New nation-state cyberattacks

blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/

March 2, 2021

Today, we're sharing information about a state-sponsored threat actor identified by the Microsoft Threat Intelligence Center (MSTIC) that we are calling Hafnium. Hafnium operates from China, and this is the first time we're discussing its activity. It is a highly skilled and sophisticated actor.

Historically, Hafnium primarily targets entities in the United States for the purpose of exfiltrating information from a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks and NGOs. While Hafnium is based in China, it conducts its operations primarily from leased virtual private servers (VPS) in the United States.

Recently, Hafnium has engaged in a number of attacks using previously unknown exploits targeting on-premises Exchange Server software. To date, Hafnium is the primary actor we've seen use these exploits, which are discussed in detail by MSTIC here. The attacks included three steps. First, it would gain access to an Exchange Server either with stolen passwords or by using the previously undiscovered vulnerabilities to disguise itself as someone who should have access. Second, it would create what's called a web shell to control the compromised server remotely. Third, it would use that remote access – run from the U.S.-based private servers – to steal data from an organization's network.

We're focused on protecting customers from the exploits used to carry out these attacks. Today, we released security updates that will protect customers running Exchange Server. We strongly encourage all Exchange Server customers to apply these updates immediately. Exchange Server is primarily used by business customers, and we have no evidence that Hafnium's activities targeted individual consumers or that these exploits impact other Microsoft products.

Even though we've worked quickly to deploy an update for the Hafnium exploits, we know that many nation-state actors and criminal groups will move quickly to take advantage of any unpatched systems. Promptly applying today's patches is the best protection against this attack.

In addition to offering new protections for our customers, we've briefed appropriate U.S. government agencies on this activity.

This is the eighth time in the past 12 months that Microsoft has publicly disclosed nation-state groups targeting institutions critical to civil society; other activity we disclosed has targeted healthcare organizations fighting Covid-19, political campaigns and others involved in the 2020 elections, and high-profile attendees of major policymaking conferences.

We are encouraged that many organizations are voluntarily sharing data with the world, among each other and with government institutions committed to defense. We're grateful to researchers at Volexity and Dubex who notified us about aspects of this new Hafnium activity and worked with us to address it in a responsible way. We need more information to be shared rapidly about cyberattacks to enable all of us to better defend against them. That is why Microsoft President Brad Smith recently told the U.S. Congress that we must take steps to require reporting of cyber incidents.

The exploits we're discussing today were in no way connected to the separate SolarWinds-related attacks. We continue to see no evidence that the actor behind SolarWinds discovered or exploited any vulnerability in Microsoft products and services.