NSA: Russia's Sandworm Hackers Have Hijacked Mail Servers

wired.com/story/nsa-sandworm-exim-mail-server-warning/

Andy Greenberg May 28, 2020

A warning that hackers are exploiting vulnerable email servers doesn't qualify as an unusual event in general. But when that warning comes from the National Security Agency, and the hackers are some of the most dangerous state-sponsored agents in the world, run-of-the-mill email server hacking becomes significantly more alarming.

On Thursday, the NSA issued an advisory that the Russian hacker group known as Sandworm, a unit of the GRU military intelligence agency, has been actively exploiting a known vulnerability in Exim, a commonly used mail transfer agent—an alternative to bigger players like Exchange and Sendmail—running on email servers around the world. The agency warns that Sandworm has been exploiting vulnerable Exim mail servers since at least August 2019, using the hacked servers as an initial infection point on target systems and likely pivoting to other parts of the victim's network. And while the NSA hasn't said who those targets have been, or how many there are, Sandworm's history as one of the most aggressive and destructive hacking organizations in the world makes any new activity from the group worth noting.

"We still consider this to be one of the most, if not *the* most aggressive and potentially dangerous actor that we track," says John Hultquist, the director of intelligence at FireEye, who also led a team at iSight Partners when that company first discovered and named Sandworm in 2014.

Hultquist notes that Sandworm, whose identity as Unit 74455 of the GRU was confirmed for the first time by the US and UK governments in February, was responsible for blackout-inducing cyberattacks in Ukraine in 2015 and 2016, the NotPetya worm that inflicted an unprecedented $10 billion in damage globally in 2017, and also the attacks on multiple US state election boards in 2016 that represented one element of Russia's meddling in the presidential election that year. "The election is right around the corner, and this is an actor that was involved in the 2016 incidents. We're very concerned they'll be involved again in this election," says Hultquist. "This is an actor that's been involved in election-related hacking in the past and the most important, destructive attack in history. Any development involving them is worth watching."

According to the NSA, Sandworm has used a vulnerability in the mail transfer agent Exim, revealed in June of last year, that allows an attacker to merely send a malicious email to the server and immediately gain the ability to run code on the server remotely. In its intrusions, the NSA warns, Sandworm has used that foothold to add its own privileged users to the server, disable network security settings, update secure shell configurations to give its hackers more remote access, and run a script on the server to enable further steps to exploiting the target network.

It's not clear from the advisory what Sandworm's motivation may be in its mail server attacks —whether the ultimate intention of the hackers has been espionage, the sort of hacking-and-leaking operation the GRU carried out in 2016, or reconnaissance for the sort of sabotage attacks it has used against everyone from Ukrainian government agencies and utilities to the 2018 Olympics. But Jake Williams, a former NSA hacker and founder of the security firm Rendition Infosec, says that a vulnerable mail server represents a powerful pivot point for hackers, since it's both exposed to the internet and can allow them to dig deeper into the network once the server is compromised. "Once you're inside the perimeter, it can talk to everything," Williams adds. A hacked mail server can also intercept all incoming mail, and in some cases allow hackers to dig through historical mail archives as well: "From an attacker standpoint, it puts you in a very good position in the network to cause all kinds of mischief. "

Williams also says that despite the vulnerability having been patched last summer, he's found in his own security assessments that mail transfer agents often lack updates, in part because administrators are reluctant to take email systems offline to patch them: "We see a lot of patching deficit in mail servers." What's more, Williams recalls noting at the time the Exim bug was exposed that it represented a particularly tempting vulnerability for intruders. "This vulnerability is absolutely trivial to exploit," he says.

The NSA recommends that administrators patch their Exim software immediately, comb their traffic logs for signs of exploitation, and segment their networks to make it harder for intruders to exploit their initial compromise of a mail server. But the naming of Sandworm specifically as the group exploiting the Exim bug may also be part of a larger effort to call out and deter the GRU's wanton hacking activities. In February, the US State Department and the UK's National Cybersecurity Center jointly condemned Sandworm's cyberattacks on the country of Georgia that took down thousands of websites, as well as TV broadcasters last fall. Those statements also represented the first government confirmation of Sandworm's identity as Unit 74455 of the GRU, a part of its Main Center for Special Technologies, or GTsST.

"They've shown a repeated willingness to flout international norms, and they've been involved in some of the most effective attacks in history," says FireEye's Hultquist. If the West hopes to hold Russia to those norms ahead of the 2020 election, among other potential targets, better perhaps to call out a rash of mail server hacking now than to wait for an October surprise.
