THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

14 August 2014

August 13, Softpedia – (International) **New Google Chrome 36 Stable fixes 12 vulnerabilities.** Google released an update for its Chrome browser, closing 12 vulnerabilities. The new version also includes the latest version of Adobe Flash Player. Source: http://news.softpedia.com/news/New-Google-Chrome-36-Stable-Fixes-12-Vulnerabilities-454790.shtml

August 13, Softpedia – (International) **iOS malware hijacks revenue from 22 million ads.** A researcher published a paper detailing the operation of the AdThief (also known as Spad) malware that infected around 75,000 jailbroken iOS devices and stole ad revenue from around 22 million ads. The researcher found that the revenue was diverted to the attackers using a Cydia Substrate extension to modify the ads developer ID to one used by the attackers. Source: http://news.softpedia.com/news/iOS-Malware-Hijacks-Revenue-from-22-Million-Ads-454866.shtml

August 13, Softpedia – (International) **Kovter ransomware thrives in Q2 2014, reaches 43,713 infections in a single day.** Damballa released its State of Infections report for the second quarter (Q2) of 2014 and found that the daily infection rate of the Kovter ransomware increased by around 153 percent between April and May, infecting 43,713 systems in one day. Source: http://news.softpedia.com/news/Kovter-Ransomware-Thrives-in-Q2-2014-Reaches-43-713-Infections-In-A-Single-Day-454891.shtml

August 12, Softpedia – (International) **Adobe Reader and Acrobat zero-day vulnerability patched in 11.0.08.** Adobe released an out-of-band patch for Adobe Acrobat and Adobe Reader to close a vulnerability in Windows versions of the software that could allow attackers to bypass sandbox protections. Attackers were observed exploiting the vulnerability in targeted attacks and all users were advised to update their installations as soon as possible. Source: http://news.softpedia.com/news/Adobe-Reader-and-Acrobat-11-0-08-Patches-Zero-Day-Vulnerability-454752.shtml

August 12, IDG News Service – (International) **Microsoft's Patch Tuesday updates focus on Internet Explorer.** Microsoft released its August round of Patch Tuesday updates August 12, which addressed 37 vulnerabilities in Microsoft products including 26 patches for Internet Explorer and a critical vulnerability in OneNote. Source: http://www.computerworld.com/s/article/9250332/Microsoft_s_Patch_Tuesday_updates_focus_on_Internet_Explorer

August 12, Softpedia – (International) **Seven critical Flash Player vulnerabilities fixed in new version.** Adobe released an update for its Adobe Flash Player product that closes seven critical security vulnerabilities. Source: http://news.softpedia.com/news/Seven-Critical-Flash-Player-Vulnerabilities-Fixed-in-New-Version-454753.shtml

August 12, IDG News Service – (International) **15 new vulnerabilities reported during router hacking contest.** A security contest held at the DefCon 22 conference resulted in researchers identifying and reporting 15 new vulnerabilities in 5 popular models of wireless routers. Source: http://www.computerworld.com/s/article/9250322/15_new_vulnerabilities_reported_during_router_hacking_contest

August 12, Dark Reading – (International) **Security holes exposed in Trend Micro, Websense, open source DLP.** Two researchers from Duo Security and Tumblr presenting at the Black Hat conference reported identifying several cross-site scripting (XSS) and cross-site request forgery (CSRF) vulnerabilities in four commercial data loss prevention (DLP) products and one open-source DLP product that could allow attackers to access or manipulate data. The majority of the flaws were in the products' Web-based interfaces. Source: http://www.darkreading.com/vulnerabilities---threats/security-holes-exposed-in-trend-micro-websense-open-source-dlp-/d/d-id/1297966

August 12, Softpedia – (International) **New Android malware Krysanec infects legitimate apps.** Researchers at ESET identified a new remote access trojan (RAT) for Android devices known as Krysanec that is integrated into legitimate apps and can allow attackers to remotely control various device functions and steal information. The malware is being spread through several methods, including social networks and pirated content Web sites. Source: http://news.softpedia.com/news/New-Android-Malware-Krysanec-Takes-Photos-Records-Audio-454754.shtml

Canonical Closes OpenJDK 6 Vulnerabilities in Ubuntu 12.04 LTS and Ubuntu 10.04 LTS
Softpedia, 14 Aug 2014: A number of OpenJDK 6 vulnerabilities have been identified and repaired in the Ubuntu 12.04 LTS and Ubuntu 10.04 LTS operating systems by Canonical developers. Only those two operating systems have been affected by these problems, because Ubuntu 14.04 LTS is using a newer iteration of OpenJDK. "Several vulnerabilities were discovered in the OpenJDK JRE related to information disclosure, data integrity and availability. An attacker could exploit these to cause a denial of service or expose sensitive data over the network," reads the security notification. Also, "several vulnerabilities were discovered in the OpenJDK JRE related to information disclosure and data integrity. An attacker could exploit these to expose sensitive data over the network." For a more detailed description of the problems, you can see Canonical's security notification. Users are advised to upgrade their systems as soon as possible. The flaws can be fixed if you upgrade your system(s) to the latest packages specific to each distribution. To apply the patch, run the Update Manager application. To read more click **HERE**

Russian Prime Minister's Twitter Account Hacked, Tweets Resignation
Softpedia, 14 Aug 2014: The Twitter account of Russia's Prime Minister, Dmitry Medvedev, was compromised on Thursday, and apart from his resignation, the hackers also tweeted anti-Putin messages to the 2.5+ million followers. After the first tweet announcing the fake resignation (shared by thousands), others followed, containing messages against President Putin and his actions regarding the Crimea region. On the same note, the hackers posted on Twitter that Putin's speech in Crimea on August 14 would not contain anything of importance; one of the messages hinted at Medvedev's future activity: "I'm going to become a freelance photographer!," according to Moscow Times, and a picture of a cabinet meeting seemed to give weight to his decision. A press release from RIA Novosti news agency informs that the Prime Minister's micro-blogging account was hacked on Thursday morning (around 06:20 GMT) and that all the false tweets have been deleted. Dmitry Peskov, Medvedev's press secretary, told the news agency that the posts appeared most likely as a result of a hack. Credit for the hack was claimed by hacker outfit Shaltay Boltay (@b0ltai), who apparently ran a more extensive "pwnage" operation, including gaining access to email accounts and other online services, as well as to his Apple devices. They published their findings in a blog post, offering some details. At the end of the post they had the following disclaimer: "All of the above (including the mail file) is a fiction. Any resemblance to real people or events is coincidental." To read more click **HERE**

KB2976897, KB2982791, and KB2970228 Patches Causing BSODs on Windows 7
Softpedia, 14 Aug 2014: Microsoft rolled out August Update plus a number of other patches on this month's Update Tuesday cycle, but it appears that a number of computers are affected by random BSODs whose cause is yet to be determined. First reported by InfoWorld, this issue shows up after installing KB2976897, KB2982791, and KB2970228 patches on Windows 7, with the BSOD error reading a simple

0x50 message. Several users have already confirmed the problems in posts on Microsoft's Community forums, with some claiming that Windows 7 64-bit could be the only version of the OS that's affected until now. "I too have had the same problem blue screen of death after installing Tuesdays updates after messing around for hours I have had to hide KB2976897, KB2982791, and KB2970228 to be able to start my computer normally I wish that Microsoft would check the updates before releasing them I suspect that these updates mentioned above are not compatible with windows 7 64bit which I am running," one user explains. Those who are experiencing the issue are recommended to hide the updates until Microsoft provides a workaround for this. The company hasn't yet commented on the cause of the problem, but it's most likely looking into reports as we speak. To read more click **HERE**

Cyber-Attacks against Turkey's Government Led by Sabu under FBI Supervision

Softpedia, 14 Aug 2014: Unsealed court documents reveal that Hector Xavier Monsegur (also known as Sabu) of the LulzSec hacker group recruited hackers still at large for breaking into foreign websites, from a specific list. Sabu recruited Jeremy Hammond, who was at the top of the list of FBI's most wanted hackers, and told him to break into several dozen websites, some of them under the administration of the Turkish government. After finding a way in, Hammond was instructed to pass the details to politically motivated Turkish hacker group RedHack. In order to hack into the official websites, Hammond leveraged a zero-day for Plesk, a web publishing platform all of the marks provided by Monsegur were operating on. The conversation between the two has been disclosed by the Daily Dot, which is in possession of sealed court documents containing about 3GB of chatroom logs and surveillance records. The current information has not been made public until now by order of a federal judge. After RedHack received the details for hacking into the websites, they proceeded to access servers and retrieve confidential emails, as well as deface the official online locations. According to the Daily Dot, not all websites provided by Monsegur were attacked by RedHack, since some of them lacked political relevance. Although the FBI did not confirm that they were aware of the numerous acts of cybercrime Monsegur instigated other hackers to, before Hammod's final court appearance, his lawyers asked: "Why was our government, which presumably controlled Mr. Monsegur during this period, using Jeremy Hammond to collect information regarding the vulnerabilities of foreign government websites and in some cases, disabling them?" However, it appears that Monsegur was under close supervision, as the authorities had his computer bugged with spyware for tracking online activities and had also installed a surveillance camera in his apartment. Hammond was arrested about two months after the aforementioned attacks and was sentenced in November 2013 to 10 years in a US federal prison for hacking into Stratfor and making public the information he had found. "I broke into numerous websites he supplied, uploaded the stolen email accounts and databases onto Sabu's FBI server, and handed over passwords and backdoors that enabled Sabu and, by extension, his FBI handlers, to control these targets," Hammond said at his sentencing. Hector Xavier Monsegur, arrested in June 2011, served seven months in prison and was free while waiting for the sentencing. In May 2014 he was given "time served" for his cooperation with the FBI and received one year of parole. To read more click **HERE**