Significant Cyber Event (SCE) Intelligence Report

SUNBURST Malware: A SolarWinds Orion Supply Chain Compromise

December 14, 2020

Executive Summary of Event

A global campaign impacting supply chain compromise was discovered with wide reaching impact against both public and private entities within North America, Europe, Asia, and the Middle East.

The SUNBURST malware was distributed using the SolarWinds Orion official updates, which allows external threat actors to gain elevated credentials access thus leading to compromising the entire network.

A security advisory that addresses the event was released through the SolarWinds Customer Portal. This campaign affects SolarWinds Orion Platform software builds versions 2019.4 HF 5 through 2020.2.1. These versions were released between March 2020 and June 2020.

deepwatch does not use SolarWinds products.

Potential Impact

SUNBURST malware results in allowing administrative permissions to a malicious actor, and thus elevated access to critical components connected to an organization’s global administrator account and/or trusted SAML token signing certificate. This enables the actor to forge SAML tokens that impersonate any of the organization’s existing users and accounts, including highly privileged accounts.

Technical Details

The SUNBURST malware leverages the supply chain attack methodology, where attackers target the trust of upstream providers in the software supply network with an ultimate goal of accessing a larger target.

In this particular case the actors targeted the SolarWinds Orion platform through software updates. FireEye posted an analysis of the SolarWinds code flaw (see link #2 in supporting information below), tracing the problem to a file called SolarWinds.Orion.Core.BusinessLayer.dll, which it describes as a "digitally-signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third-party servers.”

According to FireEye, "*The malware masquerades its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers.*"

The malware lays dormant for 14 days before attempting to resolve a subdomain of avsvmcloud[.]com. A DNS record response will return a Command and Control (C2) domain. Traffic from the malicious domain is designed to mimic normal API SolarWinds communications.

FireEye has released Indicators Of Compromise and countermeasures to their GitHub repository found in our supporting information link #3.

deepwatch Strategy

deepwatch has updated our threat intelligence platform with FireEye released IOC's (Supporting Information link #3). If any activity associated with the IOCs is observed, deepwatch will notify customers in accordance with the standard operating procedures. Additionally, deepwatch is evaluating detection options.

deepwatch Recommendations

deepwatch recommends that you reach out to your SolarWinds Vendor to verify the correct steps needed for updating your SolarWinds platform in a secure fashion, reducing the risk of reinfections.

SolarWinds recommends you upgrade to Orion Platform version 2020.2.1 HF 2 (available December 15, 2020) as soon as possible to ensure the security of your network. The latest version is available in the SolarWinds Customer Portal.

The primary mitigation steps include having your Orion Platform installed behind firewalls, disabling internet access for the Orion Platform and limiting the ports and connections to only what is necessary.

In addition to patching the Orion Platform, deepwatch recommends auditing SAML access and administrator groups and accounts and searching authentication logs and events for anomalous activity.

Supporting Information

1. https://www.solarwinds.com/securityadvisory
2. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
3. https://github.com/fireeye/sunburst_countermeasures
4. https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/