The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

21 March 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

March 20, KNTV 11 San Jose – (California) **Computers stolen, possible ID breach at UCSF.** The University of California at San Francisco reported March 19 that it notified 9,986 individuals after the university's CSF Family Medicine Center at Lakeshore was burglarized January 11 and computers were stolen containing personal health and identification information. Officials stated that there was no evidence the information was misused and will continue to monitor the situation. Source: http://www.nbcbayarea.com/news/local/Computers-Stolen-Possible-ID-Breach-at-UCSF-251194691.html

March 20, Softpedia – (International) **Tor Browser in Apple's App Store contains adware and spyware.** Representatives of the Tor Project stated that a fake Tor Browser app in the Apple App Store contains adware and spyware and that it has been present since December 2013. Source: http://news.softpedia.com/news/Tor-Browser-in-Apple-s-App-Store-Contains-Adware-and-Spyware-433152.shtml

March 20, Help Net Security – (International) **Over 31,000 IoT devices and computers infected by cryptocoin-mining worm.** Symantec researchers analyzed a new version of the Darlloz Linux worm and found that it has infected over 31,000 Internet-enabled devices and computers running x86 architectures. The main use for the new version of Darlloz was found to be mining for virtual currencies such as Dogecoin and Mincoin. Source: http://www.net-security.org/malware_news.php?id=2740

March 20, Softpedia – (International) **21-year-old Australian arrested for hacking US online gaming company.** Australian authorities arrested a man March 19 and charged him with breaking into the systems of a U.S.-based gaming company, hijacking the game developer's Twitter account, and using stolen data to set up a Web site that charged access to search players' IP addresses for use in distributed denial of service (DDoS) attacks. Source: http://news.softpedia.com/news/21-Year-Old-Australian-Arrested-for-Hacking-US-Online-Gaming-Company-433176.shtml

March 20, Threatpost – (International) **New Zorenium bot boasts ability to run on iOS.** Researchers at Terrogence analyzed a relatively-new piece of malware called Zorenium that is able to run on iOS, Windows, and Linux devices and contains several capabilities including banking trojan functionality, form-grabbing, and Bitcoin mining. Source: http://threatpost.com/new-zorenium-bot-boasts-ability-to-run-on-ios/104901

March 19, Softpedia – (International) **Oracle releases Java 8, several security improvements included.** Oracle released Java SE 8 and JDK 8, making several security improvements such as stronger algorithms for Password-Based Encryption and better support for high entropy random number generators. Source: http://news.softpedia.com/news/Oracle-Releases-Java-8-Several-Security-Improvements-Included-433097.shtml

BlackOS: New Malicious Software Used by Cybercriminals to Redirect Traffic

SoftPedia, 21 Mar 2014: Cybercriminals sometimes rely on special software to redirect traffic from malicious or compromised sites to other websites. Such a tool is BlackOS, which was analyzed by experts from Trend Micro. Malware developers started advertising BlackOS on underground forums in late February 2014. While they advertise it as being new, BlackOS is actually based on "Tale of the North," a piece of software first identified by security researchers in September 2013. "BlackOS and other similar packages are designed to automate the process of managing and exploiting websites easier. This allows a cybercriminal to squeeze out the most profit from his victims. It has a web interface which is used to manage the web traffic and its different features," Trend Micro experts explained. "It can cope with high volumes of Internet traffic, and inject iframes and redirect traffic as specified by its user." BlackOS and other tools of this kind can be used by cybercriminals to manage web traffic coming from users who click on links in spam emails. Victims can be directed to various websites depending on their geographic location. "Tale of the North" was developed by an individual called Peter Sevara and others. He's facing criminal charges for using the Kelihos botnet for spam campaigns. However, this hasn't made him put an end to his malicious activities. Recently, Sevara had a misunderstanding with his Tale of the North partners, so they decided to go their separate ways. After the break-up, Sevara's partners started working on BlackOS, which is an updated version of Tale of the North. BlackOS is not cheap. A yearly subscription costs $3,800 (€2,750), but it can also be rented for $100 (€73) per month (basic configuration). To read more click **HERE**

Microsoft Says It Can, and Will, Read Your Emails without a Court Order

SoftPedia, 21 Mar 2014: Microsoft recently managed to hunt down a former employee who previously leaked copies for Windows 7 and Windows 8 to the Internet, but according to court documents, the company has managed to determine his identity after looking into Hotmail accounts. Without court orders, that is. And still, the company claims that it's perfectly legal to look into a Hotmail or Outlook.com account without first asking a judge for permission because what it's doing is actually searching its own servers for information regarding a specific case. Microsoft vice president and general counsel Frank Shaw said in a statement that although the company is free to look into user accounts for specific information, it's not doing it, and to give users a better sense of privacy, it's also tightening internal policies to make sure that emails are stored securely on its servers. "Courts do not issue orders authorizing someone to search themselves, since obviously no such order is needed. So even when we believe we have probable cause, it's not feasible to ask a court to order us to search ourselves," Shaw explained. "To ensure we comply with the standards applicable to obtaining a court order, we will rely in the first instance on a legal team separate from the internal investigating team to assess the evidence. We will move forward only if that team concludes there is evidence of a crime that would be sufficient to justify a court order, if one were applicable." So what's the truth, you might ask. It's pretty difficult to determine whether your emails are secure on Outlook.com right now, especially with Microsoft agreeing that looking into accounts is perfectly legal, but there's no doubt that taking down whoever leaked Windows copies to the Internet was a priority for the software giant. The problem with this case, however, is that Microsoft's Scroogled campaign launched against Google and accusing the search giant for looking into users' emails to deliver ads doesn't make much sense now, especially because the Redmond company itself is doing it too, and not for a better ad experience. Microsoft, on the other hand, says that it's keen to provide a greater transparency level, so future reports will also include information regarding the number of accounts that got scanned by the company for illegal content. That's not at all a thing that could calm you down if you're a privacy advocate, but the company claims that "the privacy of our customers is incredibly important to us." To read more click **HERE**

Windows 8 Leaker Loses His Job Due to Microsoft Investigation

SoftPedia, 21 Mar 2014: Alex Kibkalo is now under custody after getting arrested by the FBI on Wednesday for stealing trade secrets from Microsoft and, according to new information, he also got fired by his current employer until the US authorities shed some light in the case. Neowin is reporting before the arrest took place, Alex Kibkalo was working for

5nine Software on project management tasks, but the company has decided to suspend him indefinitely until the FBI reveals the final results of the investigation. What's more, it appears that his current employer wasn't aware of Kibkalo's involvement in FBI investigations when he decided to hire the former Microsoft worker in 2012. Kibkalo is accused of leaking copies of Windows 7, Windows 8, and Microsoft's Activation Server Software Development Kit, Redmond's very own software platform that can be used to generate Windows keys. Kibkalo also collaborated with a French blogger who reportedly posted all details online. According to new information disclosed this morning, Kibkalo was identified by Microsoft after the company looked into the French blogger's email accounts, coming across some conversations that revealed not only his identity, but also more information on his actions and the way he managed to post details regarding Microsoft's projects to the web. To read more click **HERE**

DoD abandons DIACAP in favor of the NIST risk management framework

Fierce Government IT, 18 Mar 2014: An effort to align defense and federal civilian cybersecurity guidance culminated this month with the Defense Department jettisoning its specialized certification and accreditation process. In a March 12 instruction (**.pdf**), DoD Chief Information Officer Teri Takai said that starting that same day, defense and military systems will henceforth go through the risk management framework outlined by the National Institute of Standards and Technology rather than through the now-defunct DoD Information Assurance Certification and Accreditation Process. The change is an expected one that grew in likelihood as the DoD and NIST actively sought over the past few years through a joint task force common ground in their cybersecurity guidance documents. The change will bring about a common cybersecurity terminology across defense and civilian networks and reduce the potential for an automatic need to re-certify a system that's shared across organizational boundaries. The NIST risk management framework is governed by a handful of documents known as special publications, including SP 800-37 and SP 800-39. NIST publishes a catalog of security controls known as SP 800-53, to which defense components will now look to when implementing cybersecurity safeguards. The heart of the risk management framework is a three-tiered pyramid, each level responsible for addressing the risk a system penetration would pose according to their hierarchical perspective, ranging from strategic down to tactical. At the top of the DOD-adopted pyramid sits the DoD CIO and senior information security officer and the DoD Information Security Risk Management Committee. The framework also requires a six step process that begins with risk categorization and ends with monitoring on the security controls to ensure they're effective – a step risk management framework proponents highlight in response to criticism that federal cybersecurity is pedantic rather than dynamic. DODI 8501.01 provides more direction (**link**). To read more click **HERE**