THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

30 June 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

June 27, Help Net Security – (National) **The unlocked backdoor to healthcare data.** A CORL Technologies report found that the majority of healthcare vendors do not have minimum security and are failing to hold vendors accountable for meeting minimum acceptable standards in order to mitigate vendor-related security weaknesses. More than 58 percent scored in the "D" grade range for their culture of security. Source: http://www.net-security.org/secworld.php?id=17062

June 25, Southern California City News Service – (California) **County: More than 500 hospital patients' data on stolen laptop.** Riverside County Regional Medical Center in Moreno Valley informed 563 hospital patients June 24 that their personal information may have been compromised after a computer containing data files of patients' medical and personal information was stolen from the medical center. Source: http://www.kesq.com/news/county-more-than-500-hospital-patients-data-on-stolen-laptop/26655764

June 27, Securityweek – (International) **Pony Loader 2.0 malware source code for sale.** Researchers with Damballa stated that the source code for version 2.0 of the Pony Loader information-stealing trojan has been seen for sale in underweb markets. The trojan was offered for sale starting in May and allows attackers to steal information such as passwords as well as virtual currency such as Bitcoin and others. Source: http://www.securityweek.com/pony-loader-20-malware-source-code-sale

June 27, The Register – (International) **Android SMS worm punts dodgy downloads…from your MATES.** AdaptiveMobile researchers reported finding a piece of Android malware known as Selfmite that spreads like a worm by sending out SMS messages to infected users' contacts that contain a link that attempts to get users to install the Mobogenie app in a likely pay-per-install scheme. The malware was first observed on mobile networks in the U.S. and has since spread to several other countries. Source: http://www.theregister.co.uk/2014/06/27/selfmite_android_self_replicating_sms_worm/

June 27, Securityweek – (International) **RIG Exploit Kit used in Flash-based malvertising campaign.** Researchers with Malwarebytes stated June 26 that they have detected a malvertising campaign that attempts to lure users to a malicious Web site containing the RIG Exploit Kit, which then attempts to use Adobe Flash and Microsoft Silverlight vulnerabilities to spread a trojan identified a Trojan.Agent.ED. Source: http://www.securityweek.com/rig-exploit-kit-used-flash-based-malvertising-campaign

June 27, The Register – (International) **Yet another WordPress vuln: Image furtler plugin lets BADNESS in.** Security researchers warned users of the TimThumb plugin for Wordpress that a vulnerability exists in the plugin that could allow attackers to inject code or create, remove, and modify files. The vulnerability exists in the plugin's Webshot option, which is turned off by default. Source: http://www.theregister.co.uk/2014/06/27/wordpress_0day/

June 27, Softpedia – (International) **LZO algorithm patched after 20 years.** The CEO of Lab Mouse Security revealed that an integer overflow bug in the Lempel-Ziv-Oberhumer (LZO) compression and decompression algorithm has been present for as long as 20 years, leaving software using the algorithm vulnerable to remote code execution and denial of service attacks. The algorithm has been integrated into a variety of software, including the Linux kernel, some Android phones, medical equipment, and others, though the variety of applications means that attackers would need to build custom malicious payloads in order to exploit the issue. Source: http://news.softpedia.com/news/LZO-Algorithm-Patched-After-20-Years-448641.shtml

June 26, Softpedia – (International) **VMware implements Apache Struts security fixes in vCOps.** VMware released an update for its vCenter Operations Management Suite (vCOps) that close several vulnerabilities affecting the Apache Struts Java application framework. Source: http://news.softpedia.com/news/VMware-Implements-Apache-Struts-Security-Fixes-in-vCOps-448501.shtml

Amplification of DDoS Attacks

SoftPedia, 30 Jun 2014: The purpose of a DDoS (distributed denial-of service) attack is to disrupt the activity of a service by flooding the servers with so much junk traffic that they run out of resources to process it. This type of attacks does not lead to loss of information, as there is no penetration of the systems; however, they can be used as a means to divert the attention so that criminals can carry out other nefarious operations, such as exfiltrating sensitive information. An amplified DDoS attack works with protocols that can generate responses larger than the queries and are vulnerable to IP address spoofing, so the origin of the request is not verified through a handshake. What the attacker does is send a small query request to the server spoofing the victim's address as the return path for the response. The server than replies to the spoofed IP and all the data is directed to the victim. Generally, cybercriminals carry out amplified distributed denial-of service attacks through publicly available servers, using UDP communication, which, unlike TCP, does not require a prior connection for establishing the source and just sends the data to the terminal address indicated in the query. The requests are sent from infected machines that respond to the commands of the criminals, namely botnets. DNS and NTP servers are some of the most used for this type of activity, but other types are also susceptible. Devices supporting SNMP v2 (used for monitoring network devices such as hosts, routers, hubs and switches) have also been employed for DDoS amplification, as well as devices that relay ICMP requests to all the other devices behind the network. The Smurf Attack is known as the original example of DDoS amplification. Named so after a file from the source code of the attack program released in 1997, the Smurf Attack consisted in sending a large number of ICMP packets to a router. This would trigger a response to a spoofed address from each of the connected devices. In a DNS amplification attack, the traffic is directed to the victim from open DNS servers, and to maximize the impact, the query requests as much information as possible. Most of the times, the requests are of the type "ANY," designed to return details about a DNS zone; in such a case, the amplification factor can be of more than 50 times. NTP servers, which are used for system time synchronization, can offer a much larger amplification due to the resources available, including network connectivity. At the moment, despite efforts for raising awareness of a vulnerability that has received a fix, numerous machines capable of amplifying a request more than 700 times can be leveraged for DDoS attacks. The flaw is in the "monlist" command that can be queried for the IP addresses of the last 600 clients that have synchronized time with the NTP server. The request appears to originate from the IP address of the intended victim, which is then hit with the response. Not all SNMP v2 machines are public, but there are plenty of cases where the SNMP service is exposed to the Internet, both in business and home environments. A threat advisory from the Prolexic Security Engineering Response Team provides an example of an amplification factor of more than 1,700 times for a GetBulk response. Some of the largest DDoS attacks have been amplified by abusing NTP servers, with the most recent happening in February this year and peaking close to 400Gbps. This amount of traffic was sent from 4,529 NTP servers running on 1,298 different networks. According to US CERT (United States

Computer Emergency Readiness Team), one solution against attacks relying on UDP-based amplification is for ISPs (Internet Service Providers) to reject UDP traffic with spoofed addresses by following the specifications of the BCP 38 document. To read more click **HERE**

Content Widget Maker Taboola Is Hacked on Reuters

DarkReading, 24 Jun 2014: Syrian Electronic Army targets widget used by many publishers to surface content that the reader might like.Taboola, a widget used by many electronic publishers to help readers find additional content, was hacked by the Syrian Electronic Army (SEA) yesterday. "Today [Monday], between 7AM - 8AM EDT, an organization called the Syrian Electronic Army hacked Taboola's widget on Reuters.com," said Taboola founder and CEO Adam Singolda in a blog. "The intruder was redirecting users that accessed article pages on reuters.com to a different landing page." Taboola is also used by other popular websites, including Time, The Weather Channel, BBC, and USA Today, but the Reuters hack is the only one mentioned in the blog. Taboola did not immediately address the SEA's claims that it had also hacked Taboola's Paypal account. The SEA posted a copy of what appears be the Paypal page of Taboola on its website. "The breach was detected at approximately 7:25am, and fully-removed at 8am," said Singola. "There is no further suspicious activity across our network since, and the total duration of the event was 60 minutes. "While we use 2-step authentication, our initial investigation shows the attack was enabled through a phishing mechanism. We immediately changed all access passwords, and will continue to investigate this over the next 24 hours." "Websites need to think long and hard not only about the security of their own servers, but whether the companies who are providing widgets and plugins that power the websites are taking security as seriously themselves," said security expert Graham Cluley in a blog about the incident. To read more click **HERE**

Dropbox-themed phishing is after multiple login credentials

Heise Security, 23 Jun 2014: Phishing emails purportedly leading users to a file hosted on Dropbox are targeting Yahoo!, Gmail, Hotmail, and Aol email users, warns Malwarebytes' Jovi Umawing. Clicking on the offered link takes users to a spoofed Dropbox page hosted on the compromised website of a company selling alloy wheels and accessories, where they are asked to login with their email address and password in order to access the file. Unfortunately for those who do, the entered login credentials are immediately forwarded to the criminals behind this scheme, and the victims are redirected to the legitimate login page of the email service for which they entered the credentials. If this happened to you, and you use the same login credentials for multiple online services, consider all those accounts compromised and change the passwords on them immediately. If they have already been taken over by the crooks, contact the services to learn how you can restore access to them. To read more click **HERE**

Google Drive update fixes data-leaking flaw

Heise Security, 30 Jun 2014: Google has fixed a security issue that made some of the files stored on Google Drive and shared with friends or colleagues via a direct link potentially reachable by unauthorized third parties, and calls users to remove previously shared documents. The issue, according to Kevin Stadmeyer, Technical Program Manager at Google, is only relevant if the file in question was uploaded to Google Drive, was not converted to Docs, Sheets, or Slides, the documents was made available to "Anyone with the link," and the file contained hyperlinks to third-party HTTPS websites in its content. The flaw could allow the admins of those third-party HTTPS websites to receive header information from which the URL leading to the file could be extracted. The issue has been solved, but previously uploaded and shared documents that meet all four of the aforementioned criteria are still vulnerable, so users are advised to create a copy of the document, share the link to it with the intended recipients, and finally delete the old file. Last month, Dropbox has patched the exact same issue. To read more click **HERE**