By Joseph Marks
10/15/14 5:45 AM EDT

With help from David Perera, Tal Kopan Erin Mershon and Anila Alexander

LEADING THE MORNING: POODLE BITES INTERNET — Google disclosed a fatal flaw in widely-used website security cryptographic protocol SSL 3.0 Tuesday afternoon, dubbing the vulnerability "Poodle." The bug is so severe that Google says it will altogether abandon SSL 3.0 — one of the encryption protocols that enable the ubiquitous "Padlock-in-the-Browser" and make e-commerce possible. Poodle allows a man-in-the-middle attacker to gain control of secure online accounts by using JavaScript to exploit the way SSL 3.0 encrypts data. "To achieve secure encryption, SSL 3.0 must be avoided entirely," Google researchers said in a write up of the flaw. SSL 3.0 is nearly 15 years old and has been surpassed by better encryption protocols known as Transport Layer Security, or TLS. But Poodle is still dangerous because modern browsers are designed to be "backwards compatible," automatically downgrading from TLS to SSL 3.0 whenever they encounter a machine that still uses the older protocol. SSL 3.0 persists in part because so many people use outdated browsers and other software. Last year, according to Microsoft, 40 percent of secure web connections used SSL 3.0.

Since the man-in-the-middle attack requires the hacker to intercept a user's outgoing Web traffic, **its applicability is limited.** Anyone using unencrypted WiFi is now in grave danger, notes Errata Security's Robert Graham, but he rated Poodle's danger as half that of Heartbleed or Shellshock. CloudFlare responded to the disclosure by disabling SSL 3.0 by default across its network. Since February, Google has used a mechanism that prevents attackers from inducing browsers to use SSL 3.0, the company said in a blog post. In addition, Google will test changes to disable SSL fallback, even if "this change will break some sites and those sites will need to be updated quickly." The company hopes to remove support for SSL 3.0 completely from Google client products within the coming months, it added. The Mozilla Foundation said in a blog post that SSL 3.0 will be disabled by default in Firefox's next major upgrade, due for release Nov. 25.

The Google blog post announcing Poodle: http://bit.ly/1o9IsRs Robert Graham's blog post: http://bit.ly/1w62Q58 The CloudFlare blog post: http://bit.ly/1w7rsfH The Mozilla blog post: http://mzl.la/1DaxOwY

FIRST IN MC: RUSSIAN CYBERCRIME THRIVING, REPORT SAYS — The Russian online market for stolen credit and debit card data is estimated at $680 million a year, according to a report coming out this morning. Moscow-based security company Group IB will put out its annual report on the Russian-language cybercrime world in a few hours, but Pros get a first look. The analysis found that online carding forums are robust marketplaces — on par with any upstanding e-commerce site — where wholesalers can distribute stolen credit and debit card data to customers through automated trading platforms. On the carding platform researchers analyzed, called SWIPED, 5 million of the nearly 7 million cards came from the U.S. One hacker posted data from more than 5 million accounts — all from last year's Target breach. Check out the report: http://politico.pro/1v9IA44 And watch out for more later this morning.

HAPPY WEDNESDAY and welcome to Morning Cybersecurity, where 38 years ago today Bob Dole and Walter Mondale met for the first vice presidential debate in U.S. history. It's not the most memorable moment for either man, both of whom went on to be their party's (losing) nominee for president. But the highlights are still on YouTube: http://bit.ly/1rtNrH5 Whatever dusty video you're loading up today, drop us a line. Send your thoughts, tips and feedback this week to jmarks@politico.com and follow @talkopan, @joseph_marks_, @POLITICOPro and @MorningCybersec. Full team info is below.

MUKASEY: BUSH OFFICIALS WERE PLENTY CONCERNED ABOUT CHINA HACKING — Bush Administration officials may have been told never to publicly say "China" and "hacking" in the same sentence — but that doesn't mean they weren't talking about it behind closed doors, former Attorney General Michael Mukasey told reporters yesterday. "Everybody was aware that the Chinese were among the active hackers," Mukasey said before a dinner sponsored by the French-American Foundation. "And they still are," he added. "I don't know if they're skillful, but they're very active." Mukasey declined to opine on how the Obama Administration has handled the indictment of five members of the People's Liberation Army in May for stealing trade secrets from U.S. companies, saying he doesn't know what actions have been taken behind the scenes to follow up on the indictments. Mukasey also criticized decisions by Google and Apple to encrypt customers' smartphone content to the point even the companies can't turn data over to law enforcement in response to a court order. "I think at some point the toothpaste needs to get back in the tube," he said. "I don't know that it's in the interest of private industry to have things that can't be penetrated any more than it's in government's interest."

ICYMI: JPMORGAN: NO INCREASE IN FRAUD AFTER CYBER HACK -- JPMorgan Chase has not seen higher levels of fraud following its recent data breach, Chief Financial Officer Marianne Lake said yesterday. "We are taking every step to protect our customers and our firm," Lake said during a call with industry analysts after the bank reported its quarterly earnings. Lake added that the incident underscores the need for government and industry to work together to address the threat of cyberattacks to the financial system.

ONLINE PRIVACY: DEAD IN THE WATER, AT LEAST IN D.C. — Pro Tech's Katy Bachman takes a deep dive into online privacy today: "Washington is stalled, despite the fact that the Obama administration, the Federal Trade Commission, the Commerce Department and a host of privacy groups have sounded the alarm for years that companies know too much about every aspect of consumers' lives and have done too little to protect their privacy. A presidential push hasn't even moved the ball," she writes. But things are different in the states and overseas, Katy reports: http://politico.pro/1DakTLq

NEW .TRUST DOMAIN AIMS TO BE A SAFE HAVEN IN THE INTERNET'S WILD WEST — The information assurance company NCC Group took its first steps toward establishing an ostensible safe zone on the Internet yesterday with the publication of security requirements for its .trust domain. NCC acquired the new domain earlier this year as part of ICANN's authorization of new generic Top Level Domains. The security standards that .trust sites must adhere to run more than 100 pages. NCC Group will require applicants to prove their identities and naming rights and will undertake continuous monitoring to make sure they remain complaint. "This policy encompasses not only the best security practices but also serves as a means for companies to reclaim a corner of the Internet that will foster secure and confident engagement with like-minded businesses and customers," NCC Group CTO Gunter Ollmann said in a statement. Tal has the story: http://politico.pro/1sFmfuv

HERE'S TO HURRICANE PANDA — It's rare when an advanced persistent threat group uses a genuine zero day exploit, but that's what the China-based Hurricane Panda has been up to as it attempts to take down infrastructure companies, Crowdstrike said in a blog post yesterday that bordered on praise for the APT. The group has been using a Microsoft flaw that the company patched on Tuesday, Crowdstrike said. From the blog post: "CrowdStrike has been battling HURRICANE PANDA on a daily basis since earlier this spring, when the adversary was first detected on a victim network... Since then, they have been trying to regain access on a daily basis. These attempts begin with compromising web servers and deploying Chopper webshells and then moving laterally and escalating privileges using the newly discovered Local Privilege Escalation tool." Here's the rest: http://bit.ly/1ETQD9w

SEPULVEDA TAKES IT TO THE PEOPLE ON INTERNET GOVERNANCE – Commerce Secretary Penny Pritzker opened ICANN's 51st international meeting in Los Angeles by assuring the crowd the U.S. will not allow the internet to become a tool for national control. Now, the State Department's Ambassador to the Internet, Daniel Sepulveda, is set to deliver the same message in two public forums in as many days. Sepulveda's tour kicks off at 3 p.m. today at the Center for Strategic and International Studies. Webcast here: http://bit.ly/1rkm9Tz He'll take questions during an on-the-record roundtable at the Washington Foreign Press Center tomorrow.

THE HEALTH SECTOR DOESN'T KNOW MUCH ABOU THE NIST FRAMEWORK — Healthcare sector awareness of the NIST cybersecurity framework is "modest," says the Healthcare Information and Management Systems Society, better known as HIMSS. HIMSS IS anecdotally aware of only a few healthcare organizations implementing the framework, the organization said in a response to NIST's August RFI. NIST could improve awareness by providing a means for healthcare organizations to discuss its use, HIMSS said. Also, "We suggest that NIST consider publishing guidance on adoption and use of the Framework, tailored to the type and size of the organization," HIMSS said. The comments: http://1.usa.gov/1wDuoOY

QUICK BYTES

-- South Korea may revamp its national ID number system after a data breach left up to 80 percent of its population's ID codes susceptible to hackers. The Register: http://bit.ly/ZCINAC

-- European leaders begin debate on net security laws. The Register: http://bit.ly/1Dai1hD

-- Hacker opsec guru The Gruq is developing a secure fork of the Android operating system that will provide encrypted communications on a regular cellphone. Ars Technica: http://bit.ly/1z9JUaY

-- Cisco reports on the first day of its Internet of Things World Forum in Chicago. Cisco: http://bit.ly/1z9KiX8

-- Dropbox urges two-factor authentication after alleged hack. The Wall Street Journal: http://on.wsj.com/1se1tAF

-- A slew of security companies team up to share intel and deliver a blow to the preferred remote access Trojan of Hidden Linx APT group. Symantec: http://bit.ly/1Ci3dvg

-- The Post parses tech consequences if Republicans take the Senate. The Washington Post: http://wapo.st/1rthjDr

-- BlackBerry patched a vulnerability in its BlackBerry 10 series that could have been exploited to install malware. Threatpost: http://bit.ly/1EVhe6a

-- Social media could be a weak link in bank fraud. Reuters: http://reut.rs/1qpoCwJ

-- PLA soldiers and a bingo aficionado top the FBI's Cyber Most Wanted list. Nextgov: http://bit.ly/1EVhiCZ

FOR YOUR CALENDAR (let us know about your events at cybercalendar@politicopro.com)

All Day — The Symantec Cyber Readiness Challenge continues. http://bit.ly/1wnY6HI

8 a.m. — NCSAM hosts an event titled, "Securing Our Critical Infrastructure & The Internet of Things." San Diego, Calif. http://bit.ly/11aOc2K

8 a.m. — Gary Brown of the International Committee of the Red Cross discusses "The Law of Armed Conflict and Cyber Warfare" hosted by the American Bar Association Standing Committee on Law and National Security. The University Club. http://bit.ly/1nilSoZ

8:45 a.m. — Cisco's Internet of Things World Forum continues for its second day. Chicago. http://bit.ly/1vZlmfo

9:30 a.m. — NIST's National Cybersecurity Center of Excellence hosts its fall open house, focusing on education and workforce development. Rockville, Md. http://1.usa.gov/1vZn54p

That's all for today. Have a great Wednesday!

Stay in touch with the whole team: Tal Kopan (tkopan@politico.com, @TalKopan); Shaun Waterman (swaterman@politico.com, @WatermanReports); Joseph Marks (JMarks@politico.com, @Joseph_Marks_); and David Perera (dperera@politico.com, @daveperera).

LAST CALL FOR "WOMEN WHO RULE" AWARDS — Know a woman with entrepreneurial spirit in media, technology or business? Nominate her today for the "Women Who Rule" awards *from POLITICO, Google and the Tory Burch Foundation. Entries due Friday: http://politi.co/1oEXwD2.*

https://www.politicopro.com/tipsheet/cybersecurity/?id=9542