TIME

Why You Should Care That the White House Got Hacked

Sam Frizell @Sam_Frizell | Oct. 29, 2014

Russian hackers may have jumped the White House's digital fence

Security experts are pointing fingers at Russian hackers for a cyberattack against the White House that came to light late Tuesday, marking the latest high-profile attacks linked to that country.

The attack doesn't appear to have caused much harm. There was no evidence that hackers had breached classified networks. White House Press Secretary Josh Earnest on Wednesday said the attacks were an "inconvenience," but attributed ongoing network disruption to the government's cleanup of the incident rather than the attack itself. So why should we care that unclassified networks at the White House were hacked?

A sign warning of a restricted area is posted on the temporary barricade in front of the fence line to the White House in Washington, DC, October 23, 2014.

Jim Watson—AFP/Getty Images

First, experts say the White House attack shows just how wide a net Russian hackers appear to have cast, especially as tensions between the U.S. and Russia have heightened amid the ongoing crisis in Ukraine. The recent hack is just the latest in a slew of attacks attributed to Russian hackers who security researchers have connected to the Russian government — earlier this month, a Russian hacking group reportedly exploited a Microsoft Windows flaw to spy on NATO and the Ukrainian government. Russian hackers were also behind an attack on JPMorgan Chase that compromised customer information linked to 83 million accounts, according to a recent report. If Russian hackers are indeed behind the White House attack, we should be concerned about their possible intent to probe deeper into the White House network.

"The objective of this may have been a test to determine what the security culture is at the White House before targeting more sophisticated networks," said Armond Caglar, a senior threat specialist at the firm TSC Advantage.

Beyond that, the White House attack shows that even some of the most well-protected institutions are vulnerable, even if the hackers didn't get ahold of any national security secrets this time around. "On a regular basis, there are bad actors out there who are attempting to achieve intrusions into our system," a White House official told the Washington Post. "This is a constant battle for the government and our sensitive government computer systems, so it's always a concern for us that individuals are trying to compromise systems and get access to our networks."

Attacks on private and public sector entities—including the White House—are now par for the course. Says Adam Golodner, an attorney at Kaye Scholer who practices cybersecurity law: "This is the world in which chief information security officers now live."