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

CSPRI in the News

CSPRI Lead Research Scientist, **Dr. Anna Slomovic** discusses fitness data collection in The New York Times.

Read the article **here.**

CSPRI Director, **Dr. Lance Hoffman** discusses data and privacy in the Washington Post.

Read the article **here.**

April 13, 2015

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

New Lead Research Scientists with CSPRI

CSPRI is proud to announce two new staff members:
Dr. Anna Slomovic and Dr. Ernest McDuffie.

For their biosketches, click **here.**

Cyber Security Policy News

Hackers undetected in unclassified White House networks
-The big cybesecurity story of last week came when it was revealed that hackers had broken into

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

unclassified networks at the White House and had been there undetected for several months. Early reports suggested Russian hackers were behind the intrusions, but Russia rejected that assertion. "It has become a kind of sport to blame everything on Russia," Kremlin spokesman Dmitry Peskov told reporters on a conference call on Wednesday. "But the key thing is that they wouldn't go searching for Russian submarines in the Potomac river, like it was the case in some other countries."

While government employees are being offered training to avoid spear-phishing attacks like the one likely used to infiltrate the White House, it's not clear that many offered are taking advantage of the instruction, reports NextGov. "After a White House hack that reportedly was instigated by a malicious email from a compromised State Department account, State in March held a phishing email workshop,"writes Aliya Sternstein. "All federal security employees were invited to participate in the 90-minute online training session. But no one from the White House watched."

China tampers with web traffic

-China has been actively diverting unencrypted Web trafficdestined for its top online search service - Baidu.com - so that some visitors from outside of the country were unwittingly enlisted in a novel and unsettling series of denial-of-service attacks aimed at sidelining sites that distribute anti-censorship tools, according to research released this week. According to independent security reporter Brian Krebs, "The findings, published in a joint paper today by researchers with University of Toronto's Citizen Lab, the International Computer Science Institute (ICSI) and the University of California, Berkeley**,**track a remarkable development in China's increasingly public display of its evolving cyber warfare prowess."

Paul promises to end NSA bulk collection if elected

-Sen. Rand Paul (R-Ky.) said he would end the National Security Agency's bulk collection of Americans' phone records on his first day in the White House, if elected. The Hill quotes the now-official candidate for president: "The president created this vast dragnet by executive order. And as president on day one, I would immediately end this unconstitutional surveillance," he said in a Kentucky speechTuesday announcing his presidential bid.

-The U.S. government started keeping secret records of Americans' international telephone calls nearly a decade before the Sept. 11 terrorist attacks, harvesting billions of calls in a program

that provided a blueprint for the far broader National Security Agency surveillance that followed, USA Today reported last week. "For more than two decades, the Justice Department and the Drug Enforcement Administration amassed logs of virtually all telephone calls from the USA to as many as 116 countries linked to drug trafficking," writes Brad Heath. "The targeted countries changed over time but included Canada, Mexico and most of Central and South America."

"Stingrays" being used without warrants

In others news of unlawful government communications intercepts, Wired reports how cops in New York used the "Stingray" spyware tool 46 times without a warrant to eavesdrop on suspected crooks. "That revelation contradicts what the county sheriff said last year when he asserted that the department only used the devices under "judicial review." "In the single case in which police sought permission from a court, they asked for a court order rather than a warrant, which carries a higher burden of proof,"writes Kim Zetter. "And in their request, they mischaracterized the true nature of the tool."

-NIST last week published the long-awaited final draft (PDF) of a publication intended to guide federal agencies on supply chain management for software and hardware. The document is intended to be a starting point for federal agencies to gain greater visibility into the supply chain practices of their IT vendors. According to Politico, this version is not significantly different from the last draft. Mainly it clarifies language such as the difference between an "acquirer" and a "supplier" and the various entities that make up the supply chain, and the degree of control that government agencies have over them.

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