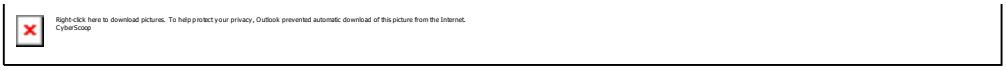
From: CyberScoop <news@cyberscoop.com>
Sent: Friday, November 4, 2016 12:13 PM
To: Haley, Nikki
Subject: The feds aren't the only ones worried about Election Day chaos

Not rendering correctly? View this email as a web page here.



FRIDAY

November 4, 2016

Both the public and private sector are preparing for chaos on Election Day. Is there anything we can learn from the latest Shadow Brokers dump? And we look at the limits of cyber insurance. This is CyberScoop for Friday, November 4.

PREPARING FOR PROBLEMS: It's not just feds that are growing increasingly worried about a cyberattack on Election Day. At least one large news company has reached out to establish relationships with officials at the Department of Homeland Security, so they know who they should contact in the event of a big internet outage or other major event on Tuesday. “I spent most of [Wednesday] visiting with DHS …. because I have this very immediate need,” David Hahn, the chief information security officer for Hearst Corporation, told the Security Innovation Network showcase in Washington Thursday. "I’ve got 33 TV stations throughout the country, 23 newspaper outlets and they’re all concerned about what the heck is gonna happen next Tuesday,” he said. Shaun Waterman looks at what's being done.

DARK WEB STING: A new global police operation against dark web marketplace users identified thousands of individuals last month, signaling unprecedented international cooperation between dozens of major law enforcement agencies across three continents. The operation was designed to spotlight law enforcement's long arm extending into the digital underground. "This is to send a message," an FBI spokesperson told CyberScoop. We're not sure if that message was well received: this was largely unnoticed when it was first made public earlier this week, due to the election-related controversies the FBI currently finds itself in. Patrick O'Neill can catch you up.

WHAT WE'RE WATCHING

A NEW PARADIGM: RSA President Amit Yoran recently spoke with CyberScoop's Greg Otto about why organizations need to shift their thinking when it comes to cybersecurity, and why this year's events show the thinking needs to shift quickly. WATCH HERE.

A FUZZY PICTURE: While the Shadow Brokers' most recent stunt of leaking an old list of supposed NSA staging servers may reveal tactics, tools and procedures once used by some of the country's most elite hackers, the newly released evidence can be easily disputed. Experts from Cylance and Anomali spoke with Chris Bing, telling him that it's tough to find data old enough to match the time in which the leaked info was possibly used, along with what groups can to do obfuscate attribution.

SPEAKING OF ATTRIBUTION: Today's nascent cyber insurance industry is largely unprepared to cover the type of damage than can be caused by the world's best hackers. And the industry isn't hiding it. Though no two insurance plans tend to be quite the same, a rare commonality exists between a vast majority of current cyber

insurance offerings: the policies exclude coverage in the case of a nation state hackers' involvement. Yet, there hasn't been a case where the insurance company or a breach victim have specifically challenged the attribution of an attack in court. Chris looks at what it all means.

TOO MANY TOOLS: The relentless push for cyberthreat information sharing and the proliferation of cybersecurity tools have left many enterprise CISOs feeling overwhelmed, officials and executives told an audience at a cybersecurity conference in Washington, D.C. Thursday. "If you look at the market for information sharing, the ecosystem, it's really, really, inefficient," said DHS Assistant Secretary for Cyber Policy Robert Silvers. "There's a lot of legacy, manual processes, sending emails of PDFs. You have incomplete information awareness with some people just talking to others bilaterally … all the information isn't getting out to all the people. It's the kind of market an innovator would want to disrupt." Shaun looks at what DHS is doing to help.

TWEET OF THE DAY

Not all hacking is complicated!

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.