# THE CYBER SHIELD

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

*30 September 2014*




*September 26, Softpedia* – (International) **Dyre banking trojan delivered via voice message email notification.** Researchers discovered that the Dyre (Dyreza) banking trojan is being employed via phishing emails claiming to be from financial institutions and bogus emails purporting to inform of a new voicemail message which include a link to a malware dropper that has five Romanian Portable Executable (PE) resources and downloads a variant of the trojan. The malware relies on the man in the middle (MitM) technique to take over the connection between the client and the server. Source: http://news.softpedia.com/news/Dyre-Banking-Trojan-Delivered-Via-Voice-Message-Email-Notification-460162.shtml

*September 29, Birmingham Business Journal* – (Georgia) **American Family Care alerts customers of stolen laptops containing patient information.** Birmingham, Alabama-based American Family Care announced that two laptops containing the personal and health information of an undisclosed amount of patients were stolen from an employee's vehicle in Marietta, Georgia, during the summer. Source: http://www.bizjournals.com/birmingham/morning_call/2014/09/american-family-care-alerts-customers-of-stolen.html

*September 29, Softpedia* – (International) **New remote code execution flaws found in Shellshock-patched Bash.** Researchers found four additional vulnerabilities with the Bash command interpreter for Linux, Shellshock, two of which were unofficially patched after new changes to the code. The two new bugs that remain could be exploited remotely and in an easier way due to the rare use of address space layout randomization (ASLR) when compiling Bash. Source: http://news.softpedia.com/news/New-Remote-Code-Execution-Flaws-Found-In-Shellshock-Patched-Bash-460348.shtml

*September 29, Softpedia* – (International) **Cisco lists 31 products vulnerable to the Shellshock vulnerability.** Cisco released a list of 31 products vulnerable to the Shellshock glitch which included connection routing, network management, and media content delivery and encoding, among others. Oracle also released a list of 32 products vulnerable to attack by the Bash bug after the company changed its initial list and appended new products. Source: http://news.softpedia.com/news/Cisco-Lists-31-Products-Vulnerable-To-the-Shellshock-Vulnerability-460303.shtml

*September 26, SC Magazine* – (International) **iThemes users asked to change passwords following attack.** The CEO if iThemes, a WordPress themes, plugins, and training provider, advised 60,000 past and current users to reset their passwords following an attack on its membership database that may have compromised usernames, email addresses, passwords, names, IP addresses, and purchase information. Source: http://www.scmagazine.com/ithemes-users-asked-to-change-passwords-following-attack/article/373939/

*September 26, IDG News Service* – (International) **Credit card breach that hit Jimmy John's is larger than originally thought.** Signature Systems reported September 26 that the breach of its point-of-sales system that affected 216 Jimmy John's sandwich shop locations also may have compromised the systems an additional 108 independent restaurants across the U.S. that use its payment products. The intrusion is believed to have started June 16 when hackers used

stolen credentials to remotely install malware onto stores' payment terminals that is capable of stealing customers' payment card information. Source: http://www.networkworld.com/article/2688453/security/credit-card-breach-that-hit-jimmy-johns-is-larger-than-originally-thought.html

## Supervalu Suffers New Payment Data Breach

Softpedia, 29 Sep 2014: A little over a month after announcing a compromise of its systems processing card information, Supervalu comes out with a new data breach disclosure, saying that some of its Shop 'n Save, Shoppers Food & Pharmacy and Cub Foods owned and franchised stores have been affected. On August 15, Supervalu revealed that the payment systems at 180 of its locations had been compromised since June 22 through July 17, sensitive information being exposed, such as account numbers, expiration date and/or cardholder's name. The recent cyber-attack is believed to have started in late August or early September. The company says that a different malware has been used than in the previous incident; no evidence has been found of a connection between the two incidents. "Upon recognition of this intrusion, the Company took immediate steps to secure the affected part of its network and believes it has eradicated the malware. An investigation of this recently discovered incident is underway," a statement from Supervalu Inc. informs. The security measures implemented after the previous attack appear to have paid off, since the company believes that the technology limited the malware's ability to collect information from payment cards. In fact, until the investigation is complete, there are no details to point to the fact that any card details have been collected in any of the affected stores, other than those at some checkout lanes at four Cub Foods franchised stores. Farm Fresh or Hornbacher's stores along with the Save-A-Lot locations also seem to be safe from the attack. The authorities have been informed of the cybercriminal attempt and an investigation has been started into the matter, with full cooperation from the company. President and CEO Sam Duncan said that although a round of security upgrades has been added to the Supervalu systems in the wake of the previous attack, the company will not stop investing in enhanced protective technology. Four franchised Cub Foods stores in Hastings, Shakopee, Roseville (Har Mar) and White Bear Lake, Minnesota, were affected by the incident because they did not benefit from the upgrades implemented after the previous breach. Data exposed at these locations consists of account numbers, as well as the expiration date in some cases. Other numerical information and/or the cardholder's name have also been put at risk. August 27 is given as the earliest start date for the intrusion, which lasted all through September 21, at the latest. To read more click **HERE**

## New Average for Shellshock Attacks: Over 1,970 Incidents Every Hour

Softpedia, 30 Sep 2014: Since Wednesday, September 24, when the original Shellshock vulnerability for the Bash command-line interpreter was disclosed to the public, the attack rate has increased to more than 1,970 events per hour, telemetry data from a security company reveals. Incapsula announced last week that since the bug became known to the public, in a 24-hour period, from Thursday until Friday, an average of about 725 attacks were recorded each hour, amounting to a total of more than 17,400 incidents for the entire monitored period. In an update issued this week, the company informs that incidents involving Shellshock have increased significantly, the information being extracted from their systems in a four-day period after the disclosure of the initial vulnerabilities assigned the CVE-2014-6271 and CVE-2014-7169 identifiers. The company says that their web application firewall managed to fend off more than 217,089 exploit attempts that involved over 4,115 domains. From Sunday to Monday, Incapsula observed increased attack rates, "transitioning from short high-volume bursts into a steady stream of malicious requests." Malicious actors relied on different tools to conduct their attacks, from scanners used to test targeted systems for the presence of the vulnerability to DDoS (distributed denial-of-service) kits designed for injecting servers with malware. A graph with the distribution of attack attempts shows that scanners were employed in 68.27% of the cases. Ofer Gayer of Incapsula says that only 6% of them "are likely to be used by website operators to identify the issue," while most have been used for probing in view of a subsequent attack. In 18.37% of the cases, attackers attempted to achieve remote shell access to compromise the servers and gain control over them. A third major attack scenario

involved DDoS malware that would add the target to a botnet used for bombarding services in order to disrupt them. According to the company, Shellshock attacks originated from more than 890 IP addresses from almost every country on the globe. However, most of them (19.46%) were initiated from the United States, followed by China, accounting for 10.20% of the incidents. Even if the point of origin of the events is located in these countries, this does not mean that the cybercriminals are also residing there; they could be anywhere on the planet. Shellshock has received the maximum points when it comes to severity, based on the Common Vulnerability Scoring System (CVSS). It is extremely easy to exploit and it consists in assigning malicious code to a variable function run in Bash, which is executed by the shell. To read more click **HERE**

### Linux No Longer Listed as Supported Platform for Adobe Reader

Softpedia, 29 Sep 2014: Adobe Reader is no longer an item of interest for the Linux users, and the company that makes it has removed the Linux platform from the list of supported OSes. All the Adobe products are slowly disappearing from the Linux ecosystem. Adobe Air is no more, Adobe Flash is now in maintenance mode and it hasn't been updated for a couple of years, and now Adobe Reader no longer lists Linux as supported platform. To be fair, it was an old version and not a lot of people used it. Life will be the same for Linux users without Adobe Reader. There are still lots of applications that provide support, like Evince, Okular, Foxit, and qpdfview, just to name a few. And we're not even mentioning Mozilla Firefox and Google Chrome, which are able to open PDF file by default. The reason for Adobe's estrangement with the Linux world is unclear. They stopped being interested in this platform a while ago, although other OSes (like iOS for example) are doing the same thing with them. It's very likely that all Linux support will stop very soon. To read more click **HERE**

### Apple patches Shellshock bug in OS X

Heise Security, 30 Sep 2014: Apple has finally released a security update for OS X that will close up the critical remote code execution Shellshock bug found in the GNU Bash UNIX shell. The update resolves both the CVE-2014-6271 issue discovered by Stephane Chazelas, as well as the CVE-2014-7169 one flagged by Tavis Ormandy. Security updates have been provided for OS X Mavericks, Mountain Lion, and Lion users. According to Ars Technica, the patch will not be provided for current OS X Yosemite developer or public beta builds, but will be built into the next ones. If you're in a hurry to patch your system, you'll have to download the update and implement it manually, as they haven't yet been made available to implement via the usual Software Update process (this will probably change soon). Once the update has been performed, you can make sure that it was successful by opening the Terminal app and execute the following command: bash -version. The information returned should be GNU bash, version 3.2.53(1)-release (x86_64-apple-darwin13) if you run OS X Mavericks. The number in the last string should be darwin12 or darwin11, depending on whether you run Mountain Lion or Lion. While the company was working on the update, a spokesperson pointed out that the vast majority of OS X users are not at risk. To read more click **HERE**

### People will do anything for free Wi-Fi

Heise Security, 30 Sep 2014: A new Wi-Fi investigation conducted on the streets of London shows that consumers carelessly use public Wi-Fi without regard for their personal privacy. In the experiment, which involved setting up a 'poisoned' Wi-Fi hotspot, unsuspecting users exposed their Internet traffic, their personal data, the contents of their email, and even agreed to an outrageous clause obligating them to give up their firstborn child in exchange for Wi-Fi use. The independent investigation, supported by Europol, was carried out on behalf of F-Secure by the UK's Cyber Security Research Institute and SySS, a German penetration testing company. For the exercise, SySS built a portable Wi-Fi access point from components costing around 200 euros and requiring little technical know-how. Researchers set the device up in prominent business and political districts of London. They then watched as people connected, unaware their Internet activity was being spied on. In a thirty minute period, 250 devices connected to the hotspot, most of them probably automatically without their owner realizing it. 33 people actively sent

Internet traffic by carrying out web searches and sending data and email. 32 MB of traffic were captured (and promptly destroyed in the interest of consumer privacy). In a surprising finding that underscores the need for encryption, the researchers found that the text of emails sent over a POP3 network could be read, as could the addresses of the sender and recipient, and even the password of the sender. For a short period, the researchers introduced a Terms & Conditions (T&C) page that needed to be accepted in order to use the hotspot. The T&C included an outlandish clause that obligated the user to give up their firstborn child or most beloved pet in exchange for Wi-Fi use. In total, six people agreed to the T&C before the page was disabled. The clause illustrated the lack of attention people typically pay to T&C pages, which are often too long to read and difficult to understand. "We all love to use free Wi-Fi to save on data or roaming charges," says Sean Sullivan, Security Advisor at F-Secure, who participated in the experiment. "But as our exercise shows, it's far too easy for anyone to set up a hotspot, give it a credible-looking name, and spy on users' Internet activity." When it comes to hotspots provided by a legitimate source, even those aren't safe, he says. Even if they aren't in charge of the hotspot, criminals can still use 'sniffer' tools to snoop on what others are doing. "The issue of Wi-Fi security is one that we at the European Cybercrime Centre (EC3) at Europol are very concerned about," says Troels Oerting, Head of Europol's EC3. "We wholeheartedly support activities which shine light on this everyday risk consumers face." The solution? Either stay away from public Wi-Fi – or use Wi-Fi security. With Wi-Fi security, your connection is invisible in the Wi-Fi network and your data made unreadable by encryption. So even if someone tries, they can't tap into your data. To read more click **HERE**

## Bitcoin Miner Malware Hidden in Free Game Downloads

Inside Bitcoins, 24 Sep 2014: That free game download you just scored could be hiding a secret bitcoin miner on your computer, invisibly robbing your system of resources while it drains computing power to make money – for someone else. Microsoft recently revealed the scam on its malware support site. "This type of system hijacking is just one of the many ways to exploit a user by utilizing their system's computing resources to earn more cash," writes Donna Sibangan of the Microsoft Malware Protection Center, in a blog post. "Malware is easily bundled with game installers that are then uploaded and shared with unsuspecting users using torrent download sites. Once a machine is infected, a downloaded Bitcoin miner silently carries out mining operations without the user's consent." Some of the game downloads infected with the malware include:

- Tom Clancy's Ghost Recon.Future Soldier.Deluxe Edition.v 1.7 + 3 DLC.(Новый Диск).(2012).Repack
- Don't Starve.(2013) [Decepticon] RePack
- Kings Bounty Dark Side by xatab
- Sniper_Elite_III_8_DLC_RePack_MAXAGENT
- TROPICO_5
- Ghost_Recon_Future_Soldier_v1.8_Repack
- Trials.Fusion.RePack.R.G.Freedom
- King's Bounty Dark Side.(2014) [Decepticon] RePack
- Watch Dogs.(2014) [Decepticon] RePack

"These files can be easily acquired by anyone who downloads games from a torrent website," Sibangan added. "The games are repacked to further lure gamers to download the compressed files for free. The installer that we detect as TrojanDropper:Win32/Maener.A is available in Russian and English languages only. It seems to be primarily affecting Russian users, as shown by its infection telemetry. When the installer application (setup.exe) is run, Trojan:Win32/Maener.A also executes in the background and downloads its Bitcoin mining components." To read more click **HERE**

## College Campuses Get an "F" In Cybersecurity

Security Watch, 23 Sep 2014: Ah, it's that time of year again on college campuses. Freshmen hurry to find their way around and seniors bask in their last year of glory. Colleges not only offer a wealth of knowledge, but also house a treasure trove of highly sensitive information. Combined with an open network and a Bring Your Own Device (BYOD) culture, cyberattackers consider colleges a prime target. This obviously isn't very welcoming news for campuses and their inhabitants. In order to assess the cyber security performance of American higher education institutions, BitSight Technologies conducted a study on the most recognized collegiate athletic conferences: the SEC, ACC, Pac-12, Big 10, Big 12, and Ivy League. These schools represent a student popular of over 2.25 million and network footprint of more than 11 million IP addresses. BitSight Technology used external data that involved identifying the type of malware infections that struck the schools to rate the groups of universities' performances on a scale from 250 to 900. The Big 12 had the best security rating with 661 while ACC performed the worst at 588. Overall, however, colleges and universities seem to fail to adequately address security challenges. BitSight notes that the security rating of the education sector as a whole is alarmingly lower than retail and healthcare, two industries that have suffered recent serious data breaches. The schools that did demonstrate a higher performance rating have a dedicated CISO or Director of Information Security on staff, which is crucial for better security on campus. As the school year progresses from September through May, security performance dips drastically due to the increase of students and devices on campus. These institutions also experience high levels of malware infections, including the Flashback malware that targets Macs, as well as adware and Conficker. Universities are forced to deal with several factors simultaneously comprising a high volume of open network access points, diverse technology needs, multiple compliance and regulatory measures, and protection of sensitive data that includes both intellectual and personal property. With so many issues to worry about, security teams at schools struggle to adequately protect all of the institutions' information. Just because schools are compliant with a number of federal regulations, this doesn't mean they're any more secure. Reports from Educause point out that there have been 551 security breaches from 2005 through 2013, which means there's about a breach per week. Schools shouldn't overlook the importance of cybersecurity; poor practices can have severe financial and reputational impacts. Despite the worrying amount of data breaches, few schools have strategic cyber plans in place or formal risk programs to assess and remedy cyber threats. Schools' security teams should constantly monitor technologies that alert them of malicious activity on the network before serious damage is done. Improved communication between these institutions about current malware threats could help mitigate attacks. To better understand their schools' needs, security teams should track and compare security changes and performance. This would allow for them to use their existing resources and advocate for better ones. Colleges and universities aren't the only ones who should be making adjustments to protect their network. Students, professors, and anyone else on campus, should make sure their devices have antivirus software. On an individual level, users should also employ password managers to generate and store hard-to-crack passcodes to protect data across different sites and networks. Improving the security of campuses is an ongoing group project between the schools and their residents; both need to pull their weight. To read more click **HERE**

## Military, Contractors Construe Breach Reporting Rules Differently

GovInfoSecurity, 24 Sep 2014: What's as disturbing as the news of the Chinese hacking U.S. defense contractors' systems, revealed in a new Senate report, is that the contractors failed to notify the military of most of those intrusions. Why so? The military and contractors don't interpret contract provisions dealing with breaches the same way. Most of the publicity arising from the release of the Senate Armed Services Committee report focused on the Chinese hacking critical systems - so, what else is new? But a big takeaway from the study, Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors, is the failure of military contractors to share cyberthreat information with the Transportation Command, known as Transcom, a unified combatant command that provides transportation and logistics services to the U.S. military. Information sharing is a hot topic these days, but what good is information sharing if parties can't agree on what information is to be shared? Sometimes, it seems that the

contractors and government don't speak the same language, interpreting specific provisions in contracts differently. "The contract language is ambiguous and none of the contractors with whom the committee discussed the clause interpreted their reporting obligation in a manner consistent with Transcom's intent," the report says. Here's how Senate investigators determined the confusion occurred: Transcom required its contractors to report intrusions that "affect DoD information." To Transcom, that means contractors must report any intrusion that allows access to a system on which DoD information resides or is in transit. But none of the contractors the committee investigators interviewed interpreted the clause that way. One contractor, a civilian airline that ferries troops and equipment during a crisis, told investigators that it interpreted the clause to require reporting of intrusions of their systems only if those attacks affected DoD data, for example, through data exfiltration or corruption. Another civilian airline said it interpreted the clause to mean intrusions that only affected nonpublic DoD information. "Setting aside the lack of common understanding between the command and its contractors about the cyber-incident reporting clause, Transcom's own view that reportable intrusions are limited to those that affect systems on which DoD information resides or transit leaves a critical gap," the report says. Senate Armed Service Committee Chairman Carl Levin, D-Mich., says military divisions must improve the way they communicate cyber-vulnerabilities with other government agencies, including the FBI, as well as with their contractors. "Our findings are a warning that we must do much more to protect strategically significant systems from attack and to share information about intrusions when they do occur," he says. The panel blamed the lack of contractor cyber-incident reporting on common misunderstandings between contractors and Transcom about the scope of cyber-intrusions that must be reported. Transcom's obliviousness to some intrusions was due to confusion about the rules governing how cyber-related information may be shared and a lack of common understanding between the command and other DoD components about what cyber-information Transcom needs to know. "It is essential that we put into place a central clearinghouse that makes it easy for critical contractors, particular those that are small businesses, to report suspicious cyber activity without adding a burden to their mission support operations," says Sen. Inhofe, R-Okla., the committee's ranking member. Committee investigators spent a year, ending in March, investigating the breaches and discovered that in a 12-month period beginning June 1, 2012, there were about 50 intrusions or other cyber-events into the computer networks of Transcom contractors. Investigators attributed at least 20 of those successful intrusions to an advanced persistent threat. Investigators attributed the 20 APT intrusions to China. Among the investigation's findings was evidence of:

- A Chinese military intrusion into a Transcom contractor between 2008 and 2010 that compromised e-mails, documents, user passwords and computer code.
- A 2010 intrusion by the Chinese military into the network of a air-carrier contractor in which documents, flight details, credentials and passwords for encrypted e-mail were stolen.
- A 2012 Chinese military intrusion into multiple systems onboard a commercial ship contracted by Transcom.

Investigators found significant gaps in sharing cyber-intrusion information, according to the committee report. For example, while the the FBI or DoD were aware of at least nine successful intrusions by China into Transcom contractors, Transcom was made aware of only two of them. The senators inserted a provision in the bill that funds Defense Department operations, the National Defense Authorization Act for Fiscal Year 2015, that directs the DoD to improve the way the department disseminates information about cyber-intrusions into the computer network of operationally critical contractors. Committee leaders hope that the proviso in the measure now before the full Senate will help resolve the communications gap that exists between agencies such as Transcom and military contractors. To read more click **HERE**