Microsoft confirms it was also breached in recent SolarWinds supply chain hack

zdnet.com/article/microsoft-was-also-breached-in-recent-solarwinds-supply-chain-hack-report/

Home Innovation Security

Microsoft denies that hackers pivoted to production systems and abused its software to attack customers.

Written by Catalin Cimpanu, Contributor on Dec. 17, 2020

-
-
-
-
-

The state-sponsored hackers who breached US software provider SolarWinds earlier this year pivoted to Microsoft's internal network, and then used Microsoft's own products to further the attacks against other companies, Reuters reported today citing sources familiar with the investigation.

SolarWinds Updates

- SolarWinds: The more we learn, the worse it looks
- CISA: US govt agencies must update right away
- A second hacking group targets SolarWinds systems
- Hackers accessed Microsoft source code
- Microsoft quarantines trojanized apps
- Microsoft identifies 40+ victims, most in US
- Microsoft and industry partners seize key domain used in hack
- SEC filing: 18,000 customers impacted

- Breach is not a marketing opportunity

The news comes after the US Cybersecurity and Infrastructure Agency (CISA) published an alert earlier today about the SolarWinds supply chain attack and its impact on government agencies, critical infrastructure entities, and private sector organizations.

Also: Best VPNs

CISA said they had "evidence of additional initial access vectors, other than the SolarWinds Orion platform."

Two Reuters reports on the alleged Microsoft hack did not say what Microsoft products the hackers abused after breaching Microsoft.

In a statement, Microsoft admitted to finding trojanized SolarWinds Orion apps in its environment, but not to hackers pivoting to production systems and then using those systems against its customers. The full, unedited statement is available below:

> "Like other SolarWinds customers, we have been actively looking for indicators of this actor and can confirm that we detected malicious Solar Winds binaries in our environment, which we isolated and removed. We have not found evidence of access to production services or customer data. Our investigations, which are ongoing, have found absolutely no indications that our systems were used to attack others."

Five new SolarWinds hack victims came to light today

Microsoft now joins a list of high-profile entities that have been hacked via a backdoored update for the SolarWinds Orion network monitoring application.

The vast majority of these victims are US government agencies, such as:

- The US Treasury Department
- The US Department of Commerce's National Telecommunications and Information Administration (NTIA)
- The Department of Health's National Institutes of Health (NIH)
- The Cybersecurity and Infrastructure Agency (CISA)
- The Department of Homeland Security (DHS)
- The US Department of State
- The National Nuclear Security Administration (NNSA) (*also disclosed today*)
- The US Department of Energy (DOE) (*also disclosed today*)
- Three US states (*also disclosed today*)
- City of Austin (*also disclosed today*)

The only private company which acknowledged getting hacked via the malware-laced SolarWinds platform is cybersecurity firm FireEye.

Both FireEye and Microsoft were the first security firms to confirm the SolarWinds hack on Sunday, both providing extensive reports of how the breach happened.

Both companies were also involved in an effort to sinkhole the domain used to command and control the malware used in the SolarWinds hack.

Article updated one hour after publication with Microsoft's statement.