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

About CSPRI

Contact Us

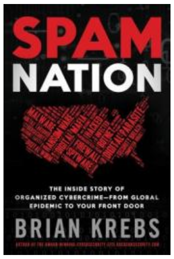
Newsletter Archive

Blog: The CSPRI Byte

Book Signing

Politics and Prose Bookstore

Thursday, December 4, 2014 at 7 p.m.



SPAM
NATION
THE INSIDE STORY OF ORGANIZED CYBERCRIME—FROM GLOBAL EPIDEMIC TO YOUR FRONT DOOR
BRIAN KREBS

December 1, 2014

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

Event Announcement

Cyber Monday 2014 is Cybersecurity Mondayin Washington. Followed immediately by Cybersecurity Tuesday.

Cyber Monday may be a term created by marketeers to encourage online shopping, but this year at least, it offers some wonderful opportunities to hear from leaders in cybersecurity and privacy and to make your own assessments about what the future will look like.

There are at least two important events on **Monday, December 1 and two more on Tuesday,December 2 in Washington.**

Click here for all the events and details!

Legislative Lowdown

Patriot Act potentially under fire?
-Congress failed to pass legislation last month that would have curbed the National Security Agency's domestic surveillance activities, but privacy advocates see another opening, according to The National Journal. Some are

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

Follow CSPRI Research Scientist, Allan Friedman:
@allanfriedman

Brian Krebs - Spam Nation: The Inside Story of Organized Cybercrime-From Global Epidemic to Your Front Door

CSPRI has worked with Brian Krebs for a number of years, and is happy to note this book signing event for his new book, Spam Nation. Details arehere.

looking to the expiration of provisions in the USA Patriot Act as a way to achieve some of their goals. "Some argue that their best shot to curb the National Security Agency's powers will be to kill core provisions of the USA Patriot Act altogether," wrote Brendan Sasso and Dustin Volz. "But other reformers aren't ready to take the post-9/11 law hostage. The debate over whether to let the Patriot Act provisions expire in June threatens to splinter the surveillance-reform coalition. If the tech industry, privacy groups, and reform-minded lawmakers can't coalesce around a strategy soon, they may have little hope of reining in the surveillance state." Read more here.

Cyber Security Policy News

The EU and the Right to be Forgotten
- European privacy regulators last week called for Google to give Web users the power to have Google take down links to embarrassing or outdated content throughout the world, The Hill reports. "The new guidelines are not binding, but they nonetheless increase pressure on Google and are sure to meet heavy opposition from transparency advocates," writes Julian Hattem. In May, the European Court of Justice ordered Google to remove links "inadequate, irrelevant or no longer relevant" websites, out of concern for people's privacy, Hattem notes. "The ruling cemented what has become known as the 'Right to be Forgotten.' The links have so far only taken down on European versions of its search engine, however, such as France's google.fr or Spain's google.es. The European panel would expand that so that google.com is caught up in the practice."

Malware alert: Regin
-Researchers have unearthed highly advanced malware they believe was developed by a wealthy nation-state to spy on a wide range of international targets in diverse industries, including hospitality, energy, airline, and research, according to Ars Technica and a host of other tech publications. "Backdoor Regin, as researchers at security firm Symantec are referring to the trojan, bears some resemblance to previously discovered state-sponsored malware, including the espionage trojans known as Flame and Duqu, as well as Stuxnet, the computer worm and trojan that was programmed to disrupt Iran's nuclear program," writes Dan Goodin for Ars. "Regin likely required months or years to be completed and contains dozens of individual modules that allowed its operators to tailor the malware to individual targets." Symantec's detailed analysis of the malware is here.

Meanwhile, some are criticizing Symantec many other antivirus companies for yet again failing to detect malware that operated in secret for years. "Anti-virus firms have been defending the timing of their disclosure of the technical capabilities of powerful Regin espionage malware," writesMatthew Schwartz at GovInfoSecurity. "Some information security experts have criticized F-Secure, Kaspersky Lab and Symantec for not more quickly issuing public warnings about the malware, which experts say has sophisticated capabilities that rival those of Stuxnet and Flame."

US government looking for ways to get around cell phone encryption
-Apple and Google both made news recently when they announced they would encrypt customers' phones by default, with the practical effect being that the companies would no longer be able to unencrypt the phones in response to secret orders from the U.S. government to do so. But as The Wall Street Journal reports, federal prosecutors are digging up some ancient ways in a bid to sidestep this logistical speed bump. "Prosecutors last month persuaded a federal magistrate in Manhattan to order an unnamed phone maker to provide 'reasonable technical assistance' to unlock a password-protected phone that could contain evidence in a credit-card-fraud case, according to court filings," writes Danny Yadron. "The court had approved a search warrant for the phone three weeks earlier. The phone maker, its operating system and why the government has not been able to unlock it remain under seal. The little-noticed case could offer hints for the government's strategy to counter new encryption features from Apple Inc. and Google Inc."

The Hewlett Foundation: new academic initiatives
- The Hewlett Foundation recently established three academic initiatives focused on laying the cornerstone for sustainable public policy to deal with the growing cyberthreats faced by governments, businesses and individuals, reports GovInfoSecurity. "The foundation awarded $15 million each to the Massachusetts Institute of Technology, Stanford University and the University of California at Berkeley to generate a robust 'marketplace of ideas' about how best to enhance the trustworthiness of computer systems and appropriately balance rights of privacy, the need for data security, innovation and the broader public interest," writes Eric Chabrow. The full story, plus an interview with Larry Kramer, the president of the William and Flora Hewlett Foundation, is 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
304 Staughton Hall
707 22nd St., NW
Washington DC, DC 20052