Counterintelligence NEW MEXICO Working Group

NMCIWG Purple Arrow

THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

10 July 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

July 9, The Register – (International) **ATTACK of the Windows ZOMBIES on point-of-sale terminals.** Researchers with IntelCrawler identified and infiltrated a Windows botnet known as @-Brt that can be used in brute force attacks against point-of-sale (POS) systems and their associated networks. The botnet targets Remote Desktop Protocol (RDP) servers with weak or default passwords in order to grant attackers the access needed to plant payment card data stealing malware. Source: http://www.theregister.co.uk/2014/07/09/botnet_brute_forces_pos/

July 8, KTRK 13 Houston– (Texas) **Security breach reported at Houstonian Hotel.** The Houstonian Hotel in Houston informed guests that the hotel was alerted by the U.S. Secret Service that the hotel had its payment card processing system breached by cybercriminals, potentially exposing an unspecified number of customers' data from cards used at the hotel between December 28, 2013 and June 20, 2014. Source: http://abc13.com/finance/security-breach-reported-at-houstonian-hotel/170410/

July 9, Softpedia – (International) **Facebook helps shut down crypto-currency mining botnet.** A joint effort by Facebook, security groups, and Greek law enforcement agencies shut down a Litecoin-mining botnet known as Lecpetex that had infected around 250,000 computers in several countries. The malware for the botnet spread through a social media spam campaign that compromised Facebook accounts and spread the malware disguised as an image file. Source: http://news.softpedia.com/news/Facebook-Helps-Shut-Down-Crypto-Currency-Mining-Botnet-450068.shtml

July 9, V3.co.uk – (International) **Microsoft releases critical Internet Explorer fix in Patch Tuesday update.** Microsoft released its monthly Patch Tuesday round of updates July 8, which included six updates, two of which were rated as critical. Source: http://www.v3.co.uk/v3-uk/news/2354331/microsoft-releases-critical-internet-explorer-fix-in-patch-tuesday-update

July 9, Securityweek – (International) **Fake Google digital certificates issued by Indian organization.** Google stated July 8 that it identified and blocked unauthorized digital certificates issued by India's National Informatics Center that could have been used to compromise users of the Chrome and Internet Explorer browsers. Source: http://www.securityweek.com/fake-google-digital-certificates-issued-indian-organization

July 9, Securityweek – (International) **FireEye fixes vulnerabilities in FireEye Operating System (FEOS).** FireEye released an update for its FireEye Operating System (FEOS), closing several security issues, including five OpenSSL vulnerabilities. Source: http://www.securityweek.com/fireeye-fixes-security-vulnerabilities-fireeye-operating-system-feos

July 8, Securityweek – (International) **Adware company linked to development and distribution of Mevade malware.** Trend Micro researchers published a research paper which stated that iBario. Ltd, an Israeli company with ties to Ukraine, is believed to be involved in the creation and distribution of the Mevade malware that has infected millions of computers worldwide. The researchers believe that the InstallBrain installer created by iBario has been used to install Mevade onto victims' computers. Source: http://www.securityweek.com/adware-company-linked-development-and-distribution-mevade-malware

July 8, CNET News – (International) **Android's phone wiping fails to delete personal data.** Researchers with Avast reported the results of a study where the researchers bought 20 used Android phones and were able to recover former users' personal data, including photos, emails, and contacts, after the Android factory reset function was used. The researchers reported that users could compromise their personal information when selling used devices because the Android factory reset only clears devices at the application layer. Source: http://www.cnet.com/news/android-phone-wiping-fails-to-delete-personal-data/

Refusing to decrypt data for investigators gets U.K. student 6 months in jail

Engadget, 9 Jul 2014: Christopher Wilson is a 22-year-old computer science student with Asperger's syndrome. He's also facing six months in prison for refusing to hand over the encryption keys to police during the course of an investigation. Wilson first found himself on the wrong side of the long arm of the law in October of 2012. At the time, he was suspected of emailing threats to the vice chancellor of Newcastle University, where he was working towards a master's degree, in which he promised to shoot members of the school's staff. The messages were able to be traced to servers that were connected to Wilson, but the allegations could never be substantiated and the charges were eventually dropped. But not before police confiscated several pieces of computer equipment from his home. Although charges were dropped in the Newcastle case, he became a suspect in a second set of threats made against the Northumbria police. In particular, he was suspected of calling and warning of an impending cyber attack, of attempting to break into the Serious Organised Crime Agency's website and of encouraging people to deface a Facebook memorial page set up for a pair of officers shot in Manchester. As part of the investigation, police wanted to look at encrypted data stored on Wilson's computer. But the password he gave them didn't work. In fact, he provided investigators with 50 passwords, none of which turned out to be correct. So police turned to the courts, which compelled him to provide the correct key to decrypt the data in the interest of national security. Since Wilson refused to comply, he was sentenced to six months in prison under the Regulation of Investigatory Powers Act, or RIPA, the UK's wiretapping law. Of course, it would seem a stretch that such threats would fall under the guise of terrorism and national security, which the particular provisions of RIPA are meant to investigate. To read more click HERE