# The Cyber Shield

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

*7 May 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





**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




*May 6, Softpedia* – (International) **Casino operator Affinity Gaming hacked again.** Casino operator Affinity Gaming reported that their systems were compromised in a data breach that allowed attackers to access the company's system for processing credit and debit cards at its casinos. The company was investigating and was unsure of how many customers were impacted or for how long attackers had access to the systems. Source: http://news.softpedia.com/news/Casino-Operator-Affinity-Gaming-Hacked-Again-440724.shtml

*May 5, Softpedia* – (International) **Man suspected of hacking Swiss banks arrested in Thailand.** A Moroccan citizen was arrested by authorities in Thailand on suspicion of working with 10 others to compromise the accounts of several Swiss bank customers and steal around $18 million. The suspect is pending extradition to Switzerland. Source: http://news.softpedia.com/news/Man-Suspected-of-Hacking-Swiss-Banks-Arrested-in-Thailand-440641.shtml

*May 5, Worcester Business Journal* – (Massachusetts) **Medical center probes possible data breach.** UMass Memorial Medical Center in Worcester notified approximately 2,400 patients May 5 whose information was accessed by a former employee after learning March 6 that the former employee may have accessed and misused personal information on up to 4 patients. Officials are investigating but believe the information that was allegedly taken may have been used to open credit cards and cell phone accounts. Source: http://www.wbjournal.com/article/20140505/NEWS01/140509978/1002

**Telecoms Company Orange Hacked Again, Details of 1.3 Million People Stolen**
SoftPedia, 7 May 2014: French telecommunications services provider Orange has suffered another data breach. This is the second time cybercriminals target the company's systems this year. According to AFP, the attackers managed to steal names, email addresses, phone numbers (both mobile and fixed), names of mobile and Internet operators, and dates of birth. 1.3 million customers are affected by the incident. The breach came to light on April 18, but the company has waited until now to inform customers to determine its full extent and to ensure that the security holes leveraged by the hackers have been patched. While no financial information has been compromised, Orange is warning customers that the details stolen by the cybercriminals can be used for phishing attacks. Reuters reports that the hackers breached the platform used by the company to send promotional messages to customers. The first incident suffered by Orange this year came to light in early February. The attackers penetrated the My Account section of the orange.fr website on January 16. They gained access to the names, mailing addresses, phone numbers and email addresses of 800,000 people. No passwords or financial data were compromised at the time. Names, email addresses and phone numbers are not as sensitive as passwords or financial data. However, such information can still be put to good use. The cybercriminals who stole it can use it for targeted phishing attacks or they can sell it on the underground market. To read more click **HERE**

**Alleged Members of Team Digi7al Charged with Hacking Systems of US Navy**

SoftPedia, 7 May 2014: Two people suspected of being members of the now-defunct hacker group called Team Digi7al have been charged earlier this week. They're said to have breached the computer systems of more than 30 entities, including some US government organizations. The suspects are Nicholas Paul Knight, 27, of Chantilly, Virginia, and Daniel Trenton Krueger, 20, of Salem, Illinois. Knight, Krueger and other members of the hacker group are said to have targeted various organizations in an effort to steal identities, obstruct justice and cause damage to protected computers. The list of targets includes the US Navy, the US National Geospatial-Intelligence Agency, the US Department of Homeland Security, the World Health Organization, the Toronto Police Service in Canada, the Los Alamos National Laboratory, the Montgomery Police Department, AT&T U-verse, Autotrader.com, the Library of Congress, and various universities. Knight, who at the time of the attacks was an active duty-enlisted Navy member assigned to the nuclear aircraft carrier USS Harry S. Truman as a systems administrator in the nuclear reactor department, is believed to be the group's leader. Softpedia covered most of the attacks carried out by the crew between April 2012 and June 2012. They started by highlighting the existence of vulnerabilities in high-profile websites, but they soon turned to leaking information from the databases they breached. The Naval Criminal Investigative Service (NCIS) detected a breach in the Navy's Smart Web Move (SWM) database in June 2012. The database stored the social security numbers, names and dates of birth of 220,000 service members. Knight and Krueger were identified after an investigation by NCIS and the Defense Criminal Investigative Service. Krueger allegedly hacked into the Navy's SWM database out of boredom. At the time of the attacks, he was a student at an Illinois community college. He studied network administration. "The Navy quickly identified the breach and tracked down the alleged culprits through their online activity, revealing an extensive computer hacking scheme committed across the country and even abroad," said Northern District of Oklahoma United States Attorney Danny C. Williams Sr. "We aggressively pursue individuals who steal personal information, especially when they victimize the men and women who bravely defend our country and our Constitution." A trial date has not been set, but the suspects face up to five years in prison. They can also be ordered to pay a fine and restitution to the victims. To read more click **HERE**

**Syrian Electronic Army Hijacks WSJ Twitter Accounts**

SoftPedia, 7 May 2014: The Syrian Electronic Army has hijacked a total of four Twitter accounts of the Wall Street Journal (WSJ) and has posted a message claiming that Ira Winker is a cockroach. The Syrian hacktivists hijacked the WSJ Africa (@wsjafrica), the WSJ Europe (@wsjeurope), the WSJ Vintage (@vsjvintage), and the WSJ.D (@wsjd) Twitter accounts, Poynter reported. They posted the message "@Irawinkler is a cockroach," along with a picture of Ira Winkler's head on the body of a cockroach. WSJ quickly became aware of the incident and removed the tweets. "We have secured our compromised Twitter accounts and they are now functioning normally," the media giant noted on Twitter a few hours ago. While it's uncertain how the hacktivists hijacked the accounts, judging by previous attacks, they either phished a WSJ employee's credentials, or they compromised a third-party service from which they were able to post messages. So why is the Syrian Electronic Army after Winkler? The hackers recently became aware of a presentation made by Winkler, the CEO of Secure Mentem, at the RSA Conference. In his presentation, the expert detailed the methods used by the hacker group and even identified some of its alleged members. He called the SEA the "cockroaches of the Internet." The hackers didn't like it, so they "defaced" the website of the RSA Conference. They haven't actually breached the RSA Conference website. Instead, they redirected the site's visitors to a defacement page after gaining access to a control panel for an analytics tool called Lucky Orange, which is used on the RSA Conference's website. "Dear Ira Winkler, Do you think that you are funny? Do you think that you are secure? You are NOT. If there is a cockroach in the internet it would be definitely you," read the message posted by the hackers on the page to which the site's visitors were redirected. The attack was carried out after the conference's organizers published a video of Winkler's presentation. Shortly after the incident, Winkler published a blog post on the Secure Mentem site to explain how the attack was carried out. He called it a "simple and basic" attack. It's unlikely that the feud between the security expert and the SEA will end any time soon. Following the latest incident, Winkler has told CNN that the Syrian hacktivists

are "imbeciles" and "more ants than cockroaches." On the other hand, the SEA says "it's not over yet." After targeting the RSA Conference website, they claimed there would be a total of three attacks. If this was the second, then there's at least one more we should expect. To read more click **HERE**

**iOS 7.1.2 with Battery and Security Fixes to Drop Soon**

SoftPedia, 7 May 2014: Although Apple isn't seeding any new iOS betas to developers, the company is hard at work patching up the latest reported bugs, including two security flaws and one potentially widespread battery drain issue that seems to be affecting even the newest generations of devices. The confirmation comes straight from the Mac maker. In responding to queries about the latest discovered security flaws, a company spokesperson said, "[Apple] is aware of the issue and [we] are working on a fix which will be delivered in a future software update." The current iOS firmware is iOS 7.1.1, so the natural way to go about it would be to release iOS 7.1.2. Given the urgency of the issue (i.e. the bad press), the firmware should drop really soon. Unless Apple decides to wait until summer / fall to unleash iOS 8, but that probably won't be the case. Even if iOS 8 comes with said patches (and it should), a lot of people will continue to stick with iOS 7, and those people need security and a decently running operating system. Plus, some will not be able to upgrade to iOS 8 because the hardware won't permit it. There's a good chance iPhone 4 and iPad 2 will be dropped out of the mix this year. The security issue Apple was responding to in the aforementioned statement is the widely reported Mail vulnerability discovered and reported by Andreas Kurtz. We did an interview with Malwarebytes to confirm that the flaw is not easily exploitable, but the company needs to take security matters serious nonetheless. However, there's another reported vulnerability in iOS 7 that Apple needs to patch. A Siri-enabled lockscreen flaw that allows a person to bypass the passcode lock has been demoed on YouTube and appears to be serious. While this one is also hard to exploit, a tinkerer with physical access to the handset can see all of the owner's contact names and numbers. Finally, there's the battery drain epidemic that, by now, has been confirmed as widespread. More and more people are reporting issues after updating to iOS 7.1 and iOS 7.1.1, and while there are some workarounds to the drainage, it has become increasingly apparent that Apple needs to jump in and offer a fix of its own. In all likelihood, iOS 7.1.2 will contain these three patches, plus some extra ones that we might not be aware of. As usual, the firmware should pack far more security patches than we're allowed to know beforehand, but that's a good thing because hackers read the news too. To read more click **HERE**

**Ruby on Rails Updated to Prevent Hackers from Stealing Files from Application Server**

SoftPedia, 7 May 2014: Ruby on Rails versions 3.2.18, 4.0.5 and 4.1.1 are available for download. The updates address a serious vulnerability so users are advised to update their installations as soon as possible. The vulnerability has been assigned the CVE identifier CVE-2014-0130 and it affects all supported versions of Ruby on Rails. It impacts the "implicit render" functionality which allows controllers to render a template even if there's no explicit action with the correspondent name. Because the module doesn't perform proper input sanitization, an attacker could use a specially crafted request to retrieve arbitrary files from the Rails application server. "In order to be vulnerable an application must specifically use globbing routes in combination with the :action parameter," reads the advisory for the security hole. "The purpose of the route globbing feature is to allow parameters to contain characters which would otherwise be regarded as separators, for example '/' and '.'. As these characters have semantic meaning within template filenames, it is highly unlikely that applications are deliberately combining these functions." While users are advised to update their installations, there's also a workaround: not using globbing matches for the ':action' parameter. To read more click **HERE**

**Phishing Alert: DSVX Virus Detect in Your Yahoo Mail Account**

SoftPedia, 6 May 2014: Yahoo Mail users are advised to be on the lookout for emails that inform them about a so-called DSVX virus. The bogus notifications are part of a phishing scheme. A sample of these emails has been submitted to millersmiles.co.uk. They carry the subject line "DSVX Virus Detect in Your Yahoo Mail Account" and they read something

like this: "We detect dsvx Virus in your Yahoo! Mail account So it's time to update, before you lose your email access. Your email service won't be affected and you'll keep all your old contacts, folders and messages." There are some pieces of malware whose name includes the string "dsvx," but in this case, the "dsvx Virus" is simply used to scare unsuspecting users into clicking on the link contained in the email. When internauts click on the link, they're taken to a Yahoo Mail phishing page. The fake login page closely replicates the legitimate one. In fact, all the links from it point to the genuine Yahoo Mail login page. However, when users enter their Yahoo! ID and their password and click the "Sign In" button, the information is transmitted to a server controlled by the cybercriminals. To avoid raising any suspicion, victims are then directed to the legitimate Yahoo Mail page hosted at mail.yahoo.com. The phishing page is hosted on an altervista.org subdomain and it has been live for at least 24 hours. The phishers can use the harvested information to hijack the victim's email account. They can also try to hijack other accounts considering that many people use the same username/password combination for multiple accounts. To read more click **HERE**

**Phishers Are Trying Out New Targets at an Alarming Rate, Study Shows**

SoftPedia, 6 May 2014: APWG's Global Phishing Survey for the second half of 2013 shows some interesting trends as far as phishing is concerned. For instance, almost half of the 681 organizations whose customers have been targeted in H2 2013 have not been targeted in H1 2013. "Phishers appear to be looking for companies that are newly popular, have vulnerable user bases, and/or are not ready to defend themselves against phishing. From the results of our latest survey, it is obvious that most any enterprise with an online presence can be a phishing target," said Greg Aaron of Illumintel, co-author of the report. Unsurprisingly, banking, e-commerce, money transfer, and social networking and email services have been the most targeted. In addition to the usual targets, the list also includes AirBNB, Hertz Rent-a-Car, Home Depot, Boise State University, Alliance Islamic Bank, the National bank of Vanuatu and several Bitcoin-related services. A total of 115,565 phishing attacks were detected in the second half of 2013. Of the 82,163 domain names used for phishing, close to 23,000 were maliciously registered. It's worth noting that in the first half of last year, only 12,000 domain names were registered by cybercriminals for phishing. Chinese cybercriminals are believed to be the cause of this increase. "Malicious domain names — meaning domain names registered by phishers directly, were at an all-time high — nearly twice any prior survey," Rod Rasmussen of IID, who has also contributed to the report, noted. Rasmussen continued, "These domains were largely registered by Chinese phishers to attack Chinese targets but were registered in several TLDs at numerous registrars around the world, making it ever more important for registrars and registries to be on the lookout for fraudulent registration attempts." A total of 210 TDLs have been used, but most of the domain names registered by cybercriminals for phishing were on .com, .tk, .pw, .net, .info, and .cf. As far as phishing attack uptime is concerned, APWG reports a considerable decrease. In fact, the company says that it has been close to a historic low. The average uptime was 28 hours and 43 minutes, but half of attacks were active for less than 8 hours. The number of attacks relying on URL shorteners has increased, but that's mainly a result of abuse at a certain provider. Close to 90% of the 999 attacks that relied on URL shortening services abused tinyURL.com. The complete Global Phishing Survey is available on APWG's website (**link**). To read more click **HERE**