ATTIVO THREATDEFEND® PLATFORM: ACCELERATING SOLARWINDS POST-BREACH INCIDENT RESPONSE FOR THE FASTEST LATERAL MOVEMENT DETECTION

The SolarWinds breach is a prime example of an ongoing supply chain breach, and one should be aware that this has happened in the past and will happen again. As with any breach, discovering an attacker inside the network is extremely alarming and potentially painful. The focus should be to detect the attacker's attempts to move laterally in the network, elevate their privileges, minimize their window of opportunity, and shut them out as fast as possible. This latest compromise with SolarWind has magnified the impact as all their customers inherited the backdoor by following industry best practices to keep their software updated.

A joint statement from the FBI, CISA, and Office of the Director of National Intelligence said the SolarWinds backdoor attacks are "ongoing" and have comprised federal agencies.

"To all looking into the SolarWinds Orion breach: Orion holds credentials, such as Domain Admin, Cisco/Router/SW root/enable creds, ESXi/vCenter Credentials, AWS/Azure/Cloud root API keys. and so much more. CONSIDER THESE CREDENTIALS COMPROMISED if you see other IOCs #SunBurst"

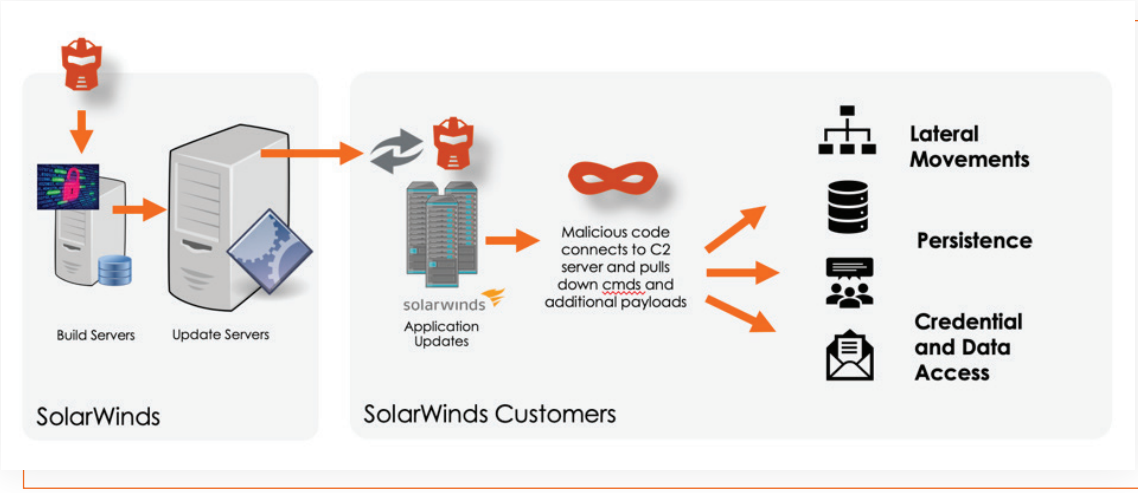
Per Rob Fuller @mubix"

Below is more visibility on the anatomy of the attack and how Attivo can help.

BREACH SUMMARY

- After the initial compromise, the attackers moved laterally within SolarWinds, gaining administrative permissions acquired through the on-premises compromise to access the organization's global administrator account and trusted SAML token signing certificate.
- The attack involved signing malicious code as part of SolarWinds software update
- SolarWinds released compromised builds between March 2020 and June 2020, potentially impacting about 18,000 customers.

SolarWind customers unknowingly downloaded and installed the malicious code.



SPEEDING UP POST-BREACH IR USING THE THREATDEFEND® PLATFORM FOR THE FASTEST LATERAL MOVEMENT DETECTION

The Attivo Networks ThreatDefend platform provides early and accurate detection of in-network threats, regardless of attack method or surface, using deception and concealment technologies. It creates a comprehensive fabric that blankets the network with deceptive decoys, credentials, shares, bait, and other misdirection while hiding sensitive or critical data to derail adversaries early in the attack life cycle. Automated intelligence collection, attack analysis, and third-party integrations accelerate incident response.

> "If you're a SolarWinds customer & use the below product, assume compromise and immediately activate your incident response team… Focus on your Crown Jewels. And let's turn our focus to what are our options to quickly detect lateral movement."
>
> - -Chris Krebs

ThreatDefend platform customers should implement the following measure to protect their organizations.

DEFENDER ACTIONS

GAIN VISIBILITY INTO ATTACKER LATERAL MOVEMENT ACROSS THE NETWORK:

- Deploy decoys mimicking critical servers, code repositories, databases, file servers, and other deceptive assets.
- Deploy ThreatDirect (TD) forwarders, either TD-VM or TD-EP, across all subnets and expand deception coverage.
- Deploy the ThreatDefend® Deflect function to detect network reconnaissance. The Deflect function turns every endpoint into a decoy and engages attackers as they fingerprint and discover network services

GAIN VISIBILITY INTO CREDENTIAL STEALING

- Deploy ThreatStrike lures across all endpoints leading attackers to decoys

DATA PROTECTION

- Deploy SMB mapped shares to decoys
- Apply DataCloak policies to restrict access to production network file shares, OneDrive mapped drives, or other sensitive storage from attacker tools
- Apply DataCloak policies to restrict access to data documents on endpoints from attacker tools

DETECT CREDENTIAL EXPOSURES AND CYBER RISKS

- Find exposed Lateral Movement Paths using the ThreatPath solution and remediate them.
- Analyze the presence of new user accounts, privilege accounts, or service accounts on endpoints, Active Directory using the ThreatPath solution

PROTECT ACTIVE DIRECTORY

- Take steps to prevent and detect kerberoasting attacks. The ADSecure solution hides the service accounts, thereby mitigating and preventing the possibility of kerberoasting attacks and silver ticket attacks while alerting in real-time.
- Analyze the presence of attackers on endpoints connected to the domain discovering privileges in Active Directory while getting real-time visibility into domain enumeration.
- Use ADSecure to detect and prevent attacker lateral movement from a domain-connected system.

SUMMARY

The SolarWinds Orion supply chain attack stresses the need for early detection of threats that evade perimeter defenses. During this time of widespread industry awareness of the issue, the adversary may have created additional beachhead accounts and gone dormant to avoid detection. The Attivo Networks ThreatDefend platform and EDN suite provide advanced defensive capabilities to protect organizations from attacks like these and many others.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in lateral movement attack detection and privilege escalation prevention, delivers a superior defense for countering threat activity. Through cyber deception and other tactics, the Attivo ThreatDefend® Platform offers a customer-proven, scalable solution for denying, detecting, and derailing attackers and reducing attack surfaces without relying on signatures. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, in the cloud, and across the entire network by preventing and misdirecting attack activity. Forensics, automated attack analysis, and third-party integrations streamline incident response. Deception as a defense strategy continues to grow and is an integral part of NIST Special Publications and MITRE Shield, and its capabilities tightly align to the MITRE ATT&CK® Framework. Attivo has won over 130 awards for its technology innovation and leadership. www.attivonetworks.com.