6-Krebs on Security-At Least 30000 US Org

At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software

March 5, 2021

154 Comments

At least 30,000 organizations across the United States — including a significant number of small businesses, towns, cities and local governments — have over the past few days been hacked by an unusually aggressive Chinese cyber espionage unit that's focused on stealing email from victim organizations, multiple sources tell KrebsOnSecurity. The espionage group is exploiting four newly-discovered flaws in Microsoft Exchange Server email software, and has seeded hundreds of thousands of victim organizations worldwide with tools that give the attackers total, remote control over affected systems.

On March 2, Microsoft released emergency security updates to plug four security holes in Exchange Server versions 2013 through 2019 *[Rebuild]* that hackers were actively using to siphon email communications from Internet-facing systems running Exchange.

Microsoft said the Exchange flaws are being targeted by a previously unidentified Chinese hacking crew it dubbed " Hafnium ," and said the group had been conducting targeted attacks on email systems used by a range of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs.

In the three days since then, security experts say the same Chinese cyber espionage group has dramatically stepped up attacks on any vulnerable, unpatched Exchange servers worldwide.

In each incident, the intruders have left behind a “web shell,” an easy-to-use, password-protected hacking tool that can be accessed over the Internet from any browser. The web shell gives the attackers administrative access to the victim’s computer servers.

Speaking on condition of anonymity, two cybersecurity experts who’ve briefed U.S. national security advisors on the attack told KrebsOnSecurity the Chinese hacking group thought to be responsible has seized control over “hundreds of thousands” of Microsoft Exchange Servers worldwide — with each victim system representing approximately one organization that uses Exchange to process email.

Microsoft’s initial advisory about the Exchange flaws credited Reston, Va. based Volexity for reporting the vulnerabilities. Volexity President Steven Adair said the company first saw attackers quietly exploiting the Exchange bugs on Jan. 6, 2021 , a day when most of the world was glued to television coverage of the riot at the U.S. Capitol .

But Adair said that over the past few days the hacking group has shifted into high gear, moving quickly to scan the Internet for Exchange servers that weren’t yet protected by the security updates Microsoft released Tuesday.

“We’ve worked on dozens of cases so far where web shells were put on the victim system back on Feb. 28 [before Microsoft announced its patches], all the way up to today,” Adair said. “Even if you patched the same day Microsoft published its patches, there’s still a high chance there is a web shell on your server. The truth is, if you’re running Exchange and you haven’t patched this yet, there’s a very high chance that your organization is already compromised.”

Reached for comment, Microsoft said it is working closely with the U.S. Cybersecurity & Infrastructure Security Agency (CISA), other government agencies, and security companies, to ensure it is providing the best possible guidance and mitigation for its customers. *[Rebuild]*

“The best protection is to apply updates as soon as possible across all impacted systems,” a Microsoft spokesperson said in a written statement *[Rebuild]*. “We continue to help customers by providing additional investigation and mitigation guidance. Impacted customers should contact our support teams for additional help and resources.” *[Rebuild]*

Meanwhile, CISA has issued an emergency directive ordering all federal civilian departments and agencies running vulnerable Microsoft Exchange servers to either update the software or disconnect the products from their networks.

Adair said he’s fielded dozens of calls today from state and local government agencies that have identified the backdoors in their Exchange servers and are pleading for help. The trouble is, patching the flaws only blocks the four different ways the hackers are using to get in. But it does nothing to undo the damage that may already have been done.

A tweet from Chris Krebs, former director of the Cybersecurity & Infrastructure Security Agency, responding to a tweet from White House National Security Advisor Jake Sullivan.

White House press secretary Jen Psaki told reporters today the vulnerabilities found in Microsoft’s widely used Exchange servers were “significant,” and “could have far-reaching impacts.”

“We’re concerned that there are a large number of victims,” Psaki said. *[Worry]*

By all accounts, rooting out these intruders is going to require an unprecedented and urgent nationwide cleanup effort. Adair and others say they’re worried that the longer it takes for victims to remove the backdoors, the more likely it is that the intruders will follow up by installing additional backdoors, and perhaps broadening the attack to include other portions of the victim’s network infrastructure.

Security researchers have published several tools for detecting vulnerable servers. One of those tools, a script from Microsoft’s Kevin Beaumont , is available from Github .

KrebsOnSecurity has seen portions of a victim list compiled by running such a tool, and it is not a pretty picture. The backdoor web shell is verifiably present on the networks of thousands of U.S. organizations, including banks, credit unions, non-profits, telecommunications providers, public utilities and police, fire and rescue units.

“It’s police departments, hospitals, tons of city and state governments and credit unions,” said one source who’s working closely with federal officials on the matter. “Just about everyone who’s running self-hosted Outlook Web Access and wasn’t patched as of a few days ago got hit with a zero-day attack.”

Another government cybersecurity expert who participated in a recent call with multiple stakeholders impacted by this hacking spree worries the cleanup effort required is going to be Herculean. *[Worry]*

“On the call, many questions were from school districts or local governments that all need help,” the source said, speaking on condition they were not identified by name. “If these numbers are in the tens of thousands, how does incident response get done? There are just not enough incident response teams out there to do that quickly.” *[Worry]*

When it released patches for the four Exchange Server flaws on Tuesday, Microsoft emphasized that the vulnerability did not affect customers running its Exchange Online service (Microsoft’s cloud-hosted email for businesses). But sources say the vast majority of the organizations victimized so far are running some form of Internet-facing Microsoft Outlook Web Access (OWA) email systems in tandem with Exchange servers internally.

“It’s a question worth asking, what’s Microsoft’s recommendation going to be?,” the government cybersecurity expert said. “They’ll say ‘Patch, but it’s better to go to the cloud.’ But how are they securing their non-cloud products? Letting them wither on the vine.” *[Anger]*

The government cybersecurity expert said this most recent round of attacks is uncharacteristic of the kinds of nation-state level hacking typically attributed to China, which tends to be fairly focused on compromising specific strategic targets.

“Its reckless,” the source said. “It seems out of character for Chinese state actors to be this indiscriminate.”

Microsoft has said the incursions by Hafnium on vulnerable Exchange servers are in no way connected to the separate SolarWinds-related attacks , in which a suspected Russian intelligence group installed backdoors in network management software used by more than 18,000 organizations.

“We continue to see no evidence that the actor behind SolarWinds discovered or exploited any vulnerability in Microsoft products and services,” the company said.

Nevertheless, the events of the past few days may well end up far eclipsing the damage done by the SolarWinds intruders.

This is a fast-moving story, and likely will be updated multiple times throughout the day. Stay tuned.

Update, 8:27 p.m. ET: Wired cybersecurity reporter Andy Greenberg has confirmed hearing the same number of victim numbers cited in this report: “It’s massive. Absolutely massive,” one former national security official with knowledge of the investigation told WIRED. “We’re talking thousands of servers compromised per hour, globally.” Read Greenberg’s account here .

Also, the first and former director of CISA, Chris Krebs (no relation) seems to be suggesting on Twitter that the victim numbers cited here are conservative (or just outdated already):

Update 8:49 p.m. ET: Included a link to one of the more recommended tools for finding systems vulnerable to this attack.

Update, 10:17 p.m. ET: Added mention from Reuters story, which said White House officials are concerned about “a large number of victims.”

Update, March 6, 10:56 a.m. ET: CISA’s Twitter account says the agency “is aware of widespread domestic and international exploitation of Microsoft Exchange Server vulnerabilities and urges scanning Exchange Server logs with Microsoft’s detection tool to help determine compromise.”

A tweet today from the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

Further Reading: