What Every Leader Needs to Know About the Ongoing APT Cyber Activity

December 2020

THE THREAT AND HOW TO THINK ABOUT IT

CISA is tracking a significant cyber incident impacting enterprise networks across federal, state, and local governments, as well as critical infrastructure entities and private sector organizations. An advanced persistent threat (APT) actor compromised the SolarWinds Orion software supply chain and is abusing commonly used authentication mechanisms. If left unchecked, this threat actor has the resources, patience, and expertise to resist eviction from compromised networks and continue to hold affected organizations at risk. CISA urges organizations to prioritize measures to identify and address this threat. For details, review the related CISA Alert, which CISA will update as information becomes available.

THE RISK IN DETAIL

A sophisticated APT actor inserted malicious code into certain trusted SolarWinds Orion software updates, which were then made available to customers as legitimate software updates. Once these updates were applied, the APT actor gained access to customer network environments. The immediate danger is that the APT actor can use this access to create new accounts, evade common means of detection, obtain sensitive data, move across a network unnoticed, and establish additional persistence mechanisms. The APT actor has only targeted some organizations with further network exploitation. However, all organizations that installed the compromised updates remain at risk without corrective action.

CISA is also investigating incidents—not connected with SolarWinds—where abuse of Security Assertion Markup Language (SAML) authentication is present. This activity is consistent with the APT actor's behavior. CISA strongly recommends that all organizations **investigate**, and, as applicable, **remediate** (potentially rebuild), and **share** information with those assisting in this massive response effort.

ACTIONS FOR TODAY

1. **Determine whether your organization is affected.** Consult with your information security team to determine if your organization has—or has ever had—one of the affected versions of SolarWinds Orion installed and initiate incident response. If you do not have in-house expertise, seek third-party support.
   a. Keep in mind that your organization's managed service providers may have been compromised as part of these events, which could have implications for your operations.
2. **If affected, make incident response and remediation your top priority.** Leadership—working with legal, financial, and operations personnel—should empower information security staff to take appropriate action based on their expertise and to collaborate with internal and external partners.
3. **Allocate sufficient resources.** Provide executive support and empower information security staff—or third-party support—to thoroughly investigate your IT environment for adversary activity.
   a. Consider engaging third-party support with experience eradicating APTs from enterprise networks.
   b. Following incident response, your organization may need to rebuild all network assets monitored by SolarWinds Orion; this will be a resource-intensive, highly complex, and lengthy undertaking.
4. **Seek further guidance.** Refer to the related CISA Alert, Emergency Directive, and National Security Agency advisory, as well as future guidance on cisa.gov/supply-chain-compromise.
5. **Maintain enhanced operational security** during the incident response and remediation processes.

CISA'S ROLE AS THE NATION'S RISK ADVISOR

CISA collaborates with industry and government partners to help organizations understand and counter critical infrastructure and cybersecurity risks associated with the malicious activities of nation-state and non-state actors. CISA provides recommendations to help partners stay vigilant and protected against potential foreign influence operations.