



# Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

**21 December 2020**

PIN Number

**20201222-001**

Please contact the FBI with any questions related to this Private Industry Notification.

Local Field Offices:

[www.fbi.gov/contact-us/field-offices](http://www.fbi.gov/contact-us/field-offices)

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This product was coordinated with members of the Federal Unified Coordination Group (UCG).

This PIN has been released **TLP: WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

## Advanced Persistent Threat Actors Leverage SolarWinds Vulnerabilities

### Summary

Based on the wide ranging scope of the investigation into SolarWinds Orion compromises by Advanced Persistent Threat (APT) actors and fast paced release of private network analysis, the FBI is providing cyber security professionals and system administrators collated and verified information to assist in determining whether APT actors have exploited the SolarWinds vulnerabilities present on their systems.

### Threat Details

Malicious actors are exploiting SolarWinds Orion products (affected versions 2019.4 through 2020.2.1 HF1) containing SUNBURST malware to gain access to network traffic management systems. These actors have been observed on victim networks pursuing several objectives, including achieving full privileged persistent access through trusted legitimate credentials, accounts, and applications. These credentials are often leveraged from victim-dedicated IPs in the victim's own

**TLP: WHITE**



# Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

country to avoid detection. Such targeted activity indicates elevated actor interest in a victim. Once the malicious update is found on a network, cyber security professionals and system administrators must determine whether the threat actor has used that vulnerability to pivot to a higher form of access.

## Recommendations

If an entity determines that they have downloaded the trojanized SolarWinds plug-in, they should conduct additional research to determine whether or not their systems have been further compromised. After installation, the malware beacons via DNS requests to resolve unique subdomains of avsvmcloud[.]com between 12 and 14 days after installation, according to FireEye's reporting. The unique subdomain follows a pattern of \*.appsinc-api\*.avsvmcloud.com.

The malware operators are able to monitor the DNS beacons to determine if additional targeting of an organization is desired. If the actor(s) decide to further compromise the network, the response to the beacon will include a new command and control server for the victim system to communicate with. If the actor(s) do not wish to further compromise the network, an IP address in a previously determined block list may be returned to the victim system.

Additionally, beacons may go unresolved, resulting in no additional compromise of the victim system. The FBI encourages network defenders to review network DNS activity for queries to the avsvmcloud[.]com domain. If DNS logs indicate the query returned a valid IP address, additional research for evidence of lateral movement, privilege escalation, or other unauthorized activity should be performed.

Some victims may have received a response that included an IP address designed to disable the malware. The list of those IP addresses is available at <https://www.fireeye.com/blog/threat-research/2020/12evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html> [under "Network Command and Control (C2)"]. Following receipt of a DNS response indicating the network was to be further targeted, the malware moved additional communications to a separate command and control address which would also make victim specific DNS queries. If this is believed to be the case, network operators should review the network for evidence of lateral movement, privilege escalation, or other unauthorized activity on the SolarWinds host.



# Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

## References

[Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations](#)

[Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor | FireEye Inc](#)

[Global Intrusion Campaign Leverages Software Supply Chain Compromise | FireEye Inc](#)

## Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at [www.fbi.gov/contact-us/field-offices](http://www.fbi.gov/contact-us/field-offices). When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

## Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

## Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: <https://www.ic3.gov/PIFSurvey>