GW CSPRI Newsletter

January 23, 2012

From the **Cyber Security Policy and Research Institute** of **The George Washington University**, www.cspri.seas.gwu.edu.

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.

Faculty and student readers of this newsletter with new and important cyber security research to report (especially new papers or results by GW faculty and students) are encouraged to send notifications of this to cspriaa@gwu.edu. A short (up to three sentences) description of why you think the research is important is required.

Contents

Events

FIND OUT WHAT ALL THE FUSS IS ABOUT WITH BLACKED OUT INTERNET SITES

On Wednesday, January 25, at noon, CSPRI is sponsoring a debate on a cyber security topic that has been much in the news recently -- "Resolved: The Internet's Domain Name System (DNS) Should be Utilized to Try to Control Bad Behavior Such as Copyright and Trademark Infringement." David Sohn, Senior Policy Counsel and Director of the Center for Democracy and Technology's Project on Intellectual Property and Technology will be debating Paul Brigner, Senior VP and Chief Technology Policy Officer for the Motion Picture Association of America. Before it starts, a ten-minute warmup, "DNS addressing explained for non-techies," will be presented by Leslie Daigle, Chief Internet Technology Officer of the Internet Society. The event starts at noon and lunch will be provided at 1 p.m. to accompany a roundtable discussion. Location: GW Marvin Center, 800 21st St. NW, Room 309. More details are available here (PDF). Preregistration is requested at http://debateinternetdns.eventbrite.com.

-Jan. 25, 8:15 a.m. - 5:00 p.m., **4th Inter-agency Information Sharing Conference** - Experts discuss the challenges in implementing the President's Executive Order on information sharing

while safeguarding information through a standards-based approach. Keynote speakers include Kshemendra Paul, program manager, Information Sharing Environment; Donna Roy, Executive Director, Information Sharing Environment Office, Department of Homeland Security; Richard Soley, president and CEO, Object Management Group; and Dennis Wisnosky, CTO and chief architect, Office of the Deputy Chief Management Officer, Department of Defense. Waterford at Springfield, 6715 Commerce Street, Springfield, VA More information.

-Feb. 2, 7:30 a.m. - 9:30 a.m., **Federal Cybersecurity: What's New in 2012** - Alan Paller, director of research for the Bethesda, Md. based SANS Institute discusses federal efforts to protect the nation from cyber-attacks on civilian, military and contractor databases. Ronald Reagan Building, 1300 Pennsylvania Avenue, NW, 8th Floor (North Tower), The Rotunda. More information.

Announcements

-The Systems & Security Group at The George Washington University Computer Science Department is looking for scholars with a desire to advance the field of computer security. It has funded PhD and postdoctoral positions available starting in Fall 2012. The successful applicant will work with Prof. Michael Clarkson and the large cybersecurity community in DC to advance the state of the art in the scientific foundations of computer security. See http://faculty.cs.gwu.edu/~clarkson/positions.php for more information.

Legislative Lowdown

-In the face of a blistering public outcry, House leaders shelved a highly controversial bill designed to tackle online piracy. Representative Lamar Smith (R-Texas), chief sponsor of the Stop Online Piracy Act (SOPA), last week removed a provision from the bill that would have required Internet service providers to alter their domain name system (DNS) records to disappear sites that were deemed by the government to be illegally facilitating online piracy. Senator Patrick Leahy (D-Vt.) has removed a similar provision from the Senate version of the measure. SOPA appears to be stalled in the US House of Representatives. Representative Darrell Issa (R-Calif.), an opponent of the proposed legislation, has said that House Majority Leader Eric Cantor (R-Va.) has said that he will not bring SOPA to the floor without a consensus. According to The Hill, House Speaker John Boehner played a part in sidelining the measure for now. *(See also debate announcement at the top of this newsletter.)*

-The Senate is likely to soon consider a bill to overhaul cybersecurity. Tommy Ross, a senior aide to Senate Majorty Leader Harry Reid (D-Nev.) said last week that Reid was preparing to schedule a floor debate on measures to security the nation's digital infrastructure. It has been a hard slog to generate broad agreement on a policy area that spans numerous committee jurisdictions and raises a tangle of technical, logistical and civil-liberties questions. CIO Magazine writes that Senate staffers have been engaged in ongoing meetings with leaders in the private sector, members of the security community, public-interest groups and others as they have worked to craft a model for securing the nation's critical digital infrastructure that can

garner strong bipartisan support. The bill that comes up for debate, a composite that is likely to include elements of many of the prior bills various lawmakers have introduced and debated in committee, will be intended only as a first draft, according to Ross, who said that Reid expects an extended debate over amendments to the legislation.

Cyber Security Policy News

-Megaupload.com, a file-sharing website, was shut down as part of an alleged $175 million copyright infringement conspiracy, triggering an online protest that disrupted websites of the U.S. Justice Department and movie and music trade groups. Charges against seven individuals, Megaupload Ltd. and Vestor Ltd. were unsealed yesterday in federal court in Alexandria, Virginia, after four of the alleged conspirators were arrested in Auckland, New Zealand. Three suspects remain at large, according to the Justice Department.

So popular and widely used was the filesharing site that the shutdown caused an immediate and significant drop in global Internet traffic, according to Arbor Networks, a company that monitors large scale Internet activity. Previous work by Arbor Networks showed that content providers and hosting sites like MegaUpload are the new "Hyper Giants,'" Arbor wrote. "With enough global data, you can actually see the traffic drop when the shutdown occurs. Based strictly on the traffic rates it appears that the shutdown started just after 19:00 GMT on January 19, with traffic plummeting down over the next two hours.'"

The Megaupload takedown also prompted a major cyber attack that took out the Justice Department's Web site, among other government sites. The hacking group Anonymous took responsibility for the attack, which it called its largest ever. According to Wired.com, the attack succeeded in part because it tricked bystanders into participating. A version of Anonymous' voluntary botnet software, known as LOIC (Low Orbit Ion Canon), was modified to make it not so voluntary, drafting unwary bystanders, journalists and even members who don't support DDoS tactics into attacks on the U.S. Justice Department. The trick snagged those who happened to click on a shortened link on social-media services, expecting information on the ongoing retaliation for the U.S. Justice Department's takedown of popular file sharing site Megaupload. Instead they were greeted by a Javascript version of LOIC — already firing packets at targeted websites by the time their page was loaded.

-Facebook and security researchers last week released information about five Russian and Eastern European men thought to be responsible for developing and maintaining the Koobface worm, a pesky pieces of malware the spread by attacking users of Facebook and other social networking sites. Facebook said it was publicizing the information in the hopes that it might lead to a break in the case, or at least a disruption of the criminal gang's activity. As if to answer that request, the Koobface gang shuttered its operations shortly after the information was picked up in the news media.

-Security researchers discovered evidence of a Trojan that tries to compromise the standard authentication cards, by working its way into the card readers, Info Security Magazine reports. AlienVault said the Trojan appears to use a keylogger to steal the smart card PIN numbers in

targeted email phishing attacks, and then allows the hacker to access sensitive information remotely when the user swipes in.

-The National Security Agency has released a security enhanced version of Android. The project is designed for agencies with strict access-control policies, such as the Defense Department, according to ComputerWorld. The biggest enhancement is the ability for users to restrict the resources available to applications. In turn, this feature will help minimize the damage if the device gets hacked.

-A Pentagon pilot program that uses classified National Security Agency data to protect the computer networks of defense contractors has had some success but also has failed to meet some expectations, The Washington Post reports. The program showed that Internet carriers could be trusted to handle the NSA data, that direct government monitoring of private networks could be avoided and that the measures could be of particular benefit to companies with less mature cyber defense capabilities, according to the Carnegie Mellon University study.

The Cyber Security Policy and Research Institute (CSPRI) is a center for GW and the Washington area to promote technical research and policy analysis of problems that have a significant computer security and information assurance component. More information is available at our website, http://www.cspri.seas.gwu.edu.