The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

6 May 2014

Purpose
Educate recipients of cyber events to aid in the protection of electronically stored corporate proprietary, DoD and/or Personally Identifiable Information from theft, compromise, espionage, and / or insider threat

Source
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
To receive this newsletter please send an email to scott.daughtry@dtra.mil

May 3, WECT 6 Wilmington – (North Carolina) **UNCW server attacked exposing sensitive information.** The University of North Carolina at Wilmington announced April 29 that a server which contained a database of personal information including Social Security numbers of employees, graduate students, and adjunct instructors was attacked, potentially exposing the information. The university removed the database from the server and is investigating the incident. Source: http://www.wect.com/story/25379044/a-server-at-uncw-breached-during-an-attack

May 2, WSVN 7 Miami – (Florida) **Teen accused of accessing public school's database, altering grades.** A Dr. Michael M. Krop Senior High School student was arrested and charged May 1 for taking money, illegally accessing the Miami-Dade Public Schools database, and changing grades for four students. Source: http://www.wsvn.com/story/25416383/teen-accused-of-accessing-public-schools-database-altering-grades

May 5, Softpedia – (International) **"Covert redirect" OAuth security flaw not as serious as it sounds, experts say.** A researcher reported finding a vulnerability dubbed "covert redirect" in OAuth and OpenID that could allow an attacker to access users' information. However, security researchers found that the vulnerability is only in certain implementations of OAuth and requires both user interaction and an open redirect to be present in a targeted application to be effective. Source: http://news.softpedia.com/news/Covert-Redirect-OAuth-Security-Flaw-Not-as-Serious-as-It-Sounds-Experts-Say-440575.shtml

Windows flaw allows access to data after accounts are revoked
Heise Security, 6 May 2014: A disabled account in Windows' network does not take effect immediately, according to Aorato. In fact, due to design considerations disabled accounts - and the same goes for deleted, expired and locked-out accounts - effectively remain valid up to 10 hours after they had supposedly been revoked. As a consequence, so-called disabled accounts expose the corporation to advanced attackers seeking to gain access to the corporate network. Leaving employees who have had their user account disabled can also potentially continue and gain access to corporate data. With 95% of Fortune 1000 companies running a Windows based network, this flaw affects enterprises across industries. Organizations seeking to comply with the PCI Data Security Standards, will find that this authentication flaw makes the requirement of the immediate revocation of any terminated user, a requirement that in reality cannot be met. The problem lies in the Kerberos authentication protocol which is based on an organizational "ticket". The ticket eliminates the need for employees to re-supply their username / password each time they access a system. However, the fact that authentication and authorization rely solely on the ticket, and not on the user's credentials, means that disabling the user's account has no effect on the employees' ability to access data and services. "Unfortunately, Windows's fails to solve this authentication flaw. Worse yet, Windows' Kerberos implementation does not externalize the ticket information through logs and events, and so exploitation of the flaw cannot be mitigated through traditional log and SIEM measures.

To mitigate, organization should monitor network traffic to Windows authentication servers in order to:

- Recouple the ticket with the user's account in order to eliminate the root cause of the problem
- Monitor changes in user's account's state and activities and in particular, to the revocation of the user's account
- Terminate requests of a disabled user requesting access to a resource using a valid ticket.

To read more click **HERE**

Tips for utilities to comply with new cybersecurity standards
Heise Security, 5 May 2014: When the North American Electric Reliability Corporation (NERC) signed Order 791 in January 2014, more than 400 utilities suddenly faced a tight timetable to plan for and comply with version 5 of the Critical Infrastructure Protection (CIP) cybersecurity standards. The reason for the change is clear and timely: A report from the Department of Homeland Security's Cyber Emergency Response Team disclosed that the energy industry faced more cyberattacks between October 2012 and May 2013 than any other sector. Before utility organizations embark on addressing the new regulations, Booz Allen offers the following best practices for NERC-CIP version 5 compliance:

1. Conduct a cybersecurity strategic simulation that will enable a utility to identify security gaps, prioritize assets, and identify areas for improvement – without the consequences of an actual cybersecurity incident or an audit. The controlled environment of a simulation allows participants to safely explore real-world situations, resulting in improved communication, coordination and the identification of any gaps in existing response plans.

2. Develop a strategic plan that positions the utility to manage future threats as well as standards. Implementing best practices from the start can serve as a footprint for success, allowing utilities to leverage existing investments in people, processes and technology that ultimately prevent them from overspending.

3. Pursue a knowledge management system that will ensure business continuity for today and the future. The aging workforce presents a major industry challenge: an exodus of institutional and technological "know how" that could hamper a company's ability to continue its mission effectively. It is important to establish a team that understands the regulatory environment, threats, and overall enterprise.

4. Implement an internal program to address employee cyber "hygiene" and the potential for insider threats. Ultimately, all staff within an organization can pose as a cyber threat – either accidental or intentional. These challenges can no longer be the sole responsibility of IT. Utilities should communicate to all employees the significance of being cyber risk aware, and knowing what to do when a concern arises.

5. Acknowledge and understand the difference between compliance and security. Keeping up with standards will help utilities avoid legal exposure, fines, and the like. But that does not necessarily make a utility company more secure – there is no silver bullet formula for security. Rather, cybersecurity is intimately tied to a utility's business strategy and operations, and must be customized to the organization.

To read more click **HERE**

Global cost of data breach goes up by 15 percent
Heise Security, 5 May 2014: The average consolidated total cost of a data breach increased 15 percent in the last year to $3.5 million, say the results of Ponemon Institute's ninth annual Cost of Data Breach Study: Global Analysis report (**registration required**). The study also found that the cost incurred for each lost or stolen record containing sensitive

and confidential information increased more than nine percent to a consolidated average of $145. The research involved the collection of detailed information about the financial consequences of a data breach. For purposes of this research, a data breach occurs when sensitive, protected or confidential data is lost or stolen and put at risk. Ponemon Institute conducted 1,690 interviews with IT, compliance and information security practitioners representing 314 organizations in the following 10 countries: United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India and, for the first time, the Arabian region (a consolidation of organizations in the United Arab Emirates and Saudi Arabia). "The goal of this research is to not just help companies understand the types of data breaches that could impact their business, but also the potential costs and how best to allocate resources to the prevention, detection and resolution of such an incident," said Dr. Larry Ponemon, Chairman and Founder of Ponemon Institute. This year's Cost of Data Breach Study also provides guidance on the likelihood an organization will have a data breach. Key takeaways:

- The most costly breaches occurred in the U.S. and Germany at $201 and $195 per compromised record, respectively. The least expensive data breaches were in India and Brazil at $51 and $70, respectively.
- Root causes of data breaches differ among countries. Countries in the Arabian region and Germany had more data breaches caused by malicious or criminal attacks. India had the most data breaches caused by a system glitch or business process failure. Human error was most often the cause in the UK and Brazil.
- The most costly data breaches were those caused by malicious and criminal attacks. The U.S. and Germany paid the most at $246 and $215 per compromised record, respectively. These types of data breaches were least costly for companies in India and Brazil at $60 and $77 per compromised record, respectively.
- A strong security posture was critical to decreasing the cost of data breach. On average, companies that self-reported they had a strong security posture were able to reduce the cost by as much as $14 per record.
- The involvement of business continuity management reduced the cost of data breach by an average of almost $9 per record.
- The appointment of a Chief Information Security Officer (CISO) to lead the data breach incident response team reduced the cost of a breach by more than $6.
- Countries that lost the most customers following a data breach were France and Italy. Companies in the Arabian region and Brazil experienced the lowest loss of customers.
- The probability of a company having a data breach involving 10,000 or more confidential records is 22 percent over a two-year period. Countries most likely to experience a data breach include India, Brazil and France.
- Consistent with previous Cost of Data Breach studies, most often the common cause of a data breach is a malicious insider or criminal attack. We asked companies what worries them most about security incidents. Following are some of the key findings:
- The greatest threats to the companies in this study are malicious code and sustained probes. According to threats increased.
- Only 38 percent of companies have a security strategy to protect its IT infrastructure. A higher percentage (45 percent) has a strategy to protect their information assets.
- Malicious code and sustained probes have increased the most. Companies estimate that they will be dealing with an average of 17 malicious codes each month and 12 sustained probes each month. Unauthorized access incidents have mainly stayed the same and companies estimate they will be dealing with an average of 10 such incidents each month.

To read more click **HERE**

Nearly 200 Million Records Compromised in Q1

Dark Reading, 1 May 2014: More than 250 breaches were disclosed in Q1 2014, SafeNet report says. More than 250 data breaches occurred in the first quarter of 2014, resulting in the compromise of nearly 200 million records, according to a report published this week. According to SafeNet's "Breach Level Index," the pace of compromised data in Q1 amounted to approximately 93,000 records per hour, a 233 percent increase over the same quarter in 2013. Interestingly, despite much discussion of retail security following breaches at Target and other retailers in Q4 2013, the retail industry accounted for just 1 percent of the records lost in Q1, and just 10 percent of the breaches. The financial industry was hit hardest during Q4, accounting for 58 percent of records lost. The technology industry accounted for 20 percent of lost records. The healthcare industry was hit hard in terms of breach events, accounting for 24 percent of all breaches, but only 9 percent of data records lost. South Korea took the top spot of all countries with four of the top five breaches worldwide and a loss of 158 million records across a variety of industries. This represents 79 percent of the total number of reported breached records worldwide. While the number of South Korean breached records was extremely high, the number of breach incidents in Asia/Pacific as a whole accounted for only 7 percent of the total number of global breaches, dwarfed by the 78 percent (199 incidents) that occurred in North America and 13 percent in Europe. Malicious outsiders accounted for 156 (62 percent) of total incidents during the first quarter, compromising more than 86 million records stolen. Malicious insiders accounted for just 11 percent of total incidents, but they were much more effective, accounting for 52 percent of records stolen. Accidental loss represented 25 percent of total incidents, while hacktivist and state-sponsored attacks added up to just 2 percent of the total. To read more click **HERE**

DrawQuest Shut Down After Hackers Gain Access to Amazon Servers

SoftPedia, 6 May 2014: DrawQuest – the free drawing community for iPhone, iPad and iPod touch – has been shut down. The decision comes after malicious hackers breached the Amazon servers used by the company. DrawQuest was launched by Chris Poole, aka moot, the founder of 4chan, back in February 2013. However, after less than a year, in January 2014, Poole announced that his startup had failed. A few days later, the DrawQuest Team announced that it would try to keep the service running for as long as it could. They've managed to do it until now, when cybercriminals compromised "the entirety of DrawQuest." "The person(s) used our account to order hundreds of expensive servers, likely to mine Bitcoin or other cryptocurrencies. When we detected this activity, we immediately locked down the account," the DrawQuest team announced in a blog post. "Unfortunately we have no way of knowing what, if any, information was accessed by the attacker(s). It's possible they only used our account to order servers, however it's also possible they accessed our database, and thus user e-mail addresses, encrypted passwords, and other information," it added. Since the company doesn't have any full-time employees, it's impossible to repair the damage. As a result, DrawQuest has been shut down. While there's no evidence that the attackers targeted DrawQuest users, and while the passwords are properly encrypted using bcrypt, customers are advised to change their passwords as a precaution. The company has promised to offer a downloadable archive of all drawings, but it's uncertain when it will become available. It could take weeks or even months. "It's a very upsetting end to a long journey. Words cannot describe how crushed, embarrassed, and sorry our team is. Although all of our former employees have moved on to roles at other companies, it can safely be said that DrawQuest and the community occupies a large part of all of our hearts," the message from the DrawQuest team reads. "We'll do our best to facilitate DrawQuesters finding a new home by linking to new forums/apps on our social media pages, and are truly sorry such a wonderful community had to go this way." This is actually the second time one of Poole's projects gets hacked over the past month. In late April, he revealed that someone had managed to breach 4chan. At the time, the attacker apparently wanted to expose "multiple abuses of power and violations of proper mod stewardship." To read more click **HERE**

Dropbox Leaks User Data on Google Through Shared Links

SoftPedia, 6 Mar 2014: Piece of advice to you all. Limit your Dropbox link sharing for a while, as apparently your stuff can turn up on Google. That's the key takeaway from an alarming post by security specialist Graham Cluley, who confirmed with Dropbox that they have a serious data leak problem. Cluley's post is insightful, as always, but it's written in the language of techies. Regular users are better off reading what Dropbox has to say on its blog. In a nutshell, the leak is real and happening, and Dropbox is already taking radical steps to address the situation. Some of your previously-shared links may no longer be functional as of now, just so you know. "We wanted to let you know about a web vulnerability that impacted shared links to files containing hyperlinks," the Dropbox post begins. "We've taken steps to address this issue and you don't need to take any further action." The cloud company begins to explain how linking to Dropbox files can lead to those particular files getting leaked on the web because of the referrer header, or HTTP referrer, which identifies the address of the web page that linked to the resource being requested, allowing the new web page to see where the request originated. Dropbox explains: "For background, whenever you click on a link in any browser, the site you're going to learns where you came from by something called a referer header. The referer header was designed to enable websites to better understand traffic sources. This is standard practice implemented across all browsers." "Dropbox users can share links to any file or folder in their Dropbox," the cloud company continues. "Files shared via links are only accessible to people who have the link. However, shared links to documents can be inadvertently disclosed to unintended recipients," Dropbox warns. A particular set of factors and situations must converge to make it all possible, but it's nevertheless very easy to get there. If you've engaged in such practices, Dropbox says it has made the links inoperable starting May 5, in order to protect your data. Users can re-create any shared links that have been turned off, and any links created starting now are free of this vulnerability. Business users have the option to restrict shared link access to people in the Dropbox for Business team. According to the company, using those access controls made it impossible for data to be breached. "We realize that many of your workflows depend on shared links, and we apologize for the inconvenience. We'll continue working hard to make sure your stuff is safe and keep you updated on any new developments," Dropbox concludes. Oh, and according to Cluley, Box users are affected as well. Update: researcher Graham Cluley tells us "Dropbox says it has fixed one of the issues, but not the one which actually resulted in Income Tax returns and mortgage applications falling into unauthorised hands. So far they've been silent about that." To read more click **HERE**

Lessons from PayPal's Exec: Don't Trash Coworkers Online…Ever

Fox News, 5 May 2014: Tweeting while mad won't get you far. Take PayPal's former director of strategy as an example, who was reportedly fired from the company for tweeting unsavory things about his coworkers. Disgruntled employees take note: Airing your grievances with your employer or colleagues, both past and present, on social media is never a good idea. Latest case in point: a twitter rant from Rakesh Agrawal, PayPal's former director of strategy, who had only been with the company for two months. Through a series of since-deleted texts filled with spelling and grammatical errors, Agrawal blasted his co-workers via Twitter (TWTR) over the weekend in a series of late-night tweets. Reports show he called Christina Smedley, PayPal's vice president of global communications, a "useless middle manager," along with other names in profanity-laden tweets. Agrawal claims he was using a new phone and that the tweets were meant to be direct messages and that he accidentally sent them public. PayPal fired back via its own Twitter account on Saturday, posting: "Rakesh Agrawal is no longer with the company. Treat everyone with respect. No excuses. PayPal has zero tolerance." FOXBusiness.com reached out to PayPal for further comment but had not received a response at press time. Agrawal says he resigned from the company before his Twitter outburst. He posted: "P.s. the tweet from paypal is factually correct but utterly misleading. I resigned before the events of Friday night." He also included a screenshot of his resignation letter, sent on Friday night, before his twitter tirade began. But Kathy Caprino, career coach, says regardless of whether Agrawal was fired for his tweets or left the company before sending them, the move is disastrous for his professional reputation. "You never trash your colleagues, and never trash your former employer on social media," she says. "It's a public forum, and it's not acceptable to do that." Social media comes back to bite workers who

share too much, she says. The proper way to handle workplace grievances is to go through the proper channels, she says: getting human resources involved and a lawyer if necessary. "If you trash the company, they are almost forced to let you go," she says. "This shows a terrible lack of judgment. The fact that he was director of strategy—what irony. Strategy is all about vision and direction, and inspiring the company towards a vision. Doing that is anti-strategic." Railing against a company in the wake of a firing or frustrating situation also does a worker disservice, she says. "You are making the situation all about you," she says, by tweeting or posting about a firing or work issue on the web. "You are missing some of the point. You co-created the situation. It doesn't mean that it's always appropriate that they let you go, but if you fire off a missive that the company is to blame, it will hurt your career. Bad mouthing won't get you where you want to go." To read more click **HERE**

2 men charged in Tulsa with hacking Navy, other government, education and business sites

AP, 5 May 2014: Federal prosecutors in Tulsa say two men are charged with conspiring to hack into computer systems of the Navy and more than 30 other government, business and university sites. United States Attorney Danny C. Williams Sr. said Monday that 27-year-old Nicholas Paul Knight of Chantilly, Virginia, and 20-year-old Daniel Trenton Krueger of Salem, Illinois, were trying to steal identities, obstruct justice and damage a protected computer. Williams says the Navy quickly discovered the breach and located the two suspects. The case is being prosecuted in Tulsa because the Navy servers that were hacked are located in the city. The men allegedly hacked a system used to manage transfers for members of all branches of the military. The system stores personal information for 220,000 service members. Knight was in the Navy. To read more click **HERE**

Cyber-security expert's experiment shows Wi-Fi users in Las Vegas vulnerable to hacking

Las Vegas Sun, 6 May 2014: James Lyne calls his road bike "The Beast," and he's brought it to Las Vegas to find out just how vulnerable wireless networks in the city and their users are to hackers. The bike's thin aluminum frame is strapped with three wireless scanners, a basic minicomputer slightly bigger than a deck of cards, a GPS unit and a battery pack to charge it all. Using this equipment, Lyne is able to track how secure a person's wireless network is, set up false hotspots and see what people are searching – all in a single bike ride. Lyne is a cyber security expert for Sophos, a British computer security firm, and has traveled to cities around the world scanning for unsecure wireless networks on "The Beast." He calls it "warbiking" and "The Beast" is his chariot. "What it says to me is if society can't get something as simple as wireless right, what hope do we have for the more complex security issues?" Lyne said during an interview Monday. "I wanted to show the world in a direct way that we have to do better." Lyne started warbiking in London and has done it in San Francisco, Barcelona and now Las Vegas. His study is designed to examine how people are securing their wireless networks, how much information people walking on the street are giving away from mobile devices and how they behave online. Lyne took "The Beast" to the street Friday in Las Vegas. Starting on the Strip, he pedaled 25 miles through Las Vegas, picking up about 56,200 Wi-Fi networks. Lyne said wireless networks throughout the city did a good job upgrading from using WEP security, which he said was an easily broken encryption network. But he also found that nearly half the users accessing the Internet on an open network did so with no encryptions. Without any encryption, even the most inexperienced hackers can access an online user's bank accounts, capture private information and upload viruses. It's like shouting out personal bank account numbers and passwords at a café and being shocked that other people steal them, Lyne said. During his ride, Lyne also set up three free separate Wi-Fi hotspots. About 4,000 people signed on, ignoring the terms of use, which specified the user was consenting to have the sites they visited tracked. The experiment was designed to replicate how easy it would be for a hacker to access people's computers or smartphones and direct them to false websites to obtain personal information. As in his previous experiments, the results from Lyne's warbiking in Las Vegas showed people and Wi-Fi networks here aren't taking security precautions they need. (Lyne destroys all personal user login data he collects.) In a world where everything from computers to refrigerators is being connected to the Internet, Lyne has found that people have never been more vulnerable to a cyber attack. "We are swimming in Wi-Fi and more convenience technology," Lyne said. "It's only going to get more pervasive

in our everyday lives… but we are opening ourselves up more and more to give cyber criminals power over our lives." To avoid being hacked, he recommends people sign up for a virtual private network encryption that protects their computer on any Wi-Fi network. Meanwhile, small businesses and local Wi-Fi routers can be installed to have WPA2 encryption to protect it from hackers. Still, Lyne said the gulf between cyber security standards and the growth of wireless networks is expanding at a rapid rate. It's a global problem, and he said he planned to present the information to the United Nations to try to change cyber security standards. To read more click **HERE**