Trojan:MSIL/Solorigate.B!dha

Published Dec 13, 2020 | Updated Apr 26, 2021

Learn about other threats

Detected by Microsoft Defender Antivirus
Aliases: No associated aliases

Summary

This threat can allow remote sophisticated attackers to gain access and perform backdoor commands on an affected device. It is a modified DLL component of a legitimate software.

Attackers use this threat to gain initial access to a device. When the related software is opened, this modified DLL is loaded and connects to command-and-control servers to listen for commands and get additional payloads.

Microsoft Defender Antivirus detects this threat. It raises an alert when it detects the threat on your device, but it doesn't automatically remediate it in order to not affect legitimate services. If this threat is detected on your environment, we recommend that you immediately investigate and manually remediate it.

NOTE: Microsoft continues to work with partners and customers to expand our knowledge of the threat actor behind the nation-state cyberattacks that compromised the supply chain of SolarWinds and impacted multiple other organizations. Microsoft previously used ‘Solorigate’ as the primary designation for the actor, but moving forward, we want to place appropriate focus on the actors behind the sophisticated attacks, rather than one of the examples of malware used by the actors. Microsoft Threat Intelligence Center (MSTIC) has named the actor behind the attack against SolarWinds, the SUNBURST backdoor, TEARDROP malware, and related components as NOBELIUM. As we release new content and analysis, we will use NOBELIUM to refer to the actor and the attack campaigns.

Read our latest reports:

To help reduce the impact of this threat, you can:

- Immediately isolate the affected device. If malicious code has been launched, it is likely that the device is under complete attacker control.
- Identify the accounts that have been used on the affected device and consider these accounts compromised. Reset passwords or decommission the accounts.
- Investigate how the affected endpoint might have been compromised. Check web and email traffic to determine how the malware arrived.
- Investigate the device timeline for indications of lateral movement activities using one of the compromised accounts. Check for additional tools that attackers might have dropped to enable credential access, lateral movement, and other attack activities.

Microsoft Defender Antivirus detects this threat. It raises an alert when it detects the threat on your device, but it doesn't automatically remediate it in order to not affect legitimate services. If this threat is detected on your environment, we recommend that you immediately investigate and manually remediate it.

You can also visit our advanced troubleshooting page or search the virus and malware community for more help.