SolarWinds hack may be much worse than originally feared

The Russia-linked SolarWinds hack which targeted US government agencies and private corporations may be even worse than officials first realized, with some 250 federal agencies and business now believed affected, the *New York Times* reported.

Microsoft has said the hackers compromised SolarWinds' Orion monitoring and management software, allowing them to "impersonate any of the organization's existing users and accounts, including highly privileged accounts." The *Times* reports that Russia exploited layers of the supply chain to access the agencies' systems.

The *Times* reports that early warning sensors that Cyber Command and the NSA placed inside foreign networks to detect potential attacks appear to have failed in this instance. In addition, it seems likely that the US government's attention on protecting the November elections from foreign hackers may have taken resources and focus away from the software supply chain, according to the *Times.* And conducting the attack from within the US apparently allowed the hackers to evade detection by the Department of Homeland Security.

Microsoft said earlier this week it had discovered its systems were infiltrated "beyond just the presence of malicious SolarWinds code." The hackers were able to "view source code in a number of source code repositories," but the hacked account granting the access didn't have permission to modify any code or systems. However, in a small bit of good news, Microsoft said it found "no evidence of access to production services or customer data," and "no indications that our systems were used to attack others."

Sen. Mark Warner (D-Virginia), ranking member on the Senate Intelligence Committee, told the *Times* the hack looked “much, much worse” than he first feared. “The size of it keeps expanding,” he said. “It’s clear the United States government missed it.”

https://www.theverge.com/2021/1/2/22210667/solarwinds-hack-worse-government-microsoft-cybersecurity