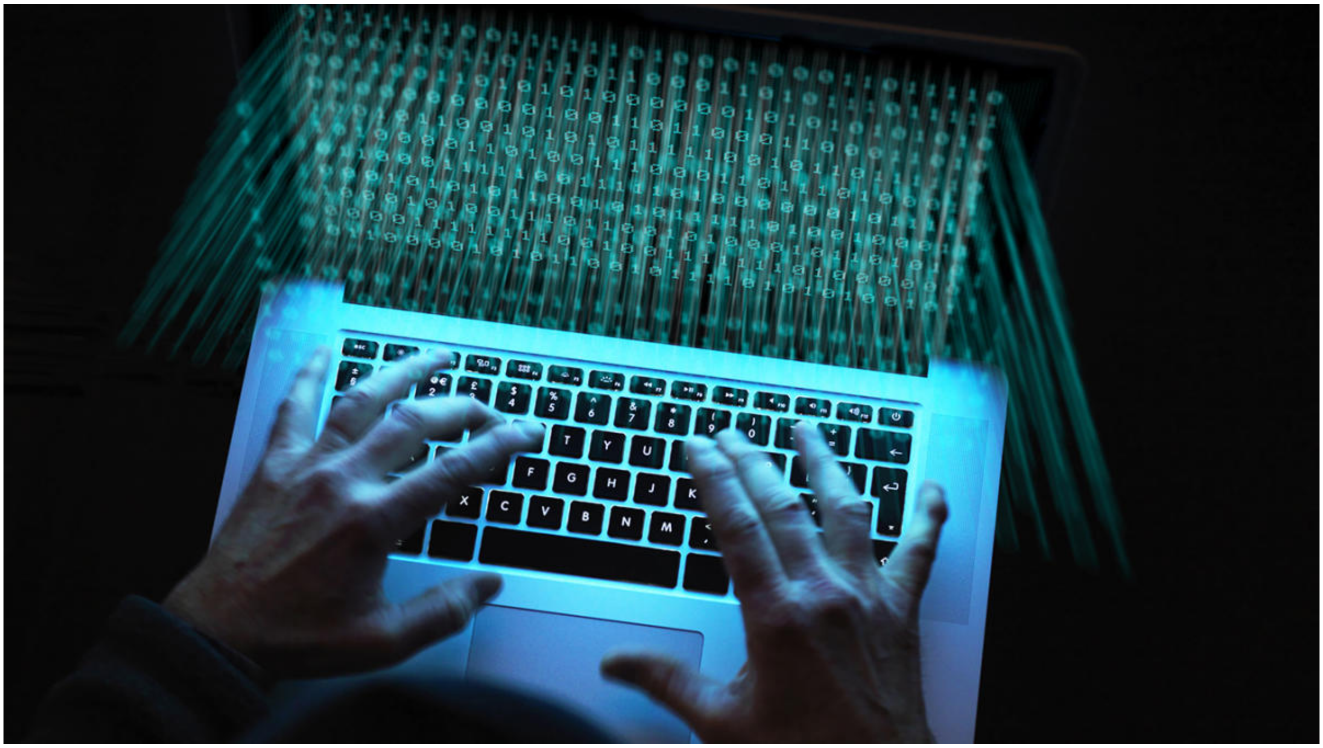
Hackers last year conducted a 'dry run' of SolarWinds breach

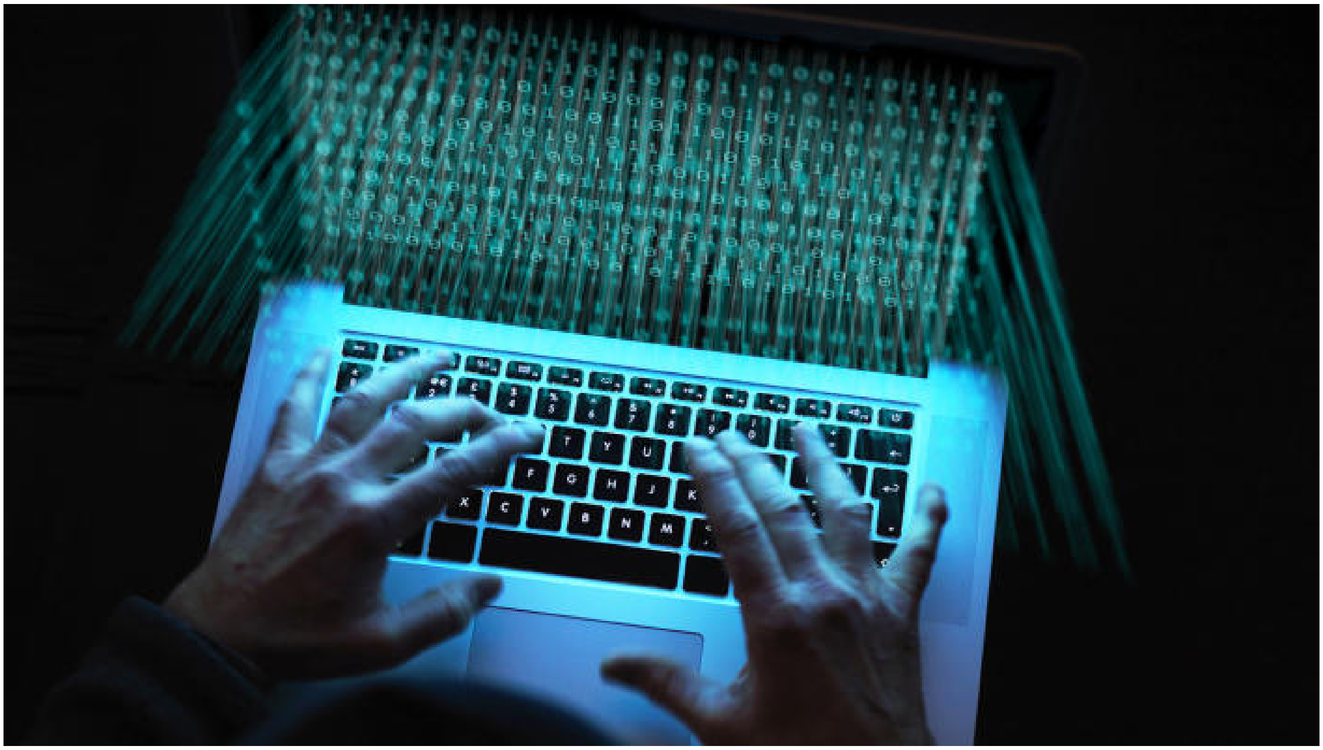
news.yahoo.com/hackers-last-year-conducted-a-dry-run-of-solar-winds-breach-215232815.html

Kim Zetter



Kim Zetter
·Contributor

December 18, 2020, 3:52 PM·7 min read



Westend61/Getty Images

Hackers who breached federal agency networks through software made by a company called SolarWinds appear to have conducted a test run of their broad espionage campaign last year, according to sources with knowledge of the operation.

The hackers distributed malicious files from the SolarWinds network in October 2019, five months before previously reported files were sent to victims through the company's software update servers. The October files, distributed to customers on Oct. 10, did not have a backdoor embedded in them, however, in the way that subsequent malicious files that victims downloaded in the spring of 2020 did, and these files went undetected until this month.

"We're thinking they wanted to test whether or not it was going to work and whether it would be detected. So it was more or less a dry run," a source familiar with the investigation told Yahoo News. "They took their time. They decided to not go out with an actual backdoor right away. That signifies that they're a little bit more disciplined and deliberate."

The October files were discovered in the systems of several victims, but investigators have so far found no signs that the hackers engaged in any additional malicious activity on those systems after the files landed on them.

Five months later, the hackers added new malicious files to the SolarWinds software update servers that got distributed and installed on the networks of federal government agencies and other customers. These new files installed a backdoor on victim networks that allowed the hackers to directly access them. Once inside an infected network, the attackers could have used the SolarWinds software to learn about the structure of the network or alter the configuration of network systems. But they would also have been able to breach other systems on the network or download new malicious files directly to those systems.

The specific number of infected victims remains unknown at this time, but some of the victims breached with the spring 2020 files reportedly include: divisions within the U.S. Treasury and Commerce departments, the Department of Homeland Security, national labs working for the Department of Energy, and the National Nuclear Security Administration, which oversees the national nuclear weapons stockpile. In the commercial sector, the security firm FireEye was also breached by the hackers through SolarWinds software, and late Tuesday Microsoft acknowledged that it had found malicious SolarWinds files on its network as well. Not all SolarWinds customers downloaded the malicious updates.

FireEye was the first to expose the espionage campaign, in a blog post on Dec. 8 after discovering the hackers in its network, though it did not mention that SolarWinds was the origin of the breach into its network. The company did not become aware of the SolarWinds connection until after publishing its post, according to a source.

The Treasury Building in Washington, D.C. (Patrick Semansky/AP)

The new information about the 2019 files expands the previously reported timeline around the intrusions and indicates that the hackers had already compromised SolarWinds' software update system at least five months earlier than reported.

“This tells us the actor had access to SolarWinds’ environment much earlier than this year. We know at minimum they had access Oct. 10, 2019. But they would certainly have had to have access longer than that,” says the source. “So that intrusion [into SolarWinds] has to originate probably at least a couple of months before that — probably at least mid-2019 [if not earlier].”

The files distributed to victims in October 2019 were signed with a legitimate SolarWinds certificate to make them appear to be authentic code for the company’s Orion Platform software, a tool used by system administrators to monitor and configure servers and other computer hardware on their network.

SolarWinds would not answer questions about how long the attackers were in their network, but a spokesperson directed Yahoo News to a list of frequently asked questions published Friday morning that addresses the 2019 files. It indicates that in October 2019, SolarWinds distributed versions of its software that “contained test modifications to the code base ... it is the first version in which we have seen activity from the attacker at this time.” The company noted that subsequent software releases it made in 2019 “did not include either test modifications contained” in that October 2019 version or the backdoor added to the spring 2020 versions.

The company did not say, however, that these files had been found on victims’ machines.

The files that infected customers on Oct. 10 were compiled the same day customers got infected with them, as were files released in the spring of 2020, infecting customers within hours — and in some cases minutes — after they were compiled.

Programmers first write code in a programming language before compiling it into a binary file that computers can read.

SolarWinds headquarters in Austin, Texas. (Sergio Flores/Reuters)

It’s not clear when each individual customer was infected by the backdoor when the files first became available for customers to download in the spring of 2020. Charles Carmakal, senior vice president and chief technology officer at Mandiant, FireEye’s incident response arm, wouldn’t say when his company was breached but did say the attackers were not in his company for the full eight months between when the malicious software updates first were made available for customers to download from the SolarWinds server and the time that FireEye discovered the breach. He told Yahoo News that their investigation shows that other SolarWinds customers infected by the malware did not download and install the malicious update until months after it became available on the update server.

There has been some confusion about how FireEye discovered the hackers in its network. A story published on Wednesday quoted sources on Capitol Hill who said the hackers had duped a FireEye employee into revealing their credentials for accessing the company’s network.

But Carmakal told Yahoo News this is incorrect. The breach was discovered after the hackers enrolled a device into FireEye’s multifactor authentication system, which FireEye employees use to remotely sign into the company’s VPN. The multifactor authentication system works similarly to how Gmail users access their accounts in a secure manner. It generates a unique code on the user’s phone that they enter, along with their username and password, each time they access their account so that even if someone has their username and password, they cannot access the account without the unique code. That unique code gets generated only on the account holder’s mobile phone that they have tied to their account.

Attendees walk by the FireEye booth during the 2016 Black Hat cybersecurity conference in Las Vegas. (David Becker/Reuters)

After the hackers registered their device with the FireEye network to obtain the unique codes that would normally go only to that employee’s device, FireEye’s security system issued an automatic alert to the employee and to the company’s security team that an unknown device was registered to the company’s multifactor authentication system as if the device belonged to the employee.

“They had to provide credentials to authenticate [their device] to the [multifactor authentication system] in order to authenticate to the FireEye VPN,” Carmakal said. “It was the process the attacker followed to enroll in the MFA solution which is what generated the alert. But at this point the attacker already had the employee’s username and password.”

The employee whose credentials were compromised told FireEye’s security team that the device didn’t belong to him, and in the course of investigating how the hackers may have obtained the employee’s credentials, they discovered the hackers had gained access to the network through malicious SolarWinds software.

Carmakal didn’t say how the hackers obtained the credentials after that or how many employee credentials they stole. But once inside a network, it’s common for skilled hackers to seek access to critical system files where employee account credentials are stored in order to use those credentials to gain deeper access into additional parts of the network.

Read more from Yahoo News:

- The 2020 election wasn’t ‘stolen.’ Here are all the facts that prove it.
- Trump’s desperate gambit to stay in office alarms Europeans, who know about coups
- In liberal San Francisco, white responses to George Floyd’s killing proved revealing
- What Biden’s Cabinet picks signal about his presidency

Our goal is to create a safe and engaging place for users to connect over interests and passions. In order to improve our community experience, we are temporarily suspending article commenting

Recommended Stories

- **Lady Gaga Dropped a Topless, No-Makeup, Unfiltered Selfie and I’m in Awe**

  Lady Gaga just shared a new selfie to Instagram and she's gone topless / no-makeup for the pic, sharing a glimpse of her natural skin texture without filters

- **Coweta man sentenced in ‘worst child molestation case’ judge had ever seen**

  He was sentenced to five consecutive life terms plus 60 years.

- **Kevin Costner Finally Finds True Love After Years**

  Kevin Costner puts his toughness away, shares new side

- **Dua Lipa's Short Shorts Are Cut So High That They Look Like Underwear**

  What's the point of shorts if they're not super short?

- **A hurricane is expected to hit Mexico next week. Forecasters have a message for Florida.**

  Could Tropical Storm Agatha, which is forecast to become a hurricane on Sunday as it approaches the southern coast of Mexico, emerge after its bout with Mexico and threaten Miami?

- **Ukrainian artillery throw Russians a "hell of a party" at a hamlet near Huliaipole**

  VALENTYNA ROMANENKO - SATURDAY, 28 MAY 2022, 11:45 The Ukrainian Armed Forces have shown a video of the destruction of Russian forces and equipment in Zaporizhzhia Oblast. Source: Ukrainian Armed Forces General Staff and the 45th Separate Artillery Brigade of the Ukrainian Armed Forces on Facebook Quote from the 45th Brigade: "On one of the farms in Zaporizhzhia Oblast, a massive commotion was organised by the orcs (Russians - ed.

- **A former tech developer bought a rusty 1955 cruise ship on Craigslist and estimates he's spent $1 million restoring it. Check it out.**

  The 293-foot cruise ship had three decks, 85 cabins with en-suite bathrooms, a swimming pool, and a lot of issues when Chris Willson bought it.

-

- **Russian media report Putins frustration with Chechen troops conduct in Ukraine**

  Ukrainska Pravda - Saturday, 28 May 2022, 16:31 Russian journalists report that, according to their sources, the Kremlin initially approved of the conduct of the Kadyrovites [units subordinate to Ramzan Kadyrov, Head of the Chechen Republic in the Russian Federation] in Ukraine.

- **The 'Top Gun' Volleyball Scene Is Not Homoerotic. It Is Homosexual.**

  A one minute and forty second sequence in which a shirtless Tom Cruise, Val Kilmer, and Rick Rossovich face off to Kenny Loggins' "Playing With The Boys."

- **Dominic Fike Under Fire for Disturbing Comment About Amber Heard**

  Dominic Fike dug his own grave by sharing controversial comments about his opinion on Amber...

-

- **Authorities say security video shows the back door of Texas school was propped open by a teacher just before the gunman attacked the school**

  Police believe the propped-open door was used by the gunman to enter Robb Elementary School on Tuesday.

- **Trump Jr. allies issue warning to Stefanik camp: Don't go after Tucker's kid**

  She faces plenty of future GOP leadership competitors, including Rep. Jim Banks. And her camp got burned after allegedly raising Banks aide Buckley Carlson.

- **2022 Indianapolis 500: Starting lineup, TV schedule for Sunday's IndyCar race**

  The 2022 Indianapolis 500 on Sunday features several storylines, including pole sitter Scott Dixon and Jimmie Johnson.

- **Hilarious Boat Names Had The Whole Harbor Laughing**

  Take a look at the funniest boat names

- **Seven People Died in Connection With the Capitol Attack. Trump Just Called the Insurrection a ‘Hoax’**

  "What a lot of crap. What a lot of crap," Trump said of using the word "insurrection" to refer to Jan. 6

- **Watch: Outrageous pin placement for a girls state championship produces quadruple-bogey average, draws criticism**

  The tournament took more than nine hours to play with groups averaging about 20 minutes on just the 18th green.

- **Faith Hill Shuts Down Latest Event in a Lace Bodysuit**

  "1883" co-stars and real-life spouses Tim McGraw and Faith Hill attended the star-powered Upfront event presented by Paramount and both looked amazing on the carpet.