THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

24 July 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

July 23, The Register – (International) **Android ransomware demands 12x more cash, targets English-speakers.** Researchers at ESET identified a new version of the Simplocker ransomware for Android that displays a fake law enforcement ransom note in English and demands a higher ransom than previous versions that were written in Russian and demanded payment in Ukrainian hryvnias. The new version of the ransomware contains additional features such as the encryption of more types of files on victims' devices and actions that make it more difficult to remove. Source: http://www.theregister.co.uk/2014/07/23/android_ransomware_simplocker_revamp/

July 23, Securityweek – (International) **Mozilla fixes 11 vulnerabilities with release of Firefox 31.** Mozilla released new versions of its Firefox Web browser and Thunderbird email client July 22, closing 11 vulnerabilities, including 3 rated as critical. Source: http://www.securityweek.com/mozilla-fixes-11-vulnerabilities-release-firefox-31

July 23, Help Net Security – (International) **40% of orgs running VMware still susceptible to Heartbleed.** Data collected and analyzed by CloudPhysics found that 57 percent of deployed VMware vCenter servers and 58 percent of ESXi hypervisor hosts remain vulnerable to the Heartbleed vulnerability in OpenSSL, affecting 40 percent of organizations in the CloudPhysics data set. Source: http://www.net-security.org/secworld.php?id=17159

July 23, Help Net Security – (International) **Internet Explorer vulnerabilities increase 100%.** An analysis by Bromium Labs surveyed vulnerabilities in popular Web browsers and common software and found that vulnerabilities in Internet Explorer increased by more than 100 percent in the first quarter of 2014. Other findings included that Action Script Sprays were leveraged in zero day attacks and that zero day vulnerabilities in Java have declined greatly in the first quarter of 2014 compared to 2013. Source: http://www.net-security.org/secworld.php?id=17158

Sony's $15 million PSN hacking settlement pays out in free games
EnGadget, 24 Jul 2014: Way back in 2011, PlayStation Network services and websites went dark due to "an external intrusion." Anonymous claimed responsibility, names, passwords and possible payment information was lost in a data breach, and everybody in general had a bad time. Sony apologized for the fiasco with a "Welcome Back" package, handing out free (older) games to anybody willing to turn their PlayStation back on -- but that wasn't the end of it. The company still had to face a class action lawsuit for losses caused by identity thefts and the needs of gamers who failed to participate in its apology giveaway before it closed. Now the company has reached a $15 million settlement. The short version? More free stuff. Claimants who didn't participate in the original "Welcome Back" program will be offered one of 14 PlayStation 3 or PlayStation Portable games and three PS3 themes, or a three-month subscription to PlayStation Plus. It's not all giveaways, though -- folks with documented identity theft charges will be able to reap up to $2,500 per claim, and users of Sony's old Qricity service will be able to get a month of Music Unlimited service in recompense. MMO gamers who lost time in virtual worlds are eligible for a $4.50 credit to their SOE accounts, too. You can check out the full court decision below. Forgot all about the 2011 breach? Well, "welcome back." To read more click **HERE**

Hacking experts build device to protect cars from cyber attacks

Reuters, 22 Jul 2014: Two security experts who a year ago exposed methods for hacking the Toyota Prius and Ford Escape say they have developed technology that would keep automobiles safe from cyber attacks. At last summer's Def Con hacking conference in Las Vegas, the two researchers, Chris Valasek and Charlie Miller, described ways to launch dangerous attacks, including manipulating the brakes of the moving Prius and the Ford Escape. Valasek told Reuters on Tuesday that he and Miller will show off a prototype vehicle "intrusion prevention device" at next month's Black Hat hacking conference in Las Vegas. They built the device with about $150 in electronics parts, though the real "secret sauce" is a set of computer algorithms that listen to traffic in a car's network to understand how things are supposed to work. When an attack occurs, the device identifies traffic anomalies and blocks rogue activity, Valasek said. The two well-known computer experts decided to pursue the project because they wanted to help automakers identify ways to defend against security vulnerabilities in their products. "I really don't care if you hack my browser and steal my credit card," Valasek said. "But crashing a car is life or death. It is dramatic. We wanted to be part of the solution." The research the two have released on the Ford and Toyota cars, as well as work by other experts on different types of vehicles has raised concerns that somebody might one day try to replicate their work to launch a real-life attack. Yet the U.S. National Highway Traffic Safety Administration said in a statement on Tuesday that it is not aware of any incidents of consumer vehicle control systems having been hacked. The auto industry has beefed up efforts to identify and mitigate potential cybersecurity risks over the past few years. A representative for Ford said she had no immediate comment on the device. Officials with Toyota could not be reached for comment To read more click **HERE**

Hibernia replaces Huawei for high-speed trading cable

Computerworld, July 24, 2014: Hibernia Network's cable project to connect New York and London traders at record speeds has resumed after coming unstuck last year, the cable company announced. Hiberna is connecting London to New York, Halifax, Nova Scotia with a low-latency fiber-optic 4,600km cable, which promises to offer traders a five millisecond advantage on other high-speed traders. Hibernia Networks claims that when the service becomes available, it will be the "newest and fastest fibre-optic path between New York and London". The fast connection will shave milliseconds off processing computer algorithms for high frequency trading, in which large volumes of transactions are made across different venues for small gains. The milliseconds the new cable will save could make a difference of millions of pounds. However, the cable took a back seat when Hibernia's chosen vendor Huawei, came under fire in the US for security issues. Hibernia Network revealed that the project will resume with new vendor TE SubCom (a subset of TE Connectivity) and is planned to go live in summer next year. To read more click **HERE**

DHS 'dos and don'ts' on cybersecurity

The Hill, 21 Jul 2014: Is a cyber-attack on America's electric grid imminent? Or will hackers sabotage a major chemical plant this year? Answers to these questions may surprise you because they're slightly counterintuitive. Many of the nation's most-at-risk "critical infrastructure" sites – like power plants and chemical facilities – have analog redundancies in place that ensure catastrophic cyber-attacks won't halt operations. For now. But as connectivity increases and as electric grids become "smarter" through efficiency and automation measures, they will only become more and more linked to the internet – and more at risk of infiltration. The good news is that we seem to have stumbled upon a short window of time where the government can work with U.S. critical infrastructure sites to beef up both cyber and physical security. The Department of Homeland Security (DHS) is taking the lead in assessing these vulnerabilities – with the private sector – as fast as they can. Just last month, DHS released information about a U.S. public utility that was infiltrated. The Department worked quickly with the company to enhance security "before there was any impact to operations." For once, we've got a plan in place to address what most experts suggest will be an ongoing problem. The not-so-good news is that some industry partners aren't comfortable or willing to partner with the government, even though attacks on U.S. utility companies are increasing steadily. California's Energy Commission chairman was quoted recently as saying, "If you're a

utility today, depending on your scale, you're under attack at this moment." Voluntary public-private partnerships remain the principal mechanism for managing critical infrastructure risk. While there are still arguments over which government agency should "own" the cyber mission, the one responsible for protecting America's energy sector, wastewater facilities and even public transportation systems is Homeland Security. For most people, cybersecurity is a complicated subject – especially when the government is involved. But it doesn't have to be. What exactly is your government doing to keep you safe? Here's what DHS is and isn't doing to protect against a cyber "Pearl Harbor."

1. What does DHS do in the cybersecurity world?

- DHS's role is to bring together all stakeholders—government officials and business leaders, security professionals and infrastructure owners and operators—to share information and best practices to reduce and manage cyber risk.
- To do that, DHS set up a space called the National Cybersecurity and Communications and Integration Center (NCCIC) where the private sector can sit with DHS and FBI analysts to talk directly to each other and respond to threats in real time.
- As part of that Center, DHS maintains the US Computer Emergency Readiness Team – a 24 hour cyber operations center that responds to incidents, provides technical assistance and notifications about current and potential security threats and vulnerabilities.
- Through this center, DHS offers threat details and analysis that is non-attributable and anonymized to private sector companies who ask for it and help companies create assessments to understand if there are security gaps that can be fixed.
- At the same time, DHS conducts regular Privacy Impact Assessments, which are released to the public, about its cyber operations and data minimization efforts.

2. What doesn't DHS do?

- DHS doesn't track the systems of companies that haven't signed up to partner through a mutual agreement and it does not have any so-called "offensive" ability to launch cyber-attacks.
- The Department doesn't force a company to change its cyber security methods, and working with the Department is completely voluntary.
- DHS doesn't view the systems of all critical infrastructure businesses. Unfortunately, that means they don't have a complete threat picture. The more private sector groups partner with DHS, the easier it will be to see threat trends and be able to address them in real time.
- The Department is responsible for and scans the systems on federal networks, but cannot fix problems. They can only alert tech teams in each particular Department or Agency. This argues for greater authority or binding guidance from OMB so that DHS can address intrusions.

3. What will DHS do in the future?

- DHS computer systems will automatically send and receive cyber threat information to private sector partners, based on current threat conditions. Its systems will get "smarter" as it is exposed to new threats.

4. Why does DHS have a cyber role at all? Just because the Department is responsible for protecting critical infrastructure doesn't mean it's capable of adding in preventing cyber-attacks, right?

    - The Homeland Security Act requires DHS to assess vulnerabilities to critical infrastructure, which has naturally evolved to include cyber security. Plus, as a result of a variety of other homeland security efforts, like border security, the Department has developed impressive cyber capabilities.

The bottom line: over the past few years, DHS has built successful partnerships and experience to protect critical infrastructure. Now, the mission is shifting from a sole focus on protection (i.e. building stronger firewalls) to building resilience into the networks, systems, and assets that America relies on for the delivery of essential functions and services. DHS is even encouraging innovators to adopt a resilient and secure by design principle. No government effort will ever be perfect, and the Department has certainly made a few mistakes that have made some wary of trusting it. But the DHS deserves credit for thinking about the long-game and making progress in the absence of cyber legislation. To read more click **HERE**

Modern electric grid fighting cyber vulnerabilities

Power Source, 22 Jul 2014: The recent push to modernize the electric grid has increased communication between utilities and consumers, enhanced reliability and created more opportunities for green energy producers. But it also has raised the risk of cyber attacks. New technology, while largely beneficial for utility companies and their consumers, has created millions of new access points that make the grid vulnerable. Utility companies are spending millions annually in cyber security costs, and the trend will continue with investments in smart meters and other technology meant to bring the electric grid up to date. Despite the enhanced risk, the effort to modernize the electric grid is largely a good thing, said Annabelle Lee, senior technical executive at the nonprofit Electric Power Research Institute, in Palo Alto, Calif. New technology has opened the grid to a two-way flow of communication, as smart meters have promoted better communication among utility companies as well as between utilities and consumers. Such real-time information about usage will help to make the grid more efficient, she said. Technology has allowed utilities to build more reliable power systems while lowering delivery costs, said Michael Assante, a board member for the Council on CyberSecurity in Washington, D.C. He is also the lead for training on industrial control systems and supervisory control and data acquisition security for the SANS Institute, a Bethesda, Md., computer security research and training center. But, Mr. Assante said, "Technology is always a double-edged sword," and the growth in reliance on technology comes with growing risk. Large-scale blackouts and brownouts, communication failures and data theft are potential damages of any cyber event. The issue drew a lot of attention late last month when U.S. security company Symantec reported that a group of hackers, known as "Energetic Bear" and "Dragonfly" had gained access to electric systems in the U.S. and Europe. Those hackers had Russian ties, according to Bloomberg. The modern grid also includes more access points that allow renewable energy generators to provide energy. These are big changes from the past, when the grid was open to only a few participants. Now, it is open to thousands. Previously, the technology used to control the grid was proprietary, often created specifically for electric utilities. But the technological overhaul that electric utilities are currently undertaking — often required by state governments — requires them to rely on commercially available hardware and software. With more access and more common hardware and software, there are more opportunities for hackers to access the system, Ms. Lee said. Unlike most cyber security incidents, which are motivated by monetary interests, the manipulation of the power sector often has geopolitical motivations, Mr. Assante said. The electric grid is an infrastructure asset, and its compromise could give an organization power, for lack of a better word. Since the electric grid is a national security interest, Mr. Assante said the federal government and utility companies share responsibilities to protect it. In February, President Barack Obama signed an executive order to assess the grid's risk. In 2010, the National Institute of Standards and Technology released guidelines for smart grid cyber security, outlining precautions companies should take as they embrace a more modern system. Last November, the Federal Energy Regulatory Commission approved a new series of critical infrastructure protection reliability standards, addressing the stability of electricity transmission. The new standards will take effect starting in 2016. They require bulk electric system operators, which handle more than 100 kilovolts of electricity, to classify all assets as high, medium or low risk and to create security plans for each. The current standards require those operators to only identify critical assets. Most cyber events, even those unrelated to the energy sector, are often accidents with no malicious intent, Ms. Lee said. But the damages are often just as severe. A technician's mistake in 2011, for instance, left 7 million people without power in the Southwest. Intentional attacks have yet to inflict that kind of harm. In complex technological systems, a minor malfunction — or manipulation — can

create widespread problems, Mr. Assante said. A survey of 61 electric utilities conducted by Bloomberg indicated companies are investing an average of $3 million annually on cyber security. Those investments need to be made in a coordinated way with any investment that companies make in new technology, as each component often carries with it certain security challenges, Mr. Assante said. And security risk — a measure of threat and vulnerability — changes often, so utility companies should constantly evaluate security needs, Ms. Lee said. The best security investment, Mr. Assante said, is in personnel who can provide that type of evaluation. He said businesses should be more willing to share information about security breaches so other companies can avoid similar problems. To read more click **HERE**