THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

30 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 26, Rapid City Journal – (South Dakota) **Indian Health Services addresses breach of private information.** Indian Health Service Rosebud Service Unit notified 620 patients July 16 after a folder containing their personal information, including Social Security numbers and U.S. Department of Veterans Affairs enrollment information, was quickly recovered after it was accidentally left in a public area of the facility's Rapid City unit May 30 by an employee. Source: http://rapidcityjournal.com/news/local/indian-health-services-addresses-breach-of-private-information/article_2ed1e8c6-089b-5b51-9113-5e1c9bb16cc0.html

July 28, Nextgov – (National) **Hacker breached NOAA satellite data from contractor's PC.** A report released by the Office of the Inspector General found that satellite data was stolen from a National Oceanic and Atmospheric Administration (NOAA) contractor's personal computer in 2013, which allowed a hacker to extract data from NOAA's National Environmental Satellite, Data, and Information Service system through a remote connection. The report found the administration had several security deficiencies and security bugs in its satellite software that remained unfixed, among other findings. Source: http://www.nextgov.com/cybersecurity/2014/07/hacker-breached-noaa-satellite-data-contractors-pc/89771/

July 29, The Register – (International) **Only '3% of web servers in tops corps' fully fixed after Heartbleed snafu.** A study by Venafi Labs found that only 3 percent of machines have been fully protected against the Heartbleed Open SSL vulnerability which includes patching servers and changing private keys, as well as being issued with new SSL certificates and having the old ones revoked. Source: http://www.theregister.co.uk/2014/07/29/only_3_of_top_firms_fully_patched_against_heartbleed_flaw/

July 28, Securityweek – (International) **Cybercriminals abuse Amazon cloud to host Linux DDoS Trojans.** Kaspersky Lab reported that Amazon cloud services and other companies are being abused by cybercriminals to host distributed denial of service (DDoS) bots, including a sophisticated Linux trojan capable of conducting domain name system (DNS) amplification DDoS attacks. The attackers are able to access the servers by exploiting vulnerabilities in versions 1.1.x of Elasticsearch. Source: http://www.securityweek.com/cybercriminals-abuse-amazon-cloud-host-linux-ddos-trojans

July 28, Securityweek – (International) **Kaspersky analyzes distribution network for Koler mobile ransomware.** Kaspersky Lab published findings on the Koler ransomware which targets Android and Internet Explorer users stating that dozens of automatically generated sites redirect traffic to a central hub using a traffic distribution system where users are again redirected. The distribution infrastructure relies on a network of at least 48 malicious adult Web sites linked to Keitaro traffic redirection system. Source: http://www.securityweek.com/kaspersky-analyzes-distribution-network-koler-mobile-ransomware

July 28, Softpedia – (International) **I2P networking tool patched against de-anonymization.** Developers of the I2P network released the 0.9.14 patch which integrates repairs for cross-site-scripting (XSS) and remote execution vulnerabilities addressing flawed components in Tails operating system enabling de-anonymization of a client. The release contains several bug fixes in i2ptunnel, i2psnark, and other updates. Source: http://news.softpedia.com/news/I2P-Networking-Tool-Patched-Against-De-Anonymization-452464.shtml

Instagram Account Hijack Code Published

SoftPedia, 30 Jul 2014: A developer in London discovered that an Instagram account could be easily hijacked, and he released to the public a proof-of concept of the method after Facebook denied him a bug bounty, saying that they were aware of the problem he described to them. Because of Instagram's insecure communication, Stevie Graham was able to intercept traffic from the Instagram app for iOS and retrieve the session cookies, which allowed him to hijack the account for the service. The flaw is not new and consists in the fact that Instagram does not have encrypted communication implemented for all of its parts, and API calls are made to endpoints over simple HTTP; these contain session cookies in the request headers. Intercepting the session cookies can be done easily, with free network traffic capture tools and loading them into a web browser provides an attacker access to the Instagram account without having to authenticate. Regular logging into the service is done over an encrypted connection, but ulterior communication with the cookies is carried out without encryption. With access to the account, a potential attacker could initiate the same actions as if they were the owner, making modifications, adding new content or editing comments. Sending spam or directing followers to pages hosting malicious files are just some of the nefarious activities that can be perpetrated by leveraging this security flaw. Graham made the proof-of-concept available after previously exchanging messages regarding the matter with the Facebook Bug Bounty team. He tweeted about the denial of a bug bounty and said that his next step would be to write an automated tool that enabled mass hijacking of accounts. “I think this attack is extremely severe because it allows full session hijack and is easily automated,” he said on the page disclosing the flaw. Graham is not the only one that made this discovery and reported it to Facebook. This week, researcher Mazin Ahmed made the same disclosure, referring to the Instagram app for Android. After contacting Facebook, he received an answer from the security team letting him know that they were aware of the problem. “Facebook has discussed this issue at length and plans on moving everything on the Instagram site to HTTPS. However, there is no definite date for the change. At the moment Facebook accepts the risk of parts of Instagram communicate over HTTP and not HTTPS. We consider this a known issue and are working toward a solution in the near future,” the Facebook team told him. To read more click HERE

NOAA’s IT Security Program Increases Risk of Cyber Attacks

SoftPedia, 30 Jul 2014: A report from the Department of Commerce regarding the security of National Oceanic and Administration Agency computer systems against cyber-attacks revealed significant deficiencies. The results of the assessment showed that the information is not restricted in any way between the networks of Polar-orbiting Operational Environmental Satellites (POES) and Geostationary Operational Environmental Satellites (GOES) projects, which would allow a potential attacker access to critical data. These are part of National Environmental Satellite, Data, and Information Service (NESDIS), which offers access to global environmental information from satellites and other sources for protecting and improving US economy and security. Lack of strong policies regulating the use of mobile devices, which are potential carriers of malware, on the NESDIS computers is another weakness that can be leveraged by an attacker for an intrusion. In particular, it has been discovered that unauthorized mobile devices had been connected to the workstations of different projects. “Mobile devices can carry malware that, when plugged into a workstation or server, could execute malicious code residing on the device and lead to a compromised system. Accordingly, there has been a long-standing requirement that agencies restrict the use of mobile devices.” “Implementing required mobile device security mechanisms helps prevent the spread of malware and limits the risk of a compromise of critical assets. Further, mobile devices are one of the means by which an attacker can access and compromise a system with restricted interconnections, such as NESDIS' satellite ground-support systems POES and GOES," says the report. Additionally, on some of the systems, Windows AutoRun feature was not disabled, which is considered a significant security risk since malicious code can be automatically executed from a removable device once plugged in. It appears that NESDIS fails to implement fundamental security requirements, such as applying patches for vulnerabilities, enforcing security measures for the remote access mechanism or adding safe configuration settings control on IT systems (operating systems, database and web servers). Briefly put, NESDIS computers are plagued by high-risk vulnerabilities, there is no two-factor authentication for remote access or a restriction for using personal computers for logging in remotely, so adopting security-conscious practices, like the use of strong passwords instead of the ones delivered by default with the software installed, would be the best way to go. Additional problems refer to assessments of National Weather Service (NWS) computer systems, provided by an independent entity that can offer an unbiased opinion about the security posture of the agency. The report found that the current entity in charge of the security evaluation did not fulfill its job at the required parameters, and that 47% of the control assessments contained inadequacies that did not offer an accurate implementation status of the system's security controls. A draft report was sent to NOAA, which agreed with some of the findings and proceeded to take remediation actions. To read more click HERE

Chinese Government Seizes Microsoft's Computers, Documents over Windows Security Claims

SoftPedia, 30 Jul 2014: Chinese authorities raided several Microsoft offices a couple of days ago, and although no reasons have been provided at first, more information is now emerging on what seems to be a new anti-trust case that could target the Redmond-based tech giant. Approximately 100 Chinese investigators paid an unexpected visit to Microsoft offices in Beijing, Shanghai, Chengdu, and Guangzhou, seizing computers, documents, and email information that mostly contain conversations between the company's employees. Copies of a number of documents, including contracts and financial statements, have also been made, WSJ writes. Although it's still unclear why exactly the government has decided to raid Microsoft's offices, a company spokesperson has said in a statement that Redmond's business does not violate any local law, which clearly makes people think about a new anti-trust case that would involve the software giant. "[Microsoft] complies with the laws and regulations of every market in which we operate around the world and we have industry leading monitoring and enforcement mechanisms in place to ensure this. Our business practices in China are designed to be compliant with Chinese law," a company spokesperson was quoted as saying by Bloomberg. In a statement published on the Chinese version of its website, China's State Administration for Industry and Commerce explains that these raids are part of an investigation following a number of complaints received in the last 12 months and targeting the security of Microsoft's products. This wouldn't be the first time when Chinese authorities are closely looking at the security offered by Microsoft's software, as several local government bodies have accused the software giant of bundling backdoors in its Windows operating system in order to spy on the government and steal state secrets. Back in May, Chinese authorities decided to ban Windows 8 on government computers, with people close to the matter saying that security concerns over a possible backdoor hidden in the source code were the main reason for this decision. Ever since, Microsoft said with several occasions that it's ready to work with the Chinese government on addressing these claims, but until now, no agreement has been reached. Microsoft said that instead of Windows 8, the company is offering the Chinese government the older Windows 7, which is similar in terms of performance and security to its successor. Microsoft is obviously avoiding to provide too many details on this new investigation, but it's pretty clear that the company hopes that it's all for the best and everything will end without a new fine. To read more click HERE

Find Out How Vulnerable Your Android Is

SoftPedia, 30 Jul 2014: Security patches for Android OS are not delivered at the same time for all users because their implementation often depends on third-parties, carriers and/or phone manufacturers. In the meantime, there is a simple way to check if the device is affected by some of the vulnerabilities. Bluebox

Security Scanner can currently detect if the device has been patched against four Android bugs, and in some cases it can provide contact information for the entity responsible for delivering the fixes. At the moment, the tool, free on Google Play, determines if bugs 8219321, 9695860, 10145349 and 13678484 have been eliminated. All of them refer to the verification process of the digital certificate for each app installed on the system. Patches have been released for all of them, but for the aforementioned reasons, not all of them reached Android users. The new tool can also check if apps leveraging one of the first three bugs (Master Key) take advantage of the phone's system. However, more importantly, the latest version of the scanner is able to detect if the patch for the latest Android OS critical vulnerability is installed. Dubbed FakeID by Bluebox Security, this flaw has the potential to compromise an Android phone completely, on operating system versions lower than 4.4 (KitKat). The security glitch is caused by the fact that the Android packager does not carry out any verification of the legitimacy of a digital certificate chain, which allows a potential attacker to create a signature for an app and claim it to be issued by a trusted developer. By doing so, an app could be awarded the same privileges as those the software from the trusted developer benefits from. Google has provided a fix for the FakeID flaw, and it is now up to the device manufacturers to integrate it in the firmware and distribute the update. Bluebox's scanner utility can also inform the user if the installation of apps from unknown sources is enabled on the device. Inherent Android problems aside, adding software from alternative, unverified app repositories is the top cause of malware infection on the operating system. Users are often deceived to install rogue apps posing as legitimate ones, exposing them to various risks. Cybercriminals can use malicious APKs to collect information relating to bank accounts or private data, such as text messages, contact and phone call lists, details about the apps installed, and stored files. Recent Android malware can encrypt specific data on the device and ask for a ransom fee in order to decrypt it. To read more click HERE

House passes DHS cyber bills

AFP, Jul. 29, 2014: The National Cybersecurity and Critical Infrastructure Protection Act, introduced by Homeland Security Committee chairman Michael McCaul, R-Texas and ranking member Bennie Thompson, D-Miss., would strengthen public-private partnerships to help deter cyber attacks, they said in a statement. The bill would require that cybersecurity incident response plans are updated regularly and amends existing legislation so that private entities can voluntarily submit their cybersecurity procedures to DHS in order to gain liability protections in the event of an attack. The bill also codifies into law the National Cybersecurity and Communications Integration Center, to facilitate the sharing of real-time cyber threat information across government and critical industries. "This bipartisan bill establishes a true partnership between DHS and the private sector to ensure the distribution of real-time cyber threat information in order to secure our nation in cyberspace without burdensome mandates or regulations," McCaul said in a statement. The Homeland Security cybersecurity Boots-on-the-Ground Act would require DHS to develop occupation classifications for employees performing cyber activities and to make those classifications uniform across the agency. The bill would also require DHS to develop a strategy to develop and recruit cyber security workers to fill gaps in its workforce. "DHS' success depends on how well it recruits, hires, and trains its cyber workforce," said Thompson, who sponsored the legislation. The Critical Infrastructure Research and Development Advancement Act requires DHS to develop a plan to help accelerate research and development into cybersecurity protections and technologies. The agency would update this plan every two years in consultation with industry and with cyber stakeholders. "The National Cybersecurity and Critical Infrastructure Protection Act—the result of consultations with hundreds of stakeholders across government, the private sector and privacy advocates—will enable government and the private sector work together to prevent and defeat cyber attacks," said Rep. Patrick Meehan, R-Pa., who sponsored the bill To read more click HERE