The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

5 March 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

Smucker's Shuts Down Online Store after Hackers Access Payment Card Data

SoftPedia, 5 Mar 2014: The systems of Smucker's – the Ohio-based company that makes fruit spreads, beverages, ice cream topping and other similar products – have been hacked. The company has been forced to shut down its online store following the incident. Smucker's says the attackers have gained "illegal and unauthorized" access to files on the online store servers. They could have accessed customer information, including names, addresses, email addresses, phone numbers, credit and debit card numbers, their expiration dates and verification codes. "The unauthorized user utilized a sophisticated scheme to illegally obtain this personal information as it was being entered during the online checkout process," Richard Smucker, the company's CEO, wrote in a statement posted on the Smucker's online store. "We are extremely disappointed this incident occurred and sincerely apologize for any inconvenience this may cause. Please be assured, we continue to thoroughly investigate this matter with federal authorities, and have taken steps to rectify the cause of this incident with the Online Store website," he added. In a letter sent out to impacted customers at the end of February, the company revealed that they discovered the breach on February 12, 2014. People who have made purchases in the online store between December 2012 and January 2014 are impacted. The attackers have relied on a piece of malware that's designed to steal the information as it is being entered by users during the online checkout process. Smucker's is offering affected individuals a full package of credit protection services for two years. The cybercriminals who breached Smucker's appear to be part of the same group that hacked into the systems of Adobe, the National White Collar Crime Center, and various data brokers such as Dun & Bradstreet, Kroll and LexisNexis. Brian Krebs, who has investigated all these attacks, says the cybercriminals in many cases target websites running vulnerable versions of ColdFusion. Krebs says the same group has also targeted the Systems of SecurePay, a credit card processing company. SecurePay, which has been acquired by Calpiancommerce.com back in early 2013, moved online operations to a new data center in October 2013. However, it appears the thieves managed to steal around 5,000 card transaction records while SecurePay operations were still at a data center in New York. The company that owned SecurePay at the time, Pipeline Data, was running outdated software on its servers. SecurePay's chief operating officer, Tom Tesmer, told Krebs that a web application firewall alert was triggered in the summer of 2013 and the administrators of the New York data center were made aware of it, but apparently they didn't take proper action. To read more click **HERE**

OS X 10.9.2 Is an Awful Update

SoftPedia, 5 Mar 2014: Apple's recently-deployed OS X 10.9.2 update for Mavericks customers was said to deliver a huge number of fixes and enhancements, but some of the most annoying bugs reported in the past six months are still there unfortunately. I'd been waiting for OS X 10.9.2 sitting on the edge of my seat, and when the update finally arrived, I quickly realized that the most annoying bugs were still not fixed. For example, scrolling. It's even more crippled than before, and now it completely freezes the Mac App Store if you do so much as scroll a millimeter horizontally. Apple has botched up Mavericks one too many times! Mail is another example. It crashes for a lot of users despite OS X 10.9.2 delivering "general improvements to the stability and compatibility of Mail," improved accuracy of unread counts, and a "fixed issue that prevented Mail from receiving new messages from certain providers." It doesn't look like

Apple is on the right track with these updates as more and more users continue to report issues with their 10.9.2 experience on the Apple Support Communities forum, including hangs and freezes of the entire OS sometimes. Safari users are also reporting crashes. Apple, what gives? To read more click **HERE**

Tor Attracts More and More Cybercriminals, Experts Warn

SoftPedia, 5 Mar 2014: Kaspersky security researchers have been monitoring the activities of cybercriminals on the Darknet, particularly Tor, and they've found that the number of operations relying on the anonymity network is increasing. According to Kaspersky Lab Expert Sergey Lozhkin, there currently are around 900 hidden services on Tor with 5,500 nodes and 1,000 exit nodes. Cybercriminals are attracted to the Tor network for a number of reasons. It enables them to create anonymous underground forums and markets, and they can use it to create malware command and control (C&C) infrastructure that's difficult to disrupt. Examples of malware that rely on Tor of C&C communications include ZeuS, ChewBacca and even the recently-discovered Backdoor.AndroidOS.Torec.a Android Trojan. While using Tor has advantages, it also has disadvantages, including the fact that Tor-based malware is larger in size and more difficult to develop. However, Lozhkin believes that their number will increase. In addition, existing malware will probably include Tor support. Silk Road is a perfect example of a successful underground market place. However, there are many others that can be used to buy or sell drugs, weapons and cybercrime tools. Another important aspect of Tor's dark side is the financial one. Since most underground markets rely on Bitcoin and other virtual currencies, it's easy for cybercriminals to commit financial fraud and launder their criminal proceeds. To read more click **HERE**

BBB Warns of Pinterest Scams

SoftPedia, 4 Mar 2014: Every single popular social media platform is being abused by scammers and cybercriminals and Pinterest is no exception. The Better Business Bureau (BBB) has published an advisory to warn Internet users of the scams making the rounds on Pinterest. According to the advisory, the scams start with an email that informs potential victims about a "pin" shared by one of their friends. The pins usually feature a celebrity, beauty photos, giveaways, infographics and diet pictures. They're always designed to trick users into clicking on the links they contain. These links can lead to a wide range of websites, but none of them contains anything good. The websites advertised in such schemes can be online stores that sell counterfeit merchandise, or fake news websites that promote work opportunities, diets and pharmaceutical products. "Scammers use many techniques to gain access to your account. They may take advantage of security holes in third party applications that connect to Pinterest (such as those that automatically post your pins on Twitter) or insert malicious code into the 'Pin This' buttons on other websites," the BBB warns. So what can you do to protect yourself against such schemes? First of all, in case you spot spam pins, report them to Pinterest by clicking the flag icon. If you fear that your account might have been compromised, change its password from the Settings menu. Be sure to set a strong password, one containing both lower and uppercase letters, numbers and symbols. If you can't remember complex passwords, use a password manager. The BBB also advises users to log out of their Pinterest accounts when they're not using it. This is particularly important if you're utilizing shared computers. When logging in to the service, make sure that you're on the genuine websites, and not a domain that looks like pinterest.websitename.com. Phishers often rely on this trick to dupe users into thinking they're on the legitimate site. In case you've connected your social media accounts, if one of them gets compromised, the attackers can send out spam on all of them. Be careful when using such services. Finally, before re-pinning on Pinterest, take a moment to make sure that you're not contributing to a scam or a cybercriminal operation. For additional details on how to keep your Pinterest account secured, check out the BBB's advisory. You can also check out the "Keep your account secure" page on Pinterest. To read more click **HERE**

Bitcoin Bank Flexcoin Shuts Down After Hackers Emptied Hot Wallet

SoftPedia, 4 Mar 2014: Six hours ago, Flexcoin, the Bitcoin bank, announced shutting its doors. The decision comes after hackers breached the service and stole all the Bitcoins from the hot wallet. According to a notice posted on the Flexcoin

website, the attackers stole close to 900 Bitcoins, transferring them into two addresses. The stolen Bitcoins are currently worth over $600,000 (€442,000). The company says it's shutting down because it doesn't have the resources to recover from such a loss. "Users who put their coins into cold storage will be contacted by Flexcoin and asked to verify their identity. Once identified, cold storage coins will be transferred out free of charge. Cold storage coins were held offline and not within reach of the attacker," reads the notice posted on Flexcoin.com. The organization is working with law enforcement to track down the attackers. Flexcoin is not the only Bitcoin company targeted by hackers. Earlier today, the owner of Bitcoin exchange Poloniex revealed that 12.3% of their coins have been stolen. Apparently, a hacker has leveraged a vulnerability in the code to make unauthorized withdrawals. "The hacker discovered that if you place several withdrawals all in practically the same instant, they will get processed at more or less the same time. This will result in a negative balance, but valid insertions into the database, which then get picked up by the withdrawal daemon," Busoni, the owner of Poloniex, explained. Since the service's auditing and security features haven't been designed to look for negative balances, the hackers managed to withdraw a lot of Bitcoins before being detected. "They add deposits and withdrawals and check that accounts are in balance. If you have 2 BTC, withdraw 10 BTC, and are left with -8 BTC, the software would see that you deposited 2, withdrew 10, and have exactly what you should: -8," Busoni added. The incident was discovered after existing security mechanisms detected unusual activities. Now, the system has been improved to ensure that accounts with negative balances are frozen. While this prevents the exploit from being leveraged, this only represents a temporary solution. The problem with such Bitcoin heists is that the transfer cannot be reversed. While anyone can see where the coins end up, because of the decentralized nature of the virtual currency, nothing can be done to recover them. News of these latest hack attacks comes shortly after Mt. Gox, the world's largest Bitcoin exchange, filed for bankruptcy. The company says hackers have stolen close to 750,000 of its customers' coins. To read more click **HERE**

19 Security Fixes Included in Latest Chrome 33 Update

SoftPedia, 4 Mar 2014: Google has announced that the stable build of Chrome has been updated to version 33.0.1750.146 for all platforms. The latest release addresses a total of 19 security issues identified by various researchers and members of Google's internal team. As always, Google has rewarded some of those who have reported security vulnerabilities. A high-impact use-after-free issue in SVG images identified by Atte Kettunen of OUSPG has been rewarded with $1,000 (€730). Khalil Zhani got $500 (€363) for finding a similar flaw in speech recognition. Another high-impact vulnerability, a heap buffer overflow, has been found in software rendering by cloudfuzzer. Google gave him $2,000 (€1,450) for responsibly disclosing the problem. Netfuzzerr has discovered a medium-severity issue. He found that Chrome allows requests in the Flash header request. Google's internal security team has also identified some flaws that could have been exploited by hackers. The list includes multiple vulnerabilities in version 3.24.35.10 of V8, and various other bugs uncovered during internal audits, fuzzing, and other initiatives. AddressSanitizer has been utilized to detect many of these security holes. Users are advised to update their installations to protect themselves against potential cyberattacks. To read more click **HERE**

March 4, Softpedia – (International) **Bitcoin bank Flexcoin shuts down after hackers emptied hot wallet.** Bitcoin bank Flexcoin announced March 4 that it was shutting down operations after attackers leveraged a vulnerability and withdrew all Bitcoins from the bank's 'hot' wallet, around 900 Bitcoins worth over $600,000. Customers' Bitcoins stored in offline 'cold' wallets were unaffected. Source: http://news.softpedia.com/news/Bitcoin-Bank-Flexcoin-Shuts-Down-After-Hackers-Emptied-Hot-Wallet-430469.shtml

March 4, SC Magazine – (National) **Stolen laptop leads to compromised unencrypted personal data.** AppleCare Insurance Services notified individuals who have enrolled in or discussed health care plan options with one agent that their personal information may have been compromised after the agent's unencrypted laptop was stolen.

Source: http://www.scmagazine.com//stolen-laptop-leads-to-compromised-unencrypted-personal-data/article/336571/

March 1, Sherman/Denison Herald Democrat – (Texas) **Security breached, patient information compromised at doctor's office.** A Sherman, Texas doctor's office was broken into January 5 and thieves took computers and at least one hard drive which contained patients' personal information. The practice notified patients of the security breach and is currently upgrading their security system while continuing to investigate the incident. Source: http://heralddemocrat.com/news/local/security-breached-patient-information-compromised-office-dr-jm-benson

March 4, Dark Reading – (International) **Researchers create legal botnet abusing free cloud service offers.** Researchers presenting at the RSA Conference the week of February 24 demonstrated how they were able to create a botnet by abusing trial accounts for several platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) offers. The botnet was created by automating PaaS and IaaS trial sign-up processes and could be used to perform massive port scans, Bitcoin mining, and to manipulate sweepstakes, among other tasks. Source: http://www.darkreading.com/researchers-create-legal-botnet-abusing/240166428

March 4, Help Net Security – (International) **300,000 routers compromised in DNS hijacking campaign.** Researchers with Team Cymru found that around 300,000 small office/home office routers have been compromised and had their DNS settings changed to two IP addresses in the U.K. in order to allow them to perform man-in-the-middle (MitM) attacks. The researchers found that the attack dates to at least mid-December 2013 and has mostly affected routers in Europe and Asia. Source: http://www.net-security.org/secworld.php?id=16473

March 3, Threatpost – (International) **Four vulnerabilities found in Oracle Demantra.** Researchers at Portcullis identified four vulnerabilities in Oracle's Demantra business software that could allow attackers to steal sensitive information, carry out phishing attacks, modify application content, or perform other attacks. Source: http://threatpost.com/four-vulnerabilities-found-in-oracle-demantra/104574