The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

17 + 21 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

January 15, Help Net Security – (International) **User financial info compromised in US Fund for Unicef breach.** The US Fund for Unicef non-profit notified the State of New Hampshire that it experienced a data breach in November 2013 that compromised personal and financial information of three New Hampshire residents, with residents in North Carolina and Maryland also potentially affected. Source: http://www.net-security.org/secworld.php?id=16213

January 16, Help Net Security – (International) **Starbucks iOS app stores passwords in clear text.** A security researcher disclosed that the Starbucks app for iOS stores user names, email addresses, and passwords in clear text. The information can be obtained even if the phone is locked. Source: http://www.net-security.org/secworld.php?id=16215

January 16, Softpedia – (International) **Highly critical vulnerability fixed with the release of Drupal 7.26 and 6.30.** The developers of Drupal released Drupal versions 7.26 and 6.30, addressing a highly critical vulnerability that could be used to impersonate users and take over accounts, and a moderately critical vulnerability that could be used to access unpublished or restricted content. Source: http://news.softpedia.com/news/Highly-Critical-Vulnerability-Fixed-with-the-Release-of-Drupal-7-26-and-6-30-417568.shtml

January 16, The Register – (International) **Microsoft confirms: Staff inboxes hijacked amid 'Syrian army' cyber-blitz.** Microsoft confirmed that a small number of Microsoft employee emails were compromised via phishing attacks during recent Twitter account and blog takeovers by the Syrian Electronic Army hacktivist group. Source: http://www.theregister.co.uk/2014/01/16/sea_microsoft_email_compromised/

January 16, Softpedia – (International) **Security patches released for IP.Gallery 4.2.1 and 5.0.5.** Invision Power Services released patches to close a cross-site scripting (XSS) vulnerability in IP.Gallery 4.2.1 and 5.0.5 related to Shockwave Flash file uploads. Source: http://news.softpedia.com/news/Security-Patches-Released-for-IP-Gallery-4-2-1-and-5-0-5-417560.shtml

January 16, Softpedia – (International) **AVG confirms one of its webservers was hacked and defaced.** AVG confirmed that one of its Web servers was breached and defaced by hackers January 10. Source: http://news.softpedia.com/news/AVG-Confirms-One-of-Its-Webservers-Was-Hacked-and-Defaced-417781.shtml

January 16, The Register – (International) **Fine! We'll keep updating WinXP's malware sniffer after April, says Microsoft.** Microsoft announced that it would continue to provide updates to antimalware programs for Windows XP beyond the operating system's April 8, 2014 end of support, through July 14, 2015. Source: http://www.theregister.co.uk/2014/01/16/microsoft_xp_security_updates_extended/

January 16, IDG News Service – (International) **Spammers target Snapchat, Bitly, and Kik Messenger.** Symantec researchers identified a spam campaign that sends unsolicited contact requests for Kik Messenger via Snapchat, which leads to a spam bot that sends links shortened by the Bitly service which lead to sites trying to sign up users for webcam services. Source: http://www.computerworld.com/s/article/9245471/Spammers_target_Snapchat_Bitly_and_Kik_Messenger

January 16, Network World – (International) **Cisco: Thousands of web hosting centers now launchpads for attacks.** Cisco released its annual security report, which found that Web hosting centers were increasingly being compromised by cybercriminals for use in launching large-scale attacks in 2013, among other findings. Source: http://www.networkworld.com/news/2014/011614-cisco-web-hosting-centers-277621.html

January 15, Dark Reading – (International) **SCADA researcher drops zero-day, ICS-CERT issues advisory.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued a security alert January 15 after a researcher revealed a zero-day vulnerability in Ecava's InegraXor supervisory control and data acquisition (SCADA) interface software. A proof-of-concept was also released for the stack buffer overflow issue. Source: http://www.darkreading.com/applications/scada-researcher-drops-zero-day-ics-cert/240165420

January 15, Softpedia – (International) **Amazon, Google, and GoDaddy cloud services increasingly abused by cybercriminals.** Solutionary released its SERT Quarterly Threat Analysis Report for the final quarter of 2013 and found that cybercriminals are increasingly abusing major cloud services to create, host, and delete malicious Web sites, among other findings. Source: http://news.softpedia.com/news/Amazon-Google-and-GoDaddy-Cloud-Services-Increasingly-Abused-by-Cybercriminals-417191.shtml

January 17, Softpedia – (International) **Hackers stole 11 Gb of customer information from Target's systems.** An analysis of the recent Target customer information data breach found that the attack worked in two phases and stole a total of 11GB of data. Source: http://news.softpedia.com/news/Hackers-Stole-11-Gb-of-Customer-Information-from-Target-s-Systems-417997.shtml

January 16, SC Magazine – (International) **Researchers discover a point-of-sale malware written in VBScript.** Researchers at IntelCrawler identified a new piece of point-of-sale (POS) malware known as Decebal for sale on underweb forums. The malware is written in VBScript and can use antivirus bypass techniques. Source: http://www.scmagazine.com/researchers-discover-a-point-of-sale-malware-written-in-vbscript/article/329775/

January 16, Orlando Sentinel – (Florida) **Orlando couple stole $550,000 in massive ID-theft 'phishing scam,' FDLE says.** Two individuals in Orlando were charged with using phishing emails targeting JPMorgan Chase and Wells Fargo customers to steal around 400 customers' account information and request replacement debit cards. The pair then allegedly used the cards to purchase money orders and deposit the funds into a personal bank account, totaling around $550,000 in stolen funds. Source: http://www.orlandosentinel.com/news/local/breakingnews/os-orlando-couple-phishing-scam-fdle-20140116,0,4776959.story

January 16, Associated Press – (National) **Neiman Marcus offers update on credit card breach.** Retailer Neiman Marcus announced January 16 that a recent data breach of customer data did not contain payment card PINs or the data of online shoppers. The company is continuing to investigate the breach. Source: http://abcnews.go.com/Business/wireStory/neiman-marcus-offers-update-credit-card-breach-21562189

January 17, Softpedia – (International) **At least one smart refrigerator used in massive cyberattack.** Researchers at Proofpoint analyzed a large-scale spam campaign that involved over 750,000 malicious emails and found that more than 100,000 Internet-connected consumer electronic devices were used in the attack, including multimedia centers, smart TVs, routers, and at least one smart refrigerator. Source: http://news.softpedia.com/news/At-Least-One-Smart-Refrigerator-Used-in-Massive-Cyberattack-417878.shtml

January 17, The Register – (International) **Bitcoin's so over. We're mining Primeco…Oh SNAP, my box is a ZOMBIE!** A researcher at Panda Security discovered several malicious mining programs for the Primecoin digital currency that include malware that can compromise users' systems, hide itself as rootkits, disable antivirus programs, and allow the computer to be used as part of a botnet. Source: http://www.theregister.co.uk/2014/01/17/primecoin_malware_miner_discovered/

January 17, Softpedia – (International) **Trojan disguised as legitimate applications uses infected PCs to mine Litecoins.** Researchers at Doctor Web identified a trojan disguised as legitimate applications and browser extensions that uses infected systems to mine for the Litecoin digital currency. The trojan is signed with digital certificates from legitimate applications and has infected over 311,000 computers, mostly in the U.S. Source: http://news.softpedia.com/news/Trojan-Disguised-as-Legitimate-Applications-Uses-Infected-PCs-to-Mine-Litecoins-418152.shtml

January 17, Softpedia – (International) **Humor website Cracked.com serves malware, again.** Barracuda Labs researchers found that humor Web site Cracked.com was compromised the week of January 13 and being used to redirect users to pages that serve malware by exploiting browser and Java vulnerabilities. The site was previously compromised to serve malware in November 2013 Source: http://news.softpedia.com/news/Humor-Website-Cracked-com-Servers-Malware-Again-418114.shtml

January 16, Softpedia – (International) **Cybercriminals are distributing malware with fake Flash Player served from SkyDrive.** Researchers at F-Secure discovered a recent spike in Trojan.JS.Blacole.Gen infections originating from a malware campaign that uses compromised Web sites to redirect users and attempts to get them to install fake Flash Player updates. The trojan is then downloaded from a Microsoft SkyDrive account. Source: http://news.softpedia.com/news/Cybercriminals-Are-Distributing-Malware-with-Fake-Flash-Player-Served-from-SkyDrive-417819.shtml

Hacker Reveals How He Cracked ObamaCare Website in Less Than Four Minutes

IJ Review, 19 Jan 2014: The hacking expert who testified before Congress last week about the security failures of HealthCare.gov, explained Sunday how he was able to penetrate the site. In less than four minutes. "There's a technique called 'passive reconnaissance,'" hacker David Kennedy explained to "Fox News Sunday" host Chris Wallace, "which allows us to query and look at how the website operates and performs." "And these type of attacks that I'm mentioning here, and the 70,000 [personal records Kennedy found] that you're referencing, is very easy to do It's a rudimentary type attack that doesn't actually attack the website itself. It extracts information from it without actually having to go into the system." "Think of it this way. Think of something where you have a car and the car doors are open and the windows are open — you can see inside of it. That's basically what they allow you to do and there's no real sophistication level here — it's just really wide open. So there's no hacking actually involved." Good to know, huh? Guess what's even more troubling? Kennedy said that gaining access to 70,000 personal records of ObamaCare enrollees via HealthCare.gov took less than four minutes, and required nothing more than a standard browser to pull off. "You can

literally just open up your browser, go to this, and extract all this information without actually having to hack the website itself." To read more click **HERE**

Lenovo Will Buy IBM's Low-End Server Business

SoftPedia, 21 Jan 2014 IBM is one of the world's largest suppliers of server and data center products and systems, but even it has some business arms that haven't been paying off lately. Lenovo is more than eager to pounce on them. Or it, since only one is about to change hands. Low-end servers are the business unit that IBM hasn't been getting much value out of recently, something that doesn't look like it will change any time soon. Indeed, the value continues to dwindle actually, and IBM is seriously thinking of divesting itself of it. And since it's not often that a business division just gets abandoned in the ditch, it makes sense that the corporation would be considering a sellout. And with Lenovo interested in the business, it shouldn't take too long for the transaction to be put together and finalized. Granted, Lenovo hasn't actually said that it would do it, or has rather said that it hasn't entered any definite agreement yet. "The company has not entered into any definitive agreement in relation to the potential acquisition," Lenovo's Chief Executive Officer Yang Yuanqing said on Tuesday. Still, reports (and Reuters) informed that Lenovo had already evaluated the acquisition, estimating a cost of around $2.5 billion / €1.85 billion. The company is said to be in discussion with IBM and is expected to complete the transaction in a few weeks, tops. Meanwhile, Dell has also thrown in a bid, though we aren't sure what sum it's offering. In any case, even though the low-end server unit of IBM seems to be a minor part of its operation, the value that Lenovo is attributing to it makes it clear that it's not really a small business at all. It's just a lot smaller than IBM as a whole. It'll be interesting to see if Lenovo tries to introduce any ARM-based technology in the server division if it does buy it. To read more click **HERE**

German Authorities Say Cybercriminals Have Compromised 16 Million Online Accounts

SoftPedia, 20 Jan 2014: Germany's Federal Office for Information Security (BSI) warns that cybercriminals have compromised around 16 million online accounts. A new service has been launched to help users find out if their credentials have been stolen. According to authorities, researchers and law enforcement agencies have determined that 16 million usernames (usually email addresses) and passwords have been compromised after analyzing botnets. Since many people use the same login information for multiple services, it's important that they take measures, if necessary. The new service has been launched by the BSI in collaboration with Deutsche Telekom, IT security company Avira, and other organizations. Internet users simply enter their email addresses on a website, after which they're informed if their credentials have been compromised. Affected individuals will receive emails containing recommendations on how to protect their online identities. First, users must scan their computers with antivirus software to ensure that the devices are not infected. Secondly, they must change all their passwords. To read more click **HERE**

Cisco : An Additional One Million Cyber Security Experts Needed Across the Globe

SoftPedia, 20 Jan 2014: According to Cisco's latest Annual Security Report [**LINK**], this year, there's a shortage of over one million security experts across the globe. The company says cybercriminals have sophisticated tactics and technology, which makes it very difficult to defend an organization against their constant attacks. The study also shows that the number of vulnerability and threat alerts has increased by 14% compared to 2012. In fact, this represents an all-time high since May 2000. After analyzing the networks of 30 of the world's largest multinational organizations, the company has determined that all of them generated visitor traffic to malware websites. In addition, 96% of the monitored networks sent out traffic to compromised servers. As far as distributed denial-of-service (DDOS) attacks are concerned, they've increased not only in volume, but also in severity. Up until recently, the electronics manufacturing, pharmaceutical and chemical industries had been most targeted in malware attacks. However, over the past couple of years, the agriculture and mining industry became increasingly targeted. Previously, it was considered a relatively low-risk sector. When it comes to malware in general, experts found that 27% of all the threats encountered in 2013 were

multipurpose Trojans. The second position is occupied by malicious scripts (23%), followed by infostealers (22%). "Although the Cisco Annual Security Report paints a grim picture of the current state of cyber security, there is hope for restoring trust in people, institutions and technologies – and that starts with empowering defenders with real-world knowledge about expanding attack surfaces," said Cisco's John N. Stewart. "To truly protect against all of these possible attacks, defenders must understand the attackers, their motivations and their methods – before, during and after an attack." To read more click **HERE**

Silver Nanowire Sensors Enable Smart Fingers, Bandages, and Wearables

SoftPedia, 18 JAn 2014 Wearables are taking off, but a team of researchers from the North Carolina State University believe that the process can go faster and evolve more quickly, so they invented a new sensor that can work like a bandage. We've already seen wearable gloves that let you hold phone calls through your hands (Call Me Gloves), vibrating gloves that help recovery from paralysis, clothing fabric that works as a battery, and even Bluetooth smart tech that can enable watches, bracelets, gloves, and hats in 2014. What Dr. Yong Zhu and his team invented could be called the next logical step in the evolution of the wearable tech concept. When we say bandage-like sensor, though, we don't mean that it is supposed to stem blood loss or keep a salve in place. What we mean is that it conforms to your skin much like a bandage would. Better even, since it's pretty much transparent. Granted, there is one, thin part that can be seen against the skin, but the rest can only be distinguished if you look closely. Zhu invented the ultra-thin, flexible sensor from silver nanowires, a silicon plate, and liquid polymer. Not all that sophisticated really. The nanowires were placed on the plate, after which the liquid polymer was poured over it and heated, turning from liquid to an elastic solid. Then the whole thing was peeled off the silicon. The result was a pair of silver nanowire conductors held safely inside a flexible polymer strip. It can be stretched 150% or more of its original length without harm, and it can bend as much as your joints and skin can. The sensor can track pressure, human touch, bioelectric signals, strain, etc., because it can store and monitor electric charges (capacitance). All in all, they're much better than the capacitive sensors used by styluses and smart utensils, which are rigid and very specific in their use. So far, Zhu and his team have tested the sensors by putting them on thumbs (controlling robotic devices) and knees (monitor walking, running, and jumping). Ultimately, they should be embedded in clothes and even skin. http://news.softpedia.com/news/Silver-Nanowire-Sensors-Enable-Smart-Fingers-Bandages-and-Wearables-418311.shtml To read more click **HERE**

Android Vulnerability Can Be Exploited to Capture Data of VPN Users

SoftPedia, 18 Jan 2014 : Security researchers from the Ben Gurion University (BGU) in Israel have uncovered another Android security issue. They've found a way to bypass active VPN configurations and intercept secure communications. In order to exploit this vulnerability, an attacker doesn't require root permissions to capture data transmissions. The worst part of it is that there's nothing that would make victims realize that they're being attacked. "[The] communications are captured in CLEAR TEXT (no encryption), leaving the information completely exposed. This redirection can take place while leaving the user completely oblivious, believing the data is encrypted and secure," BGU's Dudu Mimran noted. The experts have tested the vulnerability on several Android devices from various vendors. The video POC they made uses a Samsung Galaxy S4. SSL/TLS traffic can also be intercepted using this attack method, but the content stays encrypted. The experiments have been performed on a properly configured VPN, using Wi-Fi connections, and a computer connected on the same network as the targeted mobile device. The vulnerability has been reported to Google. It remains to be seen if the search giant classifies this issue as an Android security hole. A few weeks ago, BGU mobile security researchers claimed to have found a vulnerability impacting the Samsung Knox platform. At the time, Samsung issued an official response saying that the attack exploited legitimate Android network functions in an unintended way for a classic man-in-the-middle attack. The company noted that the researchers didn't actually identify a vulnerability in Android or Knox. Now, BGU researchers clarify that the attack impacting VPN users is different from the one targeting the Samsung Knox platform. Additional technical details on the vulnerability will be made available by the researchers at a later time. To read more click **HERE**

Chinese Government Says Ubuntu, Windows, and Android Are Not Safe, Launches New OS

SoftPedia, 18 Jan 2014: The Chinese market has been flooded by Android-based phones, iOS devices, and now even Microsoft is working its way up with Windows Phone. The Chinese government is trying to put a stop to this trend by making its own operating system based on Linux, for phones and tablets. Breaking away from Google, Apple, and Microsoft might not be so simple, but it seems that the Chinese government is really taking this issue seriously. According to the official announcement, the other operating systems from the companies mentioned above are predisposed to security problems and these issues must be addressed somehow. The interesting fact is that even Ubuntu has been mentioned among the operating systems with security issues, but not details have been given. The new operating system will be aptly named China Operating System or COS. It's being developed by The Chinese Academy of Sciences, The Software Institute, and the Shanghai Alliance Tong Network Communications Technology Co., Ltd. The new Linux-based operating system intends to feature high-performance native apps, HTML5 applications, and a JAVA virtual machine. To read more click **HERE**

Data Breaches Trigger New Wave of Malicious Experian Credit Report Emails

SoftPedia, 17 Jan 2014: Now that many Target and Neiman Marcus customers are concerned about the safety of their identities and bank accounts, cybercriminals know that it's a perfect time to revive an old Experian-themed spam campaign. The emails spotted by ThreatTrack Security carry the subject line "IMPORTANT - A Key Change Has Been Posted," and they read something like this: "A key change has been posted to one of your three national Credit Reports. Each day we monitor your Experian®, Equifax and TransUnion Credit Reports for key changes that may help you detect potential credit fraud or identity theft. Even if you know what caused your Report to change, you don't know how it will affect your credit, so we urge you to do the following: View detailed report by opening the attachment. You will be prompted to open (view) the file or save (download) it to your computer. " The file attached to the emails is not a detailed report and it has nothing to do with Experian. Instead, it's a piece of malware. More precisely, it's a variant of the Upatre downloader, which retrieves other threats, including the ZeuS banking Trojan, to infected devices. Variants of this spam email were seen making the rounds in March and April 2013. Target is offering customers whose payment card data has been compromised in the recent breach one year free identify protection services with Experian. This makes it a perfect opportunity for scammers and cybercriminals to launch Experian-themed campaigns. Unfortunately, Target isn't doing a very good job when it comes to notifying impacted customers via email. The alerts are sent out even to people who have nothing to do with the retailer, and even spam traps. Users are advised to be cautious when receiving communications related to the Target data breach. To read more click **HERE**