Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

The Weekly Newsletter of The George Washington University Cyber Security Policy and Research Institute

In This Issue

Quick Links

Vacation Notice

CSPRI will not publish a newsletter on December 22 orDecember 29 of this year.

Enjoy the holiday season!

December 8, 2014

Six (6) Cyber security Events are scheduled in the Greater Washington Area in the next few weeks.

Event Announcement

STUDENTS: Apply now for full scholarships in Cybersecurity! Deadline January 31, 2015. Details[here.](#)

Legislative Lowdown

-Sen. Ron Wyden (D-Ore.) introduced a bill last week that would bar the government from requiring that tech companies guarantee access to their software and electronics. "Lawmakers and privacy advocates have criticized reports that intelligence agencies are intentionally introducing security weaknesses into devices so they can

Events

Click [here](#) for descriptions of the upcoming events!

Click the Calendar to See Upcoming Events at a Glance!

Follow Us

Follow us on Twitter: @gwCSPRI

Follow CSPRI Director, Lance Hoffman: @lancehoffman1

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

CSPRI in the News

-**CSPRI Director Dr. Lance Hoffman** was interviewed by the Voice of America TV on the occasion of the visit of Minister Lu Wei, Head of the Cyberspace Administration of the People's Republic of China on December 2.

-**CSPRI Research Scientist Dr. Allan Friedman** has made a variety of appearance in the last few weeks:

Radio New Zealand here.

Washington Post Blog here.

GovInfo Security here.

Chicago Law Bulletin here.

eavesdrop," writes Cory Bennett for The Hill. "The law does not apply to modern mobile devices, allowing companies like Apple and Google to introduce encryption on smartphones they claim keeps the government out - warrant or not."

According to the National Journal, a similar bill was offered Rep. Zoe Lofgren (D-Calif.) in the House. "The measure, dubbed the Secure Data Act and spearheaded by Democratic Rep. Zoe Lofgren, would block the NSA and other intelligence agencies from compelling tech companies to create so-called backdoor vulnerabilities into their devices or software," writes Dustin Volz. "Sen. Ron Wyden, also a Democrat, introduced a similar version of the bill earlier Thursday.

The Hill's Bennett has another story about one piece of cyber legislation that stands a chance of passage this Congress: the National Cybersecurity and Critical Infrastructure Protection Act, a bill that would codify the DHS's cybersecurity role and officially authorize the agency's existing cybersecurity center. "House Homeland Security Committee Chairman Michael McCaul (R-Texas) is expecting the Senate to release as early as Thursday his bill to enable private companies to share cybersecurity information with the Homeland Security Department (DHS)," Bennett writes.

Cyber Security Policy News

North Korea denies involvement in Sony hack
-North Korea has denied any involvement in the massive new hack of Sony Pictures Entertainment, which reportedly exposed more than 100 terabytes of proprietary Sony data. Early analysis of the malware used in the attack pinned the blame on North Korea, and experts said the intrusion was payback for a Sony comedy film to be released on Christmas called The Interview, in which the stars are filmmakers on a trip to North Korean who are recruited by the CIA in a plot to assassinate the country's leader.

Meanwhile, the attackers released tens of thousands of internal Sony documents, including employee salary and healthcare records.

Publicly traded companies exposed
-A group of cyberspies have broken into more than 100 publicly traded companies and stolen crucial corporate information, CNN reports, citing data gathered from security firm FireEye. "The highly sophisticated hackers uncovered merger discussions, secret product pipelines and potential legal troubles, which would give them a big leg up when trading those companies' shares," David

Follow CSPRI Research Scientist, Allan Friedman: @allanfriedman

Goldman writes. "More than two-thirds of the group's targets were in the health care and pharmaceutical industries. All but three of the targeted companies are listed on the New York Stock Exchange or Nasdaq."

Banks to block Tor?

-Banks across the United States could block a great deal of fraudulent activity and account takeovers online if they barred users who attempt to transact with their sites using the global anonymity network known as Tor, KrebsOnSecurity.com reports. "In the report, released on Dec. 2, 2014, FinCEN said it examined some 6,048 suspicious activity reports (SARs) filed by banks between August 2001 and July 2014, searching the reports for those involving one of more than 6,000 known Tor network nodes," Krebs writes of a non-public report produced by a division of the U.S. Treasury Department. "Investigators found 975 hits corresponding to reports totaling nearly $24 million in likely fraudulent activity. Analysis of these documents found that few filers were aware of the connection to Tor, that the bulk of these filings were related to cybercrime, and that Tor related filings were rapidly rising. Our BSA [Bank Secrecy Act] analysis of 6,048 IP addresses associated with the Tor darknet found that in the majority of the SAR filings, the underlying suspicious activity - most frequently account takeovers - might have been prevented if the filing institution had been aware that their network was being accessed via Tor IP addresses."

Justice Department to create cybersecurity unit

-In the wake of massive hacks like the one at Sony, the Justice Department plans to create a special, dedicated unit for cybersecurity, officials announced last week. Although the DOJ already has a Computer Crime and Intellectual Property Section, this new arm would be a more tightly focused effort. NBC reports that Assistant Attorney General Leslie Caldwell cited recent cyberattacks such as retail and bank hacks, as well as the Cryptolocker malware that held files for ransom, as examples of the type of crime that would be targeted by the Cybersecurity Unit. According to The Wall Street Journal, the unit also will serve as a central hub for law enforcement officials on legal guidance regarding the criminal electronic surveillance statutes that cover complex cyber investigations.

Obama to nominate Carter

-President Obama's choice to lead the Pentagon, former deputy secretary of defense Ashton "Ash" Carter, has long been a big supporter of increasing the country's cybersecurity capabilities, The Washington Postreports. "His nomination

signals that the administration is likely to continue to aggressively build out its ability to fight adversaries in the digital world. Carter has reportedly been influential in the reorganization of U.S. Cyber Command over the last few years.

About this Newsletter

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. It is published by the Cyber Security Policy and Research Institute (CSPRI) of the George Washington University. CSPRI is a center for GW and the Washington area that promotes technical research and policy analysis of topics in or related to cybersecurity. More information is available at our website, http://www.cspri.seas.gwu.edu

CSPRI

202 994 5613. cspri@gwu.edu
304 Staughton Hall
707 22nd St., NW
Washington DC, DC 20052