Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

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

Quick Links

About CSPRI

Contact Us

Newsletter Archive

Blog: The CSPRI Byte

New Publications from CSPRI Researchers

CSPRI researchers Paul Rosenzweig and Trey Herr have an article forthcoming in the Georgetown Journal of National Security Law & Policy which outlines a definition of cyber weapons and tests it against US export control law, the Export Administration Regulation (EAR) and International Traffic in Arms Regulations (ITAR).

They find that while a technically grounded, and modular, definition is possible, only certain components of these weapons would fall under existing US law. You can find the full paper **here.**

March 2, 2015

Thirteen (13) Cyber security events are scheduled in the Greater Washington Area in the next few weeks.

New Blog Piece

CSPRI Senior Research Associate, Trey Herr discusses milware in the latest CSPRI blog post.

Click **here** for the post.

Legislative Lowdown

-The Obama administration's proposal for a Privacy Bill of Rights for Americans is getting a chilly reception from privacy groups and the tech industry, according to the National Journal. "The White House unveiled an ambitious legislative proposal Friday to restrict how companies, including Web giants like Facebook and Google, can handle private information, and it was promptly denounced by industry groups and privacy advocates alike. "Tech companies warned that the so-called "Consumer Privacy Bill of Rights Act" would impose burdensome regulations, potentially stifling exciting new online services that could benefit consumers. Privacy advocates claimed the bill is riddled with loopholes and would essentially let companies write their own rules." Read more.

Events

See Upcoming Events at a Glance

Click here for detailed descriptions

Follow Us

Follow us on Twitter: @gwCSPRI

Follow CSPRI Director, Lance Hoffman: @lancehoffman1

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

-A bill that would beef up email privacy and set limits on the government's access to content stored overseas gained support from two House members Friday. The measure is a companion bill to a measure introduced in the Senate by Sen. Orrin Hatch (R-UT). "A spate of privacy bills have been introduced early this Congress to require law enforcement to obtain a warrant when obtaining users' emails or other communication stored in the cloud," writes Mario Trujillo for The Hill. "Currently, only a subpoena is required when obtaining records more than 180 days old. The 'Email Privacy Act' introduced at the beginning of the month boasts the support of 245 House lawmakers and had broad approval in the Senate, But Hatch's bill, and the companion legislation introduced Friday, would also place restrictions on what kind of information the government can force a U.S. company to hand over when that data is stored overseas."

Cyber Security Policy News

Gemalto update

Gemalto, the cellphone chipmaker that U.S. and United Kingdom spies reportedly hacked, has confirmed the intrusion, but says its valuable encryption data was not stolen. The company makes SIM cards used in cellphones and credit cards. Last month it was forced to respond to leaks from NSA whistleblower Edward Snowden, which revealed that an operation by the U.S. National Security Agency and its British counterpart Government Communications Headquarters had had broken into Dutch company Gemalto to steal data that allowed the agencies to decrypt cellphone communications. The operation was reported last week on the website The Intercept using documents supplied by Edward Snowden, USA Today Jane Onyanga-Omara writes for USA Today. "Gemalto, which supplies major cellphone operators including AT&T, T-Mobile, Verizon and Sprint, says the attacks in 2010 and 2011 'only breached its office networks and could not have resulted in a massive theft of SIM encryption keys.'"

DoJ offers reward for help in catching cybercriminals

-The Justice Department last week announced a reward of up to $3 million leading to the arrest and/or conviction of the alleged leader of "a tightly knit gang of cybercriminals" who developed the Gameover ZeuS botnet. Ars Technica reportsthat authorities are offering the reward for Evgeniy Mikhailovich Bogachev, accused of various charges in connection to the botnet. The authorities said the botnet infected more than 1 million computers and resulted in $100 million in losses.

Anthem breached

-Anthem said last week it appears that some 78.8 million consumers were affected by the cybersecurity breach discovered last month. The company had

previously estimated about 80 million people would be impacted. The FBI says it is close to finding out who was responsible for the intrusion, which exposed Social Security numbers and other personal data. "Federal Bureau of Investigation officials are still deciding whether to publicly reveal information about the attackers in one of the biggest thefts of medical-related customer data in U.S. history," Bloomberg reports. "Agency officials don't want to compromise investigations or operations by any disclosures."

Meanwhile, it appears the Anthem hack ensnared even federal employees who weren't Anthem customers. Some of the uncertainty can be chalked up to incomplete records on about 14 million federal or nonfederal individuals, NextGov writes. "Despite our best efforts to attribute all members to a group, product or plan, a subset of unknown members still exists," the publication quoted Anthem spokeswoman Leslie Porras saying in an emailed statement. "According to the Blue Cross and Blue Shield website, as of October 2014, the BCBS Federal Employee Program Benefit Plan, or FEP, covered more than 5.3 million individuals, including Anthem federal plan members."

China tries to boost its domestic tech industry

-In a move seen as a way to help China jump-start its domestic tech industry, Cisco, Apple, McAfee, and Citrix have all been dropped from China's official list of approved products. BBC reports that the new policy means the companies' products have been removed from a list used by government departments to outfit offices and data centers. "Instead of the US tech firms, the approved list now recommends home-grown alternatives including Huawei and ZTE," BBC writes. "Router maker Cisco is one of the biggest losers in the purge. In 2012, the hi-tech firm had about 60 separate products on the Central Government Procurement Centre's list. Now, it has none.

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

Tompkins Hall, Suite 106

725 23rd Street NW

Washington DC, DC 20052