Gop Email Hack Shows How Bad Midterm Election Meddling Got

Lily Hay Newman

December 4th, 2018

Though sporadic hacker intrusions and phishing campaigns targeted political entities in the lead-up to November's midterm elections, things seemed pretty quiet overall on the election-meddling front in the US. Certainly no leaks or theatrics rose to the level of Russia's actions during the 2016 presidential election. But a belatedly revealed breach of the National Republican Congressional Committee shows just how bad the attack on the 2018 election really was.

As Politico first reported Tuesday, attackers compromised the email accounts of four top NRCC aides, surveilling their correspondences—totaling thousands of messages—for months. The NRCC discovered the intrusion in April, and has been investigating it since. The Committee kept the incident quiet, though, and didn't even inform Republican House leaders. NRCC officials told Politico that the stolen data hasn't surfaced, and that no breach-related extortion attempts have targeted the NRCC so far.

"Of course these types of activity were continuing."

“The NRCC can confirm that it was the victim of a cyber intrusion by an unknown entity," spokesperson Ian Prior wrote in a statement. Prior, a former Department of Justice public affairs officer who now works for the bipartisan strategy firm Mercury, has consulted NRCC on the incident. "The cybersecurity of the Committee’s data is paramount, and upon learning of the intrusion, the NRCC immediately launched an internal investigation and notified the FBI, which is now investigating the matter." Prior said the NRCC is declining to answer additional questions because of the ongoing investigation.

A few election-related hacking incidents were publicly known leading up the midterms, including some attempted spearphishing attacks against campaigns. But from the outside, those attempts appeared largely unsuccessful, seemingly because political organizations shored up their digital security after the wakeup call of 2016. But the major NRCC breach is a reminder that what's publicly known doesn't represent the full picture.

"Of course these types of activity were continuing," says Dave Aitel, a former NSA analyst who is now chief security technology officer at the secure infrastructure firm Cyxtera. "I was always confused when people said they were not."

Even more revelations could be in the offing as well. Government and intelligence officials are still analyzing the events of the midterm season, and new tidbits continue to emerge. For example, defense secretary James Mattis told the Reagan National Defense Forum in California

on Saturday that Russian President Vladimir Putin "tried again to muck around in our elections this last month, and we are seeing a continued effort along those lines."

It is still unclear who was behind the NRCC breach, or what they were after. The details available so far suggest at least a moderately sophisticated hacking effort, since attackers simultaneously compromised four top accounts and were able to lurk on the network for months, says Julian Sanchez, a national-security-focused research fellow at the Cato Institute. But Sanchez also cautions that it's too early to draw conclusions about what the attackers were after, or how difficult it was to persist.

"If we're assuming a government actor, this is the kind of thing you can do on general principle just to see if it might be useful," Sanchez says. "So I don't know that there needs to be a plan this was specifically in service of. For a government adversary there might be a rare case where there's enough value in embarrassing or exposing a target in some way that it's worth it to publish stolen information, but much more often the value is greater when it's kept secret."

Though the NRCC breach may turn out to be anything from a random criminal compromise to a calculated nation state espionage attack, the stolen data could be a ticking time bomb in such a charged political climate. The release of stolen emails from Hillary Clinton 2016 campaign chair John Podesta had a devastating impact on her presidential run. And while the focus during the 2016 election season was leaked emails from prominent democrats, government officials later confirmed that Russian election meddling compromised GOP accounts and old Republican National Committee emails as well.

Depending on what the hackers found in their NRCC trove, and what their intentions are, this new wave of compromised data could be used to similar effect at some point. Or the trove may never see the light of day, instead quietly bolstering some currently unknown nation state's intelligence gathering apparatus.

In either case, the long tail of the 2018 election season just got a little bit longer.