The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

14 - 15 January 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

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, Sandia 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 open source data

January 13, Softpedia – (National) **Target CEO confirms hackers installed malware on POS registers.** The CEO of Target confirmed that the cause of a recent breach of customers' payment card information was malware installed by criminals on point of sale (POS) devices at various Target stores. Source: http://news.softpedia.com/news/Target-CEO-Confirms-Hackers-Installed-Malware-on-POS-Registers-416146.shtml

January 13, The Register – (National) **Hackers slurp credit card details from US luxury retailer Neiman Marcus.** Department store Neiman Marcus confirmed that attackers breached its systems and obtained an undisclosed amount of payment card information. The company was alerted in December 2013 to unauthorized card activity and is continuing to investigate the breach. Source: http://www.theregister.co.uk/2014/01/13/neiman_marcus_credit_card_breach/

January 13, The Register – (International) **Microsoft Twitter accounts, blog hijacked by SEA.** Attackers claiming affiliation with the Syrian Electronic Army hacktivist group compromised two Twitter accounts and an official blog belonging to Microsoft between January 11-12. Source: http://www.theregister.co.uk/2014/01/13/microsoft_twitter_blog_sea_compromised/

January 13, Softpedia – (International) **Man admits hijacking YouTube channels, hacking AOL CEO's email account.** A Maryland man admitted to working with an accomplice to abuse password reset functions in YouTube, add advertisements to YouTube Channels, and make around $56,000 from the hijacked accounts. The two men also set up email accounts likely to be used as nonsense addresses at account creation and were able to breach the accounts of several AOL employees, including the company's CEO. Source: http://news.softpedia.com/news/Man-Admits-Hijacking-YouTube-Channels-Hacking-AOL-CEO-s-Email-Account-416356.shtml

January 14, Threatpost – (International) **Java version of Icefog espionage campaign hit 3 US oil, gas companies.** Kaspersky Lab researchers found that the Icefog cyberespionage campaign that targeted defense and technology companies in Japan and South Korea and that was revealed in September 2013 also compromised the systems of three U.S. oil and gas companies using a Java version of the campaign. The companies were notified of the infection and two had removed the malware from their systems by January 14. Source: http://threatpost.com/java-version-of-icefog-espionage-campaign-hit-3-us-oil-gas-companies/103567

January 13, Washington Post – (National) **Target says customers signing up for free credit monitoring after data breach.** Target announced January 13 that it is offering a year of free credit monitoring for customers following a breach of its systems that potentially exposed at least 100 million customers' personal or payment information. Source: http://www.washingtonpost.com/business/technology/target-says-customers-signing-up-for-free-credit-monitoring-after-data-breach/2014/01/13/99fcce60-7c83-11e3-95c6-0a7aa80874bc_story.html

January 14, WRC 4 Washington, D.C. – (Virginia) **Fairfax County school employee accused of refurbishing, selling stolen laptops.** Police arrested a Fairfax County Public Schools employee January 13 and charged him with two counts of embezzlement after they found 1,200 computers and 156 hard drives belonging to the school district, in his home. The employee is accused of taking used laptops, refurbishing them, and selling them online. Source: http://www.nbcwashington.com/news/local/Craig-Soderberg-Fairfax-County-School-Employee-Charged-with-Embezzlement--239990251.html

January 13, KCPQ 13 Tacoma – (Washington) **NORCOM investigating data breach of emergency calls.** The North East King County Regional Public Safety Communication Agency is investigating after its server was compromised and the medical response records of an estimated 6,000 individuals across 3 counties were potentially accessed, including 231 current and former firefighters. The agency was notified of the breach in December 2013 and the server is no longer in service. Source: http://q13fox.com/2014/01/13/norcom-investigating-data-breach-of-emergency-calls/

January 14, The Register – (International) **Vulnerability leaves Cisco small biz routers wide open to attack.** Cisco issued a security advisory January 10 warning that some of its routers and networking products contain a vulnerability that could allow attackers to gain root access via an undocumented test interface. Exploit code for the vulnerability is available, though Cisco reported that they did not observe any widespread attacks based on it. Source: http://www.theregister.co.uk/2014/01/14/cisco_small_business_router_flaw/

January 14, Softpedia – (International) **Mt. Gox fixes vulnerability that might have been exploited to hijack accounts.** A security researcher identified and reported several vulnerabilities in Bitcoin exchange Mt. Gox that could be used to hijack user accounts. Mt. Gox closed the vulnerabilities January 14. Source: http://news.softpedia.com/news/MtGox-Fixes-Vulnerability-That-Might-Have-Been-Exploited-to-Hijack-Accounts-416655.shtml

January 13, CNET News – (International) **Syrian Electronic Army hacks into Xbox Twitter accounts too.** Attackers claiming affiliation with the Syrian Electronic Army hacktivist group took control of the Twitter and Instagram accounts of Microsoft's Xbox gaming console January 11 and posted defacement messages. Microsoft regained control of the accounts later the same day. Source: http://news.cnet.com/8301-1009_3-57617174-83/syrian-electronic-army-hacks-into-xbox-twitter-accounts-too/

U.S. senators ask Target CEO for information on data breach

Reuters, 14 Jan 2014 - Two U.S. senators were seeking answers on Tuesday from the chief executive of Target Corp about the company's response to the hacking of credit and debit cards of millions of its customers during the holiday shopping season. "We ask that Target's information-security officials provide a briefing to committee staff regarding your company's investigation and latest findings," said John Rockefeller, chairman of the Senate Commerce Committee, and Claire McCaskill, who heads a Commerce subcommittee on consumer protection. The Democratic senators' Jan. 10 letter to Target CEO Gregg Steinhafel was released on Tuesday, the latest in a growing chorus of calls by lawmakers and others for inquiries into the hacking of the No. 3 U.S. retailer. "We have received the chairmen's letter and are continuing to work with them and other elected officials to keep them informed and updated as our investigation continues," Target spokeswoman Molly Snyder said in an email to Reuters. Shortly afterwards, the top Democrat on the House Oversight and Government Reform Committee sought a hearing on the theft of about 40 million credit and debit card records and 70 million other records containing customer information. Representative Elijah Cummings said the committee's focus since October has been investigating the security of the federal government's health insurance

website, HealthCare.gov, which has not been breached. He urged the committee chairman, Republican Darrell Issa, who made a fortune as head of a company that makes car alarms and other automotive security devices, to turn his attention to Target. "In addition to serving the interests of millions of American consumers affected by this breach, I believe the committee could learn from these witnesses about their failures, successes and best practices in order to better secure our federal information technology systems," Cummings wrote. An aide to Issa told Reuters the committee was likely to "do some follow up" on the Target issue. Target disclosed on Dec. 19 that it was a victim of one of the biggest credit card breaches on record, which it said lasted for 19 days in the busy holiday shopping season through Dec. 15. The company on Monday apologized for the breach. "It has been three weeks since the data breach was discovered, and new information continues to come out," Rockefeller and McCaskill wrote. "We expect that your security experts have had time to fully examine the cause and impact of the breach and will be able to provide the Committee with detailed information." The Target hacking shows the need for federal legislation on commercial data practices, the senators said. Democratic lawmakers sought a congressional hearing on Monday from the Financial Services Committee. Its Republican chairman, Jeb Hensarling, said his panel will continue to hold hearings on the security of financial information and on how to protect personal consumer information. "Americans have a right to expect that the personal information they turn over to private companies and government agencies will be protected and kept secure from loss, unauthorized access or misuse," Hensarling said in a statement. Separately, an official with the House Energy and Commerce committee's majority Republicans said that one of its subcommittees has held numerous hearings on data breaches and that it was monitoring the Target situation but has taken no specific action. The National Association of Federal Credit Unions sent letters on Monday to congressional leaders, demanding action on data security. To read more click **HERE**

Twitter Lets Advertisers Target Users by ID or Email Address

SoftPedia, 15 Jan 2014: Twitter made a few changes to its platform and now enables advertisers to find users via their Twitter IDs or email addresses. This means that you might start receiving promoted tweets on Twitter or tailored messages depending on your interests. Twitter made the announcement regarding the new changes to its "tailored audience" over its Advertising Blog. It took the company six months to test out the feature, so I'm going to assume that they studied the issue on all sides. As always, user privacy is a concern for Twitter, which means that anyone can opt out of becoming a target of advertisers through this new product. "While we want to make our ads more useful through tailored audiences, we also want to provide simple and meaningful privacy choices to our users. Twitter users can simply uncheck the box in their privacy settings next to 'Tailor ads based on information shared by ads partners,' and Twitter will not match their accounts to information from our ads partners for tailored audiences. We also have a minimum audience size for all tailored audiences to avoid overly specific targeting," the company wrote in the announcement. To read more click **HERE**

Google Chrome Extension Hijacks Searches, Gets Pulled from Store

SoftPedia, 15 Jan 2014: When it comes to browsing the Internet, the security level of your browser is particularly important and one simple extension can work against this. One example for this is a scandal that broke out several weeks ago and which ended in an extension being removed from the Google Store. Called Window Resizer, the extension hijacked people's searches to earn money for a third-party search engine. It would reroute links from Google and send them to a third-party search engine called Ecosia, which is apparently trying to save the rainforest. Basically, instead of the regular Google search, users would momentarily be pushed to Ecosia, which would, in turn, boost traffic on the site and generate ad revenue. Developers must abide by Google's policies, since the extensions don't run within Chrome, but this time around, that doesn't seem to have been the case as the company decided to remove Window Minimizer from the Store. The situation was discovered after a user tattled on the app, saying it was inserting links into the search results. He believed that while this was supposed to be a window resizing extension, it acted as a keylogger. The developer quickly fought back and had a rather harsh tone to his replies. After going back and forth with other

forum users, he eventually announced that he removed the allegedly malicious EcoLinks and sent the extension back for review. To read more click **HERE**

Target POS Systems Vulnerable to Cyberattacks Since 2007

SoftPedia, 15 Jan 2014 Several lawsuits have already been filed against Target following the massive data breach suffered by the retailer last year. However, the class action filed by law firm Hagens Berman Sobol Shapiro LLP is among the most interesting. Target has recently admitted that cybercriminals obtained the details of up to 110 million customers after installing malware on point-of-sale (POS) registers. The Hagens Berman lawsuit claims that Target was notified of vulnerabilities in its POS systems in 2007, but the company failed to do anything about the security issues. The suit references a white paper in which security expert Dr. Neal Krawetz detailed POS vulnerabilities at major retailers. The research named Target as an example. The paper estimated that the vulnerabilities in Target's POS systems exposed 58 million consumers. Krawetz sent the developer responsible for Targets POS systems a copy of the paper, which included suggestions on how to address the issues. The developer admitted that the recommendations were "good ideas" and requested permission to forward the study to other Target employees. Since the retailer failed to apply the security measures proposed in the research paper, its systems remained vulnerable. "We believe that Target not only knew its systems were vulnerable to exactly this kind of attack all the way back in 2007, but was alerted to and acknowledged suggestions that would have made its customers safer," noted Tom Loeser, a Hagens Berman partner. "However, Target did not act on this knowledge, and as a result, tens of millions have had their personal information stolen and financial accounts compromised." The lawsuit also blames Target for several other things. The retailer is accused of acting in its own interest, instead of looking out for impacted customers. The company did not immediately offer credit and identity theft protection services. To read more click **HERE**

North Korean Hackers Reportedly Targeting South Entities Tied to National Security

SoftPedia, 15 Jan 2014: South Korea's Ministry of Science, ICT and Future Planning says that North Korean hackers have been trying to breach the systems of small and mid-size IT companies and institutions that are directly linked to the country's national security. According to the Korea Joongang Daily, some of the companies have been breached because of the lack of proper security systems. The ministry has revealed that the attackers are sending out phishing emails purporting to come from Ministry of Unification officials, or members of an academic society that studies North Korea. In December, such emails were sent to 159 individuals, many of whom connected to free trade agreements and national security. In January 2014, 30 such attempts were identified. In one spam campaign, North Korea is said to have attempted to distribute malware. The malicious emails are disguised as survey requests or invitations to an event. To read more click **HERE**

Syrian Electronic Army's Website Hacked through Hosting Provider

SoftPedia, 15 Jan 2014: The website of the Syrian Electronic Army (sea.sy) and the leaks subdomain (leaks.sea.sy) have been defaced by Turkish hackers of the group Turkguvenligi. The attackers have apparently compromised the SEA's website through its hosting provider. The attack appears to come in response to the Syrian Electronic Army's attacks against Turkey. "You imbecils will attack our country with fake phishing emails and we'll accept your lies and dont do anything ? That is the end you deserve: 'And never think that Allah is unaware of what the wrongdoers do. He only delays them for a Day when eyes will stare [in horror]'," Turkguvenligi wrote on the defaced page. "The hosting company that hosts #SEA websites, including (http://leaks.sea.sy) was attacked," the Syrian Electronic Army's representatives stated. "Since the #SEA servers is managed by the hosting company, they down the servers quickly to make sure that will not happen again." The hacktivist group says such attacks don't affect their "hacks and operations." Turkguvenligi says it hacked the systems of the Russian hosting company by exploiting "many kind of web vulnerabilities." They claim to have breached the organization's systems in just 2 days. However, the Syrian Electronic Army says it actually took the Turkish hackers over 7 months to do it. "We hoped that Turkguvenligi is really

sophisticated, but when we found out the method of their hacks, we were really disappointed," the Syrian Electronic Army noted. The Turkish hackers also said they obtained the "real IDs" of the Syrian group's members. However, the SEA says they haven't put their real IDs on public websites. Judging by the last messages posted on Twitter by each group, we'll probably see more confrontations between the SEA and Turkguvenligi. To read more click **HERE**

Oracle Fixes 144 Vulnerabilities, Including 36 Java Flaws, with January 2014 CPU

SoftPedia, 15 Jan 2014: Oracle has released its Critical Patch Update (CPU) for January 2014. The latest CPU fixes a total of 144 vulnerabilities, many of which can be exploited remotely. Products such as MySQL Enterprise Monitor and Server, Database, Fusion Middleware, Enterprise Data Quality, Forms and Reports, Portal, Outside in Technology, GlassFish Server, HTTP Server, iPlanet, Reports Developer, VM VirtualBox, Siebel, Solaris, Identity Manager, Internet Directory, and E-Business Suite are impacted. The January 2014 CPU also addresses a total of 36 vulnerabilities affecting Java SE components, such as Java SE, Java SE Embedded, JavaFX and JRockit. 34 of the security holes can be exploited remotely without authentication. A large number of security researchers have been credited for finding the flaws fixed with the latest CPU. The list includes Adam Willard of Foreground Security, Arseniy Akuney of TELUS Security Labs, Borked of the Google Security Team, Christopher Meyer of Ruhr-University Bochum, Fernando Muñoz, Joseph Sheridan of Reactionis, Matthew Daley, Oliver Gruskovnjak of Portcullis, Tanel Poder, Will Dormann of CERT/CC, and Yuki Chen of Trend Micro. Users are advised to apply the patches as soon as possible. Oracle's next CPU is scheduled for April 15, 2014. To read more click **HERE**

Adobe Flash Player 12 Addresses Critical Vulnerabilities

SoftPedia, 15 Jan 2014: Apart from overall improvements and new features, the latest revision for Adobe Flash Player 12 also brings to the table a couple of security fixes that have been marked with the highest priority rating, as they cover critical vulnerabilities. Identified as CVE-2014-0491 and CVE-2014-0492 in Adobe's latest security bulletin (APSB14-02), the two vulnerabilities could allow an attacker to take control of the affected system by running malicious native code. The first flaw could be leveraged to bypass Flash Player security protection mechanisms. The second one refers to an address leak vulnerability that could allow an attacker to defeat memory address layout randomization. For Google Chrome (Flash 12.0.0.41) and Internet Explorer (Flash 12.0.0.38), the latest version of Adobe Flash Player is automatically delivered through the update mechanisms available for the web browsers; this means that Chrome receives the update with a new version of the browser, while for IE it is provided by Microsoft through the Windows automatic update feature. On Windows, the current desktop update increments the build number of Adobe Flash Player to 12.0.0.43, which extends to all NPAPI plugin-based browsers. The desktop version for Mac is 12.0.0.38. Linux users will update to build 11.2.202.335. To read more click **HERE**

Adobe Reader and Acrobat 11.0.06 Hold Critical Security Improvements

SoftPedia, 15 Jan 2014: The latest update for Adobe Reader and Acrobat includes repairs for three security glitches that would permit crashing the application and allow a potential attacker to gain control over the affected system. Previous versions of the applications are susceptible to security breaches by taking advantage of memory corruption vulnerabilities (CVE-2014-0493 and CVE-2014-0495) that could lead to code execution. A third security glitch (CVE-2014-0496) removed from the Adobe Reader and Acrobat 11.0.06 refers to a use-after-free vulnerability that could lead to code execution as well. The update priority rating for all three security flaws that received a fix is the highest, as their severity has been marked as critical, with potential of permitting surreptitious execution of native code. The company has not released information about knowledge of the vulnerabilities being leveraged in the wild. To read more click **HERE**

Windows XP Still Running on Thousands of UK Government Computers

SoftPedia, 14 Jan 2014: It's no secret that Windows XP support will come to an end very soon and every computer user that cares a little bit about his privacy and security knows that he should migrate by April. The reason is pretty simple and is brought in the spotlight by Microsoft itself with every single occasion: without security patches and fixes, Windows XP machines would be completely vulnerable after April, so hackers would be able to get into a computer running this OS version very fast. It turns out, however, that many government computers, which should be the first to be moved to newer software, are still running Windows XP, with a report published by The Register revealing that thousands of PCs in the UK are very likely to be exploited when the hacking season begins. Both the HMRC and the UK arm of NHS are running thousands of PCs powered by Windows XP and the current estimates prove that the transition to Windows 7 or 8 won't be completed in time. The Register has the exact numbers of PCs still on Windows XP right now: more than 85,000 HMRC and 3,500 NHS computers are powered by the 12-year-old operating system and using Internet Explorer 6 as the default browser. With several migration plans in place right now, officials admit that it's going to take more than only three months to move from Windows XP. HMRC started the transition to Windows 7 and Windows 8 in 2012, while NHS was late to the migration party and begun moving PCs to a newer platform in July 2013. NHS England says that while it does know how many computers are currently running Windows XP, it cannot estimate when the migration from Windows XP completes. "Local organisations are currently in the process of upgrading PCs to use the Windows 7 operating system in advance of Windows XP support ending in April 2014. Local organisations are aware of the need to migrate from Windows XP in advance of the April 2014 de-support date," NHS England told the source. Of course, that's a little bit worrying for UK taxpayers, especially because neither HMRC nor NHS plan to invest more money into extended support for Windows XP, which means that starting with April 9, all computers running this OS version will become vulnerable to attacks. To read more click **HERE**

Website of Major Japanese Publisher Hacked, Visitors Directed to Gongda Exploit Kit

SoftPedia, 14 Jan 2014: Security researchers from Symantec have identified an attack that's designed to distribute malware by taking users to a website hosting the Gongda exploit kit. Cybercriminals have compromised the website of a major Japanese company that specializes in book publishing and the distribution of magazines, comics, books, games and movies. The company has not been named. However, experts say that a malicious iframe has been injected into its website to lead visitors to a site that's set up to host the exploit kit. The iframe in question has been identified on at least three pages, including the homepage. The site started redirecting visitors to the malicious resource on the night of January 5. The issue was addressed around three days later. The Gongda exploit kit used in the attack had been designed to exploit three Java, one XML Core Services and an Adobe Flash Player vulnerability to serve malware. The malware in this case was Infostealer.Torpplar, a threat designed to steal information from Japanese users who visit certain banking, shopping, email, gaming, or credit card sites. To read more click **HERE**

Icefog Cybercriminals Use Java Backdoor to Target US Organizations

SoftPedia, 14 Jan 2014: Back in September 2013, researchers from Kaspersky published a report on Icefog, a cybercriminal campaign that mainly targeted organizations in Japan and South Korea. After further analyzing the operation, experts have found a Java backdoor used to target entities in the United States. After Kaspersky published its report, the cyber mercenaries shut down their operations. While monitoring sinkholed domains and victim connections, experts came across a domain hosted in Hong Kong called lingdona[dot]com. It was later determined that this particular domain was used by a piece of malware connected to Icefog. The threat in question is actually a Java backdoor that Kaspersky has dubbed Javafog. Javafog, which is currently detected by only 3 antivirus engines on VirusTotal, has been utilized in attacks against three targets located in the United States, including a major independent oil and gas company with operations in several countries. Two of the organizations have cleaned up their systems after being notified by the security firm. Kaspersky notes that since Java malware is not as popular as Windows malware, it's more difficult to spot. "In one particular case, we observed the attack commencing by exploiting a Microsoft Office vulnerability, followed by

the attackers attempting to deploy and run Javafog, with a different C&C," Kaspersky experts noted in their report. "We can assume that based on their experience, the attackers found the Java backdoor to be more stealthy and harder to notice, making it more attractive for long term operations." The discovery of Javafog has led researchers to believe that the backdoor might have been used for the collection of intelligence for a longer period than usual. This also shows that the malicious actors' scope is much wider than initially thought. For additional technical details on Javafog, check out Kaspersky's report [**LINK**]. To read more click **HERE**

Hacker Jeremy Hammond Will Serve His Sentence at FCI Manchester

SoftPedia, 14 Jan 2014: Jeremy Hammond, the LulzSec hacktivist who has been recently sentenced to 10 years in prison for his role in the attack that targeted Stratfor, will serve his sentence at the Federal Correctional Institution (FCI), Manchester. The Free Jeremy Hammond group has just confirmed that this is the activist's final destination, after being moved a number of times. FCI Manchester is a medium-security prison for male inmates, located in Kentucky. Just before being sentenced, Hammond made a statement in which he revealed some interesting things about how US authorities cracked down on the LulzSec group with the aid of Hector Monsegur, aka Sabu. He explained that he hadn't even heard of Stratfor before the organization was appointed as a target by Sabu, the hacker whose sentencing was delayed for the fifth time on Monday. To read more click **HERE**

Georgia Tech to Help US DoE Detect Cyberattacks on Utility Companies

SoftPedia, 14 Jan 2014: The Georgia Tech Research Institute (GTRI) has been awarded a $1.7 million (€1.2 million) contract by the United States Department of Energy (DoE) in order to come up with the technology necessary to detect cyberattacks aimed at utility companies. Georgia Tech's Strategic Energy Institute, the School of Electrical and Computer Engineering's National Electric Energy Testing, Research and Applications Center (NEETRAC), and experts in smart grid technology will work together on developing the protocols and tools needed to detect attacks against critical infrastructure systems. "Utilities and energy delivery systems are unique in several ways. They provide distribution over a large geographic area and are composed of disparate components which must work together as the system's operating state evolves," GTRI researcher Seth Walters noted. "Relevant security technologies need to work within the bandwidth limitations of these systems in order to see broad adoption and they need to account for the varying security profiles of the components within these power systems." The tools that experts will develop include advanced modeling and simulation technologies and a network of advanced sensors that's capable of taking action to protect the targeted infrastructure in real time. The system will focus on analyzing the content of the attack traffic instead of the source of the attack. Georgia Tech has already conducted comprehensive research on electric power utilities and their infrastructure. The first phase of the project consists of research and development activities. Next, there will be a testing and validation process at Georgia Tech. In the final phase, the technology will be put to the test at operational facilities. In order to simulate various types of cyberattacks and their effects, a cyber-power co-simulator will be integrated. "The proposed cybersecurity system is complex, so a disciplined approach to delivering a system of systems which embodies this complexity will be required," Walters added. "Furthermore, as part of research and development, we will be working to ensure that the tool suite, as conceptualized by the team, remains relevant to current and emerging industry needs." To read more click **HERE**

Symantec Publishes Paper on Cyberattacks Against the Energy Sector – Infographic

SoftPEdia, 14 Jan 2014: IT security firm Symantec has published a whitepaper detailing the cyberattacks launched against the energy sector. This particular sector has become increasingly targeted over the past period. In fact, in 2013, it was the fifth most targeted. A wide range of actors have set their sights on the energy industry, including governments, competitors which seek an advantage, so-called hacker mercenaries who do it for the money, and even hacktivists. The most common attack vectors used in attacks against the energy sector are application vulnerabilities, spear phishing, backdoors and default passwords. So far, the most notable attacks were the Stuxnet, Shamoon and Night

Dragon campaigns. For a summary of the report, check out the infographic. The complete report, "Targeted attacks against the energy sector," is available on Symantec's website [**LINK**]. To read more click **HERE**