The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

28 March 2014

Purpose
Educate recipients of cyber events to aid in the protection of electronically stored corporate proprietary, DoD and/or Personally Identifiable Information from theft, compromise, espionage, and / or insider threat

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, Sandia 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 open source data

March 27, Help Net Security – (International) **Hidden crypto currency-mining code spotted in apps on Google Play.** Researchers at Lookout warned that Android apps which include hidden code used to mine for several forms of cryptocurrency have been spotted being offered on Spanish underweb forums. Trend Micro researchers also spotted two apps available in the Google Play store which contain cryptocurrency mining code, similar to compromised apps originally discovered by G Data researchers. Source: http://www.net-security.org/malware_news.php?id=2746

March 27, Help Net Security – (International) **Cerberus app users warned about data breach.** Cerberus Security Team advised users of their Android security app to reset their passwords as a precaution after suspicious traffic was detected and blocked on the company's servers. Attackers were able to gain access to some users' usernames and encrypted passwords during the breach. Source: http://www.net-security.org/secworld.php?id=16588

March 27, The Register – (International) **When ZOMBIES attack: DDoS traffic triples as 20Gbps becomes the new normal.** Incapsula released a report on distributed denial of service (DDoS) attack mitigation which found that DDoS attack volumes are increasing, with 20Gbps or above attacks occurring in around one-in-three attacks, among other findings. Source: http://www.theregister.co.uk/2014/03/27/ddos_trends_incapsula/

March 26, SC Magazine – (International) **Windows trojan packs punch, downloads ransomware "Cribit."** Trend Micro researchers found that the Fareit trojan is being used to spread a ransomware known as Cribit that encrypts victims' files and demands a ransom in Bitcoins. The trojan has previously been used to download other malware such as Zeus. Source: http://www.scmagazine.com/windows-trojan-packs-punch-downloads-ransomware-cribit/article/339958/

Man Arrested for Hacking Accounts on South Korea's Naver Search Portal
SoftPedia, 28 Mar 2014: A 31-year-old man from South Korea has managed to illegally gain 160 million won ($148,000 / €107,600) after hacking into the accounts of millions of customers of Naver, South Korea's most popular search portal. According to The Korea Herald, the suspect, a man named Seo, has been arrested by police. He's said to have purchased the personal details of 25 million people from a Korean Chinese individual back in August 2013. The information included names, usernames, passwords and residential numbers. He used the information to hack into the accounts of Naver users. He sent spam and malicious emails to the accountholders in an effort to make a profit. In addition to Seo, an individual named Hong has been arrested. Hong is suspected of developing hacking software, including one that performs brute-force attacks against Naver accounts. He is believed to have provided Seo with the Naver credentials extracted with this tool. Three individuals who have worked with Seo have been charged, but they haven't been detained. Police are investigating 86 other individuals believed to have purchased hacking tools from Hong. Naver representatives have clarified that the company can't prevent hackers from accessing customers' accounts with information obtained from other sources. To read more click **HERE**

Cybercriminals Hijack WordPress Websites with Free Premium Plugins

Softpedia, 28 Mar 2014: There are a number of websites that offer premium WordPress plugins for free. However, experts warn that these "free" plugins can actually come at great cost. Researchers from Sucuri have analyzed a number of premium WordPress plugins that are offered for free on various websites such as wplist.org, wplocker.com and others. For instance, the SEOPressor plugin, which is normally priced starting at $47 (€34), has been found by Sucuri experts on the website of a customer. However, the plugin version in question wasn't the genuine one. Instead, it contained code that allowed its creator to hijack the website on which it was installed. After decoding the obfuscated code, experts found instructions to create a new WordPress administrator account with the username "wordpress" and the password "gh67io9Cjm." Once it's installed on a website, the plugin sends an email to the hacker to let him know that the site has been compromised. Then, the attacker loads the blog with the ?cms=jjoplmh parameters in the URL. This triggers the creation of the new administrator account. After that, the cybercriminal can log in to the administration panel and do whatever he wants. Similar functionality has been found in Restrict Content Pro and Flat Skin Pack Extension. The malicious code is slightly different, but it's still designed to create rogue users with administrator privileges. After analyzing wplist.org, Sucuri has determined that a user called "andrewp" uploaded a total of five plugins containing the malicious code: Restrict Content Pro WordPress Plugin V1.5.5, Ideas! v1.1.6, Ultimate Ajax Grid, User Profiles, and UberMenu – Flat Skin Pack V1.0.3. However, this andrewp is not the only one who has uploaded malicious plugins to the website. The site's admin has also submitted 5 rogue plugins in February-March 2014. The tools are Go – Responsive Pricing & Compare Tables (go_pricing), FormCraft, Custom Scrollbar WordPress, Theia Sticky Sidebar and GravityForms. "Our conclusion is that this practice of posting plugins containing malicious code is typical for these sites. Moreover, when in their very own comments area people warn about malicious 'extras' they have found in the plugins, the admin readily replaces them with 'retail' versions," Denis Sinegubko noted. Experts highlight the fact that not all webmasters who install these rogue plugins on their websites do it because they don't want to pay for them. "It's not always about the money. Oftentimes, it's likely just a lack of knowledge. We've found these plugins on sites that made decent money for their owners, on sites that used upscale hosting solutions, and on sites with owners who were willing to pay for extra services," Denis Sinegubko said. Additional details on rogue premium WordPress plugins are available on Sucuri's blog. To read more click **HERE**

Website of Turkey's Telecommunications Directorate Attacked by RedHack

SoftPedia, 28 Mar 2014: Hackers of the RedHack group have launched a cyberattack against the official website of Turkey's Telecommunications Directorate (TIB) in response to the decision to ban YouTube and Twitter in the country. The website of TIB was attacked on Thursday night. It was restored on Friday morning. "You forgot the coordinator of everything while calculating things. The ban is meant to be banned," the hackers said, cited by Today's Zaman. YouTube has been blocked in Turkey after someone leaked a recording of top security officials discussing a possible military operation in Syria. The conversation between Turkey's foreign minister, an army general and the intelligence chief was uploaded to YouTube. Since taking down the video could take time, authorities have decided to ban the website altogether. ZeroHedge provides a copy of the YouTube video and a translation of the conversation between the officials. Turkish Prime Minister Tayyip Erdogan has condemned the leak, calling it "immoral." He claims that this is just another in a long series of recent attempts to discredit him before the March 30 elections. "They even leaked a national security meeting. This is villainous, this is dishonesty...Who are you serving by doing audio surveillance of such an important meeting?" the PM said. In the case of Twitter, Turkey says that it has blocked the service because the company has failed to remove some links. In reality, the government is most likely trying to silence all those who use it to voice their discontent. To read more click **HERE**

Univ. Of Md. President Testifies To Senate About Security Data Breach

CBS Baltimore, 27 Mar 2014: The University of Maryland president testifies on Capitol Hill about the widespread data breach that exposed hundreds of thousands of people's personal information. Dr. Wallace Loh reveals how the hackers got in and how the university scrambled to deal with it. A massive data breach at University of Maryland, College Park has President Wallace Loh explaining what went to U.S. Senate members. "We were just flying by the seat of our pants," Loh said. Loh says an intricate cyber attack caught the university off guard when a hacker uploaded a Trojan horse onto a university website. The dangerous malware detects passwords for IT managers, allowing access to more than 300,000 social security numbers. "I was surprised that it even happened in the first place. I thought Maryland was more secure than that," Damilola Otukoya said. The university admits those sensitive records should have been purged. Instead, the oversight is costing them millions. "The reason they're stealing social security numbers is because they're valuable," Loh said. "If they were not valuable, nobody would be stealing them. So pass a law forbidding financial institutions from requiring social security numbers." This comes as Target and high-end retailer Neiman Marcus face breaches with the same malware attacking their online credit card processing. "I do check my credits after these events came out," said Erica Chen, UMD student. The university has set aside more than $6 million to pay for credit monitoring for victims. "I'm sure there will always be something that cyber hackers will look for or get some kind of vital information. If it's not here, then it will be somewhere else," Otukoya said. But some students remain skeptical their personal information is any safer than before. Since the breach, the university has created an 18 member task force on cyber security. Loh says, so far, 30,000 people have registered for the free credit protection services. To read more click **HERE**

Analysis of three billion attacks reveals SQL injections cost $196,000

Heise Security, 28 Mar 2014: NTT Innovation Institute has announced the release of its Global Threat Intelligence Report (GTIR), which raises awareness with C-level executives and security professionals alike that when the basics of security are done right, it can be enough to mitigate and even avoid the high-profile security and data breaches. The report focuses on five critical areas of security: Threat avoidance, threat response, threat detection, investigative and response capabilities. A key portion of the report is dedicated to business and security leaders concerned with balancing cost and risk. Recommendations and strategies for minimizing the impact of threats and reducing the threat mitigation timeline are conveyed in multiple charts and real-world case studies. Key findings in the 2014 GTIR include:

- Cost for a 'minor' SQL injection attack exceeds $196,000 – Organizations must realize the true cost of an incident and learn how a small investment could reduce losses by almost 95 per cent. Case Study: "Massive Data Exfiltration via SQL Injection".
- Anti-virus fails to detect 54 per cent of new malware collected by honeypots - Additionally, 71 per cent of new malware collected from sandboxes was also undetected by over 40 different anti-virus solutions. This supports the premise that simple endpoint solutions must be augmented with network malware detection and purpose-built solutions.
- 43 per cent of incident response engagements were the result of malware - Missing anti-virus, anti-malware and effective lifecycle management of these basic controls were key factors in a significant portion of these engagements. Read the "Administrator Releases a Worm" case study to see how it cost one organization $109,000.
- Botnet activity takes an overwhelming lead at 34 percent of events observed - Almost 50 per cent of botnet activity detected in 2013 originated from US based addresses. The fact that healthcare, technology and finance account for 60 per cent of observed botnet activity reflects the information worker burden that accompanies these industries.
- PCI assessed organizations are better at addressing perimeter vulnerabilities - Organizations performing quarterly external PCI Authorized Scanning Vendor (ASV) assessments have a more secure vulnerability profile, as well as a faster remediation time (27 per cent), than organizations performing unregulated assessments.

- Healthcare has observed a 13 per cent increase in botnet activity - Due to increased reliance on interconnected systems for the exchange and monitoring of health related data, more systems are potentially affected by malware.

The GTIR was developed using threat intelligence and attack data from the NTT Group companies - Solutionary, NTT Com Security, Dimension Data, NTT Data and support from NTT R&D. The key findings in the GTIR are a result of the analysis of approximately three billion worldwide attacks over the course of 2013. The data analysed for this report was collected from 16 Security Operations Centers (SOC) and seven R&D centers with more than 1,300 NTT security experts and researchers from around the world. To read more click **HERE**