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

Follow Us

Follow us on Twitter:
@gwCSPRI

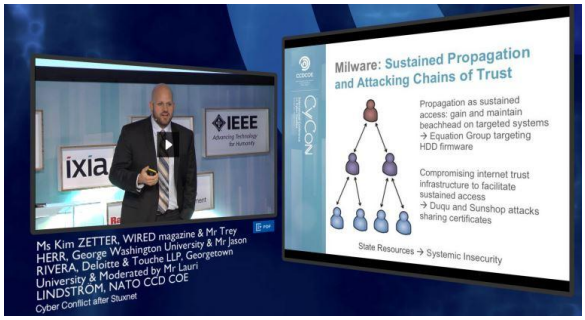
Follow CSPRI Director, Lance Hoffman:
@lancehoffman1

Follow CSPRI Associate Director, Costis Toregas:
@DrCostisToregas

October 13, 2015

Eleven (11) events scheduled in the Greater Washington Area in the next few weeks.

Trey Herr at CyCon



Trey Herr, a Senior Research Associate at CSPRI, presented at the NATO CCDCOE CyCon 2015 (7th International Conference on Cyber Conflict) on May 26 - 29, 2015 (videos were just released). He discussed Stuxnet and the rise of milware.

Click through to find videos from 27.05.15 in Room 1 of the conference. There you can find Trey's presentation on Milware and a panel with Kim Zetter and Jason Rivera on Cyber Conflict After Stuxnet.

The link for the videos can be found **here.**

Events

October 13-14
Computers, Freedom, and Privacy 2015

October 14
National Cybersecurity Policy Forum

October 14
ISACA CM Meetup

October 14
CyberIA Project Virtual Industry Meeting

October 15
ISSA NoVa Meetup: Trends in DDoS Attacks

October 15
Fall 2015 Cybersecurity Summit

October 15
Overcome by Cyber Risks?

October 15
NASA Goddard Cyber Expo

October 16-18
BSides DC

Legislative Lowdown

-California last week enacted its own email privacy law, according to The Hill. "Gov. Edmund 'Jerry' Brown (D) signed the California Electronic Communications Privacy Act, which passed out of the state assembly last month," writes Mario Trujillo. "The bill, requiring law enforcement to obtain a search warrant to access certain electronic communication, was approved alongside dozens of other bills. Advocates say the state law will require law enforcement in the state to obtain a warrant to force online providers from accessing Californians' emails, texts and geographical location data. They say it will apply to a person's own device and 'the online services that store your data,' with some emergency exceptions."

Cyber Security Policy News

Laws on online privacy: update
-Consumer advocacy groups are using the demise of a U.S.-E.U. data-sharing agreement to call for new laws governing online privacy. According to DailyDot, the European Court of Justice struck down the Safe Harbor agreement last week, "after determining that U.S. mass-surveillance programs prevented American companies from complying with European data-privacy regulations," writes Eric Geller. "U.S. businesses that operate in Europe are scrambling to develop new arrangements for transmitting data stored in Europe back to the United States. Some have already built European data centers to eliminate the need for information transfers."

Meanwhile, Bloomberg reports that technology and privacy advocates alike are praising the Obama administration's decision not to seek new laws guaranteeing government access to encrypted information on mobile phones, computers and other devices - even as companies know the U.S. hasn't given up on getting the data. Read more here.

DoD mandates reporting of cyber incidents by contractors
The Department of Defense announced a mandate last week requiring contractors to "rapidly report cyber incidents" involving sensitive information, NBC News reports.
The new rule comes months after a security breach at the Office of Personnel Management exposed the personal data of around 21.5 million people.

US Postal email scheme: update
-Months after a suspected malicious email attack breached U.S. Postal Service personnel data, a quarter of agency employees fell for a simulated email scheme, according to NextGov. "As previously reported, unknown hackers accessed the Social

Conference

October 17 - 21
CSX North America

October 20
Government Cybersecurity Forum

Click here for detailed descriptions

Security numbers of about 800,000 USPS employees, along with medical information on 485,000 personnel from workers' compensation claims, in September 2014," writes Aliya Sternstein.

Chinese government arrests hackers

-The Washington Post reports that the Chinese government has quietly arrested a handful of hackers at the urging of the U.S. government - in what's being billed as "an unprecedented step to defuse tensions with Washington at a time when the Obama administration has threatened economic sanctions. But security journalist Brian Krebs reports that this is actually not the first time the Chinese government has arrested alleged cybercriminals in China at the behest of the U.S. In a report (PDF) presented to Congress on Feb. 29, 2012, theOffice of Inspector General for the National Aeronautics and Space Administration (NASA) noted that a lengthy investigation into the cyber theft of sensitive technical data from its systems culminated in the arrest of a Chinese national in China. Read more here.

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