*Digital Workplace Service*

**First Cut**
Number: 2020-FC04
December 22, 2020

**Topics: Security**

**Issue:** How to protect the enterprise from supply chain cyberattacks?

Author: Craig Kennedy

## The Hack of SolarWinds and Why Your Enterprise May Be at Risk

### Summary

SolarWinds disclosed that it had been hacked by an undisclosed foreign government entity, resulting in at least 18,000 customers being exposed to malware hidden in its Orion software product offering. This new type of attack vector means that software supply chains are vulnerable and will put additional pressure on software vendors and enterprises to thoroughly test software products and updates before promoting them to production.

### Event

On December 18, 2020, SolarWinds President and CEO, Kevin B. Thompson confirmed via video presentation the recent cybersecurity attack on SolarWinds software products. SolarWinds issued a software patch to fix the issue on December 17, 2020 on its support site. SolarWinds is actively working with security professionals and numerous government agencies in response to the threat.

### Analysis

This attack on SolarWinds represents a new era of state-sponsored cyber war and is one of the most significant attacks in the last ten years. While it is unclear which foreign entity conducted this attack, what is clear is that every possible entry point for attack will be used now and in the future.

### US Government Agencies Were Targeted

US government agencies and other companies were targeted using an advanced persistent threat (APT) that leveraged a trusted supplier of IT management software called SolarWinds using a multi-step process to conduct an intrusion/hack. The impact on commercial and government agencies is unknown and is still being investigated.

### Who Is SolarWinds?

SolarWinds is a market leader providing IT management software to enterprises and government agencies that simplify the administration of their IT infrastructure. Its Orion product was targeted because it provides elevated access to virtually all the IT infrastructure in enterprises, both on-premise and in the cloud.

SolarWinds is broadly deployed across many enterprises and government agencies, and due to the distributed administrative features within the Orion product, it typically requires accessing the IT infrastructure with various degrees of elevated login privileges, which makes it an ideal system to gain access to all the assets in the enterprise. SolarWinds' customer base includes 85% of the Fortune 500 and is used by hundreds of thousands of companies and government agencies.

**The New Way of Hacking Enterprises Using Software Upgrades**

The cyberattack was extremely sophisticated and is currently believed to be the Russian hacker group 'Cozy-Bear,' which targeted and successfully breached SolarWinds corporate network and eventually gained access to its build servers. Once there, the hackers were able to inject malicious code into the SolarWinds Orion build process. This infected code, code-named SUNBURST, was then packaged and signed with valid SolarWinds certificates giving all recipients of this package the false assurance that this was indeed a valid and safe component of the Orion product.

SolarWinds was used as a trusted vendor in the supply chain to unwittingly distribute the malicious software to its customer base, thereby providing an unsuspecting vector for the attack.

The sophistication of this attack lies in the fact that these SolarWinds software distributions were perceived as legitimate product updates to the Orion software.

**Microsoft to the Rescue**

Cybersecurity firm FireEye was the first to discover this attack when one of its executives discovered a user's access privileges had been compromised. However, it was actually Microsoft that leveraged its might to help mitigate the attack. To do this it used a four-step process:

1. Dec 13—Microsoft removed the digital certificates on the SolarWinds file infected by the malware.
2. Microsoft updated Windows Defender to detect and alert users to the existence of the infected files.
3. Microsoft took control of the domain that the malware was sending data to (avsvmcloud.com). The approach Microsoft used was to sinkhole the domain using a combination of legal and technical methods.
4. Microsoft updated Windows Defender to automatically move the affected files to quarantine instead of only alerting the user.

**Lax Security at SolarWinds**

SolarWinds was sold to Private Equity firms Silver Lake and Thoma Bravo in October 2015 for $4.5 Billion. While SolarWinds had new owners, the CEO Kevin B. Thompson had been in place for over 10 years.

While we may never know what actually happened at SolarWinds, questions need to be asked about why these software updates had malware in them that went undetected for over 6 months. In fact, SolarWinds never discovered their software was infected, it was FireEye who made the initial discovery.

**Malware / Anti-Virus / Privacy Scanners Are Vital**

One of the vulnerabilities the hackers targeted relied on the fact that SolarWinds Orion product recommends that anti-virus scanning be disabled prior to the installation of updates. Disabling anti-virus has become somewhat of a common practice by many software providers and has now been proven to be a highly effective attack vector. Because of this issue, the entire software industry needs to revisit upgrade procedures to ensure that the upgrade package integrity is maintained while anti-virus software is running and active.

Additionally, newer end-point protection / privacy scanning solutions are needed to

mitigate the theft of data and content from the enterprise.

**Aragon Advisory**

- Enterprises can no longer trust that their software supply chain is clean. Aragon is suggesting that all service level agreements (SLA) be updated to include software cleanliness clauses to force software providers to perform extra due diligence to prevent this from happening again.
- Enterprises should avoid software providers who require malware/anti-virus scanners to be disabled on their software products and require updated service level agreements (SLA).
- Enterprises will need to revert back to traditional staging areas and rigorously validate that software updates are clean prior to promoting the updates to production.
- Enterprises should investigate procuring endpoint/privacy protection platforms as yet another tool to secure the enterprise.
- Enterprises must ensure the strict enforcement of multi-factor authentication (MFA) for all users and servers.

**Bottom Line**

Software supply chains have now been compromised in a manner that no one had anticipated. Because of the sophistication of the technique used, all enterprises will need to employ extreme diligence in order to mitigate these types of attacks. In fact, while software providers have their own QA teams, enterprises that procure software should evaluate creating their own software QA teams that will inspect inbound software offerings and upgrades in their staging environment before they are deployed to production.

Editor's Note: Enterprises should schedule an inquiry with Research Director Craig Kennedy to discuss more details on the health of their IT supply chain.