
From: CyberScoop <news@cyberscoop.com>
Sent: Friday, December 9, 2016 12:04 PM
To: Haley, Nikki
Subject: Georgia's really mad at DHS

Not rendering correctly? View this email as a web page [here](#).



Right-click here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet. CyberScoop

FRIDAY

December 9, 2016

There is something fishy going on between DHS and Georgia's secretary of state. The FBI is going to need more foreign help with cyber crime. And a renowned cryptologist is going to examine a popular VPN protocol. This is CyberScoop for Friday (Are we sure? We messed this up yesterday. Yes, indeed, it's Friday), December 9.

LESS THAN PEACHY: Georgia's secretary of state has claimed the Department of Homeland Security tried to breach his office's firewall and has issued a letter to Homeland Security Secretary Jeh Johnson asking for an explanation. Brian Kemp issued a letter to Johnson on Thursday after the state's third-party cybersecurity provider detected an IP address from the agency's Southwest D.C. office trying to penetrate the state's firewall. According to the letter, the attempt was unsuccessful. Georgia was one of two states that refused cyber-hygiene support and penetration testing from DHS in the leadup to the presidential election. [Greg Otto has more](#).

HELP US, WORLD: The emergence of cybercrime as a global phenomenon is causing the FBI and Justice Department to increasingly rely on international law enforcement collaboration,

legal treaties and informal agreements in addition to cooperation from the private sector, Assistant Attorney General for the Criminal Division Leslie Caldwell described Thursday. In an effort to fight these criminals, Caldwell said the Justice Department will be pursuing new legislative remedies next year in the same vein as recent changes made to Rule 41, which became effective as of Dec. 1. These changes to Rule 41 — a mandate first designed in the scope of wiretap authorization procedures — enables investigators to secure warrants during the course of computer crime cases even while the suspect's actual location is hidden. Chris Bing [has a look](#) at Caldwell's comments.

EVENT

DATA SECURITY IN FOCUS: The need for agencies to meet regulations and fulfill unfunded mandates will continue into the next administration. Federal IT shops are going to be saddled with protecting their data, which is only going to grow in volume. During this webinar on Jan. 18, experts will explain how agencies can embrace new forms of encryption without the worry that it will break their systems. Experts from government and HPE will take a look at how format-preserving encryption can allow for agencies to conduct their work without systems slowing down or breaking altogether. [REGISTER HERE.](#)

OPEN AUDIT: OpenVPN, a wildly popular security protocol, will be audited by renowned Johns Hopkins University cryptography professor Matthew Green. Green has a long history in this field: he's on the board at the Open Crypto Audit Project, where he led the security audit of the TrueCrypt project after intense pressure following Edward Snowden's NSA revelations in 2013. He's been a part of teams that have exposed vulnerabilities in systems like E-ZPass, and he's also currently looking at closely and critically encryption in Google's Android N. Patrick O'Neill [has more](#).

TL, DR: In an op-ed for CyberScoop, Cognito partner Bob Gourley looks at the report from the president's cybersecurity commission, saying while it was a wonderful idea, no one is going to read it in its current iteration: "In its current form the president-elect and other executives have little choice but to speed read the report and hope to glean a general gist. Or maybe take a briefing from the drafters and wish them well in its execution. Which means the actions the report will drive are hard to predict." Check out [Gourley's full thoughts](#).

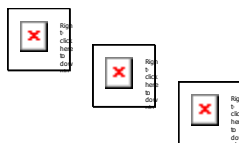
PUT THE PHONE DOWN: In another op-ed, CyberAdapt CTO Scott Millis takes a look at some steps the new administration should take to protect President-elect Trump's phone. We know Trump likes Android, which doesn't sit well with Millis: "To put it bluntly, anyone using anything but the latest version of Android should be concerned about the security of their data on that platform." [Here are his 10 steps](#) for the president-elect.

TWEET OF THE DAY



What a joyous gift for the holiday season!

In the meantime, how about tossing your favorite new website a follow on [Twitter](#) and a like on [Facebook](#)? Click those shiny social buttons below to get the best we have to offer across the social web.



This newsletter is produced by Scoop News Group.
Visit cyberscoop.com to read this newsletter on the web.

Update your [email preferences](#) to choose the types of emails you receive.
[Unsubscribe from all future emails](#)