THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

4 June 2014

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

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

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

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

Disclaimer
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

NMCIWG Members
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, and Sandia National Labs

Distribution
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings. Credit is given to the NMCIWG for the compilation of this open source data

June 3, Associated Press – (International) **US disrupts hacking schemes that stole millions.** A Russian man was indicted June 2 in federal courts in Pittsburgh and Nebraska for allegedly working with five co-conspirators to run the GameOver Zeus botnet and the Cryptolocker malware, which combined infected millions of computers and were used to steal over $100 million from businesses and individuals. Source: http://www.commercialappeal.com/news/2014/jun/03/us-disrupts-hacking-schemes-stole-millions/

June 3, Attleboro Sun Chronicle – (Massachusetts) **BCC student accused of hacking computer system; using network to tap other accounts.** A former student at Bristol Community College in Boston was charged June 2 with hacking into the school's computer system to change grades several times between September 2012 and November 2013 by allegedly using log-in credentials from three instructors. The suspect was also charged with hacking into a police department computer server and gaining access to an email account and law enforcement information, as well as obtaining payment card data for more than 14,000 account holders between May 2011 and May 2013. Source: http://www.thesunchronicle.com/news/local_news/bcc-student-accused-of-hacking-computer-system-using-network-to/article_4b039b02-ea8f-11e3-b8f4-0019bb2963f4.html

June 3, The Register – (International) **Global mobile roaming network a HOTBED of vulnerabilities.** Researchers from KPN reported in a presentation at the Haxpo convention that 15 of 25 mobile roaming network operators had systems visible to the Internet due to misconfigurations or unnecessary services, potentially exposing users on their networks to security compromises. Source: http://www.theregister.co.uk/2014/06/03/global_mobile_roaming_network_a_hotbed_of_vulnerabilities/

What are the top security concerns of senior IT executives?
Heise Security, 4 Jun 2014: Most C-level executives would agree that protecting a company's confidential data and trade secrets from the prying eyes of competitors is critical. Yet interactive polling of senior IT security executives at Courion's annual user conference, revealed that 65 percent are aware that their company has experienced a computer intrusion in which data was stolen, and 55 percent have discovered a current employee or insider taking information from the company's computer system to use in a competing business. During his presentation at the conference, Assistant U.S. Attorney Kyle F. Waldinger, who has prosecuted with the Computer Hacking and Intellectual Property (CHIP) unit of the U.S. attorney's office for the northern district of California, demonstrated through these poll questions the threat that global multinational companies face, even from their own employees. Unfortunately, current legislation makes it challenging for the federal government to prosecute potential offenders. And information security and identity and access management departments don't always work together to reduce the risks that lead to breaches caused by insiders, as revealed by a live poll conducted later in the conference by presenter Jon Oltsik, a senior principal analyst with Enterprise Strategy Group (ESG). Oltsik made the case that by better

integrating IAM analytics with security, global companies gain access to the contextual access controls needed to reduce their overall attack surface and lower IT risk. By using IAM big data security analytics, or identity and access intelligence software, companies are better equipped to eliminate ungoverned accounts and better manage Segregation of Duties (SoD) and privileged account access. "Multinational corporations should be leveraging IAM big data security analytics now, not only to improve their ability to detect and respond to possible breaches, but to streamline IAM processes and improve oversight capabilities," said Oltsik. In fact, the recent 2014 Verizon Data Breach Incident Report recommends the following IAM controls:

- Know your data and who has access to it
- Review user accounts
- Watch for data exfiltration
- Publish audit results.

Further, the SANS Institute's Version 5 Critical Security Controls include:

- Controlled use of administrative privileges
- Maintenance, monitoring and analysis of audit logs
- Account monitoring and control
- Data protection

To read more click **HERE**

NIST to help IT developers build in security

GCN, 27 May 2014: The National Institutes of Standards and Technology has launched an effort to develop guidelines (**link**) for building security into IT systems from the beginning instead of at the end of the IT development process. NIST, which is asking for public comment on initial guidelines for the project, said it wanted to bring in "widely recognized systems and software engineering principles to bear on the problem of information system security from the beginning … rather than trying to tack it on at the end." "We need to have the same confidence in the trustworthiness of our IT products and systems that we have in the bridges we drive across or the airplanes we fly in," said Ron Ross, a NIST Fellow. The guidelines represent an effort to bring the principles of building reliable physical structures to software engineering design, according to NIST. "Systems security engineering processes, supported by the fields of mathematics, computer science and systems/software engineering, can provide the discipline and structure needed to produce IT components and systems that enjoy the same level of trust and confidence," according to NIST. NIST has released the first set of those guidelines for public comment in a new draft document, Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems. The current draft -- and the first stage of the planned process -- describes the fundamentals of systems security engineering and covers 11 core technical processes in systems and software development. Later public drafts will add material supporting principles of security, trustworthiness and system resilience; use case scenarios; and important nontechnical processes such as risk management and quality control procedures. NIST asked for comments on the draft by July 11, 2014. To read more click **HERE**

Insider threat detection tools: Hard to find, harder to fund

GCN, 23 May 2014: While most of the emphasis in cybersecurity seems to be on external threats and the damage suffered when network and data defenses are breached, threats from insiders are getting more attention in the aftermath of the Snowden and Wikileaks revelations. What to do about those is another question, since the tools

currently used by organizations to track incursions don't seem up to the task. It's not a new phenomenon. The FBI a long time ago began voicing its concern about threats from privileged users of data, both in government and industry. The issue has its very own website at the FBI, and the concern within government was bolstered by a White House memo published at the end of 2012 aimed at the heads of agencies. A Ponemon Institute survey, sponsored by Raytheon, shows where the recognition/mitigation gap might exist:

- 69% - Not enough contextual information provided by security tools
- 56% - Security tools yielded too many positives
- 45% - Security tools yielded more data than can be reviewed in a timely fashion
- 28% - Behavior involved in the incident is consistent with the individual's role and responsiblities

Over all of the government and industry sources surveyed, for example, 88 percent said they recognized that the insider threat is a cause for alarm, and that the abuse will increase. At the same time, however, they said they have difficulty identifying what specific threatening action looks like. "Responders said they just don't have enough contextual information from their existing tools, which also throw up too many false positives," said Michael Crouse, Raytheon's director of insider threat strategies. "There's a real need for a different way to attack the problem." Unlike external threats, where malicious intent is assumed, the situation with insiders is more nuanced. Of those who access sensitive or confidential information that isn't necessary for their jobs, for example, survey respondents said as many as two-thirds are simply driven by curiosity. In government, you can probably add the frustration of people under increasing pressure to get the job done and who don't want to spend the time working through the red tape necessary to access information they think they need. Who hasn't asked a buddy in the office to help with that kind of thing? Other recent studies have also made the point that insider threats come from relatively innocent actions as much, or even more, than malicious events. Verizon's 2014 Data Breach Investigation Report, for example, showed that misuse by insiders could come from something as simple as sending an email to the wrong person or attaching files that shouldn't be attached. One simple move toward an answer would be for organizations to properly configure tools they do have, something Crouse said is "the easiest and most cost-effective" thing they can do. Beyond that, agencies need complementary tools, such as end-point monitoring that show how users behave when they access data through an end-point, detailing IM traffic, contextual emails and whether they are cutting and pasting information in ways they haven't previously. That's all well and good, of course, but there's a big catch. While nearly 90 percent of those surveyed in the Ponemon report said they understood the need for enhanced security, only 40 percent had any kind of a dedicated budget to spend on tools specifically aimed at insider threats. That's why most organizations — and certainly government agencies — have to limp along by trying to jerry-rig existing, and unsuitable, cybersecurity tools to do the job. One of the reasons for that budget shortfall, Crouse gamely admitted, is that companies like his have not done a good job explaining the ROI from money spent on these tools. What organizations don't understand, he said, is that while the number of actual breaches from insiders is low compared to those from external threats, the impact from those breaches is substantially higher. "I don't think they truly understand either the monetary or mission impact from these insider breaches," he said. "They're just now trying to get their heads around that." To read more click **HERE**