UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00083

SECOND STAGE SOLARWINDS ATTACK

DATE ISSUED: 21st December 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Also known as Solorigate, the Sunburst malware associated with the recent SolarWinds attacks as the preliminary stage of the targeted attacks, has been investigated to reveal a back door, command and control (C2) domain and further persistent threat capabilities.

BREAKDOWN

Kaspersky researchers have followed the trail to discover companies affected by the backdoor and which have been selected for further attack. The group dubbed DarkHalo or UNC2452 have displayed in depth knowledge of Microsoft's Office 365, Azure, Exchange and PowerShell products, leveraging this to perform their attacks and ensnare victims through email monitoring and extraction. One of the ways Sunburst managed to go undetected is the delayed kick-off and a signed SolarWinds certificate to make the DLL appear to be safe and legitimate. This supply chain attack has been carefully strategized, well thought out, and expertly executed. Using DNS requests that were altered to contain additional information and encoded to exfiltrate system information and communicated with the C2, the attackers then decide which victims should be given additional attention and move on to the second stage. These DNS records allowed researchers to more easily identify victims. While these discoveries are considered a breakthrough, much is still unknown about the attack group and their methods. A key domain used in the attacks has since been seized by Microsoft and their industry partners and is being utilised as a killswitch to prevent further malicious activities.

REMEDIATION STEPS

- Implement remediation action provided by SolarWinds https://www.solarwinds.com/securityadvisory#https://www.solarwinds.com/securityadvisory
- Locate any assets using SolarWinds applications and consider isolating servers from the network
- Change passwords linked to any SolarWinds accounts and check security configurations

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/sunburst-c2-secrets-rsolarwinds-victims/162426/
ZDNet: https://www.zdnet.com/article/microsoft-and-industry-partners-seize-key-domain-used-in-solarwinds-hack/