# THE CYBER SHIELD

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

*24 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 22, Denver Post* – (Colorado) **A laptop containing medical information stolen from Littleton medical office.** Littleton Police reported June 21 that a password-protected laptop containing patient medical data was stolen from Colorado Neurodiagnostics. The medical business informed all patients potentially affected by the theft and updated its security measures. Source: http://www.denverpost.com/news/ci_26008800/laptop-containing-medical-information-stole-from-littleton-medical

*June 23, SC Magazine* – (International) **300,000 servers still vulnerable to Heartbleed bug.** The CEO of Errata Security reported that a scan of port 443 June 22 showed 309,197 servers that are still vulnerable to the Heartbleed vulnerability in OpenSSL due to not being patched over 2 months after the vulnerability was revealed. Source: http://www.scmagazineuk.com/300000-servers-still-vulnerable-to-heartbleed-bug/article/357206/

*June 23, IDG News Service* – (International) **Ad network compromise led to rogue page redirects on Reuters site.** Hacktivists associated with the Syrian Electronic Army redirected users who accessed certain stories on the Reuters Web sites to a Web page controlled by the group for about 1 hour June 22 by compromising an ad feed run by Taboola. Taboola stated that the attackers were able to compromise one of its widgets used on the Reuters site. Source: http://www.networkworld.com/article/2366501/ad-network-compromise-led-to-rogue-page-redirects-on-reuters-site.html

*June 23, Infosecurity Magazine* – (International) **Online daters targeted by massive phishing campaign.** Researchers at Netcraft identified a large phishing campaign targeting users of several online dating Web sites. The campaign is likely intended to takeover users' profiles for use in fraud schemes. Source: http://www.infosecurity-magazine.com/view/38975/online-daters-targeted-by-massive-phishing-campaign/

*June 20, Softpedia* – (International) **Com Spammers behind Pinterest spam attack.** A cybercriminal group known as the Com Spammers was believed to be behind a recent spam attack on Pinterest that attempts to lure users to fake diet pill Web sites. The attacks are similar to recent spam attacks on compromised Tumblr blogs. Source: http://news.softpedia.com/news/Com-Spammers-Behind-Pinterest-Spam-Attack-447769.shtml

*June 20, SC Magazine* – (International) **2012 RCE bug is still highly exploited in targeted attacks, Trend Micro finds.** Trend Micro found that a remote code execution vulnerability disclosed in April 2012 affecting Windows common controls was still the most commonly exploited vulnerability in the second half of 2013. The vulnerability was patched over 2 years ago and affects a variety of products, including Microsoft Office. Source: http://www.scmagazine.com/2012-rce-bug-is-still-highly-exploited-in-targeted-attacks-trend-micro-finds/article/357004/

*June 21, Softpedia* – (International) **Hackers access Metropolitan Companies employee information.** Metropolitan Companies, Inc., a staffing company, notified employees of several organizations under the umbrella of the company that their personal information, including Social Security numbers and financial details, may have been accessed without authorization during an April 21 security breach. The company removed access to its systems in response to the breach and hired a third party to investigate the incident. Source: http://news.softpedia.com/news/Hackers-Access-Metropolitan-Companies-Employee-Information-447818.shtml

**phpMyAdmin 4.2.4 Arrives with More Fixes**
SoftPedia, 24 Jun 2014: PhpMyAdmin, the popular tool written in PHP and intended to handle the administration of MySQL databases, is now at version 4.2.4. A new build of phpMyAdmin, 4.2.4, has been released. As the version number suggests, this is just a maintenance release in the current branch. According to the changelog, Mediawiki export is now able to produce the table header row, a fix for related PHP warnings has been implemented, new lines are no longer added to query every time, a fatal error that occurred during the SQL Export of the join query has been fixed, and the binary columns in hexadecimal notation are now working. Also, the cookie encryption IV is now generated for every session, users are now able to import open_basedir, the SQL tab – Insert queries are now showing the affected row count, a missing warning about an existing account on a multi-server config has been added, the WHERE clause can no longer remain undefined, and a few other security fixes have been implemented. A complete list of changes is available in the official changelog, which can also be found in the downloaded source archive. You can download phpMyAdmin 4.2.4 source right now from Softpedia and you will need to compile the package yourself. To read more click **HERE**

**Askmen.com Website Allegedly Compromised Through Code Injection**
SoftPedia, 24 Jun 2014: Online men's publication Askmen.com is said to be the victim of a cyber-attack, with malicious code being injected in various areas of the site in order to redirect visitors to malicious pages serving a Java exploit. The portal is dedicated to providing news for men from domains ranging from sports and health to social activity and entertainment. According to their media page, there are more than 14 million readers in U.S. alone, but the portal also has localized versions for UK, Canada, Australia and the Middle East. Security researchers at Websense, a San Diego based company providing protection against cyber-attacks, reported that they detected malicious code on the Askmen.com website, taking visitors to a web address that delivers an exploit for vulnerabilities in Java (supposedly CVE-2013-2465) and Adobe Reader. This particular vulnerability in Java affects older versions of the runtime (v7 update 21 and earlier) and "allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D." Even if version 7 of Java offers update 60, many users may not have applied the patches and could fall victim to the exploit. The injected code seems to be available at the bottom of JavaScript pages of the website and it is obfuscated with simple base64 encoding. According to Websense, the landing page with the exploit is generated automatically using a domain generation algorithm (DGA) that has been cracked by the researchers, who also revealed the pages that would be accessed until June 30. The post says that the obfuscation techniques seen on the exploit page are not original, as they have been previously encountered in the Nuclear Pack exploit kit, which is known to take advantage of said security flaw in Java. "The exploit page displays similar obfuscation techniques, which are often used in the Nuclear Pack exploit kit. In addition, the above mentioned Java exploit is most often used by Nuclear Pack. These facts strongly indicate that the attacker is using either the Nuclear Pack exploit kit or a variant of it," reads the Websense post. The threat allegedly downloaded on the victim's computer has been detected by Websense as Caphaw, a threat apparently originating from Russia and Ukraine, used for a variety of purposes, from click fraud to search result hijacking and infostealing. We reached out to Askmen requesting more details on the matter. A response came quickly from Sophie Laplante, Audience Development Manager, who said they were not aware of malware or malicious code currently affecting the portal and being delivered to the visitors. Laplante told us via email that

"WebSense never got in touch with our team, as far as we are concerned. Additionally, our developers have not detected any malware on our site." To read more click HERE

## Collinsville Police Department Hit by Ransomware Trojan

SoftPedia, 24 Jun 2014: The computer systems of the police department in Collinsville, Alabama, U.S., have been affected by a ransomware Trojan that keeps all the files captive until a sum of money is paid. The attack was conducted via phishing when an employee opened an email attachment carrying the payload. The malware spread to a total of seven computers and put important files, such as criminal mug shots or videos from crime scenes, under a lock until the ransom demand is paid. Chief Gary Bowen says that the ransom will not be paid, even if the backup system that should allow retrieving most of the encrypted data does not function properly and the department may have to start working from scratch. The department has contacted the FBI's cyber unit to investigate and, according to Assistant Chief Rex Leath, authorities may already have a suspect in custody. "I think the FBI has arrested a guy from Russia who was tied in with these people at one time. This is very inconvenient, and being hacked can come in the form of an email an attachment and you click on it and they're there," he said. Assistant professor in the Criminal Justice Department at the University of Alabama, Dr. Diana Dolliver told The Gadsden Times that police departments have become a frequent target for this type of attacks. Unless awareness is raised about phishing scams, and education is provided to spot the fake emails, police departments are susceptible to ransomware, as well as other forms of malware, because emails heading their systems can impersonate messages from other departments, like an update for a file. "I think the most important thing is training people not to open a link unless they are absolutely certain it is legitimate," said Dolliver. There is no information on the Trojan that infected the computer systems, but it immediately proceeded to encrypt the data. In a similar case, Cryptowall encrypted the data on the computers of the police department in Durham, New Hampshire. No ransom was paid to get the decryption key from the cybercriminals because a backup system was in place and allowed retrieving the affected files. However, breaching the database of a law enforcement entity has serious consequences because they work with information about criminals. Under the suspicion of unauthorized access, the details are compromised and can no longer be used in court for fear of having been tampered with. Of course, forensic analysis can determine if modifications have occurred, especially if backup files are available. To read more click HERE

## Havex RAT Aims at Industrial Control Systems

SoftPedia, 24 Jun 2014: Security researchers found that cybercriminals adopted new methods for distributing Havex, a remote access Trojan (RAT), and that their attention shifted towards industrial control systems (ICS). Havex has been previously used to compromise systems in the energetic sector, but this spring, it was observed that bad actors managed to implant trojanized versions of the software on ICS/SCADA manufacturer websites in order to infect the computers it was installed on. In monitoring the activity of the Havex malware family, F-Secure collected a total of 88 variants of the RAT, all having the capability to gain access to the targeted machines or networks, as well as to retrieve information from them. Cybercriminals used compromised websites and blogs as command and control (C&C) servers, which limited their traceability. The researchers investigated 146 servers that were contacted by the malware and the result was the discovery of about 1500 IP addresses for infected machines. Provided that the criminals deliver the RAT in software for ICS/SCADA systems, it is possible that they are now seeking control of the systems. There are multiple types of ICS, among them being supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and programmable logic controllers (PLC), all used in industrial sectors like electrical, water, gas, oil and data. "This indicates that the attackers are not just interested in compromising the networks of companies they are interested in, but are also motivated in having control of the ICS/SCADA systems in those organizations," writes Daavid Hentunen, senior researcher at F-Secure. Apart from compromising the ICS vendor to reach the victim, the payload is delivered through spam and various exploit kits. The attackers seek vulnerabilities in the software run on the website in order to replace the legitimate installation file of the ICS application. Customers download it from a trusted source and become victims as soon as it is installed. "Our research

uncovered three software vendor sites that were compromised in this manner. The software installers available on the sites were trojanized to include the Havex RAT. We suspect more similar cases exist but have not been identified yet," says Hentunen. The investigation revealed that the vendors are from Germany, Switzerland and Belgium and are involved in developing programs and appliances for different industrial usages. By running a trace of the IP addresses that contacted the command and control servers, the security firm detected some of the victims, the activity of all of them being related to the development or use of industrial applications or machines. Most of the organizations affected are based in Europe (Germany, France and Russia) and carry out technology research activities, manufacture industrial machines and applications, or specialize in structural engineering. F-Secure says that they also noticed a California-based company contacting the server and sending data. Provided all this, the evidence of cyber-espionage activity is clear. The group behind these attacks collects information about the ICS hardware connected to the compromised computer, which is a sign that they "have direct interest in controlling such environments." To read more click **HERE**

## Mock email scam ensnares hundreds of federal Justice Department bureaucrats

AP, 22 Jun 2014: Many of the Justice Department's finest legal minds are falling prey to a garden-variety Internet scam. An internal survey shows almost 2,000 staff were conned into clicking on a phony "phishing" link in their email, raising questions about the security of sensitive information. The department launched the mock scam in December as a security exercise, sending emails to 5,000 employees to test their ability to recognize cyber fraud. The emails looked like genuine communications from government or financial institutions, and contained a link to a fake website that was also made to look like the real thing. Across the globe, an estimated 156 million of these so-called "phishing" emails are sent daily, and anyone duped into clicking on the embedded web link risks transferring confidential information — such as online banking passwords — to criminals. The Justice Department's mock exercise caught 1,850 people clicking on the phony embedded links, or 37 per cent of everyone who received the emails. That's a much higher rate than for the general population, which a federal website says is only about five per cent. The exercise did not put any confidential information at risk, but the poor results raise red flags about public servants being caught by actual phishing emails. A spokeswoman says "no privacy breaches have been reported" from any real phishing scams at Justice Canada. Carole Saindon also said that two more waves of mock emails in February and April show improved results, with clicking rates falling by half. "This is an awareness campaign designed to inform and educate employees on issues surrounding cyber security to protect the integrity of the department's information systems and in turn better protect Canadians," she said in an email. "In this case, this exercise specifically dealt with the threat from phishing which is increasingly being used as an attack vehicle of choice by cyber criminals." "As this project progresses, we are pleased that the effectiveness of this campaign is showing significant improvement." A February briefing note on the exercise was obtained by The Canadian Press under the Access to Information Act. The document indicates there are more such exercises planned — in June, August and October — and that the simulations will be "graduating in levels of sophistication." Those caught by the simulation are notified by a pop-up window, giving them tips on spotting malicious messages. The federal government's Get Cyber Safe website says about 10 per cent of the 156 million phishing emails globally make it through spam filters each day. Of those, some eight million are actually opened by the recipient, but only 800,000 click on the links — or about five per cent of those who received the emails. About 10 per cent of those opening the link are fooled into providing confidential information — which represents a worldwide haul of 80,000 credit-card numbers, bank accounts, passwords and other confidential information every day. "Don't get phished!," says the federal website, "Phishing emails often look like real emails from a trusted source such as your bank or an online retailer, right down to logos and graphics." The site says more than one million Canadians have entered personal banking details on a site they don't know, based on surveys. In late 2012, Justice Canada was embroiled in a major privacy breach when one of its lawyers working at Human Resources and Skills Development Canada was involved in the loss of a USB key. The key contained unencrypted confidential information about 5,045 Canadians who had appealed disability rulings under the Canada Pension Plan, including their

medical condition and SIN numbers. The privacy commissioner is still investigating the breach. The department has some 5,000 employees, about half of them lawyers. To read more click **HERE**

**DDoS + Breach = End of Business**

GovInfoSecurity, 23 Jun 2014: In addition to taking steps to mitigate the impact of DDoS attacks, organizations need to monitor for subsequent intrusions and ensure they have multiple backups to store mission-critical data that could potentially be exposed or deleted. Defense against DDoS attacks should be considered a routine cost of doing business on the Internet, says Dan Holden, a director at Arbor Networks, a security firm. "No one is immune and the possible motivations of attackers leveraging DDoS are vast," he says. "This could range from cybercrime, geo-political disagreement or competitive takeout." Code Spaces, in a message posted to the homepage of its website, says the DDoS attack against its servers and unauthorized access into the company's cloud control panel resulted in most of its data, backups, machine configurations and offsite backups being partially or completely deleted. "Code Spaces will not be able to operate beyond this point," the company says. "The cost of resolving this issue to date and the expected cost of refunding customers who have been without the service they paid for will put Code Spaces in an irreversible position both financially and in terms of ongoing credibility." During the June 17 DDoS attack against Code Spaces' servers, an unauthorized individual gained access to the company's Amazon cloud control panel, leaving a number of messages for the company to contact the intruder using a Hotmail address. "Reaching out to the address started a chain of events that revolved around the person trying to extort a large fee in order to resolve the DDoS," the company says. As Code Spaces worked to regain control of the cloud panel by changing passwords, the intruder created multiple back-up logins. "Upon seeing us make the attempted recovery of the account, [the intruder] proceeded to randomly delete artifacts from the panel," the company says. The incident took place over a 12-hour period, Code Spaces says. The company is now working on supporting affected customers and exporting back to them any remaining data stored with Code Spaces. "All that we can say at this point is how sorry we are to both our customers and to the people who make a living at Code Spaces for the chain of events that led us here," the company says. Code Spaces did not immediately respond to a request for additional information. The attack against Code Spaces points to the need for organizations to segment their core services and have multiple backups in place. What made the incident against Code Spaces particularly devastating was the combination of a DDoS attack and an intrusion into the company's systems. "DDoS is survivable," Smith says. "For it to be a business-ending event it has to be combined with other attacks. The direct cause was the hacking attack against their administration panel and the unavailability of their service because the attackers deleted storage groups and backups which were located in the same place with the same administrative access." To read more click **HERE**