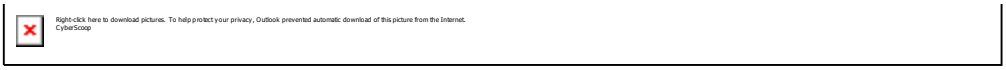
From: CyberScoop <news@cyberscoop.com>
Sent: Tuesday, November 1, 2016 12:04 PM
To: Haley, Nikki
Subject: Uh, why are so many machines still using Windows XP?

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



TUESDAY

November 1, 2016

There are wayyyyy too many machines still using Windows XP. Experts are calling for greater clarity on what companies can do to actively defend themselves against an attack. And, yes, before this letter is over, we'll talk about that whole Trump-Russia server mess. This is CyberScoop for Tuesday, November 1.

C'MON, PEOPLE: Windows XP is old, insecure, and yet somehow still one of the most popular operating systems in the world. Over 100 million users this year, including millions of consumers in China, professionals around the world in the healthcare industry, and the U.S. government. New research from Duo found tens of thousands of devices using Windows XP with Internet Explorer 7 and 8, a hurricane of insecurity boasting hundreds of critical vulnerabilities in software that hasn't been officially supported for nearly three years. Patrick O'Neill has more.

GET ACTIVE: The Justice Department should issue guidance about what kinds of "active defense" measures are permissible under U.S. law and DHS should develop procedures for working with private sector companies that want to implement them, a

report from George Washington University's Center for Cyber and Homeland Security says. Companies experiencing cyberattacks are currently often hamstrung by a lack of clarity from U.S. federal authorities on the legality of "active defense" measures, which are defined as ones that fall between merely passive defense techniques like firewalls and scans at one end of the spectrum, and "hacking back" attacks like seizing control of an adversary's server at the other end. Shaun breaks down what the report had to say.

EVENT

RED HAT GOVERNMENT SYMPOSIUM: Digital transformation is the future. And open source collaboration continues to provide the strongest foundation. As we adapt to this changing environment, our emphasis is on seamless and secure design, development and deployment. When we have the power to choose, we have the power to act. Join your friends, colleagues, and open source experts at on Nov. 2. REGISTER HERE.

OCTOBER SURPRISE: The Shadow Brokers popped their head above ground on Monday to share what looks like the domains and IP addresses of numerous infected computer networks once used as staging servers by the NSA. These staging servers — which include computers owned by international universities and overseas telecommunications companies, according to analysis conducted by a freelance security researcher — may have been leveraged to launch clandestine cyber operations. Chris Bing looks at what it all means.

HELP WANTED: The cybersecurity job gap is growing. With over 1 million job openings in the field this year and rising, professionals are in demand around the world. How can someone make sense of and keep up with the breakneck pace of the information security job market? Whether job hunting or hiring, the rapidly changing landscape is much easier to digest with Cyberseek.org, a newly

launched website backed by a public sector-private industry partnership, that aims at delivering a vast amount of valuable information on where the security jobs are, how to get them, what career tracks are available and how much money people can expect once they are hired. Patrick has more.

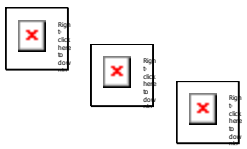
WHAT WE'RE READING

In lieu of social media, let's talk about that huge Trump story that dropped last night. Slate published a piece that examined whether someone related to Trump has set up a server to communicate with some entity in Russia. The evidence pointed to some chatter between an email server with Trump's name on it and Russia's private bank. The story caught such fire that Hillary Clinton's campaign issued a statement asking federal authorities to investigate.

Only later on did multiple people poke holes in the story. The New York Times had been chasing the story, but found that it didn't add up. Furthermore, noted security expert Rob Graham devoted a significant amount of space on his blog debunking the idea that the server traffic was a nefarious secret communication line (it looks like it was Trump hotel marketing). One of the security sources in the Slate story - Krypt3ia - said the outlet screwed up the entire thing.

Glad we could clear all of that up for you.

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.