SolarStorm Rapid Response

Request a complimentary SolarStorm Rapid Assessment to find out if you've been impacted by the SolarWinds supply chain attack.

Orchestrating one of the stealthiest attacks in history, the "SolarStorm" threat group infected countless SolarWinds Orion servers across nearly 18,000 organizations while evading detection for months.

This attack resulted in the theft of powerful red team test tools as well as unknown data loss and damage to other affected organizations. With dwell times approaching nine months, the advanced adversary likely stole sensitive information from many high-value targets.

Benefits

- Identify all your SolarWinds servers, anywhere in the world
- Learn if SolarStorm indicators of compromise (IOCs) are present in your organization
- Contain and recover from an attack with a SolarStorm Cybersecure Engagement
- Get peace of mind knowing your organization is secure

As the details of this devastating attack continue to unfold, security teams around the world are scrambling to find out whether their organizations, too, were compromised by the SolarStorm attacks. This analysis requires the following steps:

1. Identify all SolarWinds Orion servers installed and running in your organization and disconnect them from your network.
2. Determine whether the servers have been compromised.
3. Remediate any compromised servers.
4. Investigate the scope of the attack, including lateral movement to other endpoints.
5. Detect and prevent future intrusions.

SolarStorm Rapid Assessment

As your security partner, our top commitment is to ensure you're protected from cyberattacks. To help you assess, remediate, and recover from the devastating SolarStorm attack, Palo Alto Networks is extending a SolarStorm Rapid Assessment offer to you at no additional charge.

If your organization uses the SolarWinds Orion platform, you can request this complimentary assessment to help determine whether you were impacted by the SolarStorm attack. As part of the assessment, our security experts will locate and review all your SolarWinds deployments and search for indicators of malicious activity.

The assessment will combine the best-in-class capabilities in our Expanse attack surface reduction platform, together with the incident response services of the Crypsis Group, to help you quickly determine the impact SolarStorm has had on your organization. This offer reflects our commitment to securing all customers against this insidious threat.

SolarStorm Cybersecure Engagement

If our incident responders uncover indicators of a breach during our assessment, you can purchase a SolarStorm Cybersecure Engagement. As part of this engagement, our expert incident response team, Crypsis, will conduct an investigation to determine the scope of the incident and identify compromised assets, up to 200 hours. They will also help you remediate and recover from the attack. The engagement includes:

- Forensic analysis of SolarWinds servers to determine the following:
  - » Extent of unauthorized activity as a result of the trojanized version of SolarWinds Orion
  - » The presence of additional malware, utilities, and/or persistence mechanisms
  - » Potential exfiltration of data, including Personally Identifiable Information ("PII"), if any
- Live response analysis of impacted systems to determine the following:
  - » Extent of unauthorized activity in the environment
  - » Whether there is evidence of lateral movement to additional systems in the network
  - » Presence of persistent malware in the environment, if any
  - » Potential exfiltration of data, including PII, if any
- Log analysis, including:
  - » Firewall log analysis, if available, to identify indicators of unauthorized access, if any
  - » VPN log analysis, if available, to identify indicators of unauthorized access, if any
  - » SIEM log analysis, if available, to identify indicators of unauthorized access, if any
- Threat hunting by deploying Cortex XDR and/or Hadron endpoint agents to all compatible workstations and servers in environment, to determine the following:
  - » Extent of unauthorized activity in the environment, if any
  - » Whether there is evidence of lateral movement to additional systems in the network
  - » Presence of persistent malware in the environment, if any
  - » Assist with containment and remediation of any impacted endpoints
- Reporting. Upon request, Crypsis will generate a written summary report that details the analysis performed and subsequent findings

To help you detect and prevent future attacks, our incident responders will also provide two-month evaluation subscriptions to Cortex XDR™—the industry's first extended detection and response platform—and a two-month evaluation subscription to Expanse Expander® platform to help you discover, monitor, and track internet assets.[1] With the SolarStorm Cybersecure Engagement, you can rest easy knowing your organization is secure.

Lastly, the SolarStorm Cybersecure Engagement includes a 60-day evaluation subscription of Expanse's technology. The engagement includes:

- Outside in discovery of your public facing assets, designed to uncover rogue devices and unknown risks. This requires no agents or installation
- Monitoring of NetFlow traffic to uncover suspicious network traffic. This requires no installation or action from you
- 60 days access to the Expanse product, used to discover unknown risks that may be associated with SolarStorm

Crypsis Digital Investigations

The Crypsis Group, a Palo Alto Networks company, is a security advisory team working to create a more secure digital world by providing the highest quality incident response, risk management, and digital forensics services. We can help protect you from sophisticated cyberthreats, such as the SolarStorm threat group. Our global response capability, constant technological innovation, and elite cybersecurity expertise enable us to stay ahead of the rapidly evolving threat landscape.

1. Evaluations are made available to new Cortex XDR and Expanse Expander® platform customers only; for clarification purposes, existing customers with valid Cortex XDR and Expanse Expander® subscriptions are not entitled to extend their current subscriptions for an additional two months.

Expanse Attack Surface Reduction

The Expanse platform offers you a better way to manage your attack surface. Organizations today struggle to understand all their exposed assets, including rogue devices, vulnerable remote users, and sensitive applications available to anyone on the internet. Expanse detects systems and services belonging to your organization across the global internet with a massive-scale index of internet-facing assets and a unique ability to link these assets to individual organizations.

With the SolarStorm Rapid Assessment, we apply these powerful capabilities to help you hunt down and locate all your SolarWinds Orion deployments.

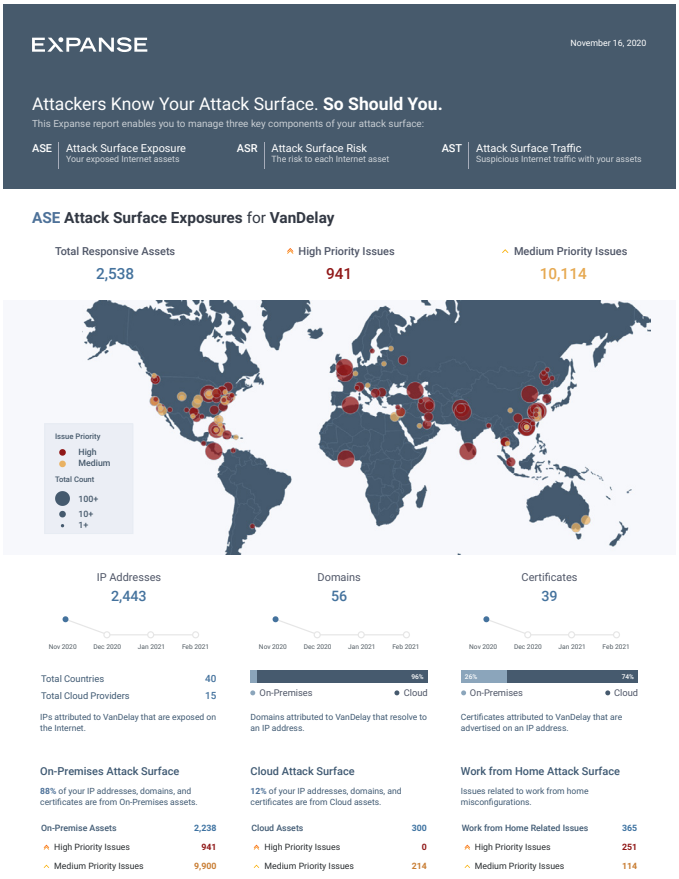

Figure 1: An Expanse Attack Surface Report

Cortex XDR

Cortex XDR™ is the industry's first extended detection and response platform that integrates data from across your organization to stop modern attacks. Cortex XDR has been designed from the ground up to deliver enterprise-wide protection while simplifying security operations by breaking down security silos. Using behavioral analytics and AI, Cortex XDR identifies unknown and highly evasive threats targeting your network.

Your analysts can quickly investigate threats by getting a complete picture of each incident. Cortex XDR reveals the root cause of alerts from any source by stitching together data from different sources, allowing analysts of all experience levels to triage incidents. Tight integration with enforcement points lets you respond to threats anywhere in your organization or restore hosts to a clean state easily.

Cortex XDR can collect rich data from your endpoints, firewalls, and other security infrastructure to reveal indicators of SolarStorm attacks. Deployed as part of a SolarStorm Cybersecure Engagement, Cortex XDR can block threats, detect suspicious activity, and secure your environment from follow-up attacks.

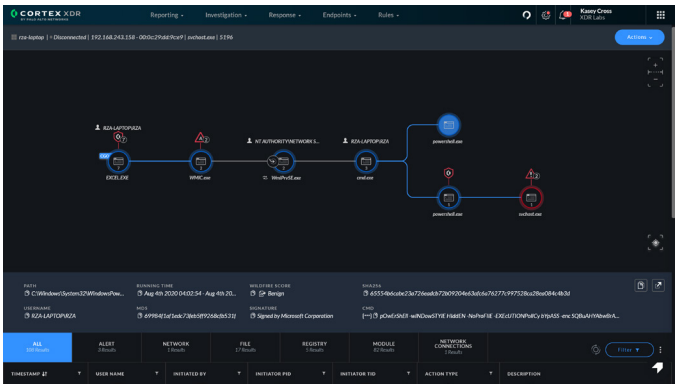

Figure 2: Cortex XDR triage and investigation view

Request a SolarStorm Rapid Assessment

If you are concerned that your organization may have been breached, sign up for a SolarStorm Rapid Assessment today at paloaltonetworks.com/solarstorm-rapid-response. We're here to help you.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

parent_ds_solarstorm-rapid-response_111720