# THE CYBER SHIELD

*Cyber News for Counterintelligence / Information Technology / Security Professionals*

*5 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


## Obamacare site hacked but nothing taken, HHS says

CNN, 5 Sep 2014: Hackers silently infected a Healthcare.gov computer server this summer. But the malware didn't manage to steal anyone's data, federal officials say. On Thursday, the Health and Human Services Department, which manages the Obamacare website, explained what happened. And officials stressed that personal information was never at risk. "Our review indicates that the server did not contain consumer personal information; data was not transmitted outside the agency, and the website was not specifically targeted," HHS spokesman Kevin Griffis said. But it was a close call, showing just how vulnerable computer systems can be. It all happened because of a series of mistakes. A computer server that routinely tests portions of the website wasn't properly set up. It was never supposed to be connected to the Internet -- but someone had accidentally connected it anyway. That left it open to attack, and on July 8, malware slipped past the Obamacare security system, officials said. As health department officials describe it, the malware was run-of-the-mill, low-level hacker stuff. It wasn't even designed to steal patient data. It was actually malware meant to turn the computer server into a zombie machine, part of a robot network, or botnet, to spews out spam or computer viruses to the rest of us. It wasn't the military-grade cyber weapons typically aimed at U.S. systems by hackers in China and Russia. But federal officials said the malware didn't do any damage. It just lay there dormant, quiet and dumb. That's one reason it wasn't found until weeks later. The website's security team conducts daily reviews, but the malware wasn't spotted until Aug. 25. The computer server was quickly disconnected and decommissioned. The FBI and Department of Homeland Security are now investigating, HHS said. Federal officials say the attack came from several Internet addresses, some overseas. HHS officials on Thursday briefed Congressional staff about the episode and assured the department has taken "measures to further strengthen security." Last year, computer researchers found a security hole found in Obamacare website. But that has since been patched. To read more click **HERE**

*September 4, Softpedia* – (International) **Updated Vawtrak banking malware strain expands target list.** Researchers with PhishLabs identified a new variant of the Vawtrak financial malware (also known as Neverquest) that has added features in the last month enabling it to expand its targets to users in the U.S., Canada, and Europe. The malware targets financial institutions as well as social networks, online retailers, gaming portals, and analytics firms and can steal credentials and automate fraudulent transactions. Source: http://news.softpedia.com/news/Updated-Vawtrak-Banking-Malware-Strain-Expands-Target-List-457656.shtml

*September 4, Softpedia* – (International) **Old Slider Revolution vulnerability massively exploited.** Researchers at Sucuri found that attackers began heavily exploiting an old vulnerability in unpatched versions of the Slider Revolution Premium plugin for WordPress during August, which could allow a Local File Inclusion (LFI) attack. The vulnerability was fixed in February and all users were advised to update to the latest version as soon as possible. Source: http://news.softpedia.com/news/Old-Slider-Revolution-Vulnerability-Massively-Exploited-457607.shtml

*September 4, Securityweek* – (International) **CERT warns of Android apps vulnerable to MitM attacks.** The Computer Emergency Response Team Coordination Center at Carnegie Mellon University (CERT/CC) published a list of popular Android apps that expose users to man-in-the-middle (MitM) attacks due to the apps not properly validating SSL certificates. CERT/CC released its findings in a spreadsheet detailing their results and is attempting to contact the authors of every app that failed the organization's tests. Source: http://www.securityweek.com/cert-warns-android-apps-vulnerable-mitm-attacks

*September 4, Softpedia* – (International) **Home router DNS settings changed via Web-based attack.** Kaspersky Lab researchers identified a Web-based attack that uses Web pages with malicious scripts to attempt to change users' home router Domain Name System (DNS) settings in order to redirect users to phishing pages of financial institutions. The attack was mostly observed in Brazil but also targeted some users in the U.S., Canada, Mexico, and other countries. Source: http://news.softpedia.com/news/Home-Router-DNS-Settings-Changed-Via-Web-Based-Attack-457668.shtml

*September 4, The Register* – (International) **VirusTotal mess means YOU TOO can track Comment Crew!** A researcher released findings on how he was able to use structured data and analysis to identify a subgroup of the Comment Crew group and an unnamed Iranian group using Google's VirusTotal service to test new versions of malware against security software and check for detection rates. Source: http://www.theregister.co.uk/2014/09/04/virustotal_blue_means_you_too_can_track_comment_crew/

*September 3, Help Net Security* – (International) **Semalt botnet hijacked nearly 300k computers.** Incapsula researchers reported that the Semalt botnet is spreading quickly and is currently made up of around 290,000 infected machines. The botnet is linked to a Ukrainian search engine optimization (SEO) service and spams millions of Web sites in a referrer spam campaign designed to fraudulently boost a site's search engine ranking. Source: http://www.net-security.org/malware_news.php?id=2857

**The Amazon.com of Stolen Credit Cards Makes It All So Easy**

Bloomberg, 4 Sep 2014: On Sept. 1, the website Rescator.cc alerted customers to a big new batch of product about to hit its digital shelves. "Load your accounts and prepare for an avalanche of cash!" a post on its News page read. The items, marketed under the names American Sanctions and European Sanctions, appeared as promised the next day, spurring such an enthusiastic response that the site was pushed offline at times by the high demand. Looking for stolen credit cards? The Rescator site has become something like the Amazon.com of the black market—an efficient, easy-to-use purveyor of quality products for cyber criminals. The latest batches were likely pilfered from Home Depot (HD), as reported on Sept. 2 by the security blogger Brian Krebs. The American Sanctions cards are broken into two installments, 1 and 2, and those who monitor the Rescator site expect many more to come. "He doesn't do that unless there are millions," says Mark Lanterman, who runs a digital forensics company, Computer Forensic Services, in Minnetonka, Minn. He applied for an account using an assumed identity and keeps an eye on the site as part of his work with law enforcement. Lanterman's search of cards with mailing addresses in five Zip codes around Minneapolis has pulled up more than 12,000 cards. Krebs found that 1,822 postal codes were represented in the card data in the Sanctions batches, only 10 of which don't have a Home Depot store, he posted on krebsonsecurity.com. If you're buying stolen cards, you purchase them to use in your local area because one of banks' most basic fraud monitoring techniques is to screen for card use that's far removed from the card billing address. Hence the importance of the Zip code. On the Rescator site, you can also filter, if you want, by bank, by card type, by expiration date, and even by the last four digits of the card number. The newest batches claim a 100 percent validity rate, meaning cyber criminals won't run into the embarrassment of having a stolen card declined while trying to make some illicit purchase. "No replacements!" the website says. For earlier lots, the validity rate appears next to the name. For one labeled "Jackie Chan"—data stolen from the restaurant chain P.F. Chang's China Bistro, according to Lanterman—the validity rate is now 50 percent, and Rescator does offer replacements in such cases. It's not clear who's behind the Rescator site. The word Rescator was embedded in malware

used in the Target (TGT) last December, and a hacker posting to some forums using that handle has also gone by the nickname Helkern. The Helkern alias can be linked to a man in Odessa, Ukraine, named Andrey Khodyrevskiy, an investigation by Businessweek earlier this year found. Not that Khodyrevskiy displayed much of a genius for online crime: He received a three-year suspended sentence for a poorly executed 2011 hack into a local Web portal in Odessa. Whoever the Rescator.cc mastermind is, customers—those to be found lurking on underground bulletin boards where cyber thieves congregate—give the latest offering five stars. "They're praising the guy like a rock star over the quality of these numbers," Lanterman says. "They love him. They think he's the second coming of Elvis." To read more click **HERE**

## Chinese Cybercrime Soars as Tools are Traded Online

InfoSecurity, 4 Sep 2014: The underground market for cybercrime products and services in China is booming, with both the number of participants and IM messages sent between those participants doubling last year, according to new research from Trend Micro. The security vendor has been monitoring China's cybercrime underground since 2011, in particular the near ubiquitous QQ messaging platform from Tencent which allows users to set up multiple chat groups of up to 2,000 contacts. By the end of 2013, it discovered more than 1.4 million QQ Groups messages related to cybercrime and in the latter 10 months of that year, the number of messages sent and participant volume doubled from the same period in 2012. In some months, the difference between 2012 and 2013 volumes was even greater. In June 2013, for example, Trend Micro uncovered 109,222 messages – over 100,000 more than in the same month the previous year. Another indicator of growing activity Trend Micro worked out is "participant per group per day" (PGD). In 2012 the figure was just 5.13, but this rose to 11.26 in 2013. Messages per group per day (MGD) also soared – from 28.74 in 2012 to 62.56 last year, the report claimed. The three most popular products/services in China were compromised hosts, distributed denial-of-service (DDoS) attack services, and remote access tools/Trojans (RATs). Compromised hosts – which are typically used to distribute malware or spam, launch DDoS attacks or run complex computing tasks – were by far the most popular. Trend Micro found these were offered on the underground market on a total of 35,112 occasions, compared to 16,471 for DDoS and 15,365 for RATs. These aren't the only products and services being offered, of course. The report details a wide variety starting at just $8 for 100 Windows XP bots. China also has a burgeoning mobile cybercrime underground and Trend Micro monitored 11 related chat groups to see how far it's grown since 2012. Although the number of messages sent by each QQ Group per day was roughly the same as that of the regular cybercrime underground and increased only slightly since 2012, the stats were different for PGD. The report had the following: "We determined the mobile PGD and found that it significantly increased from around 11 in 2012 to around 29 in 2013. This means that each mobile underground group in 2013 had around 29 participants per day, almost 2.5 times as many as in 2012. The mobile PGD was more than double the overall PGD in 2013 as well." SMS spamming services were by far the most popular being touted on the underground market, followed by SMS servers and premium service numbers." It should be noted that the criminal activity Trend Micro looked at in this report is very much financially motivated and as such usually remains within the Middle Kingdom, unlike the notorious state-sponsored espionage aimed at foreign targets. To read more click **HERE**

## 800 fake companies front cybercrime attack

SC Magazine, 4 Sep 2014: Dubbed the 'Harkonnen Operation' this reportedly large cybercrime network discovered by Israeli security company CyberTinel is claimed to have already penetrated hundreds of blue-chip companies, government institutions, research laboratories and critical infrastructure facilities throughout Germany, Austria and Switzerland. CyberTinel has issued a release saying that it detected trojans siphoning critical information at a German company which holds sensitive data on behalf of its international clients, and that further investigation led to the source of the breach, revealing that the original domain was registered by a UK company and that a further 833 companies were also registered in the UK. Subsequencly records were found in the 'Harkonnen Operation' on more than 300 additional organisations in Germany, Austria and Switzerland, targeting key executives; the company is now working

with German police investigators with the expectation that companies in other European countries, including the UK, will have also been breached. The attack was initiated using a 'spear phishing' penetration and executed by running two system Trojans created in Germany. "The network exploited the UK's relatively tolerant requirements for purchasing SSL security certificates, and established British front companies so they could emulate legitimate web services," said Jonathan Gad of Elite Cyber Solutions, CyberTinel's UK partner. "The German attackers behind the network then had total control over the targeted computers and were able to carry out their espionage undisturbed for many years." To read more click **HERE**