GW CSPRI Newsletter

August 6, 2012

From the **Cyber Security Policy and Research Institute** of **The George Washington University**, www.cspri.seas.gwu.edu.

This newsletter is a weekly summary of events related to cyber security policy and research, with a special focus on developments and events in the Washington, DC area.

Faculty and student readers of this newsletter with new and important cyber security research to report (especially new papers or results by GW faculty and students) are encouraged to send notifications of this to cspriaa@gwu.edu. A short (up to three sentences) description of why you think the research is important is required.

Contents

Events

-August 6-8, **Digital Forensic Research Workshop** - The annual Digital Forensic Research Workshop conference allows digital forensics researchers from government, industry, and academia to present their work and results to fellow researchers and practitioners. Many of the most cited digital forensics papers have been presented at DFRWS and the annual challenge has spawned research in important areas. Initial results and tool prototypes are also presented during the Works in Progress and demo sessions. Embassy Suites, 1250 22nd Street, NW. More information.

-August 7, 6:00 p.m. - 8:15 p.m., **The Ethics of E-Mail and Social Media** - The DC Bar Association will host a presentation. The speaker will be Thomas Spahn of McGuire Woods. DC Bar Conference Center, 1101 K St., NW. More information.

-August 9, 6:30 p.m. - 8:30 p.m., **OWASP NoVA Meetup** - Open Web Application Security Project (OWASP) is an open-source Web application security project. Velocity 5, 5825 Trinity Parkway, Centreville, VA. More information.

-August 13, 5:30 p.m. - 8:30 p.m., **NoVA Hackers Association Meetup** - This Northern Virginia area/ DC area infosec group will host a dinner meetup at QinetiQ, 11091 Sunset Hills Road, Reston, VA. More information.

-August 14-16, **TechNet Land Forces East: Cyber** - The operational theme, "Cyberspace Operations - Prevent, Shape, and Win" will highlight the operational security focus of DoD and Industry Networks, and Cyber Operations with Joint and Coalition partners, to prevent, shape, and win future cyber conflicts. Government, industry, and academia leaders will address a broad range of topics and focus on the opportunities for Cyber Superiority. Baltimore Convention Center, 1 West Pratt Street, Baltimore, Md. More information.

Legislative Lowdown

-The Cybersecurity Act, a measure designed to help shore up digital and information security at some of the nation's most vital networks, failed to gain the necessary 60 votes for passage in a floor vote on the measure last week, all but killing any legislative action on cybersecurity this year and punting efforts to 2013, The Hill reports. The Cybersecurity Act, introduced by Sens. Joe Lieberman (I-Conn.) and Susan Collins (R-Maine), was rejected on a 52-46 vote — 60 votes were required to move forward with the legislation. The Act would have increased cyber protections for the nation's electrical grid, financial networks, transportation system and other critical infrastructure. Senate Majority Leader Harry Reid (D-Nev.) said the bill was critical for the nation’s security, but the powerful U.S. Chamber of Commerce objected to the bill.

The bill may have one bleak hope: The White House hasn't ruled out issuing an executive order to strengthen the nation's defenses against cyber attacks if Congress refuses to act. "In the wake of Congressional inaction and Republican stall tactics, unfortunately, we will continue to be hamstrung by outdated and inadequate statutory authorities that the legislation would have fixed," White House Press Secretary Jay Carney told The Hill in an emailed response to whether the president is considering a cybersecurity order.

-Police would be required to get a warrant to use drones for certain types of surveillance under legislation introduced on Capitol Hill on Wednesday. The Huffington Post notes that the proposed bill would also tighten regulations on what kind of data can be collected by the government and private companies and how it can be used. The proposed legislation is the latest measure introduced by lawmakers in both parties who are concerned about the coming proliferation of drones and who want more transparency about the government's use of such devices.

Cyber Security Policy News

-The Federal Trade Commission on Wednesday proposed stricter online privacy guidelines aimed at making mobile devices safer for children to use and at barring third-party advertising networks and websites from collecting information on children without their parents' consent, USA Today reports. The proposal is the latest update to the Children's Online Privacy Protection

Act of 1998, which details the measures that websites must take to protect those under age 13. Congress passed COPPA long before the era of mobile devices and popular mobile apps, such as Angry Birds. Now, the FTC is making sure newer technologies comply with the legislation's intent. The FTC proposal seeks to clarify that an ad network or plug-in, such as a Facebook's "Like" button, and smartphone app makers must have parental consent before data can be collected about children under age 13.

-A security researcher who spent 18 months cataloging and tracking malicious software developed and deployed specifically for spying on governments, activists and industry executives says the complexity and scope of these cyberspy networks now rivals many large conventional cybercrime operations. KrebsOnSecurity.com writes about research from Joe Stewart, senior director of malware research at Atlanta-based Dell SecureWorks, who said he's tracked more than 200 unique families of custom malware used in cyber-espionage campaigns. He also uncovered some 1,100 website names registered by cyberspies for hosting networks used to control the malware, or for "spear phishing," highly targeted emails that spread the malware. Once you get past all the technical misdirection built into the malware networks by its architects, Stewart said, the infrastructure that frames these spy machines generally points in one of two directions: one group's infrastructure points back to Shanghai, the other to Beijing. "There have to be hundreds of people involved, just to maintain this amount of infrastructure and this much activity and this many spear phishes, collecting so many documents, and writing this much malware," Stewart said.

The research comes on the heels of a lengthy investigation by Bloomberg News about the breadth of the cyber espionage campaigns being attributed to Chinese hacking groups. The methods behind China-based looting of technology and data -- and most of the victims -- have remained for more than a decade in the murky world of hackers and spies, fully known in the U.S. only to a small community of investigators with classified clearances. "Until we can have this conversation in a transparent way, we are going to be hard pressed to solve the problem," said Amit Yoran, former National Cyber Security Division director at the Department of Homeland Security.

-The Social Security numbers and bank routing numbers of about 8,000 accounts were exposed in a cyber breach of an Environmental Protection Agency database, Federal News Radio reports. The breach occurred in March and affected 5,100 current employees and 2,700 "other individuals," according to an EPA statement. In total, EPA has about 18,000 employees. EPA is offering free credit monitoring for one year and set up a hotline for the affected individuals to call.

The Cyber Security Policy and Research Institute (CSPRI) is a center for GW and the Washington area to promote technical research and policy analysis of problems that have a significant computer security and information assurance component. More information is available at our website, http://www.cspri.seas.gwu.edu.