Weekly Infrastructure Report

*August 8, Softpedia* – (International) **Network access storage devices are highly exploitable.** A researcher from Independent Security Evaluators presenting at the Black Hat 2014 conference reported finding a wide variety of vulnerabilities in network access storage (NAS) devices from several manufacturers, including directory traversal, command injection, memory corruption, authentication bypass, or back door vulnerabilities. Source: http://news.softpedia.com/news/Network-Access-Storage-Devices-Are-Highly- Exploitable-454103.shtml

*August 8, Help Net Security* – (International) **Critical bug in WordPress plugin allows site hijacking.** Sucuri researchers identified and reported a vulnerability in the Custom Contact Forms plugin for WordPress that could allow attackers to take control of sites using the plugin. The developers of Custom Contact Forms published an update for the plugin after the issue was published by the WordPress Security team.

Source: http://www.net-security.org/secworld.php?id=17227

*August 8, Help Net Security* – (International) **Two Gameover Zeus variants targeting Europe and beyond.** Researchers at Bitdefender identified two Gameover Zeus variants in the wild, one botnet primarily targeting the U.S. while the second targets Belarus and Ukraine. The first botnet is generating around 1,000 domains per day while the second generates 10,000 per day but appears to currently be inactive.

Source: http://www.net-security.org/malware\_news.php?id=2833

*August 8, Securityweek* – (International) **Cybercriminals steal cryptocurrency via BGP hijacking.** Researchers with Dell SecureWorks reported finding cybercriminals using fake Border Gateway Protocol (BGP) broadcasts to redirect traffic from cryptocurrency mining pools to servers they control, diverting tens of thousands of dollars in cryptocurrency. The attackers compromised 51 mining pools hosted on 19 hosting companies.

Source: http://www.securityweek.com/cybercriminals-steal-cryptocurrency-bgp- hijacking

*August 7, Securityweek* – (International) **Attackers used multiple zero-days to hit spy agencies in cyber-espionage campaign.** Kaspersky Lab researchers identified the infection methods used in the Epic Turla cyber-espionage campaign (also known as Snake or Uroburos) that targeted intelligence agencies, military organizations, government agencies, education institutions, pharmaceutical companies, and research groups in over 45 countries. The attackers behind the campaign used several malware platforms and zero-day exploits in Windows XP and Server 2003 and Adobe Reader to infect systems and then could upgrade the malware with additional capabilities once in place. Source: http://www.securityweek.com/attackers-used-multiple-zero-days-hit-spy-agencies-cyber-espionage-campaign

*August 7, Dark Reading* – (International) **Attack harbors malware in images.** A researcher with Dell SecureWorks reported finding the Lurk malware being distributed within a fake digital image as part of a click fraud campaign that infected around 350,000 systems. The malware in the campaign was spread through iFrames on Web sites containing an Adobe Flash exploit, and required victims to have a vulnerable version of Adobe Flash that is used to download the fake image file, which contains an encrypted URL that downloads a second malicious payload.

Source: http://www.darkreading.com/endpoint/attack-harbors-malware-in-images/d/d-id/1297867

*August 7, Securityweek* – (International) **Flaws in email and Web filtering solutions expose organizations to attacks: Researcher.** A researcher at NCC Group presenting at the Black Hat 2014 conference published two whitepapers outlining how email and Web filtering solutions can be used by attackers in the reconnaissance phase of attacks to obtain information on a potential target network if the attackers can determine which products or services are being used on the target network.

Source: http://www.securityweek.com/flaws-email-and-web-filtering-solutions- expose-organizations-attacks-researcher

*August 8, The Register* – (International) **‘Up to two BEEELLION’ mobes easily hacked by evil base station.** Researchers from the security firm Accuvant announced at the Black Hat 2014 conference August 7 that up to 2 billion smartphone handsets are at risk for over the air hijacking and abuse which can be exploited through the Open Mobile Alliance Device Management (OMA-DM) protocol, used by approximately 100 mobile phone manufacturers. To access the handsets remotely the hacker only needs to know the handset’s unique International Mobile Station Equipment Identity (IMEI) number and a secret token. Source: http://www.theregister.co.uk/2014/08/08/two\_billeeon\_mobile\_phones\_easily\_hackabl e\_with\_dummy\_base\_station/

*August 11, Help Net Security* – (International) **Critical 0-days found in CPE WAN Management Protocol.** Check Point researchers reported finding several zero-day vulnerabilities in CPE WAN Management Protocol (CWMP/TR-069) deployments used by major Internet service providers (ISPs) to control home and business Internet equipment which could allow large-scale malware infections able to compromise privacy, steal information, or cause service disruptions. Check Point reported the vulnerabilities to ISPs and assisted in closing them before reporting their findings publicly.

Source: <http://www.net-security.org/secworld.php?id=17237>

*August 11, Help Net Security* – (International) **Smart Nest thermostat easily turned into spying device.** An independent researcher and two researchers from the University of Central Florida presenting at the 2014 Black Hat conference demonstrated how Nest smart thermostats can be compromised quickly using a USB flash drive, potentially allowing attackers to obtain information on a victim’s habits as well as network information such as WiFi credentials. Compromised thermostats could also be used to connect to the Internet and be used in a variety of malicious tasks.

Source: http://www.net-security.org/secworld.php?id=17239

*August 9, Softpedia* – (International) **10,000 impacted by resurging Facebook color changing app scam.** Researchers at Cheetah Mobile reported that a resurgence of a scam that purports to change the color scheme of Facebook has affected 10,000 users recently. The campaign steals users’ Access Tokens and then attempts to install a malicious fake antivirus program or video player.

Source: http://news.softpedia.com/news/10-000-Impacted-by-Resurging-Facebook- Color-Changing-App-Scam-454306.shtml

*August 8, The Register* – (International) **Oracle Database 12c’s data redaction security smashed live on stage.** A researcher with Datacomm TSS presenting at the Defcon 22 conference demonstrated how a remote attacker could inject SQL queries to access redacted information in Oracle Database 12c due to several coding flaws. Source: http://www.theregister.co.uk/2014/08/08/oracle\_database\_12c\_redaction\_is\_tot ally\_borked\_by\_bad\_code/

*August 12, Softpedia* – (International) **Millions of computers have backdoor enabled by default.** Researchers from Kaspersky and Cubica Labs presenting at the Black Hat conference demonstrated how the legitimate Computrace anti-theft solution can be used by attackers performing a man-in-the-middle (MitM) attack to remotely execute arbitrary code on the target device due to the lack of encryption in Computrace traffic. Most computers come with Computrace already present, leaving millions of devices vulnerable to malicious use of the solution.

Source: [http://news.softpedia.com/news/Millions-of-Computers-Have-Backdoor- Enabled-by-Default-454666.shtml](http://news.softpedia.com/news/Millions-of-Computers-Have-Backdoor-%20Enabled-by-Default-454666.shtml)

*August 12, Threatpost* – (International) **Authentication bypass bug fixed in BlackBerry Z10.** Modzero researchers identified and reported two methods for remotely exploiting an authentication bypass vulnerability in BlackBerry Z10 phones that could allow attackers to install malware or steal personal data. BlackBerry released an update that closes the vulnerability and pushed it out to phone carriers. Source: http://threatpost.com/authentication-bypass-bug-fixed-in-blackberry- z10/107715

*August 11, Softpedia* – (International) **Yahoo ad network used to spread CryptoWall ransomware.** A researcher at Blue Coat Systems identified a malicious advertising campaign that uses the Yahoo advertisement network to distribute malicious ads that direct users to malicious pages that attempt to serve a variant of the Cryptowall ransomware. The researcher also reported that the adsmail.us service was also used in the campaign.

Source: http://news.softpedia.com/news/Yahoo-Ad-Network-Used-to-Spread- CryptoWall-Ransomware-454520.shtml