THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

21 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 17, Softpedia – (International) **Neverquest banking trojan expands list of targets.** Researchers with Symantec found that the attackers operating the Neverquest banking trojan, also known as Snifula, have focused their efforts on banks in the U.S. and Japan since December 2013. The trojan is able to obtain banking login information from victims and can also steal digital certificates, among other capabilities. Source: http://news.softpedia.com/news/Neverquest-Banking-Trojan-Expands-List-of-Targets-451157.shtml

July 17, Dark Reading – (International) **Government-grade stealth malware in hands of criminals.** Sentinel Labs researchers reported that a piece of malware likely originating from a state-sponsored espionage campaign known as Gyges is being repurposed by cybercriminals to conceal and protect various pieces of malware and ransomware. Gyges contains several sophisticated features to avoid detection and prevent reverse-engineering and appears to have originated in Russia. Source: http://www.darkreading.com/government-grade-stealth-malware-in-hands-of-criminals/d/d-id/1297362

July 17, Softpedia – (International) **DDoS attacks decrease in Q2 2014, compared to Q1.** Arbor Networks reported that distributed denial of service (DDoS) attacks during the second quarter of 2014 decreased in terms of speeds and frequency compared to the previous quarter, with average DDoS attack size at 759.83 Mb/s, among other findings. Source: http://news.softpedia.com/news/Volumetric-DDoS-Attacks-Decrease-in-Q2-2014-Compared-to-Q1-451160.shtml

Nasdaq Servers Compromised Through Zero-Day Exploits

SoftPedia, 21 Jul 2014: The monitoring systems of the Federal Bureau of Investigation were alerted in 2010 of odd activity on the systems of Nasdaq Stock Market, which was consistent with malware actions. The incident was reported to the media in February 2011, and according to some sources, the origin of the attack could have been in Russia. A recent piece of news reveals that the attack was carried out by leveraging two zero-day vulnerabilities, which allowed the intruders to insert malicious code into the systems of Nasdaq and have access to them for at least three months prior to the detection of the attack. The malware was known to NSA, who pointed out that the code had previously been used by Russia's espionage agency FSB. It appears that the capabilities of the malware were beyond simple spying of the financial activity and it could also be used to disrupt the entire activity of the Nasdaq system. According to Bloomberg, the malware could have belonged to other operators too, since malicious code oftentimes falls into different hands and it's repurposed for a different type of activity. It was discovered that the malware was also used by a Chinese cyberspy, and the attention turned to China; but the leads of the examination failed to make a connection. Forensic examination of the incident revealed that the stock market's systems were poorly protected and thus highly vulnerable to intrusions. The investigators found evidence that several outside groups had access to Nasdaq information, although it was not clear who they were. Proof of information stealing was found, but it was incomplete and the investigation could not determine the type of details that were extracted. In fact, Bloomberg reports that one of the

forensic investigators referred to the Nasdaq's systems as "the dirty swamp," because very few records were available that would have revealed daily activities on the servers and would have helped retrace the steps of the intruders. During the investigation, the systems of other financial businesses that connected to the exchange were verified, in order to determine the spread of the attack. It appears that the attackers were not interested in other information, as they limited the intrusion to Nasdaq. However, if they wanted to change the target, they would have encountered no resistance, because the same vulnerabilities could have been leveraged. It's been four years since the intrusion has been detected, and the conclusions of the investigators are still far from creating a clear picture. They do not know for certain who was behind the attack and which were their exact intentions, given the destructive capabilities of the malware. To read more click **HERE**

Windows 8.1 Update 2 to Launch on August 12

SoftPedia, 21 Jul 2014: We're getting really close to the public launch of Windows 8.1 Update 2 and even though Microsoft is keeping all details secret and nobody knows for sure whether the update would go live in August or September, new evidence shows that everyone would get it next month. Previous reports indicated that Microsoft was planning to release Windows 8.1 Update 2 in mid-August, and thanks to some leaked documents that were published by the editors over at PC Portal, it appears that August 12 is the date when Redmond would officially introduce this new update. No other specifics have been provided till now, but these documents show that Windows 8.1 Update 2 could be released to users together with the other Patch Tuesday updates coming out next month. As far as features and other tools are concerned, it appears that Microsoft is only planning to use Windows 8.1 Update 2 to deliver minor improvements and other fixes to Windows 8.1 computers, so do not expect the Start menu or options to run Metro apps in separate windows on the desktop to be part of this release. Windows 8.1 Update 2 will obviously be offered free of charge to everyone running Windows 8.1 Update and is very likely to be shipped via Windows Update, despite rumors that Microsoft might actually be offered through the Windows Store. The company is actually focusing more on the next full Windows release, possibly called Windows 9, which is expected to bring many more improvements and features as compared to what's expected to be part of Windows 8.1 updates. Windows 9, for example, is expected to include a modern Start menu that would mix live tiles and traditional design elements, such as app lists and power controls to quickly shut down or reboot the computer. A desktop version of Cortana which would allow users to perform certain tasks with voice commands is also expected to be included in Windows 9, sources say. As it's the case with all the other rumors that reach the web these days, take everything with a pinch of salt, at least until Microsoft officially announces the release of a new Windows 8.1 update. If these reports are true, expect the company to at least talk about Windows 8.1 Update 2 in the next couple of weeks, before the public launch that could take place on August 12 during the Patch Tuesday rollout. To read more click **HERE**

CryptoLocker Is Still a Threat

SoftPedia, 21 Jul 2014: The recent joint operation of law enforcement agencies and private security firms that led to dismantling the Gameover Zeus and CryptoLocker botnets may not have scared off the cybercriminals completely, as new variants of the crypto malware have emerged, creating new networks of infected computers. A recent status report from the FBI about the success of taking down the Gameover Zeus and CryptoLocker botnets in what was called Operation Tovar said that the networks had been neutralized and "cannot communicate with the infrastructure used to control the malicious software." However, information from security company Webroot shows that Operation Tovar was only partially successful and that threat actors could resurrect the crypto malware through new variants that have already been detected. Webroot threat analyst Tyler Moffitt argues that Operation Tovar did not manage to seize all the servers that communicated with computers compromised by CryptoLocker variants, but only those under the control of a certain cybercriminal, who is believed to be led by Evgeniy Bogachev. However, other threat actors would leverage this malicious code, too, which means that CryptoLocker infections are still present. "Although Evgeniy Bogachev and his group had control of a major chunk of zeus botnets and command and control servers that deployed cryptolocker, it was certainly not all or even

the majority of zeus botnets in existence. "Most malware authors spread their samples through botnets that they either accumulated themselves (Evgeniy), or just rent time on a botnet from someone like Evgeniy (most common). So now that Evgeniy's servers are seized, malware authors are just going to rent from some of the many other botnets out there that are still for lease," says Moffitt in a blog post. He also presents a set of variants (CryptoWall, New CryptoLocker, DirCrypt, CryptoDefense) found by Webroot security researchers. Most of the strains show slight improvements compared to the original code. In some cases, there is no interface announcing the lock on the files and the user finds payment instructions in plain-text files created in the folders where data was encrypted. In other instances, the victim has to make the payment via TOR anonymity network, which is used for protecting the identity of the cybercrooks. A new crypto malware went for sale on underground forums under the name of Critoni. The forum post, discovered by Kafeine, advertised the use of persistent cryptography that relied on elliptic curves, making decryption impossible without the keys provided by the crooks. The general recommendation against this sort of threats is to have backups in place for all the important data. This way, if the computer is infected, the backups can be restored and no information loss occurs. To read more click **HERE**

vBulletin SQL Injection Exploit Published

SoftPedia, 21 Jul 2014: The exploit for the vBulletin SQL injection vulnerability has been published by Romanian Security Team (RST), the security researchers that reported it in the first place. Nytro, one of the team members who last week provided us information about the glitch and a video proof of its success, has posted the exploit on the group's forum, detailing how an attacker could access the admin database of a forum running version 5.x of the vBulletin software. He offered the code and all the details free of charge, although it appears that other groups are selling the zero-day for as much as $2,000 / €1,480, in Bitcoin crypto-currency. Nytro shows the entire exploit and reveals the bug that would allow an attacker to gain access to sensitive areas of the website. It appears that the issue consisted in the fact that the quote for the controlled parameter was not escaped. vBulletin was fast at releasing a fix, which became publicly available a day after RST reported the vulnerability on their forum. The latest patch for vBulletin ensures that the value is escaped and eliminates the risk of a breach. As Nytro says, the exploit is not too complex, and currently there are few forums that run a vBulletin version vulnerable to it. To read more click **HERE**

Critoni Ransomware Communicates Through Tor Anonymity Network

SoftPedia, 21 Jul 2014: A new ransomware called Critoni, is up for sale on the underground forums, its vendors touting it as a new generation of Cryptolocker as it uses the Tor network to anonymize its communication with the command and control server. The purpose of the malicious kit is to encrypt various types of files, documents and images among them, and ask for a ransom fee to revert the locking process. The post was discovered by French security researcher that goes by the name of Kafeine, who says that the advertisement has been up since the middle of June and that at the beginning it was used primarily against Russians, but lately it is leveraged against computer users in other countries, too. The piece of malware, named CTB-Locker (Curve-Tor-Bitcoin Locker) by the cybercrooks, is currently detected as Critoni.A by Microsoft and is available for $3,000 / €2,220. Critoni is advertised to use persistent cryptography relying on elliptic curves, which would make file decryption impossible; keys are generated randomly and there is no risk of collision. As the name suggests, the ransom has to be paid in Bitcoin crypto-currency in order to prevent tracing of the transaction, and if the victim does not own any, they are instructed on how to acquire them. Other forms of payment can also be integrated. The post on the underground forum says that the encryption process can be carried out in lack of Internet connection. Kafeine reports that Critoni has been seen to be delivered by the Angler exploit kit, but other forms of attack have also been detected in the wild. If the period of time set for making the ransom payment expires, the file locking program self-deletes, but victims are offered another chance to retrieve the data, instructions being provided in a TXT file located in the Documents folder. According to security experts from Kaspersky, this is the first cryptomalware to use the Tor network to annonymize its communication

with the command and control server. This sort of protection has generally been seen in banking Trojans. "Executable code for establishing Tor connection is embedded in the malware's body. Previously the malware of this type, this was usually accomplished with a Tor.exe file. Embedding Tor functions in the malware's body is a more difficult task from the programming point of view, but it has some profits, because it helps to avoid detection, and it is more efficient in general," said Kaspersky Lab senior malware analyst, Fedor Sinitsyn, to Threatpost. Kafeine asserts that Critoni "seems to be a strong, well thought piece of malware." To read more click **HERE**

Significant Deficiencies Found in Treasury's Computer Security

NextGov, 21 Jul 2014: Weaknesses in Treasury Department computer systems that track federal debt are severe enough to disrupt accounting, according to a government audit. Newly discovered security vulnerabilities at the Bureau of the Fiscal Service, coupled with older unfixed problems, constitute a "significant deficiency" for financial reporting purposes, the Government Accountability Office found. The weaknesses "increase the risk of unauthorized access, modification or disclosure of sensitive data and programs, which could result in the disruption of critical operations," Gary Engel, GAO director for financial management and assurance, wrote in an audit released July 18. The collective 20 shortcomings involve security management, computer access controls, and security settings. There were 14 new deficiencies detected, along with six defects identified in 2012 that were not corrected. As of September 2013, the Fiscal Service managed about $16,732 billion of federal debt, which was mostly money borrowed to run government operations. About $11,976 billion of that sum was debt held by the public and $4,756 billion was intra-governmental debt holdings. Interest expense on federal debt was $425 billion in fiscal 2013. The significant deficiency, while not a material weakness, "is important enough to merit the attention of those charged with governance of Fiscal Service," Engel said. The Fiscal Service commissioner acknowledged the deficiency in internal controls over financial reporting and is taking action to address it, according to agency comments on a draft report. "Fiscal Service will continue to look for efficient and effective ways to improve and ensure the consistent application of agency-wide security controls over all systems," the final audit states. GAO officials plan to re-examine the status of the 20 vulnerabilities during an audit of the fiscal year 2014 Schedule of Federal Debt. On Thursday, a separate GAO report found that information security weaknesses remain at the Federal Deposit Insurance Corporation, although none are considered significant deficiencies. FDIC, which regulates U.S. financial institutions, has not addressed vulnerabilities dating back to 2012 that affect the "confidentiality, integrity and availability of financial systems and information," the audit states. To read more click **HERE**