

[Return to the VPLS Blog](#)

Blog Post

The SolarWinds Hack: Resources and Guidance from Cybersecurity Experts

Published

Dec 18, 2020

Written by

John Headley

Filed under

[Cybersecurity, Disaster Recovery](#)

News broke to the public on Sunday, December 13th, that the SolarWinds Orion network monitoring platform had been hacked. In this sophisticated attack, SolarWinds Orion software updates had been trojanized to deliver malware, now called SUNBURST, into servers hosting the SolarWinds Orion software. Using this compromised server, the attacker is then able to move laterally in the network to compromise other assets and perform data theft.



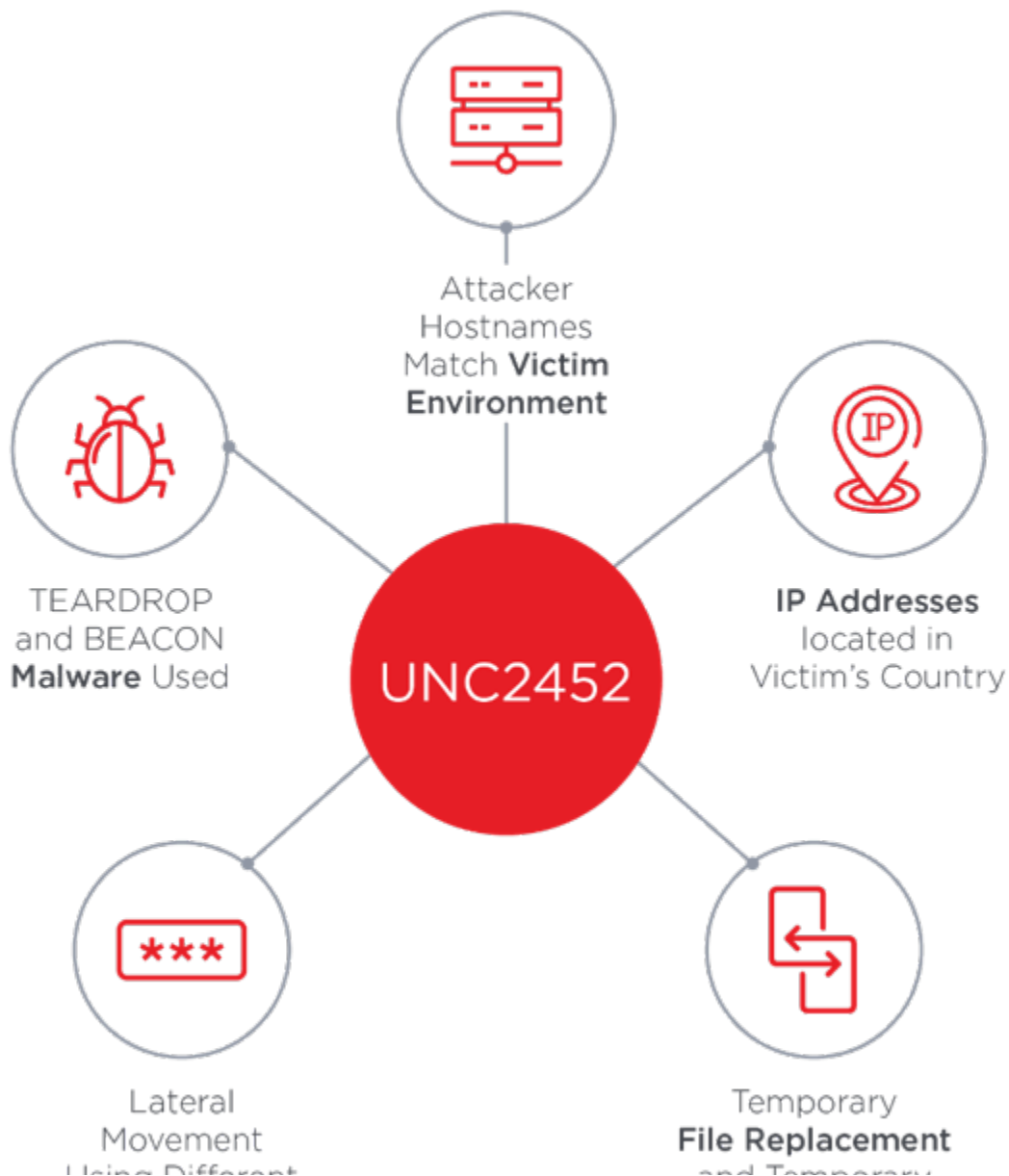
The SolarWinds Hack: Resources and Guidance from Cybersecurity Experts

How your organization can mitigate risks and respond to the SolarWinds Orion Software Attack.

[START READING](#)

Attack-at-Scale

This attack is part of a global intrusion campaign that began as early as March 2020 and is currently ongoing. The threat actors are identified as a nation-state advanced persistent threat (APT), with analysts suggesting that the data points to Russia. The victims have included government, consulting, technology, telecom, and extractive entities in North America, Europe, Asia, and the Middle East, and it is anticipated there will be additional victims in other countries and verticals. Included in this list are **several US Federal agencies**, such as the Department of Homeland Security and the State, Commerce, and Treasury Departments. **Microsoft** has also reported they were a victim of this attack, but they “have not found evidence of access to production services or customer data.”



Post-compromise tactics employed by UNC2452, FireEye's official name used for tracking the threat actors behind this intrusion campaign.

Advice

If you use SolarWinds Orion software, you will want to take immediate action to mitigate the effects of SUNBURST and determine if there are any indicators of compromise (IOC). If you don't use SolarWinds software, you may still want to take action to understand to what extent your vendors and partners use SolarWinds.

Although news around this attack is still developing, SolarWinds has since released patches to mitigate this vulnerability. SolarWinds advises:

1. Customers with any products for Orion Platform version 2020.2 with no hotfix installed, or version 2020.2 HF 1, should upgrade to Orion Platform version 2020.2.1 HF 2 as soon as possible **to better ensure the security of your environment.**
2. In the event that you are unable to upgrade immediately, ensure that SolarWinds servers are isolated from the network – disconnected or powered down.

Note that before following the steps above, imaging system memory and/or host operating systems hosting SolarWinds Orion is recommended to aid in forensic analysis. Furthermore, we recommend rebuilding SolarWinds Orion from scratch rather than patching a potentially compromised host. See CISA recommendations below.

Next, as part of your incident response plan, a comprehensive investigation should be performed and, if attacker activity is discovered in your environment, remediation steps should be taken based on the investigation findings. This will likely include removing threat-actor controlled accounts and persistence mechanisms.

The emergency directive from CISA recommends:

- ✓ Treat all hosts monitored by the SolarWinds Orion monitoring software as compromised by threat actors and assume that further persistence

- ✓ mechanisms have been deployed.
Rebuild hosts monitored by the SolarWinds Orion monitoring software using trusted sources.
- ✓ Reset all credentials used by or stored in SolarWinds software. Such credentials should be considered compromised.
- ✓ Take actions to remediate kerberoasting, including, as necessary or appropriate, engaging with a third party with experience eradicating APTs from enterprise networks.

Resources

Resources listed below are in the recommended order of reading for organizations that do have SolarWinds Orion monitoring software in their environment.

1. [SolarWinds Security Advisory](#)
2. [SolarWinds FAQs](#)
3. [FireEye Detailed Threat Analysis](#)
4. [CISA Alert AA20-352A](#)
5. [CISA Emergency Directive 21-01](#)

Overwhelmed?

This is a global-scale hack with potentially dire consequences for your organization and its or its customers' data. If your organization does run SolarWinds but does not have the time or expertise to perform any of the suggested steps above, please [call VPLS](#). We offer free consultation on how our team of certified security experts can become an extension of your IT staff and drive these necessary incident response procedures.

Read More from this Author

John Headley

John Headley, CISSP and Fortinet NSE8 #003155, is a Senior Security Engineer at VPLS where he splits his time between both pre-sales and post-sales engagements. His expertise is in security architecture and engineering, security assessment and compliance, and security operations. During his time at VPLS, he has led many security-related professional services projects, including a 35-location international firewall deployment for a publicly-traded social media company.

[More from this Author](#)



PREVIOUS

VPLS's Hawaii Team Bridges Services and Support... VPLS Ranks #26 Among Elite Managed Service Pr...

NEXT



If you enjoyed this article, you'll probably like:



5 Reasons SOC-as-a-Service Features Help You


March 29, 2022

[Read More »](#)

BLOG POST

What is SOC-as-a-Service?

SOC-as-a-Service (SOCaaS) functions as an extension of a company's IT department and helps take the guesswork out of cybersecurity.

 [READ NOW](#)

What Is SOC-as-a-Service?

March 28, 2022

[Read More »](#)

BLOG POST

VDI vs. VPN

What's Best for Remote Employees?

Many companies struggle with deciding which of these two common remote work is better for their workforce.



 [READ NOW](#)

HOW TO REACH US

VDI vs. VPN: What's Best for Remote Employees?

Corporate Headquarters

600 West 7th Street, Suite 510
[Read More »](#)
Los Angeles, CA 90017

24/7/365 Customer Service

+1 (888) 365-2656

support@vpls.com

Sales Inquiries

+1 (888) 365-2656

sales@vpls.com

WHAT WE DO

Cloud

Hosting

Colocation

Network Services

Managed Services

Professional Services

VAR

WHO WE SERVE

Financial Services

Healthcare and Life Sciences

Media & Entertainment

Telecom

Startup

Enterprise

Public Sector