VOLEXITY // INTELLIGENCE

RESPONDING TO THE SOLARWINDS BREACH

Detect, Prevent, and Remediate the Dark Halo Supply Chain Attack

16 December 2020

11654 Plaza America Dr. #774 Reston VA 20190-4700 | www.volexity.com | contact@volexity.com

INTRODUCTION

Earlier this week, Volexity published a blog post providing details observed from multiple incident response efforts involving Dark Halo, the group tied to the SolarWinds breach. Since publication, Volexity has fielded and observed countless inquiries from organizations and individuals attempting to determine if they have been compromised. As a result of widespread confusion and concern, Volexity has written this guide to address some common questions and misconceptions, and to provide additional guidance.

HAVE I BEEN BREACHED?

This is the big question people want to answer with regard to their SolarWinds Orion installations. In order to figure this out, you first need to determine if you are, or were running, a compromised version of the software. If you know for a fact that your organization was regularly updating your SolarWinds Orion software, you should assume you were running a compromised version. Below are two methods to validate:

- Examine your systems to see if you were or are running Orion Platform versions 2019.4 HF 5,2020.2 with no hotfix installed, or with 2020.2 HF 1
- Look at your organization's current and historic DNS queries to see if there have been DNS queries to hostnames on the domain avsvmcloud[.]com

If any or all of these conditions were met, you were in the sphere of impacted customers running a compromised version of the software. However, though rightfully concerning, this alone does not mean your organization experienced data loss or a real hands-on intrusion. While this alone is a major concern, Volexity would surmise the vast majority of organizations running the compromised software were never further targeted.

Determining if you were breached requires having the right data available. If your organization was targeted by Dark Halo, you will need to search and historically determine the following:

- Did any of the DNS queries back to avsvmcloud[.]com return a CNAME record?
- Are there DNS queries or connections to any of the network IOCs provided by Volexity and FireEye from your network and your SolarWinds Orion server specifically in the last nine months?
- Did your SolarWinds Orion system make DNS queries for unexpected domains in the last nine months?
- Did your SolarWinds Orion system connect out to webservers on the Internet in the last nine months, and start communicating with hosts that it clearly should not have or otherwise cannot be explained?

Observing a CNAME response from a DNS query to avsvmcloud[.]com is the best way to determine if your organization was of interest to Dark Halo and potentially the victim of much more serious breach. If you see this in your historic DNS records, a full incident response process should be initiated immediately. The same largely holds true if you see queries and/or connections to known bad IOCs. However, Volexity believes in some cases Dark Halo may have used certain domains with only one victim. The published list of IOCs should not be considered exhaustive.

In the event an organization does not have information pertaining to CNAME records or any known hits for IOCs, generally looking at DNS queries or network connections from your SolarWinds Orion server would be the next best thing. Unexplained DNS queries and/or associated outbound connections from the server should be treated as highly suspect and potentially related.

PREVENTION AND DETECTION

- Prevent unnecessary access to the Internet from servers that do not require it. Note: Volexity had multiple customers whose SolarWinds Orion servers were not permitted to talk to the Internet. This effectively mitigated the command-and-control (C2) mechanism from this malware.
- Monitor corporate assets for logins from systems where authentication should not be sourced (e.g., interactive logins such as RDP access should likely not be allowed from many devices on the network).
- Leverage historical command-line data recorded by event logging or endpoint detection software for signs of "rundll32.exe" and "cmd.exe" being spawned from "wmiprvse.exe" or the "solarwinds.businesslayerhost.exe" processes. It would also be useful to examine this data for new files observed on/around the time of any connections to the malicious IPs/domains provided in our previous blog.
- Leverage historical command-line data recorded by endpoint security software looking for indicators of the AdFind tool from Joeware.

- Look for unauthorized and broad-sweeping e-mail forwarding rules configured on gateway e-mail appliances.
- Review historic web logs from devices like on-premise Exchange server to look for signs of webshell access or downloads of files that are not typically accessed.
- Examine on-premise mail servers for signs of mailbox export requests, accounts with delegated permissions that exceed what should be permitted, or signs that e-mail is being forwarded external to the organization.
- Audit Office 365/Azure AD service principals and enterprise applications to look for those that may not be authorized or are being accessed with credentials or keys that were not authorized.
- Examine Office 365 configuration settings to ensure unauthorized mail forwarding at the system or user level is not occurring. This includes examining global transport rules.

REMEDIATION

The steps to remediate a full compromise where Dark Halo has breached an organization's network are more complicated than we can list in this blog post. Each incident is different and often involves some amount of customization unique to the victim organization. However, below are a handful of items that Volexity recommends organizations consider based on our experience conducting multiple incident response engagements involving the group.

- Rebuild impacted servers and start with a fresh updated install of SolarWinds Orion. Note: Volexity recommends this step even for organizations that are not believed to have been subject to secondary targeting.
- Reset all credentials that may have been impacted in the organization and ensure new passwords are not similar to previous passwords. This would likely include all accounts in an active directory domain, to include user accounts, service accounts, etc.
- Ensure that unique local administrative passwords are used on all devices; use a password management solution where possible.
- Reset/replace/re-issue all sensitive API key integrations, such as those leveraged by multi-factor, SAML integrations, website configuration files, etc.

STILL HAVE QUESTIONS OR CONCERNS?

Please feel free to reach out to the Volexity team via e-mail to contact@volexity.com if you still have questions or believe you may have had an incident and you need assistance.