Transforming How Texas Government Serves Texans

SolarWinds Orion Platform Breach

What You Need to Know

In early December 2020, a highly advanced threat actor breached the cybersecurity company FireEye. During its investigation, FireEye discovered a previously unknown compromise in Orion, a popular and widely used network monitoring tool by SolarWinds. It found that the same threat actor was able to compromise SolarWinds' software supply chain, allowing the actor to insert malicious code into the Orion tool.

Background

- **Extremely sophisticated** attack
- The methods and actions taken to "cover their trail" made **detection very difficult**
- Embedded in widely used SolarWinds software
- Allows **Remote Compromise**
- 18,000+ organizations at risk
- More than **250 known entities compromised**
- Most widespread threat in recent history
- Total impact still to be determined
- **Subsequent** vulnerabilities have been discovered

Terms

- **Backdoor** - A backdoor is a typically covert method of bypassing normal authentication to gain access to a system or application.
- **SolarWinds Orion** - A network and application infrastructure monitoring tool used to identify, alert, and report on device, application, and network performance issues.
- **Supply-Chain Attack** – A threat actor inserts malicious code into a component of legitimate software and the software company unknowingly distributed the compromised code to users of the software.

2020 Timeline

Mar – First affected versions distributed by SolarWinds

Dec 8 – FireEye detects compromise of their systems

Dec 11 – FireEye determines SolarWinds as source of compromise

Dec 12 – White House and National Security Council hold an emergency meeting

Dec 13 – Emergency Directive 21-01 and security alerts are published

Dec 17 – CISA issues an alert on the compromise to Federal, SLTT, and private sector entities

Who & What

- The NSA and FBI have released joint statements affirming attribution to a state-sponsored group believed to be a foreign intelligence service.
- Federal authorities have determined this threat poses a great risk to Federal, State, and Local, governments as well as critical infrastructure and private entities.
- Attribution is still ongoing but is likely the known hacking groups APT29 (Cozy Bear) or UNC2452.

Why

- Analysis indicates that this attack was for espionage/exploitation.
- Vulnerability allowed the attackers to upload more malware onto systems undetected, which could lead to future attacks.
- Post-attack activities by the attackers established alternative access to compromised systems.
- Impacted organizations report experiencing email and data theft that was extremely complex and difficult to detect.

continued

Transforming How Texas Government Serves Texans

SolarWinds Orion Platform Breach

How These Attacks are Executed

1

Supply Chain Attack

Attackers insert malicious code into a component of legitimate software. Software company unknowingly distributed the compromised code to users of the software.

2

Execution and Establishing Persistence

When the software starts, the compromised code loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

3

Defense Evasion

The backdoor has a lengthy list of checks to make sure it is running in a compromised network.

4

Reconnaissance

The backdoor gathers system information for the attackers.

5

Initial Command and Control (C2)

The backdoor connects to a C2 server. The server address it connects to is named based on information gathered from the system, making its name unique and harder to detect. The backdoor may also receive an additional C2 address in case the first one is unreachable.

6

Exfiltration

The backdoor sends the gathered information to the attackers.

7

Hands-on-Keyboard Attack

The backdoor runs commands it receives from attackers. The wide range of capabilities allow attackers to perform additional activities, such as credential theft, privilege escalation, and lateral movement.

Source: https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/.