THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

28 May 2014

Purpose
Educate recipients of cyber events to aid in protecting electronically stored DoD, corporate proprietary, and/or Personally Identifiable Information from theft, compromise, espionage

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

Disclaimer
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

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, and Sandia National Labs

Distribution
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings. Credit is given to the NMCIWG for the compilation of this open source data

How to guarantee your Android phone isn't spying on you

BGR, 27 May 2014: Last week, a developer revealed to the world just how easy it is for a nefarious hacker to use your Android phone to spy on you. With some simple code that utilized a serious security hole, the developer was able to create a program that caused an Android handset's camera to covertly capture photos on command, and then transmit those photos to a remote server without the user ever knowing. The idea that your smartphone might be taking photos of you and sending them to a hacker without your knowledge is absolutely terrifying. But as it turns out, there's an app that can guarantee your phone isn't spying on you. Shortly after our story about the aforementioned security hole was published, we were contacted by app developer Ziklag Systems. The company has created several security apps for the Android platform, but one in particular could be of interest to those who want to go the extra mile in order to ensure their privacy isn't being violated by their own smartphones. Dubbed Office Anti-Spy, Ziklag's app basically puts your Android phone in a locked down mode that disables most functions. Apps can no longer transmit data, the camera and mic are no longer accessible, and any attempts apps might make to access any system functions are blocked. Incoming phone calls and text messages will still be received while Office Anti-Spy is enabled. The app was designed to be used by companies looking to ensure information discussed during private meetings is kept private, but it can obviously be used by anyone looking to be absolutely certain that their privacy is not violated. Ziklag's app is a free download in the Google Play store, and it features a limited trial so users can ensure that Office Anti-Spy is compatible with their phones. Those looking to purchase an unlimited license can then do so for $20 on the Office Anti-Spy website. To read more click **HERE**

May 27, Help Net Security – (International) **Hybrid Zberp trojan targets bank users around the world.** Researchers with Trusteer identified a new piece of malware targeting financial institutions dubbed Zberp which combines the code and features of the Zeus malware and Carberp trojan. The malware is capable of several different information-stealing attacks and can use various methods to avoid detection. Source: http://www.net-security.org/malware_news.php?id=2774

May 23, IDG News Service – (International) **Researchers find large global botnet of infected PoS systems.** IntelCrawler researchers discovered a botnet known as Nemanja that has infected around 1,500 point-of-sale (PoS) terminals, accounting systems, and other retail systems in the U.S. and several other countries. The malware behind the botnet is able to collect payment card information and contains a keylogger to obtain other information entered into infected systems. Source: http://www.networkworld.com/news/2014/052314-researchers-find-large-global-botnet-281878.html

May 24, WMUR 9 Manchester – (New Hampshire) **Hospital data breach could affect more than 1,000 patients.** Elliot Hospital in Manchester, New Hampshire, notified 1,213 patients after 4 computers containing a limited amount of personal information were stolen from an employee's car in March. The hospital reported that the computers contained an archive of documents housed on its local drive as well as 20 emails which included patients' information. Source: http://www.wmur.com/news/hospital-data-breach-could-affect-more-than-1000-patients/26151974

May 27, Softpedia – (International) **Spotify warns Android users to upgrade app following hack.** Music streaming service Spotify advised users of its Android app to update the app in the next few days as a precaution after unauthorized access to *May 27, Softpedia* – (International) **Spotify warns Android users to upgrade app following hack.** Music streaming service Spotify advised users of its Android app to update the app in the next few days as a precaution after unauthorized access to company systems was detected in one user. Source: http://news.softpedia.com/news/Spotify-Warns-Android-Users-to-Upgrade-App-Folowing-Hack-444049.shtml

May 27, Softpedia – (International) **AVAST forum hacked, user passwords being reset.** AVAST Software reported that the company's forum was attacked during the weekend of May 24, compromising all user names, email address, and passwords. AVAST took the forum offline as a precaution while it resets all user passwords. Source: http://news.softpedia.com/news/AVAST-Forum-Hacked-User-Passwords-Being-Reset-443988.shtml

May 26, Help Net Security – (International) **In wake of breach, eBay has to deal with multiple Web vulnerabilities.** Several security researchers identified and reported two cross-site scripting (XSS) vulnerabilities and a login cookie issue with eBay Web pages that could be used to gain control of servers or steal users' information. Source: http://www.net-security.org/secworld.php?id=16919

Apple: Change Your Passwords, Apple ID Attack Is Not Our Fault

SoftPedia, 28 May 2014: A number of Apple IDs were compromised this week with Apple assuming no responsibility for the incident as the problem did not involve an iCloud breach, according to a brief statement from the company. Affected users are urged to change their passwords immediately. Earlier this week, news broke that a certain Oleg Pliss was hacking iPhones and Macs by exploiting Find My iPhone's ability to remotely lock an iCloud-enabled device. The hacker(s), most likely using a fabricated name, asked for a $100/€100 ransom via an alert to have the device unlocked. It isn't clear how the hacker(s) got their hands on the affected users' Apple IDs and passwords, but one plausible theory involves social engineering, phishing scams, etc. A user on the Apple Support Communities forums revealed that while he had not been affected, he had been prompted several days in a row to respond to a shady email that purported to be from Apple, where the Cupertino company had allegedly suspended his account for security reasons. The email asked the user to re-enter their Apple ID and password, in what would ensure a transfer of these credentials over to the cybercryminals' database. Security experts also warn that using the same name and/or password across multiple online services can also lead to this information getting leaked. While iCloud is fairly safe from hacking attacks, other services may not be so secure. Obtaining the password by exploiting one of these less secure services would then enable the hacker to try the same password on Apple's service and successfully compromise the account. In a brief statement offered to the media, Apple suggests this is pretty much what happened. Affected users are told to change their passwords ASAP, but the company fails to say what others should do to avoid falling into the same trap. "Apple takes security very seriously and iCloud was not compromised during this incident. Impacted users should change their Apple ID password as soon as possible and avoid using the same user name and password for multiple services. Any users who need additional help can contact AppleCare or visit their local Apple Retail Store." In reporting the incident, Softpedia posted a few best practices yesterday, suggesting that users employ two-factor authentication and a passcode lock on their

devices. The latter is not enough to protect against a password leak, but we hear the device can still be unlocked, buying the user time to restore their device and change their password before the device becomes unusable. Many impacted users have reported success in simply restoring their devices from a backup image, which goes to show how important it is to have a recent backup of your iOS/OS X installation at all times. To read more click **HERE**

Smartphone Hacking in Watch Dogs Is Real and Easy to Achieve

SoftPedia, 28 May 2014: I know that many of you have paid in advance to play Watch Dogs on your PCs, but you are still not able to do that despite the fact that the game has already been launched for at least 24 hours. However, the fact that Ubisoft's services are not on par with the success of its products is not our concern for now. Instead, I would like to focus on what Watch Dogs is all about and how that applies to real life. As many of you probably know by now, Watch Dogs' protagonist, Aiden Pierce, uses a smartphone loaded with sophisticated software to hack everything that's both electronically and mechanically controlled. You may be wondering how that is possible. Well, it appears that in the not so distant future, the city of Chicago is completely networked and the infrastructure is monitored and controlled from one gigantic and very complex operating system called CTOS (Central Operating System). Imagine what a person could do if it manages to hack into the system. Basically, it would have access to all the information stored on the huge server and could bend the rules to his/her own needs. For example, Pierce can hack into most of the city's ATMs and draw huge amounts of cash, or it can identify a person by simply focusing the smartphone's camera to their face. He can play with the traffic lights or disable a car's alarm if the smartphone finds vulnerability in the software, and it usually does. All that I have described above may sound futuristic, but we're living it right now. Aside from the fact that no major city relies on a single massive server, operating system to control its infrastructure, everything that's presented as "possible future" in Watch Dogs is real. Not a day goes by without a group of hackers attacking certain websites, databases, or government institutions. With the rapid technological advancement occurring in the last couple of years, the number of cyber-attacks has increased exponentially. Hackers use just about any gadget at their disposal in order to get access to sensitive data. The smartphone that helps Aiden Pierce hack into Chicago's mainframe computer is not in any way more sophisticated than today's handsets. The facial recognition technology is already standard to most smartphones on the market, so as long as a person has access to a database that contains the faces of all the persons living in a city, that person can easily identify anyone with the help of a standard smartphone. These days, sadly, it's not a big deal to listen to other people's phone conversations and record them using another smartphone. One of the newest hacking-related things that you can do with your smartphone, assuming that you have the right software installed, is tampering with the traffic lights. This is possible right now, but requires the hacker to stay at a certain range in order to be successful. I bet the procedure will be "improved" in the coming months, so anyone with certain knowledge could switch traffic lights with their smartphone while driving. Smartphones may soon replace PCs as main hacking tool. Talking about ATMs, it appears that these days, you only need to hack someone's computer in order to steal his/her bank account information. You don't really need to hack an ATM, though that has also been proven as very possible. But what about using your smartphone to hack a city's operating system and cause a major blackout, or desynchronizing that city's automatic timing for traffic lights or public transportation? That could really paralyze an entire city and could cause real disasters. Hopefully, no city will rely on a single mainframe computer and operating system to control the urban infrastructure, as that would be a huge mistake. The more powerful smartphones become, the more frequent they are used by hackers in their illegal activities. That will never change, so people need to learn how to protect their personal information, as there will always be someone that wants to take advantage of your gullibility. To read more click **HERE**

HeartBleed Virus Removal Tool Actually Carries a Trojan

SoftPedia, 28 May 2014: You can't blame anyone for not knowing malware from OpenSSL flaws in the same way you can't accuse Einstein of not figuring it all out before he expired. Case in point, a new spam campaign is trying to dupe Windows users into running a so-called HeartBleed Bug/Virus Removal Tool to clean their computers. To the untrained eye, the email in question will probably sound legitimate. Highlighted by the fine gents at Symantec, the spam campaign contains various clues that give away its malicious intent, starting with the email subject and ending with the attached file. "Symantec recently uncovered a spam campaign using Heartbleed as a way to scare users into installing malware onto their computers. The email warns users that while they may have done what they can by changing their passwords on the websites they use, their computer may still be 'infected' with the Heartbleed bug." The email goes as far as to claim that if your antivirus tries to warn you, it's because HeartBleed caused it to go insane. The campaign basically tries every trick in the book to get you to run the malicious executable hidden beneath a DOCX file. "The attached file is a docx file which may seem safer than an executable file to users. However, once the docx file is opened the user is presented with an encrypted zip file. Once the user extracts the zip file, they will find the malicious heartbleedbugremovaltool.exe file inside," Symantec explains. Whoever gets tricked into running the program will unknowingly have downloaded a keylogger that records keystrokes (containing your passwords, credit card info, and whatever you regularly type on your computer), takes screenshots, and sends this information to a free hosted email provider. "This type of social engineering targets users who may not have enough technical knowledge to know that the Heartbleed bug is not malware and that there is no possibility of it infecting computers. The email uses social and scare tactics to lure users into opening the attached file," Symantec warns. The security firm urges users to be skeptical whenever faced with emails that request personal information as well as emails containing attachments with instructions to execute the bundled program. "Users should also avoid clicking on links in suspicious messages," according to the Mountain View-based security company. The firm adds, "Symantec detects this malware as Trojan.Dropper and detects the downloaded malicious file as Infostealer [while the] Symantec.cloud Skeptic heuristics engine is blocking this campaign and detecting it as Trojan.Gen." To read more click **HERE**

Check Out Kaspersky's Real-Time Data on Cyber Attacks

SoftPedia, 28 May 2014: It's always interesting to see real-time information about the world around us, especially when it comes to the Internet. Well, Kaspersky has stepped up and it's keeping an eye on things, planning to deliver important information with as much accuracy as possible. The popular anti-virus maker has put together a site that it launched earlier this week, in which it provides real-time cyber stats. For instance, it may be interesting to know just how many cyber attacks happen in a day. The number – over 9.6 million before 5PM – should send a shiver down your spine and give you a grasp about how unsafe you are whenever you are online. Perhaps such frank numbers are what the world needs to take online security seriously. Kaspersky's site comes full of additional information. For instance, this year alone, Google users have already performed 336 billion searches, while over 148 billion emails have been sent today, while the number rises to 43,411 billion since the year began. Since we have mentioned security, it should be noted that over the past nearly six months, over 42,500 sites have been hacked, while the monthly online threats' number has risen to over 86 million. There are also over 33 million new Internet users that have joined in since the year began, which means that there are over 2.9 billion Internet users in the entire world, our of the 7.2 billion people populating Earth. More stats are available on Kaspersky's new site (link), so you should really check it out. To read more click **HERE**

Half of American adults hacked this year

CNN Money, 28 May 2014: Hackers have exposed the personal information of 110 million Americans -- roughly half of the nation's adults -- in the last 12 months alone. That massive number, tallied for CNNMoney by Ponemon Institute researchers, is made even more mind-boggling by the amount of hacked accounts: up to 432 million. The exact number of exposed accounts is hard to pin down, because some companies -- such as AOL and eBay -- aren't fully transparent about the details of their cyber breaches.

But that's the best estimate available with the data tracked by the Identity Theft Resource Center and CNNMoney's own review of corporate disclosures. The damage is real. Each record typically includes personal information, such as your name, debit or credit card, email, phone number, birthday, password, security questions and physical address. It's enough to get hunted down by an abusive ex-spouse. It makes you an easier target for scams. And even if only basic information about you is stolen, that can easily be paired with stolen credit card data, empowering impostors. Cyberattacks are growing so numerous that we're becoming numb to them. Researchers at IT company Unisys (UIS) say we're now experiencing "data-breach fatigue." To read more click **HERE**