The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

3 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

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

January 2, Help Net Security – (International) **4.6M Snapchat users' info compromised in breach.** Hackers created and published a partially-redacted list of 4.6 million Snapchat usernames and phone numbers utilizing a vulnerability disclosed the week of December 23 that was dismissed by Snapchat as theoretical. The vulnerability allows an attacker to look up an unlimited number of phone numbers and see if the number's owner has a Snapchat account. Source: http://www.net-security.org/secworld.php?id=16152

January 2, The Register – (International) **Skype's Twitter account, blog hacked to spread anti-Microsoft messages.** Attackers claiming association with the Syrian Electronic Army hacktivist group took control of Skype's Twitter account and official blog for several hours January 1 and used them to publish posts and tweets before Skype regained control of their platforms. Source: http://www.theregister.co.uk/2014/01/02/skype_social_media_hacked_to_spread_antimicrosoft_messages/

Skype Confirms Hacker Attack, Says No User Information Was Compromised
SoftPedia, 3 Jan 2014: As I've reported to you yesterday, the official social accounts and blog of Skype VoIP platform got hacked by the Syrian Electronic Army, who posted several messages asking Microsoft to stop spying on users. While Microsoft was quick to remove the tweets and take down the blog posts for an in-depth clean-up, the company now claims that no user account got compromised during the attack. "We recently became aware of a targeted cyber attack that led to access to Skype's social media properties, but these credentials were quickly reset. No user information was compromised," a company spokesperson was quoted as saying by LiveSide. While the company indeed confirmed the hack, it provided pretty vague information, so it's very hard to understand how come multiple social accounts of the same service got compromised in just a few minutes. Maybe they were using the same password for all social accounts… To read more click **HERE**

Vulnerability Exploited to Leak the Phone Numbers of 4.6 Million Snapchat Users
SoftPedia, 3 Jan 2014: Hackers have leaked the names and phone numbers of 4.6 million US-based Snapchat users in an effort to demonstrate that the recently disclosed vulnerability is more serious than the company has led users to believe. News of the security hole, which plagued the friend finder feature in Snapchat, first surfaced back in August. At the time, IT security firm Gibson Security warned that cybercriminals could leverage a flaw to obtain the phone numbers of users who had privately registered the information in order to allow their friends to find them more easily. Around Christmas, Gibson Security published another advisory. "Seeing that nothing had been really been improved upon, we decided that it was in everyone's best interests for us to post a full disclosure of everything we've found in our past months of hacking the gibson," the company noted. A few days later, on December 27, Snapchat published an advisory of its own, claiming that the attack method presented by Gibson was more theoretical. The company noted that the various safeguards they had implemented over the past year should make the attack more difficult to pull off. However, unknown hackers have launched a website called SnapchatDB.info where they published the

names and redacted phone numbers of 4.6 million internauts. "This information was acquired through the recently patched Snapchat exploit and is being shared with the public to raise awareness on the issue," the individuals behind SnapchatDB.info wrote. "The company was too reluctant at patching the exploit until they knew it was too late and companies that we trust with our information should be more careful when dealing with it." Following the leak, Snapchat published another blog post to assure customers that no other information has been compromised. The company has also promised to update its app to prevent abuse of the Find Friends feature. SnapchatDB.info has been pulled offline. Meanwhile, Gibson Security says it has nothing to do with the website. However, the company is offering people an online service that enables them to find out if they're impacted by the leak. To read more click **HERE**

Facebook Sued for Monitoring Private Messages

SoftPedia, 3 Jan 2014: Facebook is getting sued for monitoring users' private messages with the purpose of gathering consumer data for marketers. The lawsuit was filed in San Jose, California, on Thursday. Facebook is accused of tracing the contents of users' private messages, including links to other websites in order to improve its marketing algorithms and increase profit, the LA Times reports. The social network said that there was no merit to the allegation and that it would defend itself "vigorously." The case was filed by two plaintiffs who are seeking a class action on behalf of all Facebook users who have sent or received a private message containing links in the past two years. The idea that Facebook is engaging in this practice isn't exactly new. Back in 2012, Hacker News reported that the social network was scanning private messages and converted links into likes. A new study has recently showed that Facebook records everything that user's type, including the messages that are not posted. To read more click **HERE**

Two Former Purdue Students Admit Hacking Computers to Change Grades

SoftPedia, 3 Jan 2014: Roy C. Sun and Sujay Sharma, both former students of Purdue University, have admitted hacking the educational institution's computer systems in an effort to change grades. They've used keyboard keyloggers to collect access credentials from professors. According to the Journal & Courier, Sun has pleaded guilty to one count of conspiracy to commit computer tampering and two counts of computer tampering. Sharma has pleaded guilty to conspiracy to commit computer tampering. They'll both be sentenced in February. Sharma is said to have changed only one grade from a D to an A. Sun, on the other hand, is believed to have changed nine F grades to A between May 2008 and May 2010, when he graduated. Sun and Sharma are not the only suspects in this case. Authorities say Mitsutoshi Shirasaki also changed a couple of dozen grades between May 2010 and December 2012. However, Shirasaki is still wanted. Authorities say he has likely fled to Japan. To read more click **HERE**

Pakistani Hackers Leak Data from Financial Services Online Australia

SoftPedia, 3 Jan 2014: A group of Pakistani hackers called Pakiz Cyber Squad has leaked user data apparently stolen from the systems of Financial Services Online (FSO), an Australian company that provides insurance, finance, superannuation and investment services. The leaked data, published in 14 separate Pastebin pastes, includes usernames, names, addresses, phone numbers, email addresses, passwords (in clear text), and in some cases, PayPal email addresses. The FSO website has a login section for brokers and one for affiliates. The data appears to belong to affiliates. According to Cyber War News, a total of 527 record sets have been published online by the hackers. I've attempted to contact the company to see if they're aware of the breach, but so far, I haven't heard back from them. This post will be updated in case they respond to my inquiry. To read more click **HERE**

Website of the Nationalist Movement Hacked by Anonymous

SoftPedia, 3 Jan 2014: The official website of The Nationalist Movement (nationalist.org), a Mississippi-based white supremacist organization, has been hacked and defaced by members of Anonymous. The attack appears to be part of OpAntifa, a campaign against nationalists, racists and fascists. "We will take all actions to eradicate white pride from every corner of our world, physical and virtual. We will strike at all who support, promote, spread or hold fascist ideals,

and we will do so with all of our strength, which is a great strength," the hackers wrote on the defaced website. At the time of writing, the website of The Nationalist Movement is still defaced. This isn't the first time when hacktivists target nationalist.org. Anonymous first disrupted the website on December 15, 2013, when hackers claimed to have deleted all of its files. To read more click **HERE**

Facebook Fixes Open Redirect Vulnerability on "How Are You Feeling?"

SoftPedia, 3 Jan 2014: Moroccan security researcher Souhail Hammou has identified and reported an open redirect vulnerability on the mobile version of Facebook's "How are you feeling?" page. "The attacker can take users without any warning from Facebook to malicious websites that can exploit Java/Browser vulnerabilities or he can simply take them to download malware," the researcher has told me in an email. An attacker simply needed to convince his victims to click on a maliciously crafter link in order to lure them to any website. Hammou reported the security hole to Facebook around three months ago. The social media company confirmed fixing the issue on December 31, 2013. The expert has been paid an undisclosed amount of money for finding the vulnerability. Check out the video published by the researcher to see how the attack worked. To read more click **HERE**

Hackers Can Access Admin Panel of Some Netgear and Linksys Routers

SoftPedia, 3 Jan 2014: Some Linksys and Netgear routers are plagued by a vulnerability that allows a local attacker to gain unauthorized access to the administrator control panel. Eloi Vanderbeken, the one who has identified the issue, reveals that a backdoor present in the devices can be used to reset the password for the web administration panel. The existence of this backdoor has been confirmed in Linksys WAG200G, WAG320N, WAG54G2, WAG120N and WAG160n, and Netgear DGN3500, DG834 v3, DG834G V2, N150, and DM111Pv2. At least one LevelOne and Cisco router models are also impacted. In case you're wondering what these devices have in common, one Hacker News commenter believes they're made by SerComm, the company that manufactured many old Linksys DSL modems. A complete list of devices in which the backdoor might be present, and ones not affected is available in the advisory posted by Vanderbeken on GitHub. To read more click **HERE**

Chromium to Encrypt Cookies for Extra Security

SoftPedia, 3 Jan 2014: Chromium users will from now on get their cookies encrypted before they are saved as a security measure. Google's François Beaufort said on Google+ that Chromium would encrypt cookies with the users' operating system's mechanisms before writing them to the hard drive. This should be quite useful in giving them another security layer against malicious access to data from these cookies. The change is directed at desktop operating systems, namely Windows, Mac and Linux. Chrome OS and Android already apply such encryption techniques, so the alterations are mostly designed for Chromium users of all other operating systems. Web cookies are small pieces of data sent from websites and stored in a user's web browser. These are used to remember information about someone's browsing activities and may even store passwords, personal details and previously entered forms – such as credit card data and delivery addresses. If these are not encrypted, hackers could easy get access to them and, thus, to the content they carry. To read more click **HERE**

FireEye Buys Mandiant in $1 Billion Deal

DarkReading, January 02, 2014: FireEye today announced today that it has purchased privately held incident response (IR) and endpoint security firm Mandiant in a $1 billion deal consisting of 90 percent in stock and 10 percent in cash transactions. The two firms already had close ties. In April 2012, they said they would integrate FireEye's network detection with Mandiant's host-based detection features to offer more comprehensive protection against advanced attacks. The goal was to correlate FireEye's malware analysis with Mandiant's endpoint view for a more complete picture of an attack, the companies said at the time. The acquisition created quite a buzz around the industry today, with two leading-edge and widely respected security firms now under one roof. Mandiant will become a global services

and cloud solutions arm of FireEye, offering security consulting, incident response, and managed services. Its endpoint threat detection and response line will be incorporated into FireEye's new Oculus continuous monitoring platform. Kevin Mandia, founder and CEO of Mandiant, was named senior vice president and chief operating officer of FireEye. "This is an exciting day," Mandiant said in an investor call about the acquisition. "What I've learned ... is that every customer wants host-based protection and a network-based product. We want to bridge these so when there's a network alert" it's handled quickly at the affected endpoints, he said. "People have been asking us for this for years, and we're going to provide it." David DeWalt, chairman of the board and chief executive officer of FireEye, called Mandiant the "gold standard" in security. "They often get the first call when a serious breach occurs in an organization," he said. "Strategically, Mandiant brings us closer to the breach when it occurs." DeWalt said the acquisition of Mandiant, which made $100 million in revenue last year, fits with the company's stated strategy during its IPO tour last year. He said the addition of Mandiant's family of products allows the company to leverage the endpoint management framework for its virtual machine (VM)-based technology in its Multi-Vector Virtual Execution engine, which supports real-time threat protection for Web, email, data center, and mobile and is used by some 1,500 customers in the government and private sector. One of the first fruits of the acquisition: a VM-based next-generation intrusion prevention system (IPS) that will roll out in the first quarter of this year, DeWalt said. "There are other products in our pipeline that we are not announcing today" as well, he said. Mandiant's around 500 employees bring the FireEye employee count to around 2,000, he said, spanning more than 40 countries. Mandiant traditionally has had a tiny international presence, with less than 5 percent of its sales outside the U.S., so the acquisition will give the firm global exposure. "We will deliver a full array of services in vulnerability assessment, incident response management, and continuous monitoring," DeWalt said. Mandiant became more of a household name early last year when it published a detailed report exposing APT-1, a Chinese cyberespionage unit associated with the Chinese military. The firm's report on APT-1 said the unit had been behind targeted attacks on hundreds of companies across 20 major industries, mainly in English-speaking countries. "We have been on the frontlines of the cyberbattle field. Who are you gonna call? Mandiant owns that space, and it's an important space to own," Mandia said of his 9-year-old company. "We started building footprints of an attacker ... FireEye's virtual detection is the best detection" of advanced malware, he said. Mandiant has worked with 33 percent of the Fortune 100, and its 500 customers represent 13 different industry sectors. About half of its sales come from endpoint products and subscriptions, he said, and the other half from incident response engagements. Mandiant competitor Access Data says the acquisition demonstrates how IR and forensics are becoming "hot." Craig Carpenter, senior vice president of strategy for AccessData, says forensics and IR are now part and parcel of cybersecurity. "The reason for this deal is that we now live in a world of constant compromise. When you know you will be compromised, you can't just continue trying to keep the bad guys out -- you also need to investigate every compromise, figure out what happened, prevent it from ever happening again, and clean up the mess," he says. But Carpenter says Mandiant's approach to IR "only makes sense if a customer will only get compromised once" -- which is obviously not the case for virtually anyone -- "or where the compromise is a bespoke event that must be dealt with as a one-off." And "for every other compromise, companies need and want to be able to handle things in-house as much as possible," Carpenter says. To read more click **HERE**

Backdoor in wireless DSL routers lets attacker reset router, get admin

ARS Technica, 2 Jan 2014: A hacker has found a backdoor to wireless combination router/DSL modems that could allow an attacker to reset the router's configuration and gain access to the administrative control panel. The attack, confirmed to work on several Linksys and Netgear DSL modems, exploits an open port accessible over the wireless local network. The backdoor requires that the attacker be on the local network, so this isn't something that could be used to remotely attack DSL users. However, it could be used to commandeer a wireless access point and allow an attacker to get unfettered access to local network resources. Eloi Vanderbeken described the backdoor in a PowerPoint posted with the code to Github. In his illustrated report, he explained how over the Christmas holiday he was trying to get access to the administrative console of his family's Linksys WAG200G wireless DSL gateway wirelessly—mostly so he could limit how

much bandwidth the others in the house were using. But Vanderbeken had previously turned off wireless access to the administration web console (and had forgotten his administrative password). Performing a scan, he found that the router responded to messages over an unusual TCP port number: 32764. A search of the web found other Linksys and Netgear router owers had found the same service, but there was no documentation for what it did. So Vanderbecken downloaded a copy of the Linksys firmware and commenced reverse-engineering the binary MIPS code. What he found was a simple interface that allowed him to send commands to the router without being authenticated as the administrator. On his first attempt to brute-force the interface, the router flipped its configuration back to factory settings, causing his family members to all lose Internet access at the same time. After some additional testing, Vanderbecken found that the interface allowed him to execute a number of commands directly against the router, including a command-line shell. Using the commands he discovered, he was able to write a script that allowed him to turn wireless access to administration on and reset the web password, and published the script (with his cartoon report on the backdoor) to Github. The code of Vanderbecken's script to gain wireless access to the administrative console of DSL routers with the backdoor.Soon, confirmations that the backdoor worked with other models of Linksys and Netgear wireless DSL modems came flooding in. A commenter on Hacker News noted that the backdoor might effect wireless routers with DSL modems from SerComm, which manufactured many of Linksys' older DSL modems. A list of SerComm devices from various vendors matches up with the router-modems reported as vulnerable thus far.
http://arstechnica.com/security/2014/01/backdoor-in-wireless-dsl-routers-lets-attacker-reset-router-get-admin/