Overnight Cybersecurity: GOP contenders threaten cyber war with China

By Cory Bennett and Katie Bo Williams - 11/12/15 06:24 PM EST

Welcome to OVERNIGHT CYBERSECURITY, your daily rundown of the biggest news in the world of hacking and data privacy. We're here to connect the dots as leaders in government, policy and industry try to counter the rise in cyber threats. What lies ahead for Congress, the administration and the latest company under siege? Whether you're a consumer, a techie or a D.C. lifer, we're here to give you ...

THE BIG STORIES:

--I'M GOING TO CUT YOUR HEART OUT WITH A SPOON: A growing number of Republican presidential candidates are calling for the United States to take offensive action against China for persistent hacking. Beijing is widely believed to be behind the theft of 21.5 million private records from the Office of Personnel Management (OPM). Meanwhile, U.S. companies claim that Chinese hackers -- backed by the government -- are pilfering trade secrets and other intellectual property to give their domestic companies an edge. Republicans running for the White House say President Obama has been too soft on China on a slew of issues, ranging from cybersecurity to currency manipulation to navigation in the South China Sea. Most candidates have used the question of how best to respond to China's digital pilfering as an opportunity to hit the Obama administration on its foreign policy approach. "[China's cyber behavior] is a very serious threat, it's an opportunity to credibly criticize the Obama administration in an area where they've not shown leadership, and it's a reasonable criticism of China," said Matt Mackowiak, a Republican strategist. To read our full piece, click **here**.

--CASH RULES EVERYTHING AROUND ME: The team behind the world's largest anonymous online network is accusing the FBI of paying security researchers at least $1 million to uncover the identities of its users as part of a sweeping criminal investigation. If true, the payment would represent a concerning collaboration that may be illegal if the FBI didn't obtain a warrant, according to the Tor Project, which oversees the online anonymity software Tor. Tor Project Director Roger Dingledine said the FBI directed researchers at Carnegie Mellon University to find out the personal details of a wide swath of Tor users. "Apparently these researchers were paid by the FBI to attack hidden services users in a broad sweep, and then sift through their data to find people whom they could accuse of crimes," Dingledine said. "There is no indication yet that they had a warrant or any institutional oversight by Carnegie Mellon's Institutional Review Board." According to multiple reports, the unmasking efforts came during the FBI's investigation into Silk Road 2.0, the major dark Web market that, like its notorious predecessor, enabled more than 100,000 people to buy and sell illegal drugs anonymously over the Internet, according to the Justice Department. To read our full piece, click **here**.

--TELL ME YOUR SECRETS: European negotiators want a new U.S.-EU data transfer pact to require U.S. businesses to report intelligence agency requests for information on European citizens, according to EU Justice Commissioner Vera Jourova. "What we wanted was to have a double check from the side of the companies themselves, which should show us at least the number of cases when the data was used or required from the national authorities," Jourova said in an interview with The Wall Street Journal published Thursday. Jourova began meetings in Washington, D.C. today with senior U.S. officials to hammer out a new agreement to replace the so-called Safe Harbor pact, which allowed U.S. companies to legally handle European citizens' data. The EU high court **struck down** the 15-year-old agreement last month over concerns that, because of U.S. surveillance practices, American companies could not be seen as adequately protecting private information. To read our full piece, click **here**.

UPDATE ON CYBER POLICY:

--THE PROFESSOR. Sen. Rand Paul (R-Ky.) said he's struggling to explain encryption standards and encryption policy to his fellow 2016 White House hopefuls, such as New Jersey Gov. Chris Christie.

During an interview with Yahoo News about technology and politics, Paul said there is a "learning problem" when trying to explain the benefits of encryption to Christie.

Paul said his White House would make sure the public continues to have access to encryption technology to prevent the government from snooping.

"Without question," Paul responded. "And then some will respond and say: 'What about terrorists? Does that mean you don't care about terrorists?' And I've tried to explain this to the governor of New Jersey on the stage, but I think I'm having a little bit of a learning problem, learning curve -- that you can use the Fourth Amendment and still get terrorists."

Read on, **here**.

LIGHTER CLICK:

--OOPSIE. Apparently Apple forgot to renew a security certificate that expired late on Wednesday, forcing some users to delete and reinstall every app they had ever bought or downloaded from App Store. Read on at The Guardian, **here**.

A FEATURE READ:

--GET IT TOGETHER. Medical devices in hospitals are incredibly vulnerable to cyberattacks, white hat hackers found when the Mayo Clinic invited them to do their worst to 40 common devices.

"Every day, it was like every device on the menu got crushed," researcher Billy Rios said. "It was all bad. Really, really bad."

The implications for patients could be dire in an industry that Rios says is 10 years behind the standard security curve.

Read on, **here**.

WHO'S IN THE SPOTLIGHT:

--THE FINANCIAL SECTOR. The United States the U.K. carried out a planned drill to test the ability of the financial sector to react in the event of a major cyberattack.

"Confronting the cyber threat is a team effort that requires coordination at all levels. Today's exercise with our U.K. partners is an important step to ensure that we are doing all we can to share threat information, adopt best practices and support our collective resiliency," U.S. Treasury Secretary Jacob Lew said in a statement.

Details of the tests were not released. Participants included the Treasury Department, White House National Security Council, Department of Homeland Security, FBI, Secret Service, the Federal Reserve and the Securities and Exchange Commission.

Read on, **here**.

A LOOK AHEAD:

FRIDAY

--Shrug. It's almost the weekend. Do you really want to do that much on Friday? Plus, there's no big cyber events anyway.

IN CASE YOU MISSED IT:

Links from our blog, The Hill, and around the Web.

Prison phone system vendor Securus is **denying** that it improperly recorded inmates' calls to their attorneys. (The Hill)

The government on Thursday **announced** it had completed a massive auction of the bitcoins it seized during the takedown of the online black market Silk Road. (The Hill)

Google will soon **warn** its Gmail users when they are receiving an email over an unencrypted connection. (The Hill)

Nearly 7 in 10 Americans **think** Hillary Clinton acted either unethically or illegally by using a private email server while secretary of State, a new poll says. (The Hill)

Microsoft will **store** data for European cloud computing customers on servers run by a German company to reassure them that their data can't be accessed by U.S. authorities. (The Hill)

The inspector general of the Office of Personnel Management **says** a $20 million sole-source contract to offer identity theft protection to millions of hacked federal employees ran afoul of contracting regulations. (Next Gov)

Customized boarding **passes** can hack computers. (Motherboard)

Computer security firm F-Secure said Thursday morning that it **has seen** email spam telling users to verify their Amazon accounts following an alleged data breach. (Motherboard)

If you'd like to receive our newsletter in your inbox, please sign up here: ***http://goo.gl/KZ0b4A***