities in 2013 versus 169 in 2012, which clearly shows that Microsoft worked a lot to improve the overall security of its products. At the same time, Windows remained the most targeted operating system in 2013, with Windows Server 2008 affected by 104 vulnerabilities last year, while Windows 7 and Windows Vista come net with 100 and 96 flaws, respectively. Unsurprisingly, Internet Explorer is also among the most targeted applications with 128 found security flaws, up from only 41 in 2012. To read more click **HERE**

Target Determined to Deploy Chip-Enabled Card Technology in Stores by Early 2015

SoftPedia, 4 Feb 2014: Following the recent data breach in which a total of 40 million payment cards have been compromised, US retailer Target is determined to do something about the magnetic stripe payment cards that are so easy to abuse. The company wants to replace them with chip-enabled smartcards, which are much more secure. In an article posted on The Hill, John J. Mulligan, the chief financial officer and executive vice president for Target, explains that the company attempted to roll out such technology around 10 years ago. However, the program was discontinued after three years because other organizations refused to implement the new cards, making it confusing for customers. "Since the breach, we are accelerating our own $100 million investment to put chip-enabled technology in place. Our goal: implement this technology in our stores and on our proprietary REDcards by early 2015, more than six months ahead of our previous plan," Mulligan said. Mulligan gives the United Kingdom as a positive example. In the UK, where PIN and chip cards have been used, financial losses associated with lost or stolen payment cards have dropped by 67% since 2004. That's because skimming attacks don't work against such cards. On Tuesday, the Target CFO will testify before Congress regarding the recent data breaches suffered by retailers. Since the data breach, a number of lawsuits have been filed against Target. However, ABA Journal reports that it's not just consumers who are going after the retailer. Financial institutions have also filed suits. They argue that they've lost hundreds of millions of dollars because Target failed to implement proper security measures to protect customer information. The retail and the banking industries have been blaming each other for the recent data breaches right from the start. To read more click **HERE**

Hackers breach Bell Canada, leak customer info and passwords

Heise Security, 3 Feb 2014: The hacker group NullCrew has managed to access servers belonging to Bell Canada - or a third-party supplier, as Bell claims - and steal and ultimately leak usernames and passwords, email addresses, partial credit card details and more of some 20,000+ Bell customers. NullCrew hackers announced the leak a few weeks ago, and have made public the data dump this Saturday. The site hosting the dump has been taken offline, but not before some security researchers and likely some cyber crooks managed to download it. The blogger behind DataBreaches.net has interviewed the hackers, and has been shown screenshoots of conversations and of the hacking process that corroborate their claims that they they had access to Bell's server for months, and that they have (unsuccessfully) tried to inform Bell of it and of the vulnerability that allowed them to mount an SQL injection against the company's protection management login page (https://protectionmanagement.bell.ca/passwordrecovery_1.asp). After a short investigation, Bell Canada confirmed the information compromise, but said that the servers in question are not theirs. "Bell today announced that 22,421 user names and passwords and 5 valid credit card numbers of Bell small-business customers were posted on the Internet this weekend. The posting results from illegal hacking of an Ottawa-based third-party supplier's information technology system," they stated on Sunday. "In line with our strict privacy and security policies, Bell is contacting affected small business customers, has disabled all affected passwords, and has informed appropriate credit card companies. We continue to work with the supplier as well as law enforcement and government security officials to investigate the matter. Bell's own network and IT systems were not impacted." NullCrew still claims that it was Bell's own servers that got hacked, but the company reiterated their claim that they belong to a third-party supplier. Security researcher Adam Caudill commented on Twitter that Bell's version might be true. "I've seen more than once where a subdomain of a large company points to a third party," he said, adding that his company hosts one for a "very large bank". "So it's quite possible they are telling the truth. They should still take more responsibility for their data though," he concluded. To read more click **HERE**

Belarus link to ObamaCare raises concerns over possible cyber attack

Fox News, 4 Feb 2014: U.S. intelligence agencies last week urged the Obama administration to check its new health care network for malicious software after learning that developers linked to the Belarus government helped produce the website, raising fresh concerns that private data posted by millions of Americans will be compromised. The intelligence agencies notified the Department of Health and Human Services, the agency in charge of the HealthCare.gov network,

that programmers in Belarus, a former Soviet republic closely allied with Russia, were suspected of inserting malicious code that could be used for cyber attacks, according to U.S. officials familiar with the concerns. The software links the millions of Americans who signed up for ObamaCare to the federal government and more than 300 medical institutions and health care providers. "The U.S. Affordable Care Act software was written in part in Belarus by software developers under state control, and that makes the software a potential target for cyber attacks," one official said. Cybersecurity officials said the potential threat to the U.S. health care data is compounded by what they said was an Internet data "hijacking" last year involving Belarusian state-controlled networks. The month-long diversion covertly re-routed massive amounts of U.S. Internet traffic to Belarus -- a repressive dictatorship located between Russia, Poland and Ukraine. The combination of the Belarus-origin software, the Internet re-routing, and the anti-U.S. posture of the Belarusian government "makes the software written in Belarus a potential target of cyber attacks for identity theft and privacy violations" of Americans, the official said. Security officials urged HHS to immediately conduct inspections of the network software for malicious code. The software currently is used in all medical facilities and insurance companies in the United States. The officials also recommended that HHS use security specialists not related to software vendors for the inspections to reduce further risks. Officials disclosed the potential software compromise last week after the discovery in early January of statements by Belarusian official Valery Tsepkalo, director of the government-backed High-Technology Park (HTP) in Minsk. Tsepkalo told a Russian radio station in an interview broadcast last summer that HHS is "one of our clients," and that "we are helping Obama complete his insurance reform." To read more click **HERE**