The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

29 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 27, Wired.com – (International) **Bitcoin exchange CEO charged with laundering $1 million through Silk Road.** The CEO of Bitcoin exchange BitInstant was arrested and charged January 26 with allegedly engaging in money laundering for working with another individual to sell more than $1 million of Bitcoins to users of the Silk Road underweb marketplace. The individual alleged to have worked with the CEO was also arrested in Florida January 27. Source: http://www.wired.com/threatlevel/2014/01/bitcoin-exchangers-arrested/

January 24, Wall Street Journal – (International) **Coca-Cola: Stolen laptops had personal information of 74,000.** Coca-Cola Co. announced January 24 that unencrypted company laptops containing the personal information of up to 74,000 U.S. and Canadian employees were stolen from the company's Atlanta headquarters by a former employee. The laptops were recovered by Coca-Cola, but the company cannot confirm if the information was misused. Source: http://online.wsj.com/news/articles/SB10001424052702304632204579341022959922200

January 27, Sacramento Bee – (California) **UC Davis Health System emails compromised.** University of California, Davis Health System officials announced January 27 that hackers compromised the email accounts of three doctors in a December 2013 phishing attack, potentially gaining access to personal or medical information of nearly 1,800 patients. The health system notified affected patients and was continuing to investigate the incident. Source: http://www.sacbee.com/2014/01/27/6106308/uc-davis-health-system-emails.html

January 28, Softpedia – (International) **Researchers discover first Android bootkit, 350,000 devices already infected.** Researchers at Doctor Web discovered what is believed to be the first Android bootkit, dubbed Android.Oldboot, which infects Android devices and waits for commands from a server to perform actions such as the downloading, installation, or deletion of apps. Researchers believe it is being spread via modified firmware updates, with the majority of the 350,000 infected devices found in China. Source: http://news.softpedia.com/news/Researchers-Discover-First-Android-Bootkit-350-000-Devices-Already-Infected-421383.shtml

January 28, Softpedia – (International) **NetSky worm spreads via email attachments.** Researchers at Symantec identified a cybercriminal operation using a worm dubbed NetSky that sends several different phishing emails containing the worm to the same email addresses. If a user opens the attached files the worm sends a copy of itself by email to the user's contacts. Source: http://news.softpedia.com/news/NetSky-Worm-Spreads-via-Email-Attachments-421279.shtml

January 28, Softpedia – (International) **Foursquare flaw could have been exploited to obtain users' email addresses.** A researcher published findings related to a vulnerability in Foursquare that could have been used to obtain users' email addresses by altering part of a URL used to accept friend requests. The issue was fixed in 2013 but the researchers' findings were only recently disclosed. Source: http://news.softpedia.com/news/Foursquare-Flaw-Could-Have-Been-Exploited-to-Obtain-Users-Email-Addresses-421523.shtml

January 28, Softpedia – (International) **Google Chrome 32.0.1700.102 fixes memory corruption bug in V8.** Google released the latest update to its Chrome browser, including patches for 14 security issues, including a use-after-free error occurring with SVG images and a memory corruption vulnerability in the V8 JavaScript engine. Source: http://news.softpedia.com/news/Google-Chrome-32-0-1700-102-Fixes-Memory-Corruption-Bug-in-V8-421283.shtml

January 27, Dark Reading – (International) **Air Force researchers plant rootkit in a PLC.** Researchers with the U.S. Air Force Institute of Technology created a prototype rootkit that can be installed on programmable logic controllers (PLCs) via modified firmware, USB device, or connected laptop and disrupt operations. The rootkit exploits the lack of security and monitoring capability in most PLCs. Source: http://www.darkreading.com/attacks-breaches/air-force-researchers-plant-rootkit-on-a/240165715

January 27, Softpedia – (International) **Cybercriminals steal FTP credentials with fake FileZilla.** Avast researchers warned users of cybercriminals using a fake version of the FileZilla FTP client to steal users' FTP credentials. The fake FileZilla client can then upload the credentials to a server for use in hosting malware or stealing data. Source: http://news.softpedia.com/news/Cybercriminals-Steal-FTP-Credentials-with-Fake-FileZilla-421070.shtml

Many Android apps can track your location, access photos

Heise Security, 29 Jan 2014: An alarming proportion of Android applications can find and open private photographs on smartphones, track users' locations, divulge e-mail addresses over the internet and leak address books and phone logs, according to an analysis of 836,021 Play Store Android applications. Over 35% of the apps analyzed by Bitdefender can track a user's location, with almost 3% being able to access the location even when the app is running in the background without the user's knowledge. More than 6% of these apps can also send the device location over the internet. The data also revealed that up to 3% of the apps analyzed can divulge e-mail addresses over the internet: 1,749 uploaded the address over an encrypted connection, with a further 1,661 doing so over an unencrypted connection that could easily be intercepted. The findings raise further concerns in light of revelations by former US intelligence contractor Edward Snowden that the NSA and GCHQ planned to extract data from users' smartphones via apps such as the popular Angry Birds game. "Our latest study shows that most smartphone or tablet owners have at least one app – and probably several – that could be used to siphon sensitive information from their phones," states Catalin Cosoi, Chief Security Strategist at Bitdefender. "A significant proportion of applications were shown to be capable of divulging details over the internet using an unencrypted connection. With phones now bearing more resemblance to mini computers, it is particularly worrying when you consider the vast amount of highly personal data about one's identity, schedule, friends, activities and work that each device can contain," Cosoi added. Unauthorized permissions may provide access to a device's location, address books, telephone logs and geographic data from photos uploaded to the mobile versions of social networking sites. Facebook and Twitter both clear photos of metadata before publication, but a third party could duplicate the info as it travels across the carrier's mobile network and stores it for further processing. This can also happen when third-party ad providers take data from the phone to use for targeted advertisements. In this case, the ad network only serves as a vector. Bitdefender's analysis also revealed that over 5% of the apps analyzed could locate and open photos on a phone, with almost 10% including permissions to read contact lists. Many have a legitimate need for

this data but others are clearly intrusive. Cosoi adds: "Permissions related to social networks and the device's sensors such as the camera, microphone and GPS, are highly likely to collect and report inputs." To read more click **HERE**

SpyEye creator pleads guilty

Heise Security, 29 January 2014: Aleksandr Andreevich Panin, a Russian national also known as "Gribodemon" and "Harderman," has pleaded guilty to conspiracy to commit wire and bank fraud for his role as the primary developer and distributor of the SpyEye banking Trojan. Operating from Russia from 2009 to 2011, Panin conspired with others, including codefendant Hamza Bendelladj, an Algerian national also known as "Bx1," to develop, market and sell various versions of the SpyEye virus and component parts on the Internet. Panin allowed cyber criminals to customize their purchases to include tailor-made methods of obtaining victims' personal and financial information, as well as marketed versions that specifically targeted designated financial institutions. He advertised the SpyEye virus on online, invitation-only criminal forums, and sold versions of the SpyEye virus for prices ranging from $1,000 to $8,500. He is believed to have sold the SpyEye virus to at least 150 "clients," who, in turn, used them to set up their own command and control (C&C) servers. One of his clients, "Soldier," is reported to have made more than $3.2 million in a six-month period using the SpyEye virus. In February 2011 the FBI searched and seized a SpyEye (C&C) server allegedly operated by Bendelladj in the Northern District of Georgia. That server controlled over 200 computers infected with the SpyEye virus and contained information from numerous financial institutions. In June and July 2011, FBI covert sources communicated directly with Panin, who was using his online nicknames "Gribodemon" and "Harderman," about the SpyEye virus. FBI sources then purchased a version of SpyEye from Panin that contained features designed to steal confidential financial information, initiate fraudulent online banking transactions, install keystroke loggers, and initiate distributed denial of service attacks from computers infected with the malware. Bendelladj was apprehended at Suvarnabhumi Airport in Bangkok, Thailand, on Jan. 5, 2013 and was extradited from Thailand to the United States on May 2, 2013. His charges are currently pending in the Northern District of Georgia. Panin was arrested by U.S. authorities on July 1, 2013, when he flew through Hartsfield-Jackson Atlanta International Airport. The investigation also has led to the arrest of four of Panin's SpyEye clients and associates in the United Kingdom and Bulgaria. On Jan. 28, 2014, Panin pleaded guilty to conspiring to commit wire and bank fraud. Sentencing for Panin is scheduled for April 29, 2014. According to industry estimates, the SpyEye virus has infected more than 1.4 million computers in the United States and abroad, and it was the preeminent malware toolkit used from approximately 2009 to 2011. Based on information received from the financial services industry, over 10,000 bank accounts have been compromised by SpyEye infections since 2013 alone. Some cyber criminals continue to use SpyEye today. To read more click **HERE**

Weak Data-Breach Laws Leave Us All in a Compromised Position

Yahoo, Jan 27, 2014: If today's tech headlines follow the pattern of the rest of this month's news, we'll be able to celebrate the sixth anniversary of Data Privacy Day with a report that yet another company has seen its customers' information exposed through some massive, preventable data breach. Fortunately, strong federal laws ensure that we know about these incidents in time to protect ourselves—and ensure that retailers, banks and other organizations can share secrets about threats and vulnerabilities. Oh, wait, that last sentence is from the 2024 version of this post. This, however, is the 2014 edition, and so it must report that no such nationwide legal umbrella covers you and your various digits. You often have to hope that companies' own self-interests lead them to do the right thing. Most of the time, nothing too bad happens if they don't. Your credit-card firm refunds phony charges and sends you a replacement, the free credit monitoring offered to make up for the breach doesn't reveal subsequent mischief, and life goes on. But for an unlucky few, identity theft becomes an expensive and prolonged problem. Third parties can suffer too: A community theater in Redlands, Calif., saw its site used to test stolen credit-card numbers from across the country and then ate almost $30,000 in service fees levied by its payment-processing service after it refunded the bogus transactions. And we all wind up paying a little extra when poor security in credit-card terminals, subscriber databases and Web servers—none of which you have any power to fix on your own—increases the cost of doing business everywhere. Washington's

rules on the subject largely consist of privacy laws governing the health-care and finance industries. That leaves out a mall's worth of companies—Target, Neiman Marcus and Michael's, to name the last few big cases of retailers that had their networks hacked. Firms that do an especially bad job safeguarding people's data risk an investigation and fine by the Federal Trade Commission. But one of the highest-profile FTC targets, Wyndham Hotels, is questioning the commission's authority in court—and considering the last legal challenge of a regulator acting on less-than-clear authority, it could win. In effect, Washington has outsourced this work to the states. "Most kind of run-of-the-mill data-breach reporting obligations are driven by state regulations," said Jim McCullagh, a partner with Perkins Coie in Seattle and co-chair of its privacy and security practice group. But the problem with state laws is that there are so many of them. Forty-six states have passed laws with varying definitions of "personal information" and requirements for disclosure (the holdouts being Alabama, Kentucky, New Mexico and credit-card hub South Dakota), and companies doing business in more than one must figure out how to comply with all of them. That's not an easy exercise. The usual course, McCullagh explained, is that "the state that has the most stringent standard is the one that controls"—which leads to distant firms having to familiarize themselves with California or Massachusetts laws. In theory, it shouldn't take the threat of legal action to get companies to prevent breaches and notify customers promptly if they happen. They represent an expensive habit, at an estimated average cost of $204 per customer back in 2009, and customers can flee if they think a company's careless with their data. But not all companies are so easy to fire—try canning your cable company if no alternative runs to your house. Meanwhile, useful security upgrades like switching to "EMV" smart-chip security on credit cards get pushed back, and corporations responsible for breaches can still take their time to disclose. Sometimes that's for good reasons, such as not hindering a law-enforcement investigation. Sometimes you have a case like WellPoint. How to keep customer safety at bay In 2011, that Indianapolis-based insurance company waited five months to notify customers that poor security at its site exposed their information—then let Indiana's state attorney general find out about this breach from a newspaper report. This sloppiness earned the company a fine from the state… of $100,000. The Target debacle has renewed Congressional interest in the topic, in the form of bills such as the Personal Data Privacy and Security Act of 2014, introduced by Sen. Pat Leahy (D-VT) and the Data Security Act of 2014, put forth by Sens. Roy Blunt (R-MO) and Thomas Carper (D-DE). It shouldn't be that hard to adopt the best practices of the states and set a national standard—it could be a rare opportunity for Washington to lighten the regulatory burden for many companies without cutting customers loose first. But don't count on Congress switching into high gear and quickly resolving its differences. Wrote National Consumers League public-policy vice president John Breyault, an advocate for a nationwide disclosure law: "I hesitate to say that we're any closer to resolving those disagreements today than we were before the Target breach." Last year showed how thoroughly Congress could screw this up. After months of effort to craft a cyber-security bill that would encourage companies to share confidential security details with each other and with the government, the House passed a bill called the Cyber Intelligence Sharing and Protection Act. CISPA had a number of issues, but the biggest one was the in-retrospect laughable provision that gave companies blanket immunity to share information about threats and vulnerabilities with the National Security Agency—as in, the agency that was actively subverting security standards at the time. CISPA stalled out in the Senate, but the problem of companies not comparing notes about vulnerabilities remains. As my former Washington Post colleague Brian Krebs, the foremost reporter on this subject, observed in an e-mail two weeks ago about Target's troubles, "It's a month out from the breach, and we still don't have official details on what happened. That's inexcusable in my mind, and very short-sighted." To read more click **HERE**

Banks Planning Massive Transition from Windows XP

SoftPedia, 28 Jan 2014: Nearly 95 percent of the world's ATMs are still running Windows XP right now, according to a research we've told you about recently, which makes it pretty dangerous given the fact that Microsoft will discontinue the operating system in just two months. Even though the majority of banks are yet to begin the transition to a newer operating system for their cash machines, a new report claims that a massive upgrade is prepared in the last couple of months before the operating system is discontinued. Htxt.co.za is reporting that several South African banks have

prepared transition plans to either start or complete the switch to a newer platform before April. Nedbank, for example, has promised to complete the transition from Windows XP by the end of March, which means the update should be ready by the time Windows XP is retired. "The rollout [of upgraded machines] will be phased and it is earmarked for completion by 31 March 2014," says Preni Naidoo, executive for self-service banking at Nedbank. Others, on the other hand, are yet to decide on the next destination. FNB, one of the local banks whose ATMs are still running Windows XP, said that a decision is yet to be made, but several plans are under consideration right now. "We are aware that Microsoft Windows XP support ends in April 2014 and we are currently implementing a solution," a company representative told the source. Windows XP will be officially retired on April 8, with Microsoft announcing that no security patches and vulnerability fixes would be released beyond this date. Of course, the company hopes to see the majority of users migrating to Windows 8.1, but 28 percent of the desktop computers worldwide are still powered by Windows XP right now, according to third-party statistics. To read more click **HERE**

Patnote Virus Used to Distribute ZeuS Trojan

SoftPedia, 28 Jan 2014: Security researchers from Trend Micro have spotted an interesting malware distribution campaign. Cybercriminals are using the Patnote (Pioneer) virus to spread ZeuS (Zbot). When the Patnote file infector is launched, it appends its code to all executable files, including ones on removable and network drives. This code is designed to drop and execute the embedded ZeuS version (TSPY_ZBOT.PNR) into the "User Temp" folder, and infect other executables. The fact that Patnote spreads across multiple systems makes the threat more difficult to remove. It also allows ZeuS to infect networks with restricted Web access. It's also worth noting that Patnote employs some mechanisms that prevent researchers from analyzing it. It's designed to stop working if analysis tools such as StudPDE, ProcDump, OllyDbg or WinHex are detected. To avoid getting your system infected with this threat, avoid clicking on suspicious links, and always keep your antivirus software updated. To read more click **HERE**

Unprecedented Alert: State Department info-tech still riddled with security gaps

Fox News, 28 Jan 2014: More than three years after U.S. Army Pvt. Bradley Manning handed over hundreds of thousands of sensitive State Department cables to WikiLeaks, the department's inspector general has warned in stark terms that State has done little since 2010 to fix an info-tech system that is riddled with security gaps, and has no plan yet for how to fix it. At risk, the IG says, is not only "classified information vital to the preservation of national security in high-risk environments across the globe," but the personal information on file concerning about 192 million American passport-holders. The public version of the inspector general's accusations -- contained in an unprecedented "management alert" to State's top officials and in the managerial responses to the alert -- have been heavily redacted for security reasons. The alert was circulated in the State Department bureaucracy in November. After a back-and-forth process between department managers and the IG's office, it became accessible to outsiders in mid-January. The problems it describes, however, have been festering far longer than that. Among other things, the alert says that:

-- between 2011 and 2013 alone, six lengthy and detailed reports on information security (five by State's IG and one by the GAO) have found "recurring weaknesses" in a wide variety of cyber-security issues, including how State hands out and keeps track of passwords; certifies whether information systems are authorized to operate securely; protects its hardware, files and operating systems from hackers or other unauthorized users; and how it scans its systems to detect wayward patterns of behavior.

--In most cases, despite repeated warnings, State Department bureaucrats have not formally reported the shortcomings to other federal agencies, including Homeland Security, though the inspector general argues it is obligated to do so.

--Nor, the watchdog says, has the department "remediated the identified vulnerabilities and risks." Translation: it hasn't done anywhere near enough to fix things, and, in some cases, nothing at all.

--One reason is that portions of the bureaucracy that are specifically tasked with handling information security issues have already been identified by the inspector general's office as part of the problem. Among other things, the alert references a previous IG report on the Bureau of Information Resource Management (IRM), a section of the State Department, where, the alert delicately says, it "identified a number of conditions that required management's attention."

In fact, that report, published last July, described an agency in shambles, whose members often were simply no-shows at inter-departmental meetings, and can't even keep track of budget receipts. Much of its work was being done, the report said, by outside contractors, including work that should only be done by government employees. The current alert also observes that as of last August, IRM had an improbable total of 6,369 system administrators, with clearance to "collaboratively manage and troubleshoot issues" across the State Department "network wide." The report notes that Edward Snowden, the NSA employee whose theft of a huge trove of security-related documents is still reverberating across the intelligence world, was similarly a contracted systems administrator. As a further issue for concern, in a heavily censored section of the alert, the alert makes reference to 36 individuals with access to unspecified areas of IT that didn't have appropriate security clearances for the work. In essence, the alert is a higher decibel repeat of the central concern of the six previous reports it documents: plenty of the most important problems in the State Department's IT systems have been known for years, and not much has been done about them. In 2012, for example, the inspector general found that 14 conditions identified as problematic in a report the previous year on State's information security had gone uncorrected. In 2013, the number of uncorrected "findings" had risen to 20. Indeed, the lack of enough movement on critical security issues is the main reason for the use of the unprecedented "management alert," according to officials in the inspector general's office, who described the document as a "new product." It is also the product of new Inspector General Steve Linick, who was appointed to the job last September. A one-time federal prosecutor, Linick is the first IG since 2008 to hold the job on something other than an acting basis, and the management alert seems clearly intended to show the State Department bureaucracy that there is a new sheriff in town. Or, as one official in the inspector general's office told Fox News, "One of the purposes of the alert is to ensure that individuals at the highest levels of management are aware of the problems." In one sense, the stratagem has worked. In his response to the alert, James Millette, head of State's ungainly-titled Management Control Steering Committee, declared that the bureaucracy is already preparing a "corrective action plan" that is one of the inspector general's main recommendations. A State Department official told Fox News that a due date for the document is January 31; a draft of the plan began circulating in December. Whether the "corrective action plan" will get to the entire root of the matter is still an open question. Millette's response to the "management alert" says that it will be agreed to by members of his committee, but only presented to the inspector general for "comment." Moreover, the committee is pushing back hard against two IG recommendations. The first is that the deficiencies in State Department IT operations be labeled a "material weakness" a designation that would require the problems to be formally communicated to the DHS -- something that the IG's office has urged at least twice before, without success. Instead, State's managers "respectfully disagree on the level of severity that these weaknesses collectively represent," as Millette put it in his formal reply to the IG alert. They continue to insist that the problems are only a "significant deficiency," meaning that their resolution -- and exposure -- stays within the department itself. The bureaucracy also is pushing back against another IG recommendation, that "penetration tests" of the suspect information security systems be carried out by the NSA rather than State's own security department. The department's top managers would prefer the in-house solution, but the inspector general argues that the issue is not whether State Department security personnel can carry out the tests, but "its independence and perceived independence."
To read more click **HERE**