THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

2 June 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

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

Java for OS X 2014-001 – Everything You Need to Know Before Installing

SoftPedia, 2 Jun 2014: Through its Security site, Apple announced yesterday that Java for OS X was being updated. The information provided by the Cupertino giant is scarce, but we have the full scoop for you in the paragraphs below. First off, here's Apple's terse description of the new Java for OS X 2014-001. "Java for OS X 2014-001 includes installation improvements, and supersedes all previous versions of Java for OS X. This package installs the same version of Java 6 included in Java for OS X 2013-005. This update uninstalls the Apple-provided Java applet plug-in from all web browsers. To use applets on a web page, click on the region labeled 'Missing plug-in' to go download the latest version of the Java applet plug-in from Oracle." For those of you who are surprised by Apple's decision to uninstall the Java applet plug-in from all web browsers, don't be. It's a thing they've been doing for a while to protect you against security threats (Java being one of the most targeted platforms by cybercrooks). To get the latest version of Java (currently that's Java 7), Apple recommends that you go straight to java.com and grab it from there. The Cupertino company no longer collaborates with Oracle on these updates, at least not like they used to, so Oracle has been left in charge with the updates and Apple has taken on the liberty to protect its users by disabling Java the applet plug-in whenever it senses danger. If, for some reason, you need Java 6 installed on your Mac, the 2014-001 release is precisely what you need. Download Java for OS X 2014-001 for your computer straight from Softpedia. Now for a few additional notes. As some of you already know, Java 7 is actually the latest version available. According to a memo on java.com, "Oracle's Java version 7u25 and below have been disabled by Apple on OS X. Updating to the latest release will allow Java to be run on Mac OS X." If you've uninstalled Java 7 and want to restore to Java 6, Oracle directs customers to Apple's KB article HT5559: "Java for OS X 2014-001: How to re-enable the Apple-provided Java SE 6 web plug-in and Web Start features." Oracle says Java 7 requires an Intel-based Mac running Mac OS X version 10.7.3 (Lion) and above, while the browser requirements are 64-bit Safari or Firefox. According to the specs list, "32-bit browsers such as Chrome do not support Java 7 on the Mac platform." For those of you looking for Java 6 on java.com, don't bother. It's not there. "For Java versions 6 and below, Apple supplies their own version of Java," according to Oracle. Finally, while Java does come pre-installed with OS X 10.6 Snow Leopard, starting with OS X 10.7 it is disabled by Apple. Also, to get Java 7 from Oracle, you will need to be running OS X 10.7.3 and above. Here are the Mac Java 7 installation instructions, straight from the mother-ship. To read more click **HERE**

Apps on your Android phone can take photos without you knowing

Heise Security, 27 May 2014: A researcher has demonstrated that it's possible for malicious attackers to create an Android app that will surreptitiously take pictures and upload them to a remote server without the user being aware of or noticing it. "There are many apps on Play Store that aim at taking pictures without any visual indication (ACLU-NJ Police Tape, Mobile Hidden Camera and more) but from what I found all of them require app activity to be visible and phone screen to be on," security researcher Szymon Sidor explained in a blog post. "Some of them manage to record video without visible preview." But he managed to create an app that does so without displaying any notification, without the presence of the app being visible (i.e. on the list of installed applications), and even without the screen being on. The good news is that users can protect themselves from this type of spying by being extra careful when reviewing apps they want to install, and the permissions they ask. Keeping a close eye on your Google Account, and setting up two-step verification is also a good idea, because an attacker that manages to hijack the account can install apps on your phone remotely, without your approval. To read more click **HERE**

Misconfiguration to blame for most mobile security breaches

Heise Security, 29 May 2014: Nearly 2.2 billion smartphones and tablets will be sold to end users in 2014 according to Gartner, Inc. While security incidents originating from mobile devices are rare, Gartner said that by 2017, 75 percent of mobile security breaches will be the result of mobile application misconfiguration.

"Mobile security breaches are — and will continue to be — the result of misconfiguration and misuse on an app level, rather than the outcome of deeply technical attacks on mobile devices," said Dionisio Zumerle, principal research analyst at Gartner. "A classic example of misconfiguration is the misuse of personal cloud services through apps residing on smartphones and tablets. When used to convey enterprise data, these apps lead to data leaks that the organization remains unaware of for the majority of devices." With the number of smartphones and tablets on the increase, and a decrease in traditional PC sales, attacks on mobile devices are maturing. By 2017, Gartner predicts that the focus of endpoint breaches will shift to tablets and smartphones. To do significant damage in the mobile world, malware needs to act on devices that have been altered at an administrative level. The best defense is to keep mobile devices fixed in a safe configuration by means of a mobile device management (MDM) policy, supplemented by app shielding and 'containers' that protect important data. Gartner recommends that IT security leaders follow an MDM/enterprise mobility management baseline for Android and Apple devices as follows:

- Ask users to opt in to basic enterprise policies, and be prepared to revoke access controls in the event of changes. Users that are not able to bring their devices into basic compliance must be denied (or given extremely limited) access.
- Require that device passcodes include length and complexity as well as strict retry and timeout standards.
- Specify minimum and maximum versions of platforms and operating systems. Disallow models that cannot be updated or supported.
- Enforce a "no jailbreaking/no rooting" rule, and restrict the use of unapproved third-party app stores. Devices in violation should be disconnected from sources of business data, and potentially wiped, depending on policy choices.
- Require signed apps and certificates for access to business email, virtual private networks, Wi-Fi and shielded apps.

IT security leaders also need to use network access control methods to deny enterprise connections for devices that exhibit potentially suspicious activity. "We also recommend that they favor mobile app reputation services and establish external malware control on content before it is delivered to the mobile device," said Mr. Zumerle. To read more click **HERE**

Hackers put security tool that finds payment card data into their arsenal

Computerworld, 2 Jun 2014: Bootleg versions of a powerful tool called "Card Recon" from Ground Labs, which searches for payment card data stored in the nooks and crannies of networks, have been appropriated by cybercriminals. Like a crowbar, security software tools can be used for good and evil. Bootleg versions of a powerful tool called "Card Recon" from Ground Labs, which searches for payment card data stored in the nooks and crannies of networks, have been appropriated by cybercriminals. This month, the security companies Trend Micro and Arbor Networks published research into point-of-sale malware, which has been blamed for data breaches at retailers such as Target and Neiman Marcus, sparking concerns over the security of consumer data. Both companies found that unauthorized copies of Card Recon had been incorporated into a malware program and a toolkit designed for finding and attacking POS terminals. "Card Recon looks to be a useful tool when wielded by an auditor or security staff, but it is clearly dangerous in the wrong hands," Arbor Networks wrote in its report. Card Recon is intended for organizations seeking to comply with the Payment Card Industry's Data Security Standard (PCI-DSS), a set of recommendations to safeguard payment card data. The software tool scans all parts of a network to see where payment card data is stored. Often, companies find card details stashed in unlikely and unknown places. Card Recon compiles a thorough report, and companies can then move to secure the data. The software requires license authorization before it will run, which prevents direct illegitimate use, said Stephen Cavey, Ground Labs' co-founder and director of corporate development, via email. But it's impossible to restrict access to Card Recon's software executable after a genuine customer has obtained it. More than 300 security auditors worldwide and thousands of merchant companies use

Card Recon, he said. "This is the unfortunate reality for all software vendors: It is common for criminals to acquire a copy of commercial software via unauthorized means and then reverse engineer that software to circumvent the licensing mechanisms that are designed to prevent its unauthorized use," Cavey said. When Card Recon is scanning, it has to be able to separate 16-digit numbers and other random data it finds from valid 16-digit credit card numbers. Credit card numbers can be validated by using a checksum formula called the Luhn algorithm. The malware Huq studied used Card Recon to validate and identify cards by brands such as Discover, Visa and MasterCard. Using Card Recon was faster than other validation methods, especially for large volumes of card data, he wrote. Arbor Networks wrote in its report that the attack toolkit it observed contained two cracked copies of Card Recon. In that instance, it appears Card Recon was being used for its intended purpose -- to find card numbers -- but for cybercriminals. If anything, the abuse of Card Recon strengthens a case for its legitimate use. Ground Labs' Cavey said the best defense is to remove sensitive data. To read more click **HERE**

Study: 432M hacked accounts in a year, large part of U.S. at risk

SC Magazine, 30 May 2014: About 432 million accounts were hacked in one year. Over the last 12 months, approximately 110 million Americans have had their accounts hacked, a study has found. The bleak figure was said to be a conservative estimate by the Ponemon Institute, which calculated the findings at the request of CNNMoney. According to the outlet, the number of hacked accounts among impacted Americans topped 432 million accounts during that time period. CNNMoney reported the stats on Wednesday, taking into consideration data tracked by the Identity Theft Resource Center and its own analysis of "corporate disclosures." In a Friday interview with SCMagazine.com, Larry Ponemon, head of the Ponemon Institute, said that the organization came up with the statistic – 110 million Americans impacted and 432 million accounts hacked – by pouring over data breach findings collected since last May. "Not every person that is a victim of the Target breach, for instance, will become the victim of identity theft," Ponemon said. "But they are still victims," he added, referring to the risk associated with exposed records. The study focused on breaches that were the result of "criminal or malicious activity," Ponemon said, not those induced by human error or system glitches. Left out of the data set was eBay's massive breach announced last week, Ponemon added, which reportedly impacted as many as 145 million customers, whose names, addresses, phone numbers, dates of birth, email addresses and encrypted passwords, were exposed to attackers. Ponemon continued, saying that the overlap of data breaches was another troubling consequence of such incidents. "Collecting a lot of information about an individual is more valuable [for attackers]," Ponemon said. "They'll take the data, and wait patiently. Then, two or three years after the breach, [the impacted] become the victim of identity theft." In March, security research and advisory firm NSS Labs released a report examining the impact of repeated breaches on personally identifiable information (PII), specifically, data that is hard, or impossible, for victims to change. The study noted that "static" data, such as Social Security numbers, dates of birth, and even physical addresses, are often stockpiled by criminals after breaches so that profiles are created using victims' leaked data. That study found that the PII of around 319 million Americans had been "repeatedly compromised" in the decade's 10 largest breaches. To read more click **HERE**

Home Depot staffer fired, tapped 30,000 accounts, shared card data

SC Magazine, 30 may 2014: Home Depot, which last experienced an insider breach in February, has fired and is prosecuting an employee who, for two weeks in May, accessed information on more than 30,000 customer accounts. Approximately 30,000 accounts were compromised. Less than 500 accounts had information distributed to third parties. Customer's names, addresses, phone numbers, dates of birth, brands, primary account numbers (payment card numbers) and expiration dates were stolen; the former employee accessed account information that he had access to and then distributed it to third parties. The employee was fired and is being prosecuted. Home Depot is reviewing access controls to ensure a similar incident does not occur in the future. All impacted individuals are being notified and offered a free year of credit monitoring services. The former employee was accessing the accounts from May 7 to May 21. The information related to transactions in the tool rental area of Home Depot stores. To read more click **HERE**

A beginner's guide to BitLocker, Windows' built-in encryption tool

Computerworld, 2 Jun 2014: The creators of TrueCrypt shocked the computer security world this week when they seemingly ended development of the popular open source encryption tool. Even more surprising, the creators said TrueCrypt could be insecure and that Windows users should migrate to Microsoft's BitLocker. Conspiracy theories immediately began to swirl around the surprise announcement. The creators of TrueCrypt shocked the computer security world this week when they seemingly ended development of the popular open source encryption tool. Even more surprising, the creators said TrueCrypt could be insecure and that Windows users should migrate to Microsoft's BitLocker. Conspiracy theories immediately began to swirl around the surprise announcement. Regardless of the true motivations behind the message, the TrueCrypt fiasco gives us a chance to talk about BitLocker — and how to use it. BitLocker is Microsoft's easy-to-use, proprietary encryption program for Windows that can encrypt your entire drive as well as help protect against unauthorized changes to your system such as firmware-level malware. BitLocker is available to anyone who has a machine running Windows Vista or 7 Ultimate, Windows Vista or 7 Enterprise, Windows 8.1 Pro, or Windows 8.1 Enterprise. If you're running an Enterprise edition chances are your PC belongs to a large company so you should discuss enabling BitLocker encryption with your company's IT department. To run BitLocker you'll need a Windows PC running one of the OS flavors mentioned above, plus a PC with at least two partitions and a Trusted Platform Module (TPM). A TPM is a special chip that runs an authentication check on your hardware, software, and firmware. If the TPM detects an unauthorized change your PC will boot in a restricted mode to deter potential attackers. If you don't know whether your computer has a TPM or multiple partitions, don't sweat it. BitLocker will run a system check when you start it up to see if your PC can use BitLocker. Here's the thing about BitLocker: It's a closed source program. That's problematic for extremely privacy-minded folks, since users have no way of knowing if Microsoft was coerced into putting some kind of backdoor into the program under pressure from the U.S. government. The company says there are no back doors, but how can we be certain? We can't. Sure, if BitLocker was open source most of us wouldn't be able to read the code to determine if there was a backdoor anyway. But somebody out there would be able to meaning there would be a much higher chance of any faults with the program being discovered. So with BitLocker's closed source nature in mind, I wouldn't count on this encryption program defending your data against a government actor such as border agents or intelligence services. But if you're looking to protect your data in case your PC is stolen or other situations where petty criminals and non-government types might mess with your hardware then BitLocker should be just fine. Installing/using BitLocker is straightforward; the first thing you'll need to do is fire up the Control Panel. When the Control Panel opens, type BitLocker into the search box in the upper right corner and press Enter. Next, click Manage BitLocker, and on the next screen click Turn on BitLocker. Now BitLocker will check your PC's configuration to make sure your device supports Microsoft's encryption method. If you're approved for BitLocker, Windows will show you a message like this one. If your TPM module is off then Windows will turn it on automatically for you, and then it will encrypt your drive. To activate your TPM security hardware Windows has to shut down completely. Then you will have to manually turn your PC back on. Before you go ahead with this process make sure any flash drives, CDs, or DVDs are ejected from your PC. Then hit Shutdown. Once you restart your PC, you may see a warning that your system was changed. In my case I had to hit F10 to confirm the change or press Esc to cancel. After that, your computer should boot back up and once you login again you'll see the BitLocker window. After a few minutes, you should see a window with a green check mark next to "Turn on the TPM security hardware." We're almost at the point where we'll encrypt the drive! When you're ready, click Next. Before you encrypt your drive, however, you have to save a recovery key just in case you have problems unlocking your PC. Windows gives you three choices for saving this key in Windows 8.1: save the file to your Microsoft account, save to a file, or print the recovery key. You are able to choose as many of these options as you like, and you should choose at least two. In my case, I chose to save the file to a USB key and print the key on paper. I decided against saving the file to my Microsoft account, because I don't know who has access to the company's servers. That said, saving your key to Microsoft's servers will make it possible to decrypt your files if you ever lose the flash drive or paper containing your recovery key code. Once you've created two

different instances of the recovery key and removed any USB drives, click Next. On the following screen, you have to decide whether to encrypt only the disk space used so for or encrypt your PC's entire drive. If you are encrypting a brand new PC without any files then the option to encrypt only the used disk space is best for you since new files will be encrypted as they're added. If you have an old PC with a few more miles on the hard drive you should choose to encrypt the entire drive. Once you've chosen your encryption scheme click Next. We're almost there. Make sure the box next to "Run BitLocker system check" is clicked so that Windows will run a system check before encrypting your drive. Once the box is checked click Continue...and nothing happens. You'll see an alert balloon in the system tray telling you that encryption will begin after you restart the PC. Restart your PC. When you log in this final time you should see another system tray alert telling you that the encryption is in progress. You can continue to work on your PC during the encryption phase, but things may be working a little more slowly than usual. Consider holding back on anything that might tax your system during initial encryption, such as graphics-intensive programs. After all those clicks, that's it! Just leave Windows to do its thing and in a few hours you'll have a BitLocker-encrypted drive. The length of time it takes BitLocker to fully encrypt your files depends on the size of your drive, or how much data you're encrypting if you're only encrypting existing data on a new PC. To read more click **HERE**