THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE
Thoughtful Analysis of Cyber Security Issues

GW CSPRI Newsletter

April 18, 2011

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

Upcoming Events

-Apr. 19, 9:00 - 10:45 a.m., **Release of In the Dark: Crucial Industries Confront Cyberattacks** - McAfee will release the findings of a follow up report on cybersecurity for critical infrastructure worldwide, conducted by the Center for Strategic and International Studies. National Press Club, Holeman Lounge, 529 14th Street, NW. More information.

-Apr. 19, **Stuxnet Redux: Malware Attribution & Lessons Learned** - Stuxnet has dominated much of the information security media since its public acknowledgment in June 2010. Multiple schools of thought have emerged, casting speculation over the identities of those responsible for the authorship and operalization of what some suggest is the most advanced piece of malware observed in the public domain. Nation-state? Organized crime? Disgruntled vendor employee? This talk will take a close look at what

we really know about this mysterious culmination of bits, closely analyzing some of the popular hypotheses, and identify others which have perhaps not drawn as much momentum. Conference Center at the Maritime Institute, 692 Maritime Blvd., Linthicum, Md. More information.

-Apr. 19, **Why Online Criminals "Like" Social Networks: Financial Crimes Within Social Networking, and Associated e-Discovery Issues** - The themes for this event will be social networks, their influence on and facilitation of crime and investigation, and the associated E-Discovery issues which emerge. The featured keynote speaker is Magistrate District Judge John M. Facciola, D.C. District Court. Waterview Conference Center, 1919 N. Lynn St, Arlington, Va. More information.

-Apr. 20, 2:00 p.m., **Cyber Espionage and State of the Art Defensive Technology** - This free, virtual event features presentations from Chenxi Wang, Vice President and Principal Analyst of Forrester, and Eddie Schwartz, Chief Security Officer of NetWitness. The two will discuss the concepts of cyber adversaries and real-time security defenses through new approaches to network monitoring and advanced threat analytics. More information.

-Apr. 20, 11:30 a.m. - 1:45 p.m., **The Importance and Impact of NSA and Cyber Command's Mission to Protect America -** Baltimore-Washington Corridor Chamber of Commerce annual meeting features a discussion with Chris Inglis, deputy director of the National Security Agency. Four Points by Sheraton BWI Airport Hotel, 7032 Elm Road, Linthicum. Registration and more information.

-Apr. 20, 2:00 p.m., **Beyond Cybersecurity: Managing Security Threats Across Your Entire Agency.** This free Webinar will cover steps to reduce the complexity, cost, and risk in security infrastructure, defend IT resource investments, protect agency data, and maintain continuity of operations. Speakers include Chris Whitener, chief security strategist at Hewlett-Packard, and Malcolm Harkins, chief information security officer, Intel Corp. More information.

-Apr. 27, 9:00 a.m. - 1:00 p.m., **Social Networking, Cloud Computing, Hacking Mitigation to Address Threats to Your Business and Personal Data** - The Washington County Chamber of Commerce and Rep. Roscoe G. Bartlett (R-Dist. 6) hold a cybersecurity seminar and expo. Hagerstown Community College, 11400 Robinwood Drive. Free. Registration: 301-694-3030 or bartlett.house.gov.

Publications

Several new reports are out from CSPRI this week, based on lectures given earlier this year by GWU faculty, including:

-The Mess We're in: And Why It's Going to Get Worse (PDF) - This publication, authored by GWU's **Julie J.C.H. Ryan**, offers a high-level look at the major challenges facing cybersecurity defenders, network architects and engineers, and policymakers.

-Security and Privacy: Clinical Case Studies (PDF) - **Dr. Neal Sikka**, of the GW School of Medicine and Health Sciences, examines case studies that highlight the dual challenges for medical practitioners of balancing the security and privacy of patient data.

-Investigating Cyber Security Threats: Exploring National Security and Law Enforcement Perspectives - **Frederic Lemieux**, associate professor of GWU's Department of Sociology, focuses on how federal agencies define success in computer crime investigations and how they can facilitate the development and refinement of a comprehensive law enforcement strategy for addressing cyber threats.

Legislative Lowdown

-Sens. **John Kerry** (D-Mass.), and **John McCain** (R-Ariz.) introduced legislation designed to give consumers more control over what information about them is collected online, but privacy advocates say the bill will do little to curb wide-spread data-collection practices now in place, writes Computerworld. The Commercial Privacy Bill of Rights Act (PDF) would require Web-based businesses to collect only as much information as necessary to complete a transaction or deliver a service, and it would require collectors to take security measures to protect the data. The legislation was well received by several groups, including the Information Technology and Innovation Foundation, which said the bill provides "a co-regulatory framework that allows industry to partner with government to potentially create more flexible rules for businesses that could help reduce the negative impact on the Internet ecosystem." But some consumer groups, like Consumer Watchdog and the Center for Digital Democracy, said the bill doesn't go far enough. Both groups said they couldn't support the bill because it would take away some policy-making authority from the U.S. Federal Trade Commission and would take away the right of consumers to file lawsuits against companies for privacy violations.

A senator who has been active in the area of cybersecurity said Monday that he is optimistic that Congress will be able to complete negotiations with the White House and pass a major cyber bill by the end of this year. A holdup in that process, **Sen. Sheldon Whitehouse** (D-R.I) has said, was an internal, interagency review process intended to identify areas of law in need of modification in the cyber arena. Whitehouse, who chaired a classified six-month review of cyber policy for the Intelligence Committee last year, has been critical of the administration's pace in proposing a plan to Congress, saying that lawmakers could not coalesce around cyber legislation without knowing precisely where the administration stood on the issues. But in testimony before the Senate Judiciary Committee last week, Cameron Kerry, the Commerce Department's general counsel, told Whitehouse that the administration was "a matter of some weeks away from being able to share some proposals with Congress."

Cyber Security Policy News

-The FBI last week shut down three of the largest poker Web sites in what appears to be the largest crackdown on Internet gambling to date. Federal officials also charged 11 executives at **PokerStars**, **FullTiltPoker** and **Absolute Poker** with bank fraud, money laundering and illegal gambling offenses. Prosecutors have shut down the sites and are seeking to recover $3 billion from the companies. "In their zeal to circumvent the gambling laws, the defendants also engaged in massive money laundering and bank fraud. Foreign firms that choose to operate in the United States are not free to flout the laws they don't like simply because they can't bear to be parted from their profits," U.S. Attorney for Manhattan **Preet Bharara** said in a statement. The Financial Times writes that after Congress passed laws in October 2006 banning online gambling transactions, operators fled the US and regrouped in Europe, where laws on online gambling were at the time opaque. PokerStars and Full Tilt, which continued to take US customers after the 2006 exodus, have in recent years moved into the regulated market that was beginning to take shape in Europe, advertising in jurisdictions such as the UK.

-A lengthy report from Reuters delves deep in to the growing cyber conflicts between the United States and China over the past few years. The story, which draws upon access to several confidential State Department cables obtained by **Wikileaks** and made available to Reuters, suggests that as America and China grow more economically and financially intertwined, the two nations have also stepped up spying on each other. "Today, most of that is done electronically, with computers rather than listening devices in chandeliers or human moles in tuxedos," reporters Brian Grow and Mark Hosenball wrote. "And at the moment, many experts believe China may have gained the upper hand."

-The U.S. Justice Department and the FBI were granted unprecedented authority this week to seize control over "Coreflood," a criminal botnet that enslaved millions of computers and to use that power to disable the malicious software on infected PCs. On April 11, 2011, the U.S. Attorney's Office for the District of Connecticut filed a civil complaint (PDF) against 13 unknown ("John Doe") defendants responsible for running Coreflood, and was granted authority to seize 29 domain names used to control the daily operations of the botnet. The government also was awarded a temporary restraining order (PDF) allowing it to send individual PCs infected with Coreflood a command telling the machines to stop the bot software from running. No U.S. law enforcement authority has ever sought to commandeer a botnet using such an approach.

-While US law requires reporting of requests to intercept communications data in real-time, no such requirement exists for requests for stored communications data, new research suggests. **Christopher Soghoian**, a doctoral candidate at the School of Informatics and Computing at Indiana University, found that law enforcement agencies have made tens of thousands of requests for stored data from companies like AOL and Facebook. Soghoian discovered that not only is it easier for law enforcement to get their hands on the information once it has become stored communication, but it's also more cost-effective for law enforcement agencies this way. "Cox Communications, a major

U.S. service provider, charges $3,500 for a wiretap and $2,500 for a pen register. Account information, however, costs a mere $40," Soghoian wrote in a newly-published paper.

-The White House proposed last week a single, secure online identification system, Bloomberg reports. The proposal, titled National Strategy for Trusted Identities in Cyberspace (PDF), charts a course for the public and private sectors to collaborate to raise the level of trust" connected to online identities. At a news conference announcing the strategy, **Commerce Secretary Gary Locke** said the administration will play a supporting role and let the private sector take the lead in developing and operating the voluntary network. Bloomberg notes that a $24.5 million Commerce Department allocation in fiscal 2012 goes toward the development of a network of credentials that would allow consumers to prove their identities while conducting online transactions.

-Under a White House plan, the Homeland Security Department will have far-reaching oversight over all civilian agency computer networks, according to a draft copy of a legislative proposal viewed by FederalNewsRadio. The proposal would codify much of the administration's memo from July 2010 expanding DHS's cyber responsibilities for civilian networks, but the White House is taking those responsibilities further, the publication said. "The administration drafted a legislative proposal to give DHS many, if not all, of the same authorities for the .gov networks that the Defense Department has for the .mil networks," FNR Executive Editor Jason Miller wrote.

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.