Dark Halo Leverages SolarWinds Compromise to Breach Organizations

By mindgrub

Published: 2020-12-14 · Archived: 2026-04-05 16:44:04 UTC

Volexity is releasing additional research and indicators associated with compromises impacting customers of the SolarWinds Orion software platform. Volexity has also published a guide for responding to the SolarWinds breach, and how to detect, prevent, and remediate this supply chain attack.

On Sunday, December 13, 2020, FireEye released a blog detailing an alleged compromise to the company SolarWinds. This compromise involved a backdoor being distributed through an update to SolarWind's Orion software product. FireEye attributed this activity to an unknown threat actor it tracks as UNC2452. Volexity has subsequently been able to tie these attacks to multiple incidents it worked in late 2019 and 2020 at a US-based think tank. Volexity tracks this threat actor under the name **Dark Halo**.

At one particular think tank, Volexity worked three separate incidents involving Dark Halo. In the initial incident, Volexity found multiple tools, backdoors, and malware implants that had allowed the attacker to remain undetected for several years. After being extricated from the network, Dark Halo then returned a second time, exploiting a vulnerability in the organization's Microsoft Exchange Control Panel. Near the end of this incident, Volexity observed the threat actor using a novel technique to bypass Duo multi-factor authentication (MFA) to

access the mailbox of a user via the organization's Outlook Web App (OWA) service. Finally, in a third incident, Dark Halo breached the organization by way of its SolarWinds Orion software in June and July 2020.

The primary goal of the Dark Halo threat actor was to obtain the e-mails of specific individuals at the think tank. This included a handful of select executives, policy experts, and the IT staff at the organization. Volexity notes its investigations are directly related to the FireEye report based on overlap between command-and-control (C2) domains and other related indicators such as a backdoored server running SolarWinds Orion.

Major Incidents

Volexity has worked three major incidents involving the Dark Halo threat actor. In most cases, the actor aimed to live off the land, primarily focusing on weekly operations to extract e-mail messages from the organization. Dark Halo did use malware and red-teaming tools but largely only for specific one-time tasks as a fallback mechanism when other avenues of access were cut off. For the purposes of this write-up, Volexity will share novel and useful information from the second and third incidents. The second incident involved a sophisticated way to obtain unauthorized access to an account via OWA that had MFA protection in place. The third incident involved a breach by way of the SolarWinds Orion platform.

Bypassing Multi-Factor Authentication

Toward the end of the second incident that Volexity worked involving Dark Halo, the actor was observed accessing the e-mail account of a user via OWA. This was unexpected for a few reasons, not least of which was the targeted mailbox was protected by MFA. Logs from the Exchange server showed that the attacker provided username and password authentication like normal but were not challenged for a second factor through Duo. The logs from the Duo authentication server further showed that no attempts had been made to log into the account in question. Volexity was able to confirm that session hijacking was not involved and, through a memory dump of the OWA server, could also confirm that the attacker had presented cookie tied to a Duo MFA session named **duo-sid**.

Volexity's investigation into this incident determined the attacker had accessed the Duo integration secret key (**akey**) from the OWA server. This key then allowed the attacker to derive a pre-computed value to be set in the duo-sid cookie. After successful password authentication, the server evaluated the duo-sid cookie and determined it to be valid. This allowed the attacker with knowledge of a user account and password to then completely bypass the MFA set on the account. It should be noted this is not a vulnerability with the MFA provider and underscores the need to ensure that all secrets associated with key integrations, such as those with an MFA provider, should be changed following a breach. Further, it is important that not only are passwords changed after a breach, but that passwords are not set to something similar to the previous password (e.g., *Summer2020!* versus *Spring2020!* or *SillyGoo$e3* versus *SillyGoo$e2*).

SolarWinds

In the third incident, which took place in July 2020, Volexity identified suspicious administrative commands and ActiveSync anomalies in the organization's Exchange environment. Further review of the organization's endpoint software and network traffic confirmed a breach. The attacker had executed commands to export e-mail for

specific users in the organization, and then exfiltrated the data via the organization's Outlook Web Anywhere (OWA) server.

Many of the technical details regarding the malware used are covered in the FireEye notification. However, in this blog, Volexity can share examples of command-line actions the attacker took after gaining access to the target network and provide insight into additional tools, infrastructure, and attacker objectives.

Reconnaissance

The attacker was quite adept with Exchange and immediately listed various organization configuration settings via PowerShell. Below are a few of the operations that the attacker executed.

- Get a list of users on the Exchange server and their current role using Get-ManagementRoleAssignment:

```
C:\Windows\system32\cmd.exe /C powershell.exe -PSConsoleFile exshell.psc1 -Command "Get-ManagementRoleAssignment -GetEffectiveUsers | select Name,Role,EffectiveUserName,AssignmentMethod,IsValid | ConvertTo-Csv -NoTypeInformation | % {$_ -replace '`n','_'} | Out-File C:\temp\1.xml"
```

- Retrieve information about the configured Virtual Directory using Get-WebServicesVirtualDirectory:

```
C:\Windows\system32\cmd.exe /C powershell.exe -PSConsoleFile exshell.psc1 -Command "Get-WebServicesVirtualDirectory | Format-List"
```

The attacker also made use of a file called sqlceip.exe, which upon first glance might appear as the legitimate version of SQL Server Telemetry Client provided by Microsoft. However, Volexity determined this tool was actually a version of AdFind from joeware.net. AdFind is a command-line tool used for querying and extracting data from Active Directory. During the course of its investigations, Volexity discovered the attacker using AdFind with the following command line:

```
C:\Windows\system32\cmd.exe /C sqlceip.exe -default -f (name="Organization Management") member -list | sqlceip.exe -f objectcategory=* > .\SettingSync\log2.txt
```

Lateral Movement

The attacker used PowerShell to create new tasks on remote machines:

```
$scheduler = New-Object -ComObject ("Schedule.Service");$scheduler.Connect($env:COMPUTERNAME);$folder = $scheduler.GetFolder("\Microsoft\Windows\SoftwareProtectionPlatform");$task = $folder.GetTask("EventCacheManager");$definition = $task.Definition;$definition.Settings.ExecutionTimeLimit = "PT0S";$folder.RegisterTaskDefinition($task.Name,$definition,6,"System",$null,5);echo "Done"
```

They also attempted this on a number of machines using schtasks.exe directly. For example:

> C:\Windows\system32\cmd.exe /C schtasks /create /F /tn "\Microsoft\Windows\SoftwareProtectionPlatform\EventCacheManager" /tr "C:\Windows\SoftwareDistribution\EventCacheManager.exe" /sc ONSTART /ru system /S [machine_name]

Exfiltration

The attacker exfiltrated e-mail data from targeted accounts using the New-MailboxExportRequest command followed by Get-MailboxExport-Request command. In this case, the attacker was only interested in mail received this year.

> C:\Windows\system32\cmd.exe /C powershell.exe -PSConsoleFile exshell.psc1 -Command "New-MailboxExportRequest -Mailbox foobar@organization.here -ContentFilter {(Received -ge '03/01/2020')} -FilePath '\<MAILSERVER>\c$\temp\b.pst'"

The attacker created password-protected archives on the victims' OWA server so that they could be exfiltrated via a simple HTTP request.

> C:\Windows\system32\cmd.exe /C .\7z.exe a -mx9 -r0 -p[33_char_password] "C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Redir.png" C:\Temp\b.pst

An example URL for the attacker to collect the exfiltrated data would be:

> https://owa.organization.here/owa/auth/Redir.png

On disk, this was located at the following path:

> \Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\

Volexity also saw the attacker stage other exfiltration in another folder on the server located here:

> \Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resources\

Finally, the attacker added their own devices as allowed IDs for active sync for a number of mailboxes using Set-CASMailbox:

> C:\Windows\system32\cmd.exe /C powershell.exe -PSConsoleFile exshell.psc1 -Command "Set-CASMailbox -Identity <UserID> -ActiveSyncAllowedDeviceIDs @{add='XXXXXXXXXXXXX'}"

Attacker Cleanup

After successfully exporting mail they wished to steal, the attacker would remove the evidence of the export request using Remove-MailboxExportRequest:

> C:\Windows\system32\cmd.exe /C powershell.exe -PSConsoleFile exshell.psc1 -Command "Get-MailboxExportRequest -Mailbox user@organization.here | Remove-MailboxExportRequest -

> Confirm:$False”

Attacker Infrastructure

During the July 2020 incident, Volexity observed at least two indicators that overlapped with indicators of compromise posted by FireEye. The organization’s SolarWinds server conducted DGA-style DNS queries under the following subdomain:

> appsync-api.us-west-2.avsvmcloud[.]com

The vast majority of queries were met with SERVFAIL responses. In most other cases, the hostnames resolved to IPs that fell in the ranges 184.72.0.0/16, 20.141.48.0/24, 8.18.144.0/24, and 8.18.145.0/24. However, the critical responses to the organization came by way of CNAME responses that occurred between June 30, 2020, and July 16, 2020. These DNS resolutions returned a CNAME for the domain **freescanonline[.]com**. In late July, the attacker took advantage of their access and started moving laterally throughout the organization, which will be described a bit later. Most notably the attacker pushed malware to other systems that beaconed back to the following additional infrastructure:

> lcomputers[.]com
>
> webcodez[.]com

At the time of the incident (July 2020), the attacker had accidentally configured their servers to be open to the Internet, accepting arbitrary requests on port 80. Since then, the attacker has fixed this issue; however, at the time, Volexity was able to identify a number of C2 addresses based on server profiling.

Specifically, at the time there were only a handful of servers that responded with the following HTTP headers in the following order:

- Transfer-Encoding
- Connection
- Server
- X-Powered-By
- Date

The “Server” value also specified IIS10.0, but this header order does not match the order used by IIS 10.0.

Based on this pattern Volexity was able to identify the following IP addresses in July 2020:

> 13.57.184.217
> 13.59.205.66
> 18.217.225.111
> 18.220.219.143
> 3.16.81.254
> 3.87.182.149
> 34.219.234.134

> 54.193.127.66
> 54.215.192.52

These IPs hosted SSL certificates for the following domains:

> deftsecurity[.]com
> digitalcollege[.]org
> freescanonline[.]com
> globalnetworkissues[.]com
> kubecloud[.]com
> seobundlekit[.]com
> solartrackingsystem[.]net
> thedoccloud[.]com
> virtualwebdata[.]com

Notably, some of these domains were set up prior to the earlier known compromise date published by FireEye, such as solartrackingsystem[.]net, which was assigned its current nameserver in January 2020. Several of the domains also have very long registration histories going back several years. Volexity believes that attacker obtained these domains through auctions or from registrants after they expired but before they were deleted. This allowed the attacker to use domains with a long history and avoid being detected based on detections tied to a domain being newly registered.

Conclusion

At the time of the investigation, Volexity deduced that the likely infection was the result of the SolarWinds box on the target network; however, it was not fully understood exactly how the breach occurred (i.e., whether there was some unknown exploit in play, or other means of access), therefore Volexity was not in a position to report the circumstances surrounding the breach to SolarWinds. The machines involved in this incident had been rebooted several times prior to Volexity's involvement in incident response efforts, meaning that a great deal of evidence that would have been in volatile memory had been lost.

Volexity believes that Dark Halo is a sophisticated threat actor based on the following characteristics of their attacks:

- Generally, the attacker displayed a reasonable level of operational security throughout the attack, taking steps to wipe logs for various services used and to remove evidence of their commands from infected systems.
- The server profile used to identify the C2 domains was only visible for a snapshot in time, where the attacker likely became aware that their C2 addresses could be identified in this way, they went on to secure their C2 servers further.
- Despite an ongoing campaign lasting one year, very few files related to this attacker have made their way to VirusTotal.

During the investigation Volexity discovered no hints as to the attacker's origin or any links to any publicly known threat actor.

To protect against these attacks, Volexity recommends the following:

- Look for traffic to any of the related malicious domains identified in Appendix A.
- Follow the advice from SolarWinds in their response to this incident.
- Use the signatures provided by FireEye to identify related activity.
- Ensure that all secret keys associated with MFA or other sensitive integrations are reset following a breach.
- Make sure all credentials in an organization, including service accounts, are reset following a breach and that default passwords or those similar to previous passwords are not used.
- If you run an on-premise Exchange environment, consider adding alerting mechanisms to any EDR solutions for processes using the Exchange Management Shell PowerShell cmdlets listed in Appendix B. This may or may not be a valid detection approach depending on how frequently this is used within your organization.
- More generally, if the Exchange Management Shell is rarely used in a legitimate Administrative context, it may be worth investigating any historical use of this shell.

Appendix A – IP and Domain IOCs

> 13.57.184.217
> 13.59.205.66
> 18.217.225.111
> 18.220.219.143
> 196.203.11.89
> 3.16.81.254
> 3.87.182.149
> 3.87.182.149
> 34.219.234.134
> 54.193.127.66
> 54.215.192.52
> avsvmcloud[.]com
> deftsecurity[.]com
> digitalcollege[.]org
> freescanonline[.]com
> globalnetworkissues[.]com
> kubecloud[.]com
> lcomputers[.]com
> seobundlekit[.]com
> solartrackingsystem[.]net
> thedoccloud[.]com
> virtualwebdata[.]com
> webcodez[.]com

Appendix B – Exchange Management Shell Powershell cmdlets

> Get-AcceptedDomain
>
> Get-CASMailbox
>
> Get-Mailbox
>
> Get-ManagementRoleAssignment
>
> Get-OrganizationConfig
>
> Get-OwaVirtualDirectory
>
> Get-Process
>
> Get-WebServicesVirtualDirectory
>
> New-MailboxExportRequest
>
> Remove-MailboxExportRequest
>
> Set-CASMailbox

Appendix C – DGA Domain Resolutions

> 184.72.1.3
> 184.72.101.22
> 184.72.113.55
> 184.72.145.34
> 184.72.209.33
> 184.72.21.54
> 184.72.212.52
> 184.72.224.3
> 184.72.229.1
> 184.72.240.3
> 184.72.245.1
> 184.72.48.22
> 20.141.48.154
> 8.18.144.11
> 8.18.144.12
> 8.18.144.130
> 8.18.144.135
> 8.18.144.136
> 8.18.144.149
> 8.18.144.156
> 8.18.144.158
> 8.18.144.165

> 8.18.144.170
> 8.18.144.180
> 8.18.144.188
> 8.18.144.20
> 8.18.144.40
> 8.18.144.44
> 8.18.144.62
> 8.18.144.9
> 8.18.145.131
> 8.18.145.134
> 8.18.145.136
> 8.18.145.139
> 8.18.145.150
> 8.18.145.157
> 8.18.145.181
> 8.18.145.21
> 8.18.145.3
> 8.18.145.33
> 8.18.145.36
