THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

27 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

June 26, Help Net Security – (International) **Data breaches in 2013 exposed 14% of all debit cards.** PULSE released the results of a study which found that 14 percent of debit cards from institutions in the study were affected by data breaches in 2013, and that consumers are continuing to shift to electronic payments, among other findings. Source: http://www.net-security.org/secworld.php?id=17055

June 26, NetworkWorld – (International) **Hackers found controlling malware and botnets from the cloud.** Researchers at Trend Micro released a blog post detailing the company's findings regarding botnets and malware being hosted and controlled through cloud servers. The researchers reported that they observed a malicious command and control server hosted on DropBox in order to disguise its traffic as legitimate corporate traffic, among other findings. Source: http://www.networkworld.com/article/2369887/cloud-security/hackers-found-controlling-malware-and-botnets-from-the-cloud.html

June 25, Securityweek – (International) **22 vulnerabilities found in Oracle Database Java VM implementation.** Security Explorations researchers reported finding 22 vulnerabilities affecting the Java Virtual Machine implementation used in Oracle Database which can be leveraged by an attacker to escalate privileges and execute arbitrary Java code on vulnerable Oracle Database servers. Six of the vulnerabilities have been fixed in the main codeline and are scheduled for a future Critical Patch Update. Source: http://www.securityweek.com/22-vulnerabilities-found-oracle-database-java-vm-implementation

Security Flaw Fixed in Android 4.4, Earlier Versions Still Affected
SoftPedia, 27 Jun 2014: A stack buffer overflow vulnerability that has been eliminated in the KitKat edition of Android is still affecting previous versions of the mobile operating system. Researchers at IBM discovered the security problem in the Android KeyStore service, which maintains cryptographic keys and their owners. By exploiting this vulnerability, an attacker could gain access to important information, such as the device's lock credentials, encrypted and decrypted master keys, data, and hardware-backed key identifiers from the memory, as well as the ability to perform crypto operations on behalf of the user. The flaw occurs when a stack buffer is created by the "KeyStore::getKeyForName" method. Roee Hay, who leads the application security research team at IBM, said that "this function has several callers, which are accessible by external applications using the Binder interface (e.g., 'android::KeyStoreProxy::get'). Therefore, the 'keyName' variable can be controllable with an arbitrary size by a malicious application" and, as a result, "the 'encode_key' routine that is called by 'encode_key_for_uid' can overflow the 'filename' buffer, since bounds checking is absent." In theory, taking advantage of the security risk can be achieved through a malicious app, but an exploit to leverage this vulnerability is not too easy to create because it has to get around memory protection mechanisms like Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) and Stack Canaries. "However, the Android KeyStore is respawned every time it terminates. This behavior enables a probabilistic approach; moreover, the attacker may even theoretically abuse ASLR to defeat the encoding," says Hay in the disclosure. IBM disclosed the findings privately to the Android Security Team on September 9, 2013, who provided a fix on November 11, 2013, making it a zero-day for a total of 63 days. The delay for

making the finding public was motivated by the fact that this is a critical vulnerability since it can lead to code execution. The security issue is considered critical and the recommended course of action is to update the operating system to the latest major version, which remains unaffected. At the moment there is no information of an exploit being used in the wild. Most owners of Android devices use the Jelly Bean edition of the operating system, versions 4.1.x, 4.2.x and 4.3, accounting for 58.4% of the total distribution. The KitKat revision has reached 13.6%. This means that in case an exploit for the aforementioned stack buffer overflow vulnerability occurs, the majority of Android users are susceptible to it. To read more click HERE

Windows 8.1 Update 2 "Close" to Reaching RTM

SoftPedia, 27 Jun 2014: There are a lot of Windows rumors swirling around these days and nobody can tell for sure whether they're true or not since Microsoft goes on all in on the secrecy card, but it appears that the company is very close to signing off the new Windows 8.1 Update 2. Russian leaker WZor, who until now provided us with pretty accurate info on what's to come for Windows users, says in a new tweet that Windows 8.1 Update 2 is very close to reaching RTM this week, which means that users could indeed receive it in August or September as it was rumored. This new report comes only two days after another rumor which claimed that Windows 8.1 Update 2 had already reached RTM, so there definitely must be some truth behind all these words. Windows 8.1 Update 2 might be presented for the first time to users and developers next month at the WPC 2014 conference that kicks off on July 13, before eventually receiving the green light for getting shipped to everyone running Windows 8.1 Update in mid-August. Although it didn't provide any information on this new Windows update, Microsoft confirmed at the BUILD 2014 developer conference in April that a second pack of improvements for its modern operating system is indeed coming, promising some pretty big changes that would make the desktop more familiar. Terry Myerson, head of the operating systems unit at Microsoft, said at that time that this update could include a Start menu and options to run Metro apps in their dedicated windows right on the desktop. It turns out, however, that such features might be delayed a little bit until early 2015 when two other projects are likely to get the go-ahead, namely Windows 8.1 Update 3 and Windows 9. "We set out to do this is a thoughtful way – one where we could enable more productivity for customers working in desktop mode, while building smart bridges to the new modern user experience and ensuring customers can get access to all your great apps in the Windows Store no matter where they are in the experience, or which device type they're on," Myerson explained in early April. Since Microsoft keeps all details secret, nobody can tell for sure whether Windows 8.1 Update 2 is indeed close to reaching RTM, but we wouldn't be too surprised to hear that these new tidbits are indeed true. Redmond clearly wants to tweak its operating system in such a way that it would tackle consumers' needs better on both desktops and tablets, so bringing Windows 8.1 Update 2 to the market faster is most likely a priority for everyone within the company. To read more click HERE

Zeus-Laden Parking Fines Affecting UK Citizens

SoftPedia, 26 Jun 2014: Computer users in the United Kingdom are assaulted by phishing emails claiming penalties for unpaid parking and containing a variant of the Zeus Trojan disguised as a PDF file. Zeus Trojan, also known under the name of Zbot, is famous for its infostealing capabilities that target sensitive banking details and online credentials. The email, with the subject line "Reminder notice do not ignore," has the letterhead of the UK Ministry of Justice and informs the potential victim that they have to pay £72/$122/€90 as a result of penalties accumulated in 28 days. It also says that a previous notice has been sent, allowing the victim to challenge the issue of paying the fine. There are vague details about the driveway where the car was parked, but the scammers are accurate as far as the parking duration is concerned. An attachment is provided for "photographic evidence." To make the matter look legitimate and convince the user to download the attachment, the perpetrators elevate the alleged risks of not paying the fine by saying that one of the consequences could be the inability to obtain credit in the future. "Failure to pay the full outstanding balance within 14 days of the date of this notice could result in the outstanding balance being registered as a debt against you," the message reads. The file (Form-STD-

Vehicle-150514.scr) is a malware dropper, identified by Bitdefender as Trojan.GenericKD.1681628, and it proceeds to download the Zeus Trojan variant. Bitdefender researchers determined that the dropper connects to a pharmaceutical website that is under the control of the criminals. It is unknown whether it is a legitimate location compromised by the attackers or a website specifically created for nefarious purposes such as malware distribution. The Zeus variant is then executed and the system infection is complete. Apart from stealing sensitive information that can lead to financial fraud, the threat can also receive remote instructions to download other types of malware or components that would increase its stealing capabilities or improve antivirus evading tactics. It appears that such emails began invading the inboxes of UK citizens a couple of months ago, with a spike recorded on May 15. According to Bitdefender, "in a two-hour period, one out of five samples was a bogus parking fine message." Attachments coming from suspicious sources should never be opened. Some of the signs of deceit include the email address from which the message was sent, which in this case is justice.gov.uk instead of the real one, that is justice.alerts@public.gov.delivery.com. To read more click **HERE**

This Animated Map Shows Who's Hacking Who in Real Time

Business Insider, 25 Jun 2014: A new animated map created by the U.S.-based computer security firm Norse illustrates just how ubiquitous hacking is around the world. The map lists of the countries doing the most hacking, the countries getting hacked the most, and the types of attacks happening. As Quartz points out, the animated map looks kind of like the vintage video game Missile Command. Norse explains that "attacks shown are based on a small subset of live flows against the Norse honeypot infrastructure, representing actual worldwide cyber attacks by bad actors." So while it doesn't show all of the hacking going on in the world, it could be a representative snapshot of today's hacking ecosystem, according to Smithsonian Magazine. Companies like AT&T and Domino's have recently experienced security breaches. Even zero-character messaging app Yo has been the victim of hackers. To read more click **HERE**

Italy's 'Hacking Team' spy Trojan targeting Android and iOS devices, researchers discover

Techworld, 26 Jun 2014: Italy's infamous and dubious hackers-for-hire Hacking Team (or HackingTeam) have set up a worldwide command and control network comprising several hundred servers and expanded into Android and iOS surveillance, a study by Kaspersky Lab and the University of Toronto's Citizen Lab has revealed. The collaboration is just one of a handful that have attempted to keep tabs on one of the oddest organisations in the entire world of malware. Conventionally speaking Hacking Team fits the bill of a professional malware gang except that what these guys work for numerous governments and are considered by police forces to be paid white hats. Along with similar organisations such as Britain's Gamma International, they are seen as having commercialised the market for 'legitimate' state spying. The controversy follows not far behind; what is legal and justifiable in one country might be viewed as the road to a police state in another. The researchers discovered that the command and control servers for the group's 'DaVinci' Remote Control System (RCS) now comprises at least 326 servers across 40 countries. Top of the list is the US with 64 servers, followed by Kazakhstan with 49, Ecuador with 35, the UK with 32, Canada with 24, China with 15 and Colombia with 12; the rest of the list is made up of a number of countries with usually only one server each. Make of that list what you will. Normally, where C&C servers are sited doesn't mean a whole lot except that Hacking Team works for states and police forces that for legal reasons might be keen to keep their surveillance caches on-shore. This implies but does not prove that some of these countries work with the group monitoring their own citizens for purposes unknown. More significant perhaps is that the researchers have discovered more about Hacking Team's mobile campaigns mobile platforms such as Android and iOS. The iOS Trojan is the blunter surveillance tool because it only works on jailbroken devices, a small minority globally but probably more common among the sort of dissident targets that the group wants to watch. The researchers also found evidence that attackers might try and jailbreak or root the device remotely. The status of the Android equivalent remains less certain but both appear to infect mobile devices via a Mac or Windows PC to which they are connected. The mobile Trojans would give the group the ability to monitor not only the target's communications but their location, something that underlines the importance of penetrating these

platforms. "The new data we are publishing on Hacking Team's RCS is extremely important because it shows the level of sophistication and scale of these surveillance tools," said Kaspersky Lab principal security researcher, Sergey Golovanov in a blog. To read more click **HERE**