SolarWinds TED Talk

By: Jessica Taylor

CSCI 352

SolarWinds Cyberattack

Overview

The SolarWinds cyberattack was a sophisticated and destructive attack on a software company, SolarWinds, and involved compromised software updates. Dates of this attack range from the end of 2019 to beginning of 2020.

https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

SolarWinds Cyberattack
Who Did It Affect?

- The Texas based software company, SolarWinds
- Federal government
- Private Sector

- https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/
- https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

18,000 - 300,000

Number of customers impacted by compromised Orion update

https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

SolarWinds Cyberattack

What is Orion

- SolarWinds' most popular product
- Network Management System (NMS)
- "The SolarWinds® Orion® Platform is a powerful, scalable infrastructure monitoring and management platform designed to simplify IT administration for on-premises, hybrid, and software as a service (SaaS) environments in a single pane of glass." (solarwinds.com)

https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

https://www.solarwinds.com/orion-platform

SolarWinds Cyberattack

What makes Orion a good target?

- Network Management Systems (NMS) communicate with all devices that it manages and monitors
- This makes it a “prime location”
- NMS’s make changes based on configuration
- If compromised, an attacker can also make changes

https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

SolarWinds Cyberattack

What Happened?

- 2019/2020
- A threat actor gained access to SolarWinds’ computing networks
- Initially, injected test code into Orion
- Later injected hidden code that was included in Orion software updates

https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

SolarWinds Cyberattack

What Happened? ... Continued

- The Orion software updates were released to SolarWinds' customers (not knowing they are compromised)
- The code in the compromised updates included a back door ...
- The threat actors were then able to exploit the networks and systems of SolarWinds' customers who downloaded this compromised update

https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

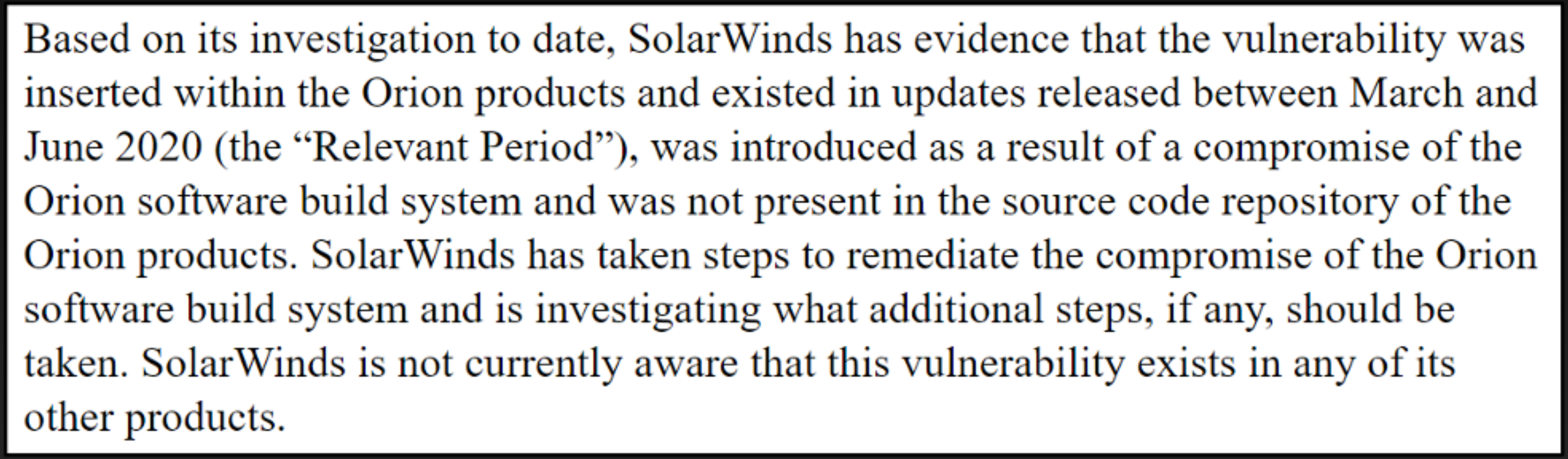
Were the threat actors identified?

YES!

Russian Foreign Intelligence Service

https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

SolarWinds’ Response To Incident



Based on its investigation to date, SolarWinds has evidence that the vulnerability was inserted within the Orion products and existed in updates released between March and June 2020 (the “Relevant Period”), was introduced as a result of a compromise of the Orion software build system and was not present in the source code repository of the Orion products. SolarWinds has taken steps to remediate the compromise of the Orion software build system and is investigating what additional steps, if any, should be taken. SolarWinds is not currently aware that this vulnerability exists in any of its other products.

https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

Thank You!

References

https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

https://www.solarwinds.com/orion-platform