TUESDAY
August 9, 2016

We may see changes at U.S. Cyber Command, after all. Two cybersecurity companies found a nasty APT floating around. And for all the vitriol, hackers largely ignored the RNC. This is CyberScoop for Tuesday, August 9.

CHANGES AT CYBER COMMAND?: News has it that the White House is evaluating an important and yet expedited series of changes at U.S. Cyber Command, so we spoke with President Obama's top cyber adviser to learn more. The reported plan to elevate the status of the Pentagon's Cyber Command to a unified combatant command would effectively detach the organization from the NSA's purview and grant it autonomy and additional operational authority to conduct both offensive and defensive cyber missions. But should such a transformation be solely made by the White House? Here's the latest.

SUMMER OF SAURON: Cybersecurity researchers generally agree that the term APT — or advanced persistent threat — is overused. Too many so-called APTs are only a step above the script kiddie level, using off-the-shelf malware and well-crafted but very general phishing lures to get into a network. But a newly discovered group — variously dubbed "Strider" or "Project Sauron" — appears to be a true APT with custom-designed malware and a command and control infrastructure that's used once and then burned.

1

The super stealthy group has targeted networks in China and Russia and its tools appear to be written by native English speakers (Hmmm....) Shaun has more.

THE ONLY QUIET PART OF THE RNC: The Republican National Convention saw very little cyber attacks, according to convention Chief Information Officer Max Everett. While the potential threat of hackers was a hot topic for tech blogs [with this newsletter being no different], Everett said his team saw little activity from malicious actors and moreover, that previous conventions actually saw more complex attacks. Even with Donald Trump's controversial rhetoric, the convention dodged hackers' attention. Chris talked with Everett about his relatively quiet convention.

THE PASSWORD PROBLEM: Because most consumers — ignoring expert advice — continue to reuse the same passwords across multiple different accounts, even an old hack — if it was big enough — can have reverberations across the whole Internet. We examine how consumer-facing web service providers like email, social media or cloud storage companies are still wrestling with the impact of the huge trove of hacked passwords stolen from LinkedIn in 2012.

WHAT WE'RE WATCHING

'YOU'RE NEVER GOING TO BE COMPLETELY PATCHED': How have agencies reacted to the Cybersecurity National Action Plan? Greg Otto spoke with Paul Morris, acting CISO for the Transportation Security Administration, who highlighted three ways cybersecurity has improved inside the agency. Watch here.
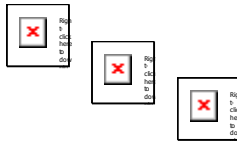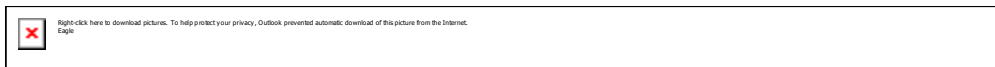

EVENTS

FEDERAL CYBERSECURITY SUMMIT Presented by HPE, Produced by FedScoop: How do government IT thought leaders and innovators perceive, manage and respond to cybersecurity breaches in order to protect digital and virtual assets? At the Federal Cybersecurity Summit, join cybersecurity experts from the public and private sectors to explore combat-ready strategies to prepare for and uncover invisible threats, transform adversaries into competitors and overcome legacy challenges. On September 15, arm your digital units with the know-how and expertise to master cybersecurity in an ever-evolving virtual IT world. REGISTER HERE.

CHECK THIS OUT

A nice little easter egg inside the source code for the White House's new code.gov. OMB finalized its open source policy for agencies yesterday: Check it out if you haven't gotten the chance.

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

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