IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

CISA INSIGHTS

DEFEND TODAY, SECURE TOMORROW

March 9, 2021

Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise: Risk Decisions for Leaders

Since December 2020, the Cybersecurity and Infrastructure Security Agency (CISA) has been responding to a significant cybersecurity incident. An advanced persistent threat (APT) actor added malicious code to multiple versions of the SolarWinds Orion platform and leveraged it—as well as other techniques—for initial access to enterprise networks of U.S. government agencies, critical infrastructure entities, and private sector organizations.

The threat actor targeted and gained persistent, invasive access to select organizations' enterprise networks, their federated identity solutions, and their Active Directory/M365 environments. The actor used that privileged access to collect and exfiltrate sensitive data and created backdoors to enable their return.

The threat actor only targeted a select group of organizations affected by the SolarWinds Orion supply chain compromise for follow-on network exploitation. Additionally, the APT actor used techniques other than the supply chain compromise to access targeted networks.

This Insights applies to organizations with affected versions of SolarWinds Orion who have evidence of follow-on threat actor activity.

THE RISK

The threat actor may be deeply burrowed in compromised networks, and full eviction will be costly, highly challenging, and complex; however, **failure to perform comprehensive remediation activity and evict the adversary will expose enterprise networks and cloud environments to substantial risk for long-term undetected APT activity**, and compromised organizations will risk further loss of sensitive data and erode the public trust of their networks.

ACTIONS FOR LEADERS

Leaders of organizations with compromised networks should immediately:

1. **Assess the risk**. Determine the severity of the network compromise and long-term risk to their organization if the actor is not evicted from networks.
2. **Allocate time and resources**. Eviction is a three-phase process: Pre-Eviction, Eviction, Post-Eviction. This will be complex and resource intensive and will require your network to be disconnected from the internet for several days. Provide all resources and tools necessary to your IT personnel and incident responders.
3. **Consider engaging with third-party companies experienced with APT activity**. If your organization does not have the in-house resources to investigate and remediate this activity, consult with third-party companies that have experience evicting sophisticated cyber threat actors.
4. **Seek further guidance**. Refer to the following for more general information as well as technical detection and remediation guidance and resources.
    a. CISA.gov Supply Chain Compromise web page.
    b. CISA Insights: What Every Leader Needs to Know about the Ongoing APT Cyber Activity
    c. US-CERT.CISA.gov Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise web page

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.