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](#)

[Announcements](#)

[Cyber Security Policy News](#)

[Events](#)

Quick Links

About CSPRI

Contact Us

Newsletter Archive

Blog: The CSPRI Byte

Did you know?

Cybersecurity is increasingly seen as an interdisciplinary field.

Students of **all majors** are encouraged to apply for the CyberCorps Scholarship Program.

For more information on the program, click **here.**

January 5, 2015

Four (4) Cyber security Events are scheduled in the Greater Washington Area in the next few weeks.

Event Announcement

STUDENTS: Apply now for full scholarships in Cybersecurity! Deadline January 31, 2015. Detailshere.

CYBER CORPS THE GEORGE WASHINGTON UNIVERSITY Scientia est Potentia

Cyber Security Policy News

North Korea: Internet outages and sanctions
-A number of interesting events followed the Obama Administration blaming North Korea for the malicious attack against Sony Pictures Entertainment, in which hackers stole and leaked terabytes of sensitive, internal data from Sony computers and proceeded to wipe the computers

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

clean of all data. For starters, North Korea inexplicably went offline, twice. On Dec. 22, the North Korean internet space went offline for nearly 10 hours. Then, later in the week, another unexplained outage struck the country. North Korea blamed the United States, prompting North Korean leader Kim Jong Un to call President Obama a "monkey," Reuters reports.

-Barely a day into 2015, the United States announced new sanctions on North Korean government officials and the country's defense industry for a cyberattack against Sony. According to The Associated Press, the U.S. government insists Pyongyang was to blame despite lingering doubts by the cyber community. "The White House warned this was just the opening move in the U.S. response," writes Josh Lederman. "While the sanctions will have limited effect, as North Korea is already under tough U.S. sanctions over its nuclear program, American officials portrayed them as a swift, decisive response to North Korean behaviour they said had gone far over the line. Never before has the U.S. imposed sanctions on another nation in direct retaliation for a cyberattack on an American company."

Hacking group "Lizard Squad" interrupts PlayStation and Xbox Live

-Sony's woes didn't end with the attack on Sony Pictures. On Christmas Day, millions of people around the world who received Sony Playstation and Microsoft Xbox Live game consoles and games found themselves unable to play the games. A low-skilled, teenage hacking group calling itself the Lizard Squad took credit for the attacks, which swamped Sony and Microsoft servers with an overwhelming amount of Internet bandwidth from compromised computers and Internet servers. Two days after the attack, the group announced it was launching its own Lizard-branded attack service online that lets anyone launch crippling attacks for just a few dollars per month. Independent journalist Brian Krebs has been tracking these kids, a number of whom were arrested or questioned by authorities in Finland, the U.K. and the United States.

NSA: Update

-The National Security Agency late last year quietly released more than a decade of reports detailing surveillance activities that potentially violated U.S. citizens' privacy rights, The Hill reports. "Covering NSA activities from mid-2001 to 2013, the heavily-redacted reports document possible abuses, including instances of employees emailing classified information to unauthorized recipients or issuing 'overly broad or poorly constructed data queries that potentially targeted' Americans," writes Jesse Byrnes. "The agency, required by executive order to submit the reports to the President's Intelligence Oversight Board, posted the information publicly on Christmas Eve in response to a Freedom of Information Act request from the American Civil Liberties Union."

US Postal Service: Health data breach
-Network intruders compromised health information on current and former U.S. Postal Service employees who filed for workers' compensation, according to NextGov. "The files were accessed during a previously reported September cyber intrusion that netted the Social Security numbers of about 800,000 USPS employees," writes Aliya Sternstein. "Details of the health data breach are just now being revealed for the first time."

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