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

Scholarship portal is open

The GW CyberCorps Program is accepting applications for the upcoming 2016 - 2017 academic year.

The scholarship includes fully funded tuition and fees, a living stipend, book allowance, and a professional development fund.

Completed scholarship packages are due byJanuary 31, 2016.

Click **here** for more information.

January 11, 2016

Five (5) events scheduled in the Greater Washington Area in the next few weeks.

CSPRI goes to ShmooCon

Trey Herr and Eric Armbrust of CSPRI will be presenting 'Making MIlware: An Interdisciplinary Tryst' at ShmooCon 2016.

For more, please read the paper their talk is based on.

Legislative Lowdown

-Lawmakers pushing for global cyberspace norms have scored an early win, according to The Hill. "The major cybersecurity bill that President Obama signed into law two weeks ago includes a clause requiring the State Department to publicly produce an international cyberspace policy within 90 days," writes Cory Bennett. "The edict is the product of months of cajoling from cyber-focused lawmakers on Capitol Hill, who regularly have warned that the lack of global cyberspace rules poses serious dangers." Read more here.

Events

January 12
Wassenar: Cybersecurity and Export Control

January 12
B2G & Commercial Cyber Forum: Importance of Breach Response Planning

January 14
Privacy Con

January 15 - 17
ShmooCon

January 18
ShmooCon Epilogue

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

Bennett also writes about a surveillance bill in the United Kingdom that is getting some stiff resistance from some of the biggest technology giants. "The draft measure, known as the Investigator Powers Bill, would require Internet companies to retain customers' Web activity for up to a year and compel them to help investigators access that data upon request," Bennett reports.

Cyber Security Policy News

Ukraine cyber attack: Power outage
-A cyber attack on Dec. 23 in Ukraine appears to have caused a power outage for hundreds of thousands of people there. Ars Technica reports that the outage left about half of the homes in the Ivano-Frankivsk region of Ukraine without electricity, and that local reports blamed the outage on malicious software that disconnected electrical substations. "On Monday, researchers from security firm iSIGHT Partners said they had obtained samples of the malicious code that infected at least three regional operators," wrote Dan Goodin. "They said the malware led to 'destructive events' that in turn caused the blackout. If confirmed it would be the first known instance of someone using malware to generate a power outage."

In follow-up analysis of the malware allegedly used in the attack, a central European software firm said the Ukrainian attack was broader than initially reported. "While Prykarpattyaoblenergo was the only Ukraine electric firm that reported an outage, similar malware was found in the networks of at least two other utilities," according toReuters.

Juniper software backdoor discovered
-Security experts continue to ask questions surrounding the mysterious and apparently unauthorized addition of a software "backdoor" in Internet routers made by Juniper, a software firm whose technology is run by some of the biggest tech giants. Wired.com writes that since news of the backdoor broke last month, Juniper "has refused to answer any questions about the backdoor, leaving everyone in the dark about a number of things," writes Kim Zetter. "Most importantly, Juniper hasn't explained why it included an encryption algorithm in its NetScreen software that made the unauthorized party's backdoor possible."

Microsoft takes a stance
-Microsoft Corp. said last week that it will begin telling users of its e-mail and cloud storage services whenever government-backed hackers may have targeted them. According to a blog post by Microsoft Corporate Vice President Scott Charney, the policy expands on existing procedures where Microsoft tells users if they believe an account has been targeted or compromised by a third party.

FTC on data breaches
-The Federal Trade Commission is again weighing into the debate over whether companies are doing enough to protect their customers from data breaches. GovInfoSecurity reports that last week the FTC announced a $250,000 settlement with Henry Schein Practice Solutions, a New York-based provider of practice management software for dental practices, stemming from the company's false advertising about encryption capabilities.

State lawmakers on student data
-The Washington Examiner found that state lawmakers are questioning whether limits should be placed on how much information tech giants are allowed to harvest from students. "The legislation was modeled after a California law passed in early 2014, he said. Dubbed the Student Online Personal Information Protection Act, or SOPIPA, the law prohibits companies from amassing student data and using it for commercial purposes," writes Rudy Takala. "Since California approved its legislation, the backlash has grown against companies seeking to profit off student data. That sentiment made it to Washington in early December, when the Electronic Frontier Foundation filed a complaint against Google with the Federal Trade Commission."

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