Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:33:10 UTC

Tool: SUNBURST

Names	SUNBURST Solorigate
Category	Malware
Type	Backdoor
Description	(US-CERT) The threat actor has been observed leveraging a software supply chain compromise of SolarWinds Orion products. The adversary added a malicious version of the binary solarwinds.orion.core.businesslayer.dll into the SolarWinds software lifecycle, which was then signed by the legitimate SolarWinds code signing certificate. This binary, once installed, calls out to a victim-specific avsvmcloud[.]com domain using a protocol designed to mimic legitimate SolarWinds protocol traffic. After the initial check-in, the adversary can use the Domain Name System (DNS) response to selectively send back new domains or IP addresses for interactive command and control (C2) traffic. Consequently, entities that observe traffic from their SolarWinds Orion devices to avsvmcloud[.]com should not immediately conclude that the adversary leveraged the SolarWinds Orion backdoor. Instead, additional investigation is needed into whether the SolarWinds Orion device engaged in further unexplained communications. If additional Canonical Name record (CNAME) resolutions associated with the avsvmcloud[.]com domain are observed, possible additional adversary action leveraging the backdoor has occurred.
Information	<https://us-cert.cisa.gov/ncas/alerts/aa20-352a> <http://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html> <https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html> <https://github.com/fireeye/sunburst_countermeasures> <https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html> <https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/> <https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-

compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/>
<https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>
<https://www.guidepointsecurity.com/analysis-of-the-solarwinds-supply-chain-attack/>
<https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html>
<https://blog.malwarebytes.com/threat-analysis/2020/12/advanced-cyber-attack-hits-private-and-public-sector-via-supply-chain-software-update/>
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-solarwinds-supply-chain-attack>
<https://unit42.paloaltonetworks.com/fireeye-solarstorm-sunburst/>
<https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline/>
<https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>
<https://www.cadosecurity.com/post/responding-to-solarigate>
<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds>
<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-unique-dga>
<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-sunburst-command-control>
<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-sunburst-sending-data>
<https://www.picussecurity.com/resource/blog/ttps-used-in-the-solarwinds-breach>
<https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth>
<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/sunburst-malware-and-solarwinds-supply-chain-compromise/>
<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/additional-analysis-into-the-sunburst-backdoor/>
<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/how-a-device-to-cloud-architecture-defends-against-the-solarwinds-supply-chain-compromise/>
<https://www.tripwire.com/state-of-security/vert/vert-alert-solar-winds-supply-chain-attack/>
<https://blog.cyberint.com/solarwinds-supply-chain-attack>
<https://blog.checkpoint.com/2020/12/21/best-practice-identifying-and-mitigating-the-impact-of-sunburst/>
<https://research.checkpoint.com/2020/sunburst-teardrop-and-the-netsec-new-normal/>
<https://mp.weixin.qq.com/s/UqXC1vovKUu97569LkYm2Q>
<https://blog.qualys.com/qualys-insights/2020/12/22/qualys-security-advisory-solarwinds-fireeye>
<https://www.cyfirma.com/solarwinds-hack-sunburst-supernova-and-more/>

	<https://gist.github.com/SwitHak/8b59e740b187511caad1bf06caa44df1> <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039a>
MITRE ATT&CK	<https://attack.mitre.org/software/S0559/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sunburst>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool SUNBURST

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=e0b7942d-4f1d-4565-a5fe-e9ac69a68d5b