WHITEPAPER

SOLARWINDS BREACH – SUPPLY CHAIN ATTACK DETECTION WITH THE THREATDEFEND® PLATFORM

TABLE OF CONTENT

EXECUTIVE SUMMARY

As organizations continue to embrace third-party vendors for software and applications, they expose themselves to potential risks in their supply chain. New types of attacks increase the risks associated with a supply chain attack considerably. Attackers have more resources and tools at their disposal than ever before, creating a perfect storm.

In December 2020, the world witnessed the SolarWinds hack, one of the most significant cyberattacks that targeted US government agencies and private companies. The SolarWinds hack by suspected nation-state threats actors has impacted an estimated 18,000 of its 300,000 customers worldwide. The SolarWinds Orion security breach is unfolding rapidly, and the number of victims continues to grow.

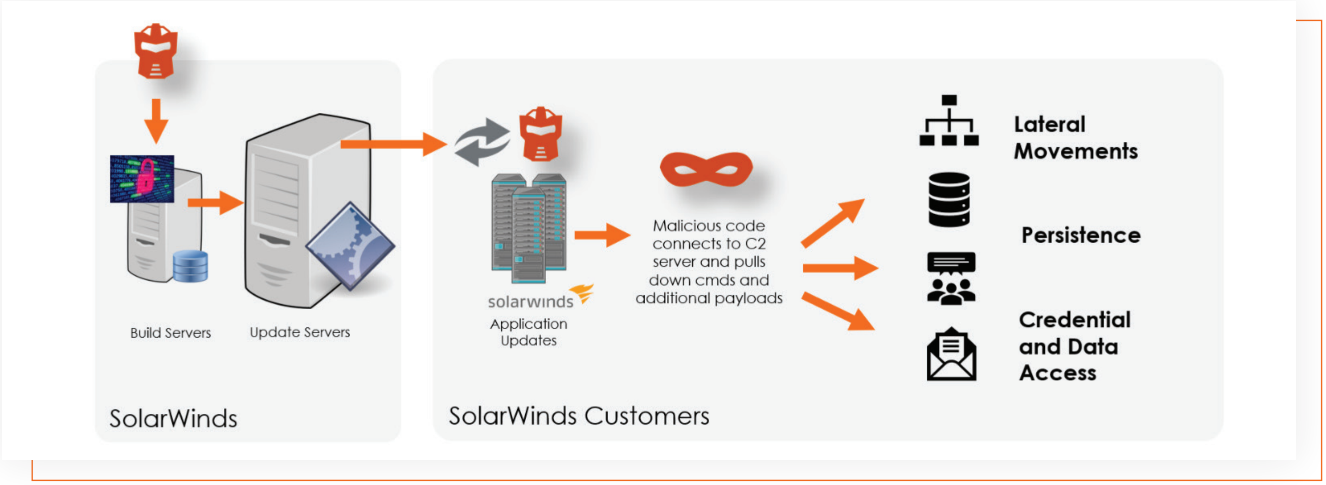
Reviewing the SolarWinds supply chain attack and identifying key detection opportunities in each stage gives organizations options to reduce their exposure and identifies mitigations that enable them to survive supply chain attacks.

WHAT IS A SUPPLY CHAIN ATTACK?

In information security, a supply chain attack seeks to damage an organization by targeting less-secure elements in its supply chain. A supply chain or third-party attack can occur in any industry, from the financial sector, healthcare, manufacturing, or government sector, which uses outside products and services. Cybercriminals typically target organizations using third-party hardware or software products, deliberately tampering with a product's manufacturing process by installing malicious software or hardware-based spying components. These tactics allow attackers to infiltrate systems through a partner and access an organization's sensitive data.

ANATOMY OF A SUPPLY CHAIN ATTACK

Supply chain attacks are not new to the IT world, but they are becoming more sophisticated. According to a survey conducted in June 2020 by Opinion Matters, 77% of organizations have limited visibility around their third-party vendors, and 80% have suffered a third-party related breach by one of their vendors. As organizations invest in third-party software and services, it is imperative to evaluate each downloaded application or software update and monitor for potential security risks.

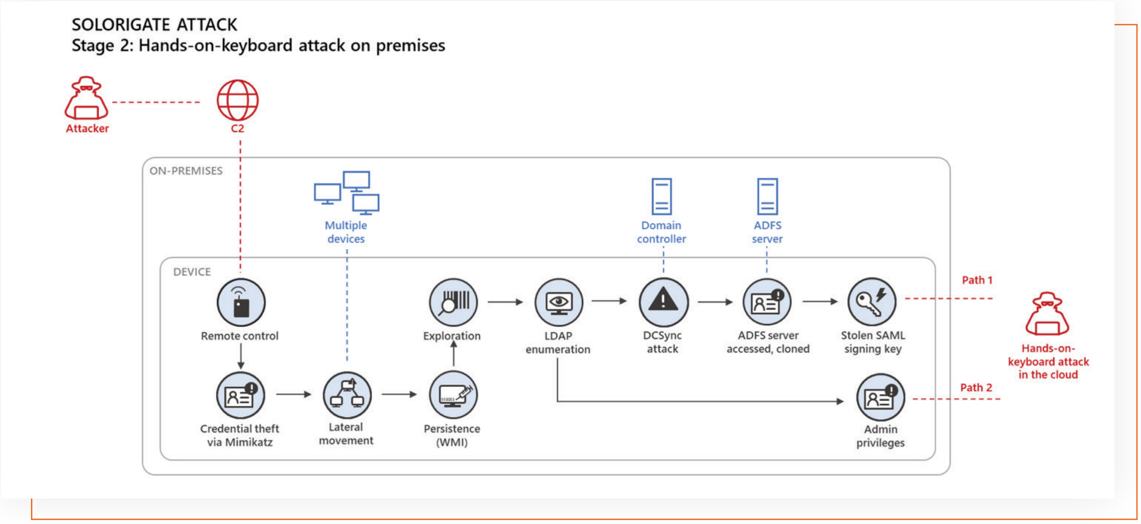


The following analysis examines the SolarWinds supply-chain incident, which allowed attackers to access the organization's critical assets.

In March 2020, SolarWinds released updates to its Orion product, an IT monitoring and management software solution, which unbeknownst to them contained a malicious component added by threat actors. The attackers managed to modify an Orion platform plug-in called SolarWinds.Orion.Core.BusinessLayer.dll, which installs as part of the Orion platform. Customers downloaded the latest available package on the update servers and installed it, unknowingly infected themselves. After lying dormant for up to two weeks, the malicious component, which contained a backdoor, contacted a command-and-control (C2) server and executed scheduled tasks to gain remote network access. Once the attackers completed the initial compromise, they moved laterally through the network and stole SAML token keys to access the organization's critical assets.

MICROSOFT ANALYSIS OF SOLARWINDS ATTACK

Microsoft has published a blog detailing the attacker's lateral movement after establishing a backdoor into an organization. The attacker's primary goal is to escalate privileges to SAML keys from ADFS servers and gain access to an organization's cloud resources.



There are multiple detection opportunities at various stages to detect the attacker's lateral movement inside the network. The following is an in-depth analysis from Attivo Networks of the tactics and behaviors attackers will use in attacks such as the SolarWinds supply-chain attack after compromising the network. It also identifies the detection opportunities that prevent damage to the organization's critical assets.

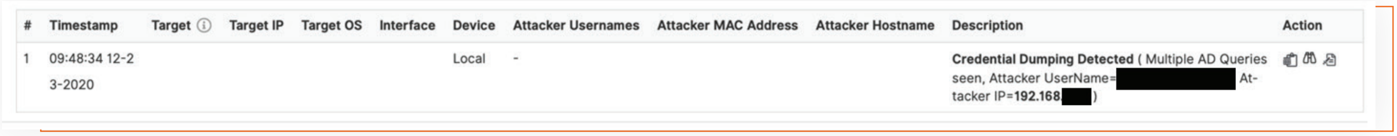
CREDENTIAL THEFT

Credential theft consists of techniques to steal authentication information such as account names, passwords, and cloud access keys. The attackers will exploit an infected endpoint to extract credentials and locate targeted assets. They will try to gain an initial foothold into the network by leveraging remote access mechanisms from external locations. Attackers will use tools like Mimikatz to extract cleartext passwords and password hashes from memory to obtain account login and password information. They use these credentials to perform lateral movement and access to restricted information. Attackers will also exfiltrate stolen data and established backdoors for subsequent attacks.

DETECTION OPPORTUNITY

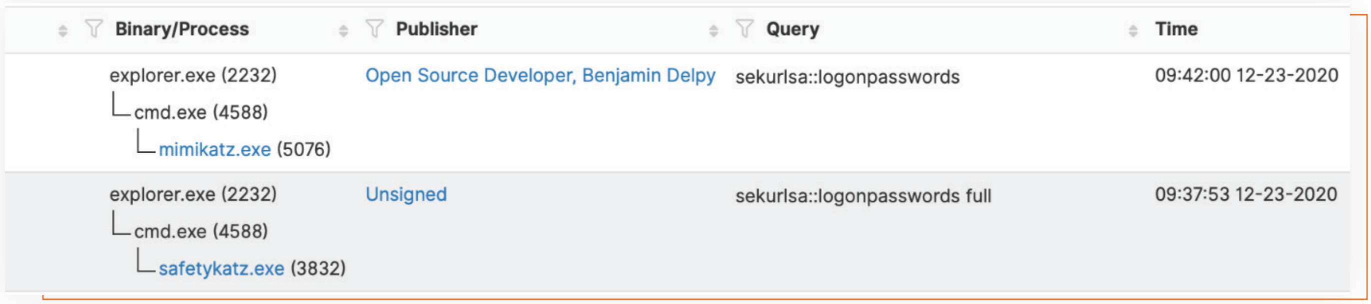
The Attivo Networks® ThreatDefend platform combats supply-chain attacks and related malware by deploying decoy systems and deceptive assets on the endpoints, including decoy credentials and fake file shares. The ThreatDefend® platform provides early visibility into attackers using in-memory credential theft or password dumping tools to steal and use the decoy credentials. The Attivo Endpoint Deception Net (EDN) suite includes the ThreatStrike solution, which provides deceptive lures with real data to redirect attackers towards deceptive assets or detect when they use decoy credentials in the network. The EDN suite also detects various memory dumping techniques attackers use to steal credentials. The following images show a detection event with detailed process information.

Credential Dumping Event:



#	Timestamp	Target	Target IP	Target OS	Interface	Device	Attacker Usernames	Attacker MAC Address	Attacker Hostname	Description	Action
1	09:48:34 12-23-2020					Local	-			**Credential Dumping Detected** (Multiple AD Queries seen, Attacker UserName=[redacted] Attacker IP=**192.168**[redacted])	

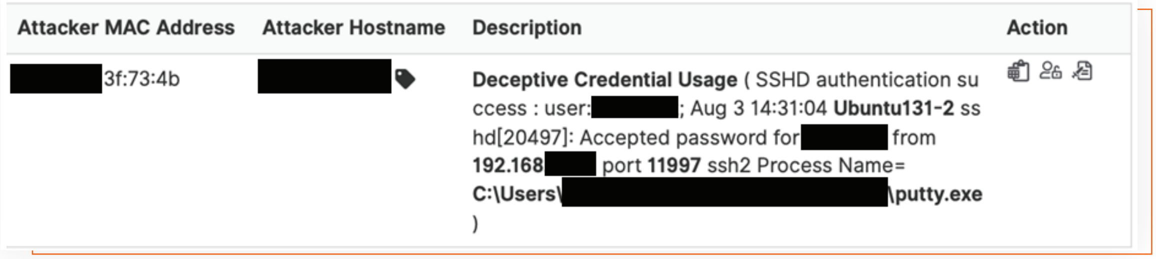
Attack Tool Details:



Binary/Process	Publisher	Query	Time
explorer.exe (2232) └cmd.exe (4588) └mimikatz.exe (5076)	Open Source Developer, Benjamin Delpy	sekurlsa::logonpasswords	09:42:00 12-23-2020
explorer.exe (2232) └cmd.exe (4588) └safetykatz.exe (3832)	Unsigned	sekurlsa::logonpasswords full	09:37:53 12-23-2020

USING STOLEN CREDENTIALS

The ThreatDefend® platform also identifies attackers stealing and using stolen deceptive credentials from endpoints. The below detection alert shows an attacker's attempts to use stolen credentials and move laterally from the endpoints using the "putty.exe" terminal application.



Attacker MAC Address	Attacker Hostname	Description	Action
[redacted]3f:73:4b	[redacted]	**Deceptive Credential Usage** (SSHD authentication success : user:[redacted]; Aug 3 14:31:04 **Ubuntu131-2** sshd[20497]: Accepted password for[redacted] from **192.168**[redacted] port **11997** ssh2 Process Name= **C:\Users\**[redacted]**\putty.exe**)	

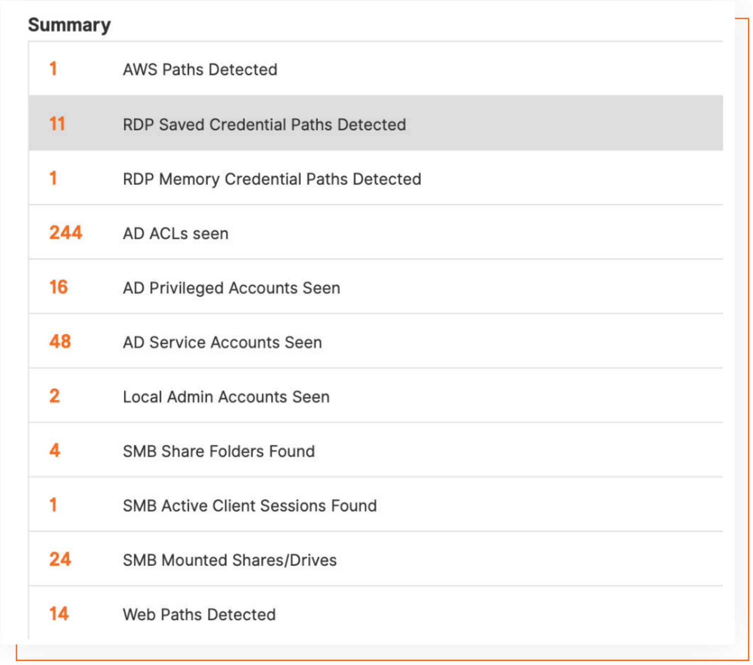
LATERAL MOVEMENT

In the Lateral Movement stage, attackers actively explore an organization's network to find vulnerable components. From a compromised endpoint, attackers can leverage the credentials and artifacts stored locally to move across the network, obtain administrative privileges, and maintain persistent access within the environment.

DETECTION OPPORTUNITY

The Attivo EDN suite includes the ThreatPath solution, which provides a continuous assessment to detect exposures and Lateral Movement Paths (LMPs) that an attacker would exploit. The solution exposes and provides topographical visual graphs showing the LMPs an attacker would traverse through the internal network once they engage with the beachhead endpoint system and locate other hosts susceptible to compromise. Additionally, organizations can configure policies in the ThreatPath solution to remediate exposed LMPs to high-value assets as it discovers them.

The image below lists LMPs the ThreatPath solution has detected, which attackers can exploit to move laterally.



Summary

1	AWS Paths Detected
11	RDP Saved Credential Paths Detected
1	RDP Memory Credential Paths Detected
244	AD ACLs seen
16	AD Privileged Accounts Seen
48	AD Service Accounts Seen
2	Local Admin Accounts Seen
4	SMB Share Folders Found
1	SMB Active Client Sessions Found
24	SMB Mounted Shares/Drives
14	Web Paths Detected

The Attivo ThreatDefend® platform also supports deploying decoys, forwarders across endpoints, networks, and within the cloud to detect attacker reconnaissance activities and lateral movement attempts.

LDAP & IDENTITY ENUMERATION

The Lightweight Directory Access Protocol (LDAP) is a protocol used to access directory listings within Active Directory (AD) or other directory services. Attackers query LDAP services to enumerate and gather identity information and the permissions associated with them, such as users, security groups, and such that they can further use to perform sophisticated attacks. In the SolarWinds supply chain attack, attackers used the native Windows administrative tool to anonymously perform enumeration techniques, extracting a great deal of information they could then use in a DCSync attack or admin privileges attack.

For example, in several instances during the SolarWinds attack, the attackers renamed adfind.exe, a popular Active Directory query tool, to “sqlceip.exe”, “csrss.exe”, or other well-known process avoid discovery while extracting information using commands such as those listed below.

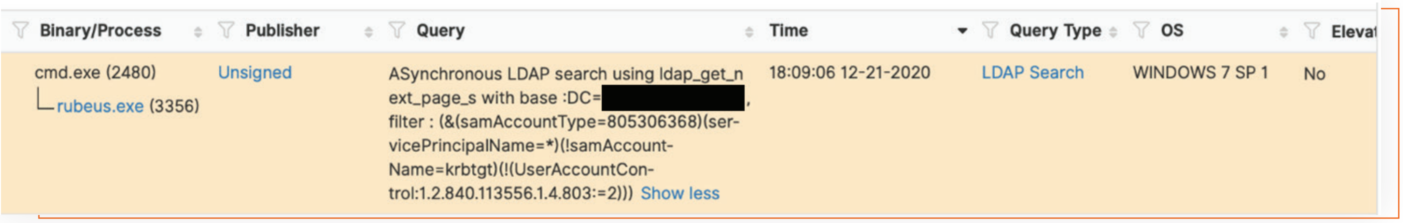
```
C:\Windows\system32\cmd.exe /C sqlceip.exe -default -f (name=”Organization Management”) member -list | sqlceip.exe -f objectcategory=* > .\SettingSync\log2.txt
```

```
C:\Windows\system32\cmd.exe /C csrss.exe -h breached.contoso.com -f (name=”Domain Admins”) member -list | csrss.exe -h breached.contoso.com -f objectcategory=* > .\Mod\mod1.log
```

DETECTION OPPORTUNITY

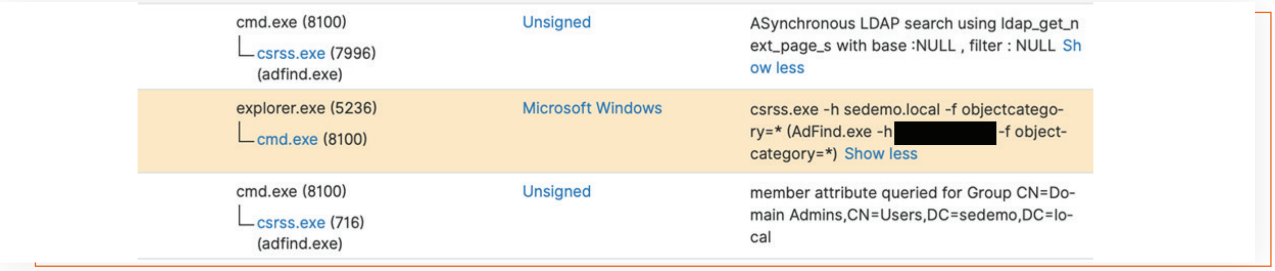
The Attivo EDN suite comes with the ADSecure solution (which also comes as a standalone deployment) to detects unauthorized LDAP queries and alerts. It also reduces the attack surface by hiding query results from the production AD and returning fake objects such as user accounts, groups, or service accounts. The ADSecure solution supports creating policies to prevent attackers from discovering privileged information from Active Directory.

Detecting attackers LDAP activity:



Binary/Process	Publisher	Query	Time	Query Type	OS	Elevat
cmd.exe (2480) └rubeus.exe (3356)	Unsigned	ASynchronous LDAP search using ldap_get_next_page_s with base :DC=[redacted], filter : (&(samAccountType=805306368)(servicePrincipalName=*)(!samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2))) Show less	18:09:06 12-21-2020	LDAP Search	WINDOWS 7 SP 1	No

Detecting attackers renaming popular tools and performing LDAP activity:



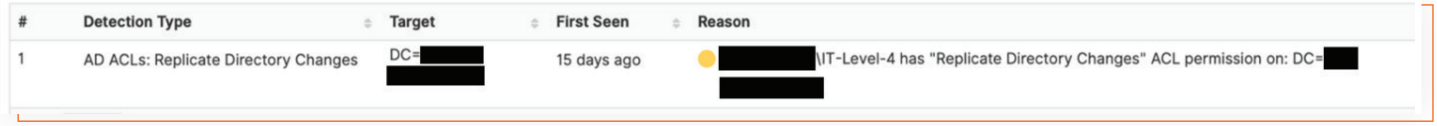
cmd.exe (8100) └ csrss.exe (7996) (adfind.exe)	Unsigned	ASynchronous LDAP search using ldap_get_next_page_s with base :NULL , filter : NULL Show less
explorer.exe (5236) └ cmd.exe (8100)	Microsoft Windows	csrss.exe -h sedemo.local -f objectcategory=* (AdFind.exe -h [redacted] -f objectcategory=*) Show less
cmd.exe (8100) └ csrss.exe (716) (adfind.exe)	Unsigned	member attribute queried for Group CN=Domain Admins,CN=Users,DC=sedemo,DC=local

DCSYNC ATTACKS

DCSync attacks enable an attacker to target an organization's Active Directory domain controller. Once attackers obtain access to domain admins or special accounts with "domain replication rights," they can perform a DCSync attack to replicate information using the Directory Replication Service Remote Protocol (MS-DRSR). Attackers can use this information on the domain to retrieve NTLM hashes, including the KRBTGT account, enabling attackers to create Golden Tickets.

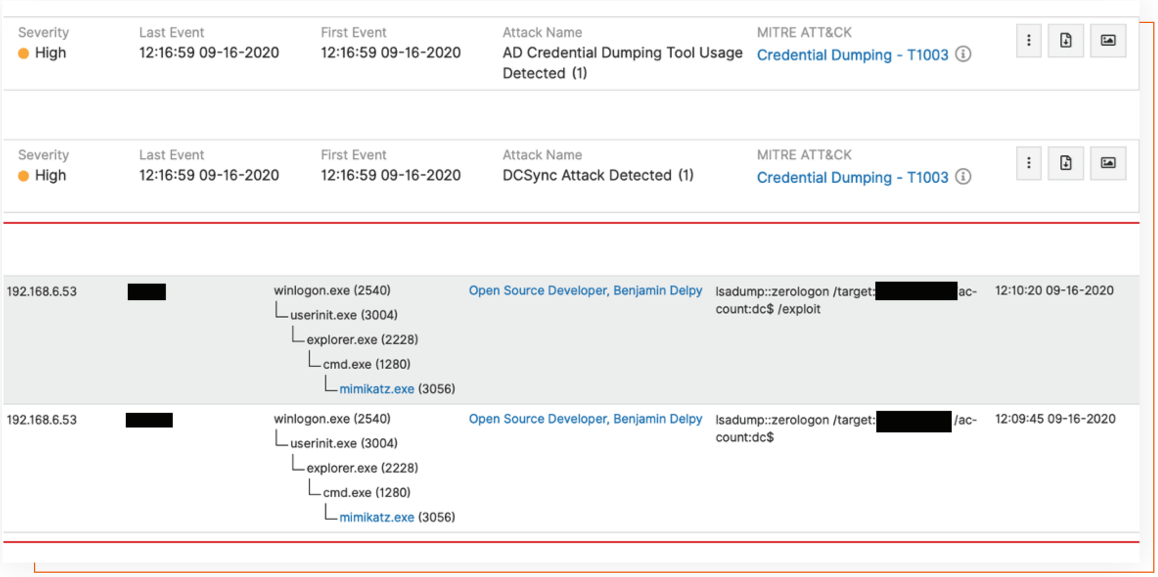
DETECTION OPPORTUNITY

Attackers need access to domain admins or special accounts with "domain replication rights" to initiate DCSync attacks. Organizations can deploy the ADSecure solution to prevent attackers from discovering accounts with "domain replication rights" and "domain admin" permissions, as demonstrated below, which lists users with "Replicate Directory Changes" permissions.



#	Detection Type	Target	First Seen	Reason
1	AD ACLs: Replicate Directory Changes	DC=[redacted]	15 days ago	● [redacted]\IT-Level-4 has "Replicate Directory Changes" ACL permission on: DC=[redacted]

Organizations can apply ADSecure protection policies to prevent attackers from discovered users with "Replicate Directory Changes." The solution detects attackers attempting to enumerate Active Directory and perform a DCSync attack.



Severity	Last Event	First Event	Attack Name	MITRE ATT&CK
● High	12:16:59 09-16-2020	12:16:59 09-16-2020	AD Credential Dumping Tool Usage Detected (1)	Credential Dumping - T1003 ⓘ

Severity	Last Event	First Event	Attack Name	MITRE ATT&CK
● High	12:16:59 09-16-2020	12:16:59 09-16-2020	DCSync Attack Detected (1)	Credential Dumping - T1003 ⓘ

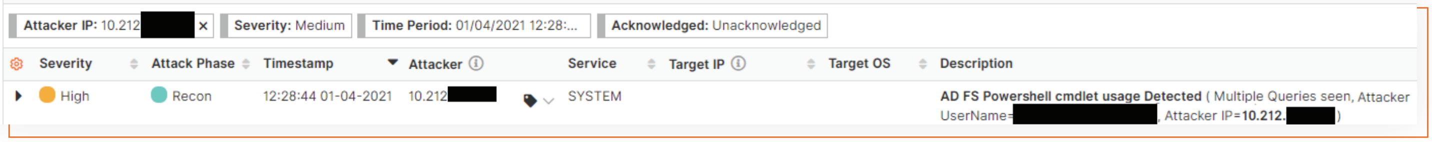
192.168.6.53	[redacted]	winlogon.exe (2540) └ userinit.exe (3004) └ explorer.exe (2228) └ cmd.exe (1280) └ mimikatz.exe (3056)	Open Source Developer, Benjamin Delpy	lsadump::zerologon /target:[redacted]account:dc$ /exploit	12:10:20 09-16-2020
192.168.6.53	[redacted]	winlogon.exe (2540) └ userinit.exe (3004) └ explorer.exe (2228) └ cmd.exe (1280) └ mimikatz.exe (3056)	Open Source Developer, Benjamin Delpy	lsadump::zerologon /target:[redacted]/account:dc$	12:09:45 09-16-2020

ADFS DISCOVERY

Active Directory Federation Service (ADFS) is a software component developed by Microsoft to provide Single-Sign-On (SSO) authorization service for users on Windows Server Operating Systems. ADFS allows users across organizational boundaries network access using a single set of login credentials. This function increases the attack surface and provides more opportunities for attackers who attempt ADFS enumeration to access private keys.

DETECTION OPPORTUNITY

The Attivo ADSecure solution identifies attacker queries to AD, generates an alert with the corresponding query detail, and hides real AD objects and data from the response. The ADSecure solutions provide real-time alerting on attackers enumerating ADFS. The ADSecure solution detects and prevents the use of AD enumeration tools and PowerShell cmdlets. Additionally, the solution returns alternative deceptive data that lead attackers into the decoy environment while providing real-time visibility into their activities, as shown below.



Attacker IP: 10.212[redacted] × | **Severity:** Medium | **Time Period:** 01/04/2021 12:28:... | **Acknowledged:** Unacknowledged

Severity	Attack Phase	Timestamp	Attacker		Service	Target IP	Target OS	Description
High	Recon	12:28:44 01-04-2021	10.212[redacted]		SYSTEM			**AD FS Powershell cmdlet usage Detected** (Multiple Queries seen, Attacker UserName=[redacted], Attacker IP=**10.212.**[redacted])

MITRE TTPS COVERAGE

The Attivo Networks ThreatDefend® platform comprehensively covers capabilities to detect Tactics, Techniques, and Procedures (TTPs) used in SolarWinds supply chain attack summarized by MITRE ATT&CK. Attivo also delivers the most comprehensive active defense with detection coverage for 123 of the 190 MITRE Shield use cases. Attivo's detection opportunities mapped for MITRE TTPs are shown in the below table.

SolarWinds Supply Chain Attack – UNC2452 Analysts	The MITRE Corporation		Microsoft Corporation	Mandiant Solutions FireEye, Inc.
Attivo's Detection Opportunity mapped to MITRE ATT&CK TTPs	T1059.001	T1003.006	T1072	T1012
	T1059.003	T1057	T1078	T1057
	T1555	T1018	T1005	T1083
	T1005	T1218.011		T1518
	T1484.002	T1558.003		T1518.001
	T1482	T1082		T1569.002
	T1562.004	T1552.004		T1078.004
	T1036.005	T1078		TA0006
	T1027			T1552
				T1552.004
				T1199

RECOMMENDED MITIGATIONS

SolarWinds has recommended that all their customers update to a new release of the software hit by the embedded Trojan in the Orion network-monitoring platform. The Cybersecurity and Infrastructure Security Agency (CISA) also recommends the best practices listed below to mitigate the impact.

- Reimage system memory or host operating systems hosting all instances of SolarWinds Orion versions 20194 through 2020.2.1 HF1,

- Analyze for new user or service accounts, as well as identify the existence of "SolarWinds.Orion.Core.BusinessLayer.dll" and "C:\WINDOWS\SysWOW64\netsetupsvc.dll."

- Reset credentials used by SolarWinds software and implement a rotation policy for these accounts with long and complex passwords.

In addition to the above, Attivo Networks also recommend mitigation strategies that give organizations best-in-class detection and prevention of sophisticated supply-chain attacks.

Protect endpoints:

- Deploy deceptive lures and map decoy SMB shares across all endpoints leading attackers to decoys

- Apply the EDN suite's DataCloak policies to restrict access to production network file shares, mapped cloud shares, or removable storage.

Detect lateral movement and persistence mechanisms:

- Deploy decoys mimicking critical servers, code repositories, databases, file servers, and other sensitive assets.

- Deploy decoys across all network subnets and expand deception coverage.

- Utilize the EDN suite's Deflect function to detect network reconnaissance.

Protect Active Directory & Credential Exposures:

- Analyze the presence of new user accounts, privilege accounts, or service accounts using the ThreatPath solution.

- Take steps to prevent kerberoasting attacks. The ADSecure solution hides AD service accounts, thereby mitigating and preventing the possibility of kerberoasting and silver ticket attacks.

- Detect the presence of attackers on endpoints connected to the domain and their discovery mechanisms. The ADSecure solution can detect and prevent further attacker movement from a domain-connected system.

CONCLUSION

Whether big or small, every organization should thoroughly review its security landscape and implement supply chain security strategies. As software gets integrated into every third-party product and solution, It is essential to identify any potential weaknesses in a system and implement best-in-class solutions that mitigate the evolving threat landscape.

REFERENCES

1. https://attack.mitre.org/groups/G0118/
2. https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/
3. https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
4. https://www.fireeye.com/content/dam/collateral/en/wp-m-unc2452.pdf
5. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
6. https://medium.com/mitre-attack/identifying-unc2452-related-techniques-9f7b6c7f3714
7. https://www.fireeye.com/blog/threat-research/2021/01/remediation-and-hardening-strategies-for-microsoft-365-to-defend-against-unc2452.html

ABOUT ATTIVO NETWORKS®