THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

23 September 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

September 19, Reuters – (National) **U.S judge awards $40.7 million in SEC case over bitcoin Ponzi scheme.** A federal judge ruled September 18 that a Texas man who operated Bitcoin Savings and Trust operated a Ponzi scheme that defrauded investors and ordered the man to pay $40.7 million following U.S. Securities and Exchange Commission charges of investment fraud. The scheme raised investments using the Bitcoin virtual currency between February 2011 and August 2012 on the promise of weekly returns but the funds were instead used for the owner's personal expenses. Source: http://www.reuters.com/article/2014/09/19/us-sec-bitcoin-fraud-idUSKBN0HE1Z820140919

September 22, Softpedia – (International) **Hackers target Destiny and Call of Duty servers with DDoS attack.** Several servers for online games Destiny and Call of Duty: Ghost went down during the weekend of September 20 due to a distributed denial of service (DDoS) attack that affected PlayStation and Xbox users. Attackers claiming affiliation with the Lizard Squad group claimed responsibility for the attacks. Source: http://news.softpedia.com/news/Hackers-Target-Destiny-and-Call-of-Duty-Servers-with-DDoS-Attack-459494.shtml

September 22, The Register – (International) **Exercise-tracking app not QUITE fit for purpose.** A researcher identified and reported a direct object reference vulnerability in the MyFitnessPal app that allowed users' personal information, including location and dates of birth, to be accessed by any user. The vulnerability was closed 2 days after being reported. Source: http://www.theregister.co.uk/2014/09/22/exercise_tracking_app_not_quite_fit_for_purpose/

September 22, Securityweek – (International) **Yahoo fixes RCE flaw leading to root server access.** A researcher identified and reported a series of vulnerabilities in a Yahoo domain which led to a remote code execution vulnerability that was leveraged to gain root access to a Yahoo server. The vulnerability was reported September 5 and closed September 7. Source: http://www.securityweek.com/yahoo-fixes-rce-flaw-leading-root-server-access

September 22, Help Net Security – (International) **Payment card info of 880k Viator customers compromised.** Viator representatives confirmed September 19 that the company was made aware September 2 that its network was breached and the encrypted personal and financial information of about 1.4 million customers may have been compromised. Customers were advised to update their Viator online account information, including passwords. Source: http://www.net-security.org/secworld.php?id=17391

Number of malicious eBay listings rises, accounts are hijacked
Heise Security, 22 Sep 2014: Pressure is mounting against eBay to quickly detect and remove bogus listings triggering cross-site scripting flaws to redirect users to phishing and other malicious pages. This particular problem exists for years because eBay allows the use of custom Javascript and Flash content on listings pages so that they might "pop out" and attract more potential buyers. EBay has generally been doing a good job removing malicious listings, but every now and then they slip up and the number of these listings spikes for a while, as it's

currently happening. The onslaught started last week, when an IT worker from Scotland spotted a few listings that redirected him to a well-made eBay login phishing page. The e-commerce giant has reacted, but not soon enough, and the listings were up for over 12 hours, tricking who knowns how many users. According to the BBC, the number of listings using the same trick to redirect users to malicious pages has, in the meantime, risen to at least 100, and possibly even more. Some of these listings have been placed via hijacked eBay accounts with 100% positive feedback, which made them look legitimate. The listings are offering iPhones, television sets, clothing, and other attractive items, and redirect to fake eBay Security & Resolution Center pages designed to harvest users' credit card details, bank account details, some personal information, and so on. EBay has commented the matter by saying that many of their sellers use active content like Javascript and Flash to make their eBay listings perform better. "We have no current plans to remove active content from eBay," they stated. "However, we will continue to review all site features and content in the context of the benefit they bring our customers as well as overall site security." "Until eBay has the ability to automatically identify malicious links, it should disable Javascript until they have some way of better controlling the risk," opined Brian Honan, BH Consulting CEO. To read more click **HERE**

CipherShed: A replacement for TrueCrypt

Heise Security, 22 Sep 2014: Ever since TrueCrypt developers terminated the development of the popular encryption utility and announced that it was not safe to use, users who need such a tool have been looking for an alternative, safe solution. While the Open Crypt Audit Project, headed by cryptographer Matthew Green and Kenneth White, Principal Scientist at Social & Scientific Systems, has been considering whether to take over the development of TrueCrypt and is working on the second phase of the audit process (a thorough analysis of the code responsable for the actual encryption process), one of TrueCrypt's developers has expressed his disapproval of a project that would fork the software. "I don't feel that forking TrueCrypt would be a good idea, a complete rewrite was something we wanted to do for a while," he said. "I believe that starting from scratch wouldn't require much more work than actually learning and understanding all of TrueCrypt's current codebase. I have no problem with the source code being used as reference." But, as the need for a secure alternative to TrueCrypt is great, there have been attempts to fork the software. One of these projects, initially found on Truecrypt.ch, will definitely be forking TrueCrypt. The developers, who in this case are publicly known, have renamed the fork into CipherShed. According to the TrueCrypt open source license, the forking of the code is permitted if all references to TrueCrypt are removed from it, and if the final software hasn't got "TrueCrypt" in its name. "CipherShed is cross-platform; it will be available for Windows, Mac OS and GNU/Linux," the developers say. It will also be open source and free of charge. They are now auditing the TrueCrypt code for security issues and are cleaning up the code, and according to project initiator Jos Doekbrijder, an alpha release of CipherShed will be made available for download soon. This release will be based on the latest full version of TrueCrypt (v7.1a), but eventually the group is aiming to create an entirely new product that will contain none of TrueCrypt's code. They want to create a simple tool that will do a few things well, will be able to work with old TrueCrypt containers, and will work on newer systems. The developers also mean to implement new crypto algorithms as they come along. To read more click **HERE**

5 Ways to Monitor DNS Traffic for Security Threats

Dark Reading, 18 Sep 2014: Here are five ways to implement real-time or offline traffic monitoring using common commercial or open source security products to detect cyber security threats:

1. Firewalls: Let's begin at the most prevalent security system: your firewall. All firewalls should let you define rules to prevent IP spoofing. Include a rule to deny DNS queries from IP addresses outside your allocated numbers space to prevent your name resolver from being exploited as an open reflector in DDoS attacks. Next, enable inspection of DNS traffic for suspicious byte patterns or anomalous DNS traffic to block name server software exploit attacks. Documentation describing how popular firewalls provide this feature is readily available (e.g., Palo Alto Networks, Cisco

Systems, WatchGuard). Sonicwall and Palo Alto can detect and block certain DNS tunneling traffic, as well.

2. Intrusion detection systems: Whether you use Snort, Suricata, or OSSEC, you can compose rules to report DNS requests from unauthorized clients. You can also compose rules to count or report NXDOMAIN responses, responses containing resource records with short TTLs, DNS queries made using TCP, DNS queries to nonstandard ports, suspiciously large DNS responses, etc. Any value in any field of the DNS query or response message is basically "in play." You're essentially limited only by your imagination and mastery of DNS. Intrusion prevention services in firewalls provide permit/deny rules for many of the most common of these checks.

3. Traffic analyzers: Use cases for both Wireshark and Bro show that passive traffic analysis can be useful in identifying malware traffic. Capture and filter DNS traffic between your clients and your resolver, and save to a PCAP file. Create scripts to search the PCAP for the specific suspicious activities you are investigating, or use PacketQ (originally DNS2DB) to SQL query the PCAP file directly. (Remember to block your clients from using any resolver or nonstandard port other than your local resolvers).

4. Passive DNS replication: This involves using sensors at resolvers to create a database that contains every DNS transaction (query/response) through a given resolver or set of resolvers. Including passive DNS data in your analysis can be instrumental in identifying malware domains, especially in cases where the malware uses algorithmically generated domain names (DGAs). Palo Alto Networks firewalls and security management systems that use Suricata as an IDS engine (like AlienVault USM or OSSIM) are examples of security systems that pair passive DNS with IPS to block known malicious domains.

5. Logging at your resolver: The logs of your local resolvers are a last and perhaps most obvious data source for investigating DNS traffic. With logging enabled, you can use tools like Splunk plus getwatchlist or OSSEC to collect DNS server logs and explore for known malicious domains.

To read more click **HERE**

Microsoft Gives Office Completely Free to More Students

Softpedia, 23 Sep 2014: Microsoft is one of the companies that are aggressively investing in the educational sector, and it's a well-known fact that several schools have already signed up for a program that brings Surface tablets, Windows 8.1 devices, and free Office 365 for students and teachers. But there are some cases when schools failed to register for Microsoft's programs, so a lot of students actually never got the chance to receive a free copy of Office. That's going to change thanks to a new program announced by Microsoft, that allows students to request free software as part of the Student Advantage program on their own, without the need for schools to give their go-ahead. The only thing you need is a valid email address provided by your school in order to register for the program and thus get access to free Microsoft goodies. Office 365 ProPlus available free of charge. Once you register, Microsoft emails you a list of links with access to Office 365 ProPlus, the same version of the cloud-based productivity suite that was until now available to schools. Office 365 ProPlus comes with the standard productivity tools, including Word, Excel, PowerPoint, OneNote, Outlook, Access, and Publisher, support for five different devices, be they PCs, Macs, or tablets, an additional of 1TB of OneDrive cloud storage, and access to Office Online. "The new self-service sign-in is quick and easy for students, but still allows school IT managers to maintain all the control, flexibility and security that Office is known for while reducing the amount of administrative work needed to provide these free services to students. This same service will be available worldwide in the next few months," Anthony Salcito, vice president of Worldwide Education at Microsoft, has said today. Unfortunately, this new program is only aimed at students in the United States

for now, but the company has promised to add support for new countries in the coming months. "Eligible educational institution employees in the U.S. can sign up at office.com/teachers beginning in October with availability worldwide starting in December," the company says. At the same time, Microsoft has also announced that organizations will also receive a free subscription for Office 365 ProPlus for all students, faculty and staff once they purchase an Office license. "With Office 365 ProPlus, teachers get continual updates, which means they are always using the latest, best version of Office. They can install Office on up to five PCs or Macs and can unlock the editing capabilities of Office apps for iPad. Using their Office 365 ID also means they can access the same Office content while on the go with the mobile apps on Windows Phone, iPhones and Android Phones," Microsoft concludes. To find out if you're eligible for the new US-only program, click this link. To read more click **HERE**