The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

10 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 9, Softpedia – (International) **Malware stole data from computer at Japanese nuclear power plant.** Malware installed on an administrative computer at the Monju nuclear power plant in Japan could have potentially stolen around 42,000 private documents from the plant's systems. The malware was installed when a worker attempted to update a video playback program. Source: http://news.softpedia.com/news/Malware-Stole-Data-from-Computer-at- Japanese-Nuclear-Power-Plant-415175.shtml

January 9, Softpedia – (International) **40% of iOS banking apps leak sensitive data through system logs.** A researcher at IOActive analyzed 40 mobile banking apps for iOS devices and found several security issues, including that 40 percent of apps were vulnerable to man-in-the-middle attacks. Source: http://news.softpedia.com/news/40-of-iOS-Banking-Apps-Leak-Sensitive-Data-Through-Systems-Logs-415274.shtml

January 9, Softpedia – (International) **Scam emails distribute malware that steals Bitcoins from Bitcoin-Qt users.** Researchers at LogRythm analyzed an email attack campaign targeting users of the Bitcoin-Qt wallet service that directs users to a Web site hosting malware that steals Bitcoins from the user's wallet. Source: http://news.softpedia.com/news/Scam-Emails-Distribute-Malware-That-Steals-Bitcoins-from-Bitcoin-Qt-Users-415253.shtml

January 8, FCW – (National) **GAO: Security breach response by feds is uneven.** The U.S. Government Accountability Office released a report January 8 citing that several U.S. agencies are inconsistent with responding to security breaches that involved personally identifiable information (PII) and do not consistently document the evaluation of incidents and lessons learned. Source: http://fcw.com/Articles/2014/01/08/GAO-security-PII.aspx

January 9, Softpedia – (Virginia; Arizona) **Man admits hacking former employer's systems to damage servers and reputation.** A Tucson, Arizona man who previously worked for an undisclosed cloud computing services provider in Virginia admitted to continuing to access the systems of his former employer and to shutting down a key data server, causing hundreds of thousands of dollars in damage and making customers' data inaccessible for several hours. Source: http://news.softpedia.com/news/Man-Admits-Hacking-Former-Employer-s-Systems-to-Damage-Servers-and-Reputation-415363.shtml

January 9, The Register – (International) **Anatomy of a 22-year-old X Window bug: Get root with newly uncovered flaw.** A flaw in the X Window System, which underpins many Linux desktops, was discovered that could allow a logged-in users to crash the X server or execute injected code as a supervisor. The stack buffer overflow issue has been in existence since 1991 and is present in all versions of X11. Source: http://www.theregister.co.uk/2014/01/09/x11_has_privilege_escalation_bug/

January 9, Softpedia– (International) **The Straight Dope forum hacked, user passwords stolen.** The forum of newspaper column The Straight Dope was compromised by attackers that accessed usernames, hashed passwords, and email addresses. Source: http://news.softpedia.com/news/The-Straight-Dope-Forum-Hacked-User-Passwords-Stolen-415094.shtml

January 9, Softpedia – (International) **Network Time Protocol abused in DDoS attacks on gaming servers.** Researchers found that recent distributed denial of service (DDoS) attacks against several online gaming services by a group called DERP Trolling were launched by abusing the Network Time Protocol. Source: http://news.softpedia.com/news/NTP-Protocol-Abused-in-DDOS-Attacks-on-Gaming-Servers-415059.shtml

January 8, IDG News Service – (International) **Nvidia takes customer site offline after SAP bug found.** Nvidia took their customer service Web site offline January 8 after a vulnerability in their version of SAP NewWeaver was reported. The vulnerability could let an unauthorized attacker take full control of the portal platform and was patched by SAP 3 years ago. Source: http://www.networkworld.com/news/2014/010914-nvidia-takes-customer-site-offline-277527.html

January 8, Softpedia – (International) **Spammers use Asprox botnet to distribute malicious Atmos Energy emails.** Researchers at Solutionary found that a recent spam campaign using Atmos Energy-themed emails was launched using the Asprox botnet. The researchers also found that the group behind the spam emails has recently been varying the themes of the spam it sends according to holidays and news events. Source: http://news.softpedia.com/news/Spammers-Use-Asprox-Botnet-to-Distribute-Malicious-Atmos-Energy-Emails-414836.shtml

Keyloggers Become Irrelevant with the SecurePro Keyboard

SoftPedia, 10 Jan 2014: If you're afraid someone will steal your passwords via keylogging, consider buying the totally awesome SecurePro keyboard from Matias. It has more benefits than you probably need. To get one thing out of the way quickly, the thing is not cheap. To own it, you'll have to shell out $169.95 (€125.00), which is three times more than Apple's own Wireless Keyboard. The reason is because it's stellar! According to its makers, "The Secure Pro connects wirelessly to your computer via an AES encrypted USB nano receiver — the strongest level of encryption available in a keyboard. Even with a supercomputer, it's been estimated to take a billion-billion years to crack." The design is brilliant, and although it's not the thinnest keyboard out there, it's said to have such a powerful battery that it can hold up to a full year without a single charge. This feature alone makes one throw Apple's wireless keyboard into a drawer somewhere and never look back. Apple's device requires a fresh supply of batteries on a monthly (sometimes weekly basis). There's more. The SecurePro is said to be extremely quiet, and its creators even have a sound demo available on their site to compare it to the noise made by other keyboards. The keys are laser-etched, meaning they'll never wear off, and the buttons are curved – reminiscent of old-style keyboards. According to Matias, that's how keyboards should have stayed. The company explains: "The latest trend in keyboards is to have very flat & wide keys, with little or no space between them. You see this a lot on laptops and netbooks. While they look great, they can also be a little tricky to type on. The flatness makes it very easy to slide out of home row and lose your bearings. The Secure Pro bucks this trend. It has traditional sculpted keytops, curved to fit your fingertips, and keep you from sliding out of home position." Other key features include the high-polling rate (which has to do with the lag between when you hit a key and when it registers), anti-ghosting circuitry, audio and media controls via Fn key, two USB charging ports which can be used to charge other devices, and Mac and PC compatibility. "We designed it for PCs, but you can use it on a Mac. Simply plug in the USB nano receiver, and then configure the Alt & Win keys to be Option & Command, just like a standard Mac keyboard," says Matias. Oh and, there's a bonus for Mac users. To read more click **HERE**

Target Says the Personal Details of 70 Million People Have Been Stolen by Hackers

SoftPedia, 10 Jan 2014: Target continues to investigate the recent data breach. In a statement published on Friday, the retailer revealed that the hackers stole the personal details of up to 70 million individuals. The information includes names, mailing addresses, and phone numbers or email addresses. The company says that much of the data "is partial in nature." Target says that it will notify customers whose email addresses they have. However, the organization highlights the fact that the emails it will be sending out contain general tips on how to avoid falling victim to scams. The communications will not request recipients to provide any personal information. It's important to remember this, because cybercriminals and fraudsters have already started launching scams that leverage news of the breach. "I know that it is frustrating for our guests to learn that this information was taken and we are truly sorry they is having to endure this," stated Gregg Steinhafel, president and CEO of Target. "I also want our guests to know that understanding and sharing the facts related to this incident is important to me and the entire Target team." The company also emphasizes the fact that in case any fraudulent charges are made as a result of the breach, impacted individuals are not liable for them. In addition, victims of the incident are being offered one year of free credit and identity protection services. Initially, Target noted that around 40 million people were impacted. However, as the breach is being investigated, more details are coming to light. It's still uncertain how the cybercriminals managed to hack the retailer's systems, but experts say they've most likely used a piece of malware. Krebs has identified an individual who appears to be responsible for selling the stolen information on the underground market. To read more click **HERE**

Peru's Ministry of Interior Admits Being Hacked by LulzSec Peru

SoftPedia, 10 Jan 2014: In late December 2013, hackers of LulzSec Peru announced hacking into the systems of the country's Ministry of Interior. At the time, they leaked what appeared to be classified documents and email communications. According to Elgolfo.info, the Ministry of Interior has admitted that the hackers breached its systems and intercepted the emails of several officials. The leaked files also include information related to mining plans of the Newmont Mining Corporation. The ministry says it will file a report with the prosecutor. If they'll be identified and convicted for their crimes, the hackers face up to 10 years in prison. The group has attacked numerous government organizations from Peru, including the National Police, the Ministry of Women and Vulnerable Populations, and the presidency. To read more click **HERE**

Facebook Scam: Win a Disney Cruise with $2,000 Spending Money

SoftPedia, 10 Jan 2014: Scammers have created Facebook pages called "Walt Disney World" on which they claim to be giving users the chance to win a trip via Disney Cruise. "Great news, we're giving you a chance to get a Disney Cruise for you and 5 friends to 50 people from us with $2,000 spending money for a date of your choice. To enter Just Share this video then go here: www.disney-cruise-lines.com," the posts entitled "Win a Disney Cruise with $2,000 spending money" read. The so-called competition has nothing to do with Disney. Furthermore, the link doesn't actually point to the Disney Cruise Lines website, but to a site where users are instructed to complete a survey in order to allegedly win various prizes, Hoax Slayer warns. Each time one of these surveys is completed, the scammers make some money via affiliate networking services. Furthermore, some of the sites also instruct users to hand over personal information, which can also be monetized in various ways. Finally, by tricking users into liking their bogus Facebook pages, the cybercrooks are actually increasing their values. Pages with a large number of likes can be worth a lot of money on the underground market since they can be repurposed for other shady activities. If you're a victim of this scam, remove the post you've shared on your timeline. If you've completed the survey and handed over some personal information, watch out for other scams, since it's likely that you've ended up on the scammers' list of potential victims. I've seen three of these fake "Walt Disney World" pages, but others might appear soon. If you come across such pages, report them to Facebook. To read more click **HERE**

There Are Still at Least 22,000 Devices Infected with Flashback Mac Malware

SoftPedia, 10 Jan 2014: At its peak, the notorious Flashback Trojan infected over 600,000 Macs. However, while the threat has been mostly neutralized, experts say there are still at least 22,000 infected devices. Intego researchers have spotted 14,248 unique identifiers of the latest version of the threat that's designed to allow cybercriminals to steal information from infected devices. Apple has taken some steps to disrupt the Flashback botnet, including the release of a malware removal tool and the shutdown of the domains utilized by the malware. Intego owns some of the command and control (C&C) servers used by the Trojan. The security firm says it has spotted connections from infected devices trying to contact the sinkhole servers. For the time being, Apple and security outfits are closely monitoring the servers so it's difficult to revive the botnet. However, experts warn that the malware author could buy the C&C domain names in the future. To read more click **HERE**

Windows 8.1 Update 1 to Be Released via Windows Update

SoftPedia, 9 Jan 2014: Windows 8.1 Update 1 will be officially launched in April at the BUILD developer conference, but some important details are still unavailable at this point. For example, nobody knows for sure whether Windows 8.1 Update 1 will be delivered as downloadable patch, via Windows Store or through Windows Update, as Microsoft clearly needs to find a way to make it easy for users to get their hands on the update. Information provided by leaker Wzor and published by WinSuperSite reveals that Windows 8.1 Update 1 will be provided via Windows Update, as users experienced quite a lot of issues when trying to download Windows 8.1 from the store. To read more click **HERE**

Ireland's Office of the Data Protection Commissioner Investigates Adobe Breach

SoftPedia, 9 Jan 2014: Ireland's Office of the Data Protection Commissioner has confirmed that it has been investigating the data breach suffered by Adobe last year. The DPC's representatives have told ZDNet that the organization received complaints from a number of people regarding the Adobe data breach that affected at least 38 million customers. Adobe has notified the Irish data watchdog of the breach because Adobe Ireland is responsible for the information of customers from outside North America. At the end of the investigation, the company might be fined if the DPC determines that Adobe hasn't done enough to make sure that its customers' information is properly protected. The maximum fine that the organization can hand out is $340,000 (€250,000). In addition to customer information being stolen, source code for a number of products was also compromised. To read more click **HERE**

Israeli Expert Says Islamic Group Hasn't Hacked Systems of Airports Authority

SoftPedia, 9 Jan 2014: Earlier today, we reported that the Islamic Cyber Resistance Group claimed to have breached the systems of the Israel Airports Authority. However, an Israeli expert says they haven't hacked anything. Tal Pavel, a lecturer at Netanya Academic College and director of the MiddleEastNet website, has told the Times of Israel that this is just another example of "psychological warfare" conducted by Iran. He believes that the hackers, who posted the files they allegedly stole from the IAA on the website Wikileak.ir, likely obtained the IAA training manual from someone in Israel. However, the information that's in it is publicly available on the Internet. "Anytime this group can put together a plausible story they do," Pavel explained. "Anti-Israel groups feel better about themselves, and their patron governments and organizations are impressed, so they keep the funding up. Meanwhile, impressionable Israelis or potential tourists to Israel read these claims, so the hackers figure it may have an effect on some of them," he added. He says that all of the Islamic Cyber Resistance Group's claims are false, including the fact that they've hacked the system of the Israeli Defense Force, Israel's banking networks, and Saudi Arabia's aviation systems. This isn't the first time when Iran is said to be behind what appears to be a hacktivist group. In 2012 and 2013, a group called Izz ad-Din al-Qassam Cyber Fighters launched DDOS attacks against US banks for several months. US officials said the group was just a front used by Iran. Nothing has been heard of Izz ad-Din al-Qassam Cyber Fighters over the past months. At the time when they launched their attacks, they claimed that their goal was to get YouTube to remove the controversial Innocence of Muslims movie. To read more click **HERE**

Mexican Drug Lord Arrested Thanks to His Instagram Posts

SoftPedia, 8 Jan 2014: Jose Rodrigo Arechiga Gamboa, best known as "El Chino Antrax," one of Mexico's most wanted drug lords, was arrested in Amsterdam after arriving on the airport from Latin America under a fake name. The top drug handler of one of South America's most powerful cartels is also one of the two leaders of a group of hit men known as "Anthrax." Like many of today's criminals, Gamboa couldn't help himself not brag about his luxurious and extravagant lifestyle on the social media, thing that is believed to have led officers and investigators to build a case against him. The group, the notorious drug lord is believed to belong to, is accused of a series of murders, both for revenge and just to intimidate people. They were also in the middle of a bloody cartel war that took several lives and caused massive damage in 2008. Gamboa is suspected of being one of the right-hand men of the Sinaloa cartel bosses who control most of the drug trafficking in the area. El Chino Antrax was described as a fit and elegant person, with a passion for expensive champagne, sports cars and yachts, according to Daily Mail. The Instagram and Twitter accounts allegedly belonging to him were filled with photos of a guy fitting the description, with a blurred out face, posing with incredibly expensive items. From the most luxurious cars to customized automatic weapons and incredibly happy beautiful women, the man resembled the perfect description of the drug lord. The account even featured a photo of him appearing besides Paris Hilton, but reports say he just photobombed the star during an interview, notes Daily Mail. The detail appearing in most photos is a prominent skull-shaped ring that also appeared in a photo posted online while Gamboa was in custody, making people doubt the account was actually his. The photo posted just a few hours ago featured a hand wearing that particular ring on a newspaper article about his arrest. Authorities managed to gather important intel from the accounts that the man had, helping them build up a case and find details useful for his arrest. To read more click **HERE**

LinkedIn Sues Cybercriminals Responsible for Creating Fake Accounts

SoftPedia, 8 Jan 2014: LinkedIn has filed a lawsuit against the cybercriminals responsible for creating fake accounts which they use for spam and other malicious purposes. The social media company doesn't know who they are, but that doesn't mean the suit is in vain. The complaint filed by the company has been obtained by Bloomberg. It shows that the cybercrooks have tools that automate the account registration process. Interestingly, the tools are designed in such a way so that LinkedIn's monitoring doesn't detect any suspicious activities. LinkedIn is unhappy because if it's flooded with bogus accounts, the social media network becomes less useful. On one hand, the lawsuit might help the company identify the culprits, because it enables LinkedIn to enforce subpoenas to third parties, such as ISPs. On the other hand, even if the cybercriminals can't be identified, some experts say the social network might simply want to intimidate them. Facebook and Craigslist also filed similar lawsuits, but in their cases, they knew exactly whom they were targeting. LinkedIn is apparently following on the footsteps of Microsoft. Legal action plays an important role in disrupting the infrastructure used by the cybercriminals. To read more click **HERE**