Using Microsoft 365 Defender to protect against Solorigate

microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/

December 28, 2020



UPDATE: 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 <u>NOBELIUM</u>. As we release new content and analysis, we will use NOBELIUM to refer to the actor and the campaign of attacks.

Microsoft security researchers continue to investigate and respond to the <u>sophisticated</u> <u>cyberattack</u> known as <u>Solorigate</u> (also referred to as <u>Sunburst</u> by FireEye) involving a supply chain compromise and the subsequent compromise of cloud assets. While the related investigations and impact assessments are ongoing, Microsoft is providing visibility into the attack chains and related threat intelligence to the defender community as early as possible so organizations can identify and take action to stop this attack, understand the potential scope of its impact, and begin the recovery process from this active threat. We have established a resource center that is constantly updated as more information becomes available at <u>https://aka.ms/solorigate</u>.

This blog is a comprehensive guide for security operations and incident response teams using Microsoft 365 Defender to identify, investigate, and respond to the Solorigate attack if it's found in your environment. The description of the attack in this blog is based on current analysis and investigations by researchers across Microsoft, our partners, and the intelligence community who are actively collaborating to respond to the attack. This is an active threat that continues to evolve, and the findings included here represent what we know at the time of publishing. We continue to publish and update intelligence, indicators, tactics, techniques, and procedures (TTPs), and related details as we discover them. The <u>report</u> from the Microsoft Security Response Center (MSRC) includes the latest analysis of this threat, known indicators of compromise (IOCs), and initial recommended defenses, and will be updated as new data becomes available.

This blog covers:

Tracking the cross-domain Solorigate attack from endpoint to the cloud

The Solorigate attack is an example of a modern cross-domain compromise. Since these kinds of attacks span multiple domains, having visibility into the entire scope of the attack is key to stopping and preventing its spread.

This attack features a sophisticated technique involving a software supply chain compromise that allowed attackers to introduce malicious code into signed binaries on the SolarWinds Orion Platform, a popular IT management software. The compromised application grants attackers "free" and easy deployment across a wide range of organizations who use and regularly update the application, with little risk of detection because the signed application and binaries are common and are considered trusted. With this initial widespread foothold, the attackers can then pick and choose the specific organizations they want to continue operating within (while others remain an option at any point as long as the backdoor is installed and undetected). Based on our investigations, the next stages of the attack involve on-premises activity with the goal of off-premises access to cloud resources through the following steps:

- 1. Using the compromised SolarWinds DLL to activate a backdoor that enables attackers to remotely control and operate on a device
- 2. Using the backdoor access to steal credentials, escalate privileges, and move laterally to gain the ability to create valid SAML tokens using any of two methods:
 - 1. Stealing the SAML signing certificate (Path 1)
 - 2. Adding to or modifying existing federation trust (Path 2)
- 3. Using attacker-created SAML tokens to access cloud resources and perform actions leading to the exfiltration of emails and persistence in the cloud

SOLORIGATE ATTACK High-level end-to-end attack chain



Figure 1. High-level end-to-end Solorigate attack chain

This attack is an advanced and stealthy campaign with the ability to blend in, which could allow attackers to stay under the radar for long periods of time before being detected. The deeply integrated cross-domain security capabilities in <u>Microsoft 365 Defender</u> can empower organizations and their security operations (SOC) teams to uncover this attack, scope out the end-to-end breach from endpoint to the cloud, and take action to block and remediate it. This blog will offer step-by-step guidance to do this by outlining:

- How indicators of attack show up across endpoints, identity, and the cloud
- How Microsoft 365 Defender automatically combines alerts across these different domains into a comprehensive end-to-end story
- How to leverage the powerful toolset available for deep investigation, hunting, and response to enable SOCs to battle the attackers and evict these attackers from both on-premises and cloud environments

Threat analytics: Understanding and responding to active attacks

As soon as this attack was discovered, Microsoft researchers published two <u>threat analytics</u> reports to help organizations determine if they are affected, assess the impact of the attack, and identify actions to contain it.

- <u>Sophisticated actor attacks FireEye</u> provides information about the FireEye breach and compromised red team tools
- <u>Solorigate supply chain attack</u> provides a detailed analysis of the SolarWinds supply chain compromise

The reports are published in <u>Microsoft 365 security</u> center, available to all Microsoft Defender for Endpoint customers and Microsoft 365 Defender early adopters. In addition to detailed descriptions of the attack, TTPs, and indicators of compromise (IoCs), the reports provide real-time data aggregated from signals across Microsoft 365 Defender, indicating the all-up impact of the threat to the organization, as well as details about relevant incidents and alerts to initiate investigation on. These reports continue to be updated as additional information becomes available.

Given the significance of this threat, we are making similar relevant Microsoft threat intelligence data, including the updated list of IOCs, available to everyone publicly. A comprehensive list of guidance and insights is available at <u>https://aka.ms/solorigate</u>.

	Microsoft Defender Security Center	Device										
≣	Threats > Solorigate supply chain attack											
0	Overview Analyst report Mitigations											
۲												
	Microsoft security researchers recently discovered a sophisticated attack where an adversary inserted malicious code in and then signed with a legitimate certificate. The resulting binary included a backdoor and was then discreetly distribu	to a supply chain development process. A malicious software class was included among many other legitimate classes ted into targeted organizations. This attack was discovered as part of an ongoing investigation.										
Ş	Cybercriminals target supply chains and look for weaknesses they can exploit to discreetly enter another target environment. In this case, attackers targeted the SolarWinds Orion Platform to infiltrate the supply chain that helps businesses manage networks, systems, and information technology infrastructure. This attack leveraged the trust associated with the supplier and certificate to insert targeted code to use in a larger campaign.											
Ø	Based on research, this attack represents nation-state activity at significant scale, aimed at both the government and pi companies.	ivate sector. The actor is known to be focused on high value targets such as government agencies and cybersecurity										
ß	Microsoft Defender for Endpoint detects this attack. It raises an alert when it detects the threat on your device; howeve	r, to avoid adverse impact on legitimate services Microsoft Defender for Endpoint will not automatically remediate it.										
Ł	Microsoft Defender Antivirus protects against this threat. It blocks the known malicious SolarWinds binaries associated with this threat on your device.											
۰đ	Read the full analyst report											
щ ² ~	Devices with alerts over time $^{\odot}$	Devices with alerts										
S	1	0 devices with active alerts										
6	0 11/19 11/27 12/05 12/13											
	Devices with active alerts											
	Secure configuration status	Vulnerability patching status										
	1.41k misconfigured devices	0 vulnerable devices										
	Exposed ESecure Unknown Not applicable	Exposed Secure	1									
	View mitigation details	View mitigation details										

Figure 2. Threat analytics report on Solorigate attack

We recommend Microsoft 365 Defender customers to start their investigations here. After gaining deep understanding of the threat and getting the latest research findings, you can take the following recommended steps:

Find devices with the compromised SolarWinds Orion application

The threat analytics report uses insights from <u>threat and vulnerability management</u> to identify devices that have the compromised SolarWinds Orion Platform binaries or are exposed to the attack due to misconfiguration.

From the *Vulnerability patching status* chart in threat analytics, you can view the mitigation details to see a list of devices with the vulnerability ID TVM-2020-0002, which was added specifically to help with Solorigate investigations:

reats > Solorigate supply chain attack Overview Analyst report Mitigations												
Secure configuration status $^{\odot}$	Vulne	rability patching status $^{\odot}$										
15 misconfigured devices	0 vulr	nerable devices										
Exposed Secure Unknown	Not applicable	oosed 📕 Secure										
Mitigation details												
Secure configuration	Product/Component	Vulnerability IDs	Exposed devices									
Vulnerabilities	orion_user_device_tracker	TVM-2020-0002	0									
	highavailability_orion_plugin	TVM-2020-0002	0									
	orion_netflow_traffic_analyzer	TVM-2020-0002	0									
	orion_improvement_program	TVM-2020-0002	0									
	orion_core_services	TVM-2020-0002	0									
	orion_network_performance_monitor	TVM-2020-0002	0									
	orion_network_configuration_manager	TVM-2020-0002	0									

Figure 3. Threat and vulnerability management data shows data on exposed devices

Threat and vulnerability management provides more info about the vulnerability ID TVM-2020-0002, as well as all relevant applications, via the *Software inventory* view. There are also multiple security recommendations to address this specific threat, including instructions to update the software versions installed on exposed devices.

See	curity recommendations										Update Solarwinds Orion Monitor	$\uparrow ~~ \downarrow$ Network Performance
2	Solarwinds orion X										🗜 Open software page 🔋 Remediation	n options 🛛 Exception options \cdots
	Security recommendation	OS platfor	Weaknesses	Related component	Threats	Exposed devi	ices	Status	Remediation type	R	Description	
•	Update Solarwinds Orion Network Performance Monitor	Windows	2	Solarwinds Orion	000	7/8	/	Active	Software update	c	Update Orion Network Performance Monit vulnerabilities affecting your devices.	tor to a later version to mitigate 2 known
	Update Solarwinds Orion Core Services	Windows	1	Solarwinds Orion	@ Ø Q	4 / 12	/	Active	Software update	с	Vulnerability details	
	Update Solarwinds Orion Network Configuration Manager	Windows	1	Solarwinds Orion	000	1/6	/	Active	Software update	c	Number of vulnerabilities 2	Exploit available No
											Exposed devices 7 / 8	Impact ▼ <0.01
											Exposed operating systems Windows Server 2016, Windows Server 2012 R2	

Figure 4. Security recommendations from threat and vulnerability management

Investigate related alerts and incidents

From the threat analytics report, you can quickly locate devices with alerts related to the attack. The *Devices with alerts* chart identifies devices with malicious components or activities known to be directly related to Solorigate. Click through to get the list of alerts and investigate.

Some Solorigate activities may not be directly tied to this specific threat but will trigger alerts due to generally suspicious or malicious behaviors. All alerts in Microsoft 365 Defender provided by different Microsoft 365 products are correlated into incidents. Incidents help you

see the relationship between detected activities, better understand the end-to-end picture of the attack, and investigate, contain, and remediate the threat in a consolidated manner.

Review incidents in the <u>Incidents</u> queue and look for those with alerts relevant to this attacker's TTPs, as described in the threat analytics report (also listed at the end of this blog).



Figure 5. Consolidated Incident view for Solorigate

Some alerts are specially tagged with <u>Microsoft Threat Experts</u> to indicate malicious activities that Microsoft researchers found in customer environments during hunting. As part of the Microsoft Threat Experts service, researchers investigated this attack as it unfolded, hunting for associated attacker behaviors, and sent <u>targeted attack notifications</u>. If you see an alert tagged with Microsoft Threat Experts, we strongly recommend that you give it immediate attention.

	Microsoft Defender Security Center	P	✓ Search Microsoft Defender for Endpoin	а , Р		☆⊕?	Θ	8				
=	$\label{eq:Alerts} Alerts \geq \mathbf{SolarWinds} \ \mathbf{DLL} \ \mathbf{associated} \ \mathbf{with} \ \mathbf{a} \ \mathbf{digital} \ \mathbf{su}$	pply			The new Ale							
0	SolarWinds DLL associated with a digi	ital supply chain a	attack loaded into memory	,								
۰					Details							
=	Alaktevel •••• Alaktevel •••• Alaktevel ••••				SolarWinds DLL associated with a digital supply cha							
ş	ALERT STORY			Collapse all		to memory						
0	What happened			Ť.	13 See in timeline	Unk to another incident 9	Assign to me					
L () 4% Å K	Executive summary Microsoft Threat Experts has observed this device in your environment load Digital Supply Chain attack against the software provider Solarwicks. We have that appare compromise durin tor malicous - handles for all are in the indi- serveral executables inside the Solar/Winds installation directory. These DLS others have been observed globally as a erily as October 2019. Pasas with It While we have ggl observed malicious activity attributed to this DLL in you We recommend you investigate this device immediately and consider isolar Indicators of Compromise	sing a malicious DLL Solar/Winds.Drik ave attributed 14 different versions o ators of Compromise section below. all have valid digital signatures sign is Thest Analytics architec to learn in the Comproment , a threat actor may ha ting the device(s) as part of your inci-	on.Cone.BusinessLayer.dll, which has been associated with df the DLU with this attack: 12 that include mailcolur ode three DLs are part of SolarWinds platform code loaded of by a SolarWinds digital certificate. This DLL as well as a or about this threat. we accessed the device prior to our investigation time wird dent response process.	na and 2 Iby several ndow.	Manage alert / Classify this alert True alert False alert Status New / Classification Select classification /							
8	IOC	Type Notes			Alert details			^				
5-ja	76640508b1e7759e548771a5359eaed353bf1eec [explore]	hash SHA-1 hash SolarWinds	h for malicious version of LOrion.Core.BusinessLayer.dll		Incident	Multi-stage incident involving I endpoints (🛙 open in Microso	nitial access & Exfiltratio ft 365 Defender)	on on multiple				
٢	d130bd75645c2433f88ac03e73395fba172ef676 [explore]	hash SHA-1 hash Solar/Winds	h for malicious version of .Orion.Core.BusinessLayer.dll		Detection source Category	Microsoft Threat Experts InitialAccess						
	1acf3108bf1e376c8848fbb25dc87424f2c2a39c [explore]	hash SHA-1 hash SolarWinds	h for malicious version of LOrion.Core.BusinessLayer.dll		First activity	Dec 15, 2020, 1:37:37 PM Dec 15, 2020, 1:37:37 PM	Ge					
	e257236206e99f5a5c62035c9c59c57206728b28 [explore]	hash SHA-1 hash SolarWinds	h for malicious version of Orion.Core.BusinessLayer.dll		Generated on Assigned to	Dec 15, 2020, 4:52:53 PM (Unassigned)						
	6fdd82b7ca1c110ec67c05b36d14c9517065353b [explore]	hash SHA-1 hash SolarWinds	h for malicious version of Orion.Core.BusinessLayer.dll		Alast description							
	2f1a5a7411d015d01aaee4535835400191645023 [explore]	hash SHA-1 hash SolarWinds	h for malicious version of Orion.Core.BusinessLayer.dll		Avert description Executive summary							
		SH&.1 had	h for malirinus varsion of	*	Microsoft Threat Exp	perts has observed this device in y	our environment	Need help?				

Figure 6. Microsoft Threat Experts targeted attack notification

Additionally, Microsoft Threat Experts customers with <u>Experts on demand</u> subscriptions can reach out directly to our on-demand hunters for additional help in understanding the Solorigate threat and the scope of its impact in their environments.

Hunt for related attacker activity

The threat analytics report also provides <u>advanced hunting</u> queries that can help analysts locate additional related or similar activities across endpoint, identity, and cloud. Advanced hunting uses a rich set of data sources, but in response to Solorigate, Microsoft has enabled streaming of Azure Active Directory (Azure AD) audit logs into advanced hunting, available for all customers in <u>public preview</u>. These logs provide traceability for all changes done by various features within Azure AD. Examples of audit logs include changes made to any resources within Azure AD, such as adding or removing users, apps, groups, roles, and policies. Customers who do not have Microsoft Defender for Endpoint or are not early adopters for Microsoft 365 Defender can see our <u>recommended advanced hunting queries</u>.

Currently, this data is available to customers who have Microsoft Cloud App Security with the <u>Office365 connector</u>. Our intent is to expand availability to more Microsoft 365 Defender customers. The new log data is available in the <u>CloudAppEvents</u> table:

CloudAppEvents | where Application == "Office 365" The log data contains activity logs useful for investigating and finding Azure AD-related activities. This data further enriches the CloudAppEvents table, which also has <u>Exchange</u> <u>Online and Microsoft Teams activities</u>.

As part of making this new data available, we also published a handful of relevant advanced hunting queries, identified by the suffix *[Solorigate]*, to the GitHub repo.

Here's an example query that helps you see when credentials are added to an Azure AD application after 'Admin Consent' permissions were granted:

```
CloudAppEvents
| where Application == "Office 365"
| where ActionType == "Consent to application."
| where RawEventData.ModifiedProperties[0].Name == "ConsentContext.IsAdminConsent"
and RawEventData.ModifiedProperties[0].NewValue == "True"
| extend spnID = tostring(RawEventData.Target[3].ID)
| parse RawEventData.ModifiedProperties[4].NewValue with * "=> [[" dummpy "Scope: " After
"77" *
| extend PermissionsGranted = split(After, "]",0)
| project ConsentTime = Timestamp , AccountDisplayName , spnID , PermissionsGranted
ioin (
CloudAppEvents
| where Application == "Office 365"
| where ActionType == "Add service principal credentials." or ActionType == "Update
application – Certificates and secrets management "
| extend spnID = tostring(RawEventData.Target[3].ID)
| project AddSecretTime = Timestamp, AccountDisplayName , spnID
) on spnID
| where ConsentTime < AddSecretTime and AccountDisplayName <> AccountDisplayName1
```

Microsoft 356 Defender advanced hunting can also assist in many of the recommended incident investigation tasks outlined in the blog, <u>Advice for incident responders on recovery</u> <u>from systemic identity compromises</u>.

In the remaining sections, we will discuss select examples of alerts raised by Microsoft 365 solutions that monitor and detect Solorigate activities across the attack chain on endpoint, identity, and the cloud. These are alerts you may encounter when investigating incidents in Microsoft 365 security center if your organization is affected by this threat. We will also indicate activities which are now blocked by Microsoft 365 Defender. Lastly, each section contains examples of hunting queries you will find useful for hunting for various attacker activities in your environment.

Detecting and blocking malware and malicious behavior on endpoints

SOLORIGATE ATTACK Stage 1: Initial access and command-and-control



Figure 7. Solorigate attack chain: Initial access and command-and-control

Discovering and blocking backdoor activity

When the compromised SolarWinds binary *SolarWinds.Orion.Core.BusinessLayer.dll* gets loaded on a device through normal update channels, the backdoor goes through an extensive list of checks to ensure it's running in an actual enterprise network and not on an analyst's machine. It then contacts a command-and-control (C2) server using a subdomain that is generated partly with information gathered from the affected device, which means a unique subdomain is generated for each affected domain. The backdoor allows the attackers to remotely run commands on the device and move to the next stages of the attack. For more information, read our <u>in-depth analysis of the Solorigate malware</u>.

Microsoft Defender for Endpoint delivers comprehensive protection against this threat (see full list of detection and protection alerts at the end of this blog). Microsoft Defender Antivirus, the default antimalware solution on Windows 10, <u>detects and blocks</u> the malicious DLL and its behaviors. It quarantines the malware, even if the process is running.

The new Alert page
is prevented
IS prevented
as prevented
gn to me
gn to me
Waiting for device
~
access & Defense evasion on
osoft 365 Defender)
Need help?
BCS SSO

Figure 8. Microsoft Defender for Endpoint blocks malicious binaries

If the malicious code is successfully deployed, the backdoor lies dormant for up to two weeks. It then attempts to contact numerous C2 domains, with the primary domain being **.avsvmcloud[.]com*. The backdoor uses a domain generation algorithm to evade detection. Microsoft 365 Defender detects and blocks this behavior.

8
The new Alert page
ack
e
^
False alert
^
dpoint (🗹 open
software.
night be under
late nd m

Figure 9. Microsoft Defender for Endpoint prevented malicious C2 callback

Discovering potentially tampered devices

To evade security software and analyst tools, the Solorigate malware enumerates the target system looking for certain running processes, loaded drivers, and registry keys, with the goal of disabling them.

The Microsoft Defender for Endpoint sensor is one of the processes the malware attempts to disable. Microsoft Defender for Endpoint has built-in protections against many techniques attackers use to disable endpoint sensors ranging from hardened OS protection, <u>anti-tampering policies</u>, and detections for a variety of tampering attempts, including "Attempt to stop Microsoft Defender for Endpoint sensor", "Tampering with Microsoft Defender for Endpoint sensor tampering in memory".

Successfully disabling Microsoft Defender for Endpoint can prevent the system from reporting observed activities. However, the multitude of signals reported into Microsoft 365 Defender provides a unique opportunity to hunt for systems where the tampering technique used might have been successful. The following advanced hunting query can be used to locate devices that should be reporting but aren't:

```
// Times to be modified as appropriate
let timeAgo=1d;
let silenceTime=8h;
// Get all silent devices and IPs from network events
let allNetwork=materialize(DeviceNetworkEvents
| where Timestamp > ago(timeAgo)
and isnotempty(LocalIP)
and isnotempty(RemoteIP)
and ActionType in ("ConnectionSuccess", "InboundConnectionAccepted")
and LocalIP !in ("127.0.0.1", "::1")
| project DeviceId, Timestamp, LocalIP, RemoteIP, ReportId);
let nonSilentDevices=allNetwork
| where Timestamp > ago(silenceTime)
| union (DeviceProcessEvents | where Timestamp > ago(silenceTime))
| summarize by DeviceId;
let nonSilentIPs=allNetwork
| where Timestamp > ago(silenceTime)
| summarize by LocalIP;
let silentDevices=allNetwork
| where DeviceId !in (nonSilentDevices)
and LocalIP !in (nonSilentIPs)
project DeviceId, LocalIP, Timestamp, ReportId;
// Get all remote IPs that were recently active
let addressesDuringSilence=allNetwork
| where Timestamp > ago(silenceTime)
| summarize by RemoteIP;
```

// Potentially disconnected devices were connected but are silent silentDevices | where LocalIP in (addressesDuringSilence) | summarize ReportId=arg_max(Timestamp, ReportId), Timestamp=max(Timestamp), LocalIP=arg_max(Timestamp, LocalIP) by DeviceId | project DeviceId, ReportId=ReportId1, Timestamp, LocalIP=LocalIP1

Microsoft is continuously developing additional measures to both block and alert on these types of tampering activities.

Detecting hands-on-keyboard activity within an on-premises environment



Figure 10. Solorigate attack chain: Hands-on-keyboard attack on premises

After establishing a backdoor connection on an affected device, the attacker's next goal is to achieve off-premises access to the organization's cloud services. To do this, they must find a way to gain permissions to those services. One technique we have seen the attackers use is to go after the organization's Active Directory Federation Services (<u>AD FS</u>) server to obtain the proverbial "keys" to the identity kingdom. AD FS enables federated identity and access management by securely sharing digital identity and entitlement rights across security and enterprise boundaries; effectively, it is the "LSASS for the cloud." Among other things, AD FS stores the Security Assertion Markup Language (<u>SAML</u>) token signing certificate, which is used to create authorization tokens for users or services in the organization so they can access cloud applications and resources after authentication.

To attack the AD FS infrastructure, the attackers must first obtain appropriate domain permissions through on-premises intelligence gathering, lateral movement, and credential theft. Building from the backdoor described above, the attackers leverage fileless techniques for privilege escalation, persistence, and lateral movement, including evading analysis by using system binaries and exploration tools that masquerade as other benign binaries. The attackers also carefully chose organization-specific command-and-control (C2) domains and use custom organization-specific tool naming and locations.

Microsoft Defender for Endpoint detects a wide array of these attack techniques, allowing SOC teams to track the attacker's actions in the environment and take actions to contain the attack. The following section covers detections for the techniques used by the attackers to compromise the AD FS infrastructure.

Identifying attacker reconnaissance

Attackers collect data from Active Directory using a renamed version of the utility ADFind, running queries against Domain Controllers as part of the reconnaissance stage of the attack. Microsoft Defender for Endpoint detects this behavior and allows the SOC analyst to track compromised devices at this stage to gain visibility into the information the attacker is looking for.

	Microsoft	Defend	der Se	ecurity Center											8
≣	Alerts >	Susp	icio	us LDAP query										The ne	w Alert page
@ 0	Susp	icio	us	LDAP query											
۰									Details						
=	🖪 wi	n-9njrns	9ohht	Latp.local Risk level	High ···· 🔍 atp\mInd0xp ····				Masqueradir	ng Active Directory exploration to	loc				
¢ ©	ALERT STOP	r.						Collapse all	 Open alert page 	e 😽 See in timeline Unk to another incident	8 As	ign to me	e 🔏 Create	e a suppression rul	le
¢.	~	[3368]	userini	Love			、	~							-
h-									Manage alert						^
_	~ -		3576] e	xplorer.exe			\	~	 Classify this all 	ert			True alert	False aler	t
-0 		- 3	Us	er ATP\mind0xp executed p	rocena cuidasse			~	Status	New M					
슢			Ģ	Suspicious file launch		Low • New	Detected		Classification	New V					
Q		File	create sq	(celp.exe			`	-		Seed Cassing Joint					
C2			9	System file masquerad	6	Medium 🔹 New	Detected		Alert details						^
-									Incident	Multi-stage incident involving Execution & Collect Defender h	tion on o	ne endpo	sint (🗈 open	in Microsoft 365	
52	~	- 8	(35	552] cmd.exe				~	Detection source	EDR					
			Ģ	Suspicious file launch		Low • New	Detected		Detection	Behavioral					
0			ş	Suspicious process lau	nched using cmd.exe	Low • New	• Detected		Detection status	Detected					
			0	[5004] sqlceipurse -defau	R -f (names" Organization Management") member -list			~	Category	Collection					
				Masquerading Ac A	tive Directory exploration tool	High • New	Detected		rectinques	T1036.003: Rename System Utilities T1087: Account Discovery					
				🖉 System file masq	erade	Medium • New	Detected		First activity	T1087.002: Domain Account Dec 22, 2020, 3:49:46 PM					
									Last activity	Dec 22, 2020. 3:51:24 PM					
			Ģ	cmd.exe created a proce Original PE name	as sqlcelp.exe with mismatching original PE name AdHind.exe AdFind exe		,	^	Generated on Assigned to	Dec 22, 2020. 3:52:15 PM (Unassigned)					
				Action time Mitre techniques	Dec 22, 2020, 3:49:45 PM T1086.005: Match Legitimate Name or Location										
				Target file	D sqlceip.exe		📀 Open f	le	Alert description						^
				🖗 System file masq	zerade	Medium 🔹 Naw	• Detected -		exploration tools to	launch a collective sensitive Active Directory informa	ate an at tion to n	sove later	ally in your ne	etwork or organiza	stion.
			0	187521 solcelo.exe - E-side	ctcateoov=*			~	Recommended acti	ions					
				& Masquerading Ad	tive Directory exploration tool	High • New	Detected -		 samulate the alert. 1. Inspect the to 2. Contact the d 	ool activity and the parent process. Sevice owner to verify if the activity was leadingate. In	spect the	script as	part of the ve	lidation process.	
				🖗 System file masq	verade	Medium • New	Detected		3. Check the de 4. Locate any ur 5. Identify unus	vice timeline for other suspicious behavior. nfamiliar processes in the process tree. Check files for ual system activity with system owners.	prevaler	ice, locati	on, and digita	al signatures.	

Figure 11. Microsoft Defender for Endpoint detects usage of masquerading exploration tools

	Micros	soft De	fende	r Secu	urity Center					8
=	Alert	s > Si	uspio	ious	s LDAP query				The new Ale	rt page
@ 0	Su	spic	iou	s LC	DAP query					
۰								Details		
=	E	1			Rick level 🚥 High 🚥			Suspicious L	LDAP query	
8	ALER	I STORY					Collapse all			
ø					у такцистаниц ислис опессоту ехронации цин			📆 See in timeline	😻 Link to another incident 🔒 Assign to me 🔏 Create a suppression rule 💡 Consult a threat expr	ert
0					🖗 System file masquerade	📕 Medium 🔶 New 🖕 Detected		Manage alert	^	- i
Ł				0	cmd.exe created a process sqlcelp.exe with mismatching original PE name AdFind.exe		~	Character the al	ied True alert False alert	11
φ 4 8					Original FE name AdFind ese Action time Dec 22, 3200, 3:50:02 PM Mare techniques T1056.031: Match Legismute Name or Location			Status [New V	1
O				1	Target file 🗅 sqlcelp.exe		~	Classification	Select classification V	- 1
C2					🖗 System file masquerade	Medium • New • Detected		Alert details	~	-
					14600 estudo era defe in escalar (at			Incident	Multi-stage incident involving Execution & Collection on one endpoint (13 open in Microsoft 365	- 1
_			^		Justvoj sejcelipuese -berault memoer -list		~		Defender)	- 1
5-e				1	Masquerading Active Directory exploration tool	High • New • Detected		Detection source Detection	EDR Bchavioral	- 1
0				1	System file masquerade	Medium New Detected		technology		- 1
				0	valceinese performed an exploratory IDAP merv		~	Detection status	Detected	- 1
					LOM Search garry El SpcClass*1 Distriptioned searce Distributioned Searce Searce Distributioned Searce Searce Distributioned Searce Searce Distributioned Sea			Techniques	11018 Remote System Discovery 11033 System Connect/User Discovery 11036 Remote Geouge Discovery 110907 Account Geouge 110907 Account Giocovery 11139 Nature Share Discovery	
					🖗 Suspicious LDAP query	Medium . New . Detected		First activity	Dec 22, 2020, 3:51:24 PM	
								Last activity	Dec 22, 2020. 3:51:24 PM	
				9	cmd.exe created a process sqlcelp.exe with mismatching original PE name AdFind.exe		~	Generated on	Dec 22, 2020, 3:57:17 PM (Instringed)	
				4	§ System file masquerade	Medium 🔹 New 🎍 Detected		Assigned to	(Chasagnea)	
			3	User A	ATP\mind0xp executed process cmd.exe		~	Alert description	^	
				Ģ St	uspicious file launch	Low New Detected		A suspect LDAP (U) LDAP queries are of	ghtweight Directory Access Protocol) query was executed, indicating potential reconnaissance activity. Ren used by attackers in attempt to learn the organization's structure, by querying the domain controller for	
			3	cmd.e	exe script interpreter process was created by explorer.exe		~	Using this informat	is an a groups and misrissing assess, tion, an attacker can gain higher privileges and access important assets in the organization, med an emprovation I DBR or early.	
				∲ Si	uspicious process launched using cmd.exe	Low New Detected		Recommended act	ieu an exploratory solve qu'ery tions	

Figure 12. Microsoft Defender for Endpoint detects usage LDAP query for reconnaissance.

Stopping lateral movement and credential theft

To gain access to a highly privileged account needed for later steps in the kill chain, the attackers move laterally between devices and dump credentials until an account with the needed privileges is compromised, all while remaining as stealthy as possible.

A variety of credential theft methods, such as dumping LSASS memory, are detected and blocked by Microsoft Defender for Endpoint. The example below shows the detection of lateral movement using Windows Management Instrumentation (WMI) to run the attacker's payload using the *Rundll32.exe* process.

	Microsoft Defender Security Cent	ter			 Search Microsoft Defender for 	Endpoint 🤳	> ★ ⊕ ? ⊕
=	Alerts > Suspicious Remot	te W	MI Execution				The new Alert pa
30	Suspicious Remote	e V	MI Execution				
•							Details
-	D No	sk level	High ···· R				Modum New
\$	ALERT STORY					Collapse all	
0						*	Consult a thread expert Consult a thread expert
6	~ - 0	[at	on) Wimin rescuese -secures -cmoedding			÷	O Automated investigation 27604 triggered by this alert is O No threats found
F	^ -	- 0	(8840) rundll32.exe rundl32.clpsindowsijlegi	t, pişloid.dl Entry⊄sint		~	Hanna dat
~8			Suspicious behavior by a sychost.	.exe was observed	Medium New Detected		
슐			Process launched with the securit	ty context of another user	Low • New • Detected	•••	Classify this alert True alert False alert
٢			I rundli32.exe was invoked remotely			^	Status New V
1			Execution type Wmi Source machine name Mitre techniques T1047: Wind	ons Management Instrumentation			Classification Select dassification V
Ě			Source machine lp a 😑 10.10.5	0.110			Alert details
~ _			Suspicious Remote WMI Exe	cution	••• Medium • New • Detected		Incident Multi-stage incident involving Execution & Collection on one endpoint (12 open in Microsoft 365 Detender)
			C rundll32.exe process was created from	m a remote machine 'WINDOWS10-ATP-X' using Window	s Management Instrumentation (WMI)	~	Detection source EDR Detection Behavioral Network
			Suspicious WMI process crea	ation	Mcdium New Detected		technology Detection status Detected
			*				Category LateralMovement
			C rundl32.ease process was created from	m a remote machine 'WINDOWS10-ATP-X' using Window	n Management Instrumentation (WMI)	^	Techniques T1047: Windows Management Instrumentation
			Execution source Remote Remote machine Ne				Prist activity Dec 22, 2020, 1294/38 PM Last activity Dec 22, 2020, 1294/38 PM
			Remote machine FQ Action time Dec 22 2020	12:44:58 PM			Generated on Dec 22, 2020, 12:55:50 PM
			Mitre techniques T1047: Wind	ows Management Instrumentation			Assigned to Automation
			Suspicious WMI process creations	ation	Medium • New • Detected		Alert description
			nage load				WMI are be used by stitutions to superite commands on preside mechanisms and superingly take spatial of it. This allows stitutions
			legit_payload.dll			~	to gather information about the internal network, access additional resources, steal credentials and elevate their permissions in
			Suspicious Remote WMI Exe	cution	Medium New Detected		order to reach their desired assets.
			S Abnormal Remote Service E	xecution	Medium New Detected		Recommended actions 1. Find the propagation entry point - check which users were logged on to this machine and which other machines they were
			G rundli32.exe loaded a suspicious DLL	legit_payload.dll		~	observed on to find additional compromised machines 2. Gather information - analyze the executed process and if possible block it from running on any machines in the
			& Suspicious dynamic link libro	arv loaded	Motion A New A Detected		organization. 3. Analyza loss - analyza all loss from this machine to fully understand what commands were even sted, their numous and

Figure 13. Microsoft Defender for Endpoint alert for suspicious remote WMI execution highlighting the attacker's device and payload

Microsoft Defender for Identity also detects and raises alerts on a variety of credential theft techniques. In addition to watching for alerts, security analysts can hunt across identity data in Microsoft 365 Defender for signs of identity compromise. Here are a couple of example Microsoft Defender for Identity queries looking for such patterns:

Enumeration of high-value DC assets followed by logon attempts to validate stolen credentials in time proximity

```
let MaxTime = 1d;
let MinNumberLogon = 5;
//devices attempting enumeration of high-value DC
IdentityQueryEvents
| where Timestamp > ago(30d)
| where Application == "Active Directory"
| where QueryTarget in ("Read-only Domain Controllers")
//high-value RODC assets
| project Timestamp, Protocol, Query, DeviceName, AccountUpn
| join kind = innerunique (
//devices trying to logon {MaxTime} after enumeration
IdentityLogonEvents
| where Timestamp > ago(30d)
```

| where ActionType == "LogonSuccess" | project LogonTime = Timestamp, DeviceName, DestinationDeviceName) on DeviceName | where LogonTime between (Timestamp .. (Timestamp + MaxTime)) | summarize n=dcount(DestinationDeviceName), TargetedDC = makeset(DestinationDeviceName) by Timestamp, Protocol, DeviceName | where n >= MinNumberLogon

High-volume of LDAP queries in short time filtering for non-DC devices

```
let Threshold = 12:
let BinTime = 1m:
//approximate list of DC
let listDC=IdentityDirectoryEvents
| where Application == "Active Directory"
| where ActionType == "Directory Services replication"
| summarize by DestinationDeviceName;
IdentityQueryEvents
| where Timestamp > ago(30d)
//filter out LDAP traffic across DC
| where DeviceName !in (listDC)
| where ActionType == "LDAP query"
| parse Query with * "Search Scope: " SearchScope ", Base Object:" BaseObject ", Search
Filter: " SearchFilter
| summarize NumberOfDistinctLdapQueries = dcount(SearchFilter) by DeviceName,
bin(Timestamp, BinTime)
| where NumberOfDistinctLdapQueries > Threshold
```

At this point, SOC teams can take containment measures within the Microsoft 365 security center, for example, using <u>indicators</u> to isolate the devices involved and block the remotely executed payload across the environment, as well as mark suspect users as compromised.

Detecting and remediating persistence

Microsoft Defender for Endpoint also detects the advanced defense evasion and masquerading techniques used by the attackers to make their actions as close to normal as possible, such as binding a WMI event filter with a logical consumer to remain persistent. Follow the recommended actions in the alert to remove persistence and prevent the attacker's payload from loading after reboot.

	Microsoft Defender Security Center						* @ ? © 🔞
=	Alerts > A WMI event filter was bound to a suspicious	s ev					The new Alert page
@ 0	A WMI event filter was bound to a susp	picious event consumer					
۰						Details	
п \$	Risklevel BBB High ···					A WMI ever	nt filter was bound to a suspicious event consumer New
0	ALERT STORY				Collapse all	💐 See in timeline	🔨 Link to another incident 🔗 Assign to me 💲 Create a suppression rule ? Consult a threat expert
6	Windows Management Instrumentation (WMI) binding event filter to consum	mer			^	Manage alert	^
₽ \$	Consumer CommerConsumer*OfficeLauncherConsumer*OfficeLauncherConsum Eis OfficeLauncherEinet Namespace ///neoh/subcryston Pesible cause Binding funet/item instance ofSemifiker (CeatodSD Mitte technisuue	.er" D D = (1.5.0.0.0.0.5.21.0.0.0.117.61.61.178.179.75.246,184,181	, 65, 166, 61, 233, 3, 0, 0); EventNamespa	ce = "roofilcimv2"; Name = "OfficeLauncherEvent"; Query = "SELECT	· FR (D	O Classify this a	ert True alert False alert
4	A A WMI event filter was bound to a supplicing spect	f_EventFiter		Martine & New & Deter	Net	Status	New 🗸
1	5° Creatoralu 179, 75, 24 Eventiam	1 = (1, 5, 0, 0, 0, 0, 0, 5, 21, 0, 0, 0, 117, 61, 61, 178, 46, 184, 181, 65, 166, 61, 233, 3, 0, 0); Hespace = "root\\cimv2";				Classification	Select classification V
	Name = "C Query = "S	OfficeLauncherEvent": SELECT * FROMInstanceModificationEvent				Alert details	^
ø	WiTHIN 60 Win32, Per Tercentents	J WHERE TargetInstance ISA InfFormattedData_PerfOS_System' AND				Incident	Multi-stage incident involving Execution & Lateral movement on one endpoint ((2 open in Nicrosoft 365 Defender)
5	TargetInsta Querdi acc	ance.SystemUpTime < 320":				Detection source	EDR
٢	li Bern Con	page - mar ;				Detection technology	Behavioral
	instance of	f CommandLineEventConsumer				Detection status	Detected
	{ Command	/LineTemplate = "rundll32.exe				Category	Persistence
	<\\window CreatorSID	vs\\temp\\error.dll.MainFunc"; D = (1, 5, 0, 0, 0, 0, 0, 5, 21, 0, 0, 0, 117, 61, 61, 178,				Techniques	T1084: Windows Management Instrumentation Event Subscription T1546.003: Windows Management Instrumentation Event Subscription
	179.75.24 Name # "C	46, 184, 181, 65, 166, 61, 233, 3, 0, 0); OfficeLaurcherConsumer";				First activity	Dec 21, 2020, 11:52:20 PM
	3					Last activity Generated on	Dec 21, 2020, 11:52:20 PM
						Assigned to	(Unassigned)
						Alert description	^
						An event consume and CommandLine of flexibility for an	represents the action to take upon the fining of an event. Attackers can use the ActiveScriptEventConsumer "KentConsumer classes when responding to their events. Both event consumers offer a tremendous amount attacker to execute any payload they want all without needing to drop a single malicious executable to disk.
						Recommended act 1. Find the propag- observed on to fin 2. Gather infor organization 3. Analyze logi impact.	tions atox entry point - dheck which users were logged on to this machine and which other machines they were a address compromosed multiches. mation - analyse the executed process and if possible block it from running on any machines in the - analyse all logs from this machine to fully understand what commands were executed. their purpose and

Figure 14. Microsoft Defender for Endpoint alert for WMI event filter bound to a suspicious consumer showing the persistence and the scheduled command line

Catching AD FS compromise and the attacker's ability to impersonate users in the cloud

The next step in the attack focuses on the AD FS infrastructure and can unfold in two separate paths that lead to the same outcome—the ability to create valid SAML tokens allowing impersonation of users in the cloud:

- Path 1 Stealing the SAML signing certificate: After gaining administrative privileges in the organization's on-premises network, and with access to the AD FS server itself, the attackers access and extract the SAML signing certificate. With this signing certificate, the attackers create valid SAML tokens to access various desired cloud resources as the identity of their choosing.
- Path 2 Adding to or modifying existing federation trust: After gaining administrative Azure Active Directory (Azure AD) privileges using compromised credentials, the attackers add their own certificate as a trusted entity in the domain either by adding a new federation trust to an existing tenant or modifying the properties of an existing federation trust. As a result, any SAML token they create and sign will be valid for the identity of their choosing.

In the first path, obtaining the SAML signing certificate normally entails first querying the private encryption key that resides on the AD FS container and then using that key to decrypt the signing certificate. The certificate can then be used to create illicit but valid SAML tokens that allow the actor to impersonate users, enabling them to access enterprise cloud applications and services.

Microsoft Defender for Endpoint and Microsoft Defender for Identity detect the actions that attackers take to steal the encryption key needed to decrypt the SAML signing certificate. Both solutions leverage unique LDAP telemetry to raise high-severity alerts highlighting the attacker's progress towards creating illicit SAML tokens.

	Microsoft Defender Security Center				Ŷ	● ?	٢	8
≡	Alerts > ADFS private key extraction attempt						•	The new Alert page
Ø	ADFS private key extraction attempt							
۲					Details			
므	⊐ Risk level ■■■ High ···· Q			ŀ	ADFS privat	e key extrac	tion attempt	
Ş					High Ne	w		
Ô	ALERT STORY		Collapse	all	😸 See in timeline	Link to anoth	er incident 🔗 Assi	ign to me
Ř	[4280] SecurityHealthSystray.exe		~	•				A
U)	(3) [7448] OneDrive.exe /background		~	N	Vanage alert			^
ĸ	File create				(i) Classify this a	ert	True alert	False alert
۰đ	dump_em_all.exe		~		0,			
	${\mathscr G}$ Suspicious file dropped	Medium • New • Detected		s	itatus	New	~	
Ê	∧ (7956) dump_em_all.exe		~	c	lassification	Select classification	h	
-	Image load							
LZ	D dump_em_all.exe		~	A	Alert details			^
8	Suspicious file dropped	Medium • New • Detected		h	ncident	Multi-stage inci access on one e Defender)	dent involving Execut Indpoint (🗹 open in	tion & Credential Microsoft 365
0-6	() dump_em_all.exe ran an LDAP query		^	C	Detection source	EDR		
۲	LDAP Search query (&(thumbnail) Distinguished name CN=ADFS.CN	photo=*)(objectClass=contact)(!(cn=CryptoPolicy))) 👔 =Microsoft.CN=Program Data.DC=ATP.DC=local 📭		C tr	Detection echnology	Behavioral		
	Action time Jan 10, 2021, 7	7:09:02 PM		C	Detection status	Detected		
				c	Category	CredentialAcces	.s	
	<i>ADFS private key extraction a</i>	ittempt High • New • Detected		т	echniques	T1003: OS Cred T1528: Steal Ap	ential Dumping plication Access Toke	n
	්ට [7936] WerFault.exe -u -p 7956 -s 1428		~	F	irst activity	Jan 10, 2021, 7:0	J9:02 PM	
				- L	ast activity	Jan 10, 2021, 7:0)9:02 PM	-

Figure 15. Microsoft Defender for Endpoint detects a suspicious LDAP query being launched and an attempted AD FS private key extraction

Active Direct An actor on 3:50 PM Dec 21, 20	ory attributes sent a suspicious	Reconnaissan s LDAP query, search	ce using L ning for ADFS_	DAP Key on	OPEN
		ADFS_Key			
0	searching for		on	○►	

Figure 16. Microsoft Defender for Identity detects private key extraction via malicious LDAP requests

For the second path, the attackers create their own SAML signing certificate outside of the organization's environment. With Azure AD administrative permissions, they then add the new certificate as a trusted object. The following advanced hunting query over Azure AD audit logs shows when domain federation settings are changed, helping to discover where the attackers configured the domain to accept authorization tokens signed by their own signing certificate. As these are rare actions, we advise verifying that any instances identified are the result of legitimate administrative activity.

ADFSDomainTrustMods

let auditLookback = 1d; CloudAppEvents
| where Timestamp > ago(auditLookback)
| where ActionType =~ "Set federation settings on domain."
| extend targetDetails = parse_json(ActivityObjects[1])
| extend targetDisplayName = targetDetails.Name
| extend resultStatus = extractjson("\$.ResultStatus", tostring(RawEventData), typeof(string))
| project Timestamp, ActionType, InitiatingUserOrApp=AccountDisplayName,
targetDisplayName, resultStatus, InitiatingIPAddress=IPAddress, UserAgent

If the SAML signing certificate is confirmed to be compromised or the attacker has added a new one, follow the <u>best practices</u> for invalidating through certificate rotation to prevent further use and creation of SAML tokens by the attacker. Additionally, affected AD FS servers may need to be isolated and remediated to ensure no remaining attacker control or persistence.

If the attackers accomplish either path, they gain the ability to create illicit SAML tokens for the identities of their choosing and bypass multifactor authentication (MFA), since the service or application accepting the token assumes MFA is a necessary previous step in creating a properly signed token. To prevent attackers from progressing to the next stage, which is to access cloud resources, the attack should be discovered and remediated at this stage.

Detecting the hands-on-keyboard activity in the cloud environment



Figure 17. Solorigate attack chain: Hands-on-keyboard attack in the cloud

With the ability to create illicit SAML tokens, the attackers can access sensitive data without having to originate from a compromised device or be confined to on-premises persistence. By abusing API access via existing OAuth applications or service principals, they can attempt to blend into the normal pattern of activity, most notably apps or service principals with existing *Mail.Read* or *Mail.ReadWrite* permissions to read email content via Microsoft Graph from Exchange Online. If the application does not already have read permissions for emails, then the app may be modified to grant those permissions.

Identifying unusual addition of credentials to an OAuth app

Microsoft Cloud App Security (MCAS) has added new automatic detection of unusual credential additions to an OAuth application to alert SOCs about apps that have been compromised to extract data from the organization. This detection logic is built on an anomaly detection engine that learns from each user in the environment, filtering out normal usage patterns to ensure alerts highlight real attacks and not false positives. If you see this alert in your environment and confirm malicious activity, you should take immediate action to suspend the user, mark the user as compromised, reset the user's password, and remove the credential additions. You may consider disabling the application during investigation and remediation.

🐁 Unusu	al addition of credentials to an OAuth app 1 Office 365	上 User Name [1.1.1.1	1				
Reso	lution options:						Close alert 🛩
escription he user l hishing,	on User Name (username@domain.com) performed an unu exfiltration, or lateral movement. The user added a cred	usual addition of credentials lentials of type Password, w	s to App Name. This usage p here an application is using .	attern may indicate t a clear text passworc	hat an attacker has I to authenticate.	compromised t	the app, and is using it for
Admin Office	t information nistrative activity was performed for the first time in 180 2365 (Default) was used for administrative activity for th 1 was used for the first time in 180 days by this user.	days by this user. e first time in 180 days by t	his user.				
ctivity lo	og						
ctivity lo	29	1 - 3 of 3 activities ①)			Investigate in a	Activity log
ctivity lo	Activity	1 - 3 of 3 activities ① User) App	IP address	Location	Investigate in a	Activity log 🔹 🗔 🗸
sctivity lo	Activity Update service principal: application App Name;	1 - 3 of 3 activities ① User User Name	App Office 365	IP address	Location	Device	Activity log : Date ~ Dec 28, 2020, :
3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	Activity Update service principal: application App Name; Update application configuration: application Ap	1 - 3 of 3 activities ① User User Name User Name	App Office 365	IP address 1.1.1.1 1.1.1.1	Location 태화 India 태화 India	Investigate in . Device	Activity log
 A ctivity location A ctivity locatio	Pg Activity Update service principal: application App Name; Update application configuration: application Ap Update application – Certificates and secrets man	1 - 3 of 3 activities ① User User Name User Name User Name	App Office 365 Office 365 Office 365	IP address	Location I를 India I를 India I를 India	Investigate in . Device	Activity log
 Activity la Activity la Activity la Activity la Activity la 	2g 2g Activity Update service principal: application App Name: Update application configuration: application Ap Update application – Certificates and secrets man	1 - 3 of 3 activities ① User User Name User Name User Name	App Office 365 Office 365 Office 365	IP address 1.1.1.1 1.1.1.1 1.1.1.1	Location I용I India I용I India I용I India	Investigate in a Device	Activity log Date Dec 28, 2020, Dec 28, 2020, Dec 28, 2020,
3 3 3 3 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Pg Activity Update service principal: application App Name; Update application configuration: application Ap Update application – Certificates and secrets man	1 - 3 of 3 activities () User User Name User Name User Name 1 - 1 of	App Office 365 Office 365 Office 365 Office 365 Office 365 Office 365	IP address 1.1.1.1 1.1.1.1 1.1.1.1	Location I용 India I용 India I용 India	Investigate in a Device	Activity log Date Dec 28, 2020, Dec 28, 2020, Dec 28, 2020, Trace
B B B B B B B	>g Activity Update service principal: application App Name; Update application configuration: application Ap Update application – Certificates and secrets man Update application – Certificates and secrets man Update application – Certificates and secrets man Update application – Certificates and secrets man	1 - 3 of 3 activities () User User Name User Name User Name 1 - 1 of Type	App App Office 365 Office 365 Office 365 Office 365 I office 365 I office 365 Email	IP address IP address I 1.1.1.1 I 1.1.1 I 1.1.	Location IIII India IIII India IIII India	Investigate in a Device 	Activity log

Figure 18. Microsoft Defender Cloud App Security alert for unusual addition of credentials to an OAuth app

SOCs can use the following Microsoft 365 Defender advanced hunting query over Azure AD audit logs to examine when new credentials have been added to a service principle or application. In general, credential changes may be rare depending on the type and use of the service principal or application. SOCs should verify unusual changes with their respective owners to ensure they are the result of legitimate administrative actions.

NewAppOrServicePrincipalCredential

let auditLookback = 1d; CloudAppEvents
| where Timestamp > ago(auditLookback)
| where ActionType in ("Add service principal.", "Add service principal credentials.", "Update
application - Certificates and secrets management ")
| extend RawEventData = parse_json(RawEventData)
| where RawEventData.ResultStatus =~ "success"
| where AccountDisplayName has "@"
| extend targetDetails = parse_json(ActivityObjects[1])

```
| extend targetId = targetDetails.Id
| extend targetType = targetDetails.Type
| extend targetDisplayName = targetDetails.Name
| extend keyEvents = RawEventData.ModifiedProperties
| where keyEvents has "KeyIdentifier=" and keyEvents has "KeyUsage=Verify"
| mvexpand keyEvents
| where keyEvents.Name =~ "KeyDescription"
| parse keyEvents.NewValue with * "KeyIdentifier=" keyIdentifier:string ",KeyType="
keyType:string ",KeyUsage=" keyUsage:string ",DisplayName=" keyDisplayName:string "]" *
| parse keyEvents.OldValue with * "KeyIdentifier=" keyIdentifierOld:string ",KeyType" *
| where keyEvents.OldValue == "[]" or keyIdentifier != keyIdentifierOld
| where keyUsage == "Verify"
| project-away keyEvents
| project Timestamp, ActionType, InitiatingUserOrApp=AccountDisplayName,
InitiatingIPAddress=IPAddress, UserAgent, targetDisplayName, targetId, targetType,
keyDisplayName, keyType, keyUsage, keyIdentifier
```

Discovering malicious access to mail items

OAuth applications or service principals with *Mail.Read* or *Mail.ReadWrite* permissions can read email content from Exchange Online via the Microsoft Graph. To help increase visibility on these behaviors, the *MailItemsAccessed* action is now available via the new Exchange mailbox advanced audit functionality. <u>See if this feature is enabled by default for you</u>. Important note for customers: If you have customized the list of audit events you are collecting, you may need to <u>manually enable this telemetry</u>.

If more than 1,000 *MailItemsAccessed* audit records are generated in less than 24 hours, Exchange Online stops generating auditing records for *MailItemsAccessed* activity for 24 hours and then resumes logging after this period. This throttling behavior is a good starting point for SOCs to discover potentially compromised mailboxes.

MailItemsAccessedThrottling

```
let starttime = 2d;
let endtime = 1d;
CloudAppEvents
| where Timestamp between (startofday(ago(starttime))..startofday(ago(endtime)))
| where ActionType == "MailItemsAccessed"
| where isnotempty(RawEventData['ClientAppId']) and RawEventData['OperationProperties']
[1] has "True"
| project Timestamp, RawEventData['OrganizationId'],AccountObjectId,UserAgent
```

In addition to looking for throttled telemetry, you can also hunt for OAuth applications reading mail via the Microsoft Graph API whose behavior has changed prior to a baseline period.

```
//Look for OAuth App reading mail via GraphAPI — that did not read mail via graph API in
prior week
let appMailReadActivity = (timeframeStart:datetime, timeframeEnd:datetime) {
CloudAppEvents
| where Timestamp between (timeframeStart .. timeframeEnd)
| where ActionType == "MailItemsAccessed"
| where RawEventData has "00000003-0000-0000-c000-0000000000000" // performance
check
| extend rawData = parse json(RawEventData)
| extend AppId = tostring(parse json(rawData.AppId))
| extend OAuthAppId = tostring(parse json(rawData.ClientAppId)) // extract OAuthAppId
summarize by OAuthAppId
};
appMailReadActivity(ago(1d),now()) // detection period
| join kind = leftanti appMailReadActivity(ago(7d),ago(2d)) // baseline period
on OAuthAppId
```

Microsoft 365 Defender's cross-domain XDR correlation enables stronger response to critical security incidents

Like the rest of the security industry, Microsoft continues to track the Solorigate attack, an active threat that continues to unfold as well as evolve. As part of empowering our customers and the larger security community to respond to this attack through sharing intelligence and providing advice, this blog serves to guide Microsoft 365 customers to take full advantage of the comprehensive visibility and the rich investigation tools available in Microsoft 365 Defender. This blog shows that many of the existing capabilities in Microsoft 365 Defender help address this attack, but the unique scenarios created by the threat resulted in some Solorigate-specific detections and other innovative protections, including ones that are made possible by deeply integrated cross-domain threat defense.

For additional information and further guidance, refer to these Microsoft resources:

Microsoft will continue to provide public information about the patterns and techniques of this attack and related intelligence for customers to defend themselves, in addition to enhancing the protection capabilities of Microsoft security solutions.

Appendix: Additional details for detection and hunting

Detection details

Attack stage	Microsoft 365 Defender detection or alert
Initial access	 Microsoft Defender for Endpoint: 'Solorigate' high-severity malware was detected/blocked/prevented (<u>Trojan:MSIL/Solorigate.BR!dha</u>) SolarWinds Malicious binaries associated with a supply chain attack
Execution and persistence	 Microsoft Defender for Endpoint: 'Solorigate' high-severity malware was detected/blocked/prevented (<u>Trojan:Win64/Cobaltstrike.RN!dha</u>, <u>Trojan:PowerShell/Solorigate.H!dha</u>) Suspicious process launch by Rundll32.exe Use of living-off-the-land binary to run malicious code A WMI event filter was bound to a suspicious event consumer
Command and Control	Microsoft Defender for Endpoint: An active 'Solorigate' high-severity malware was detected/ blocked/prevented (<u>Trojan:Win64/Cobaltstrike.RN!dha</u>)
Defense evasion	Microsoft Defender for Endpoint: Suspicious audit policy tampering
Reconnaissance	 Microsoft Defender for Endpoint: Masquerading Active Directory exploration tool Suspicious sequence of exploration activities Execution of suspicious known LDAP query fragments
Credential access	 Microsoft Defender for Endpoint: Suspicious access to LSASS (credential access) AD FS private key extraction attempt Possible attempt to access ADFS key material Suspicious ADFS adapter process created
	Microsoft Defender for Identity:
	 Unusual addition of permissions to an OAuth app Active Directory attributes Reconnaissance using LDAP
	Microsoft Cloud App Security:
	Unusual addition of credentials to an OAuth app
Lateral movement	 Microsoft Defender for Endpoint Suspicious file creation initiated remotely (lateral movement) Suspicious Remote WMI Execution (lateral movement)

Exfiltration

- Microsoft Defender for EndpointSuspicious mailbox export or access modificationSuspicious archive creation

Advanced hunting queries

Attack stage	Query link in GitHub repo
General	Microsoft Defender for Endpoint Threat and Vulnerability Management: <u>SolarWinds Orion software in your org</u>
Initial access	 Microsoft Defender for Endpoint: <u>Malicious DLLs loaded in memory</u> <u>Malicious DLLs created in the system or locally</u> <u>Compromised SolarWinds certificate</u>
Execution	Microsoft Defender for Endpoint: • <u>SolarWinds processes launching PowerShell with Base64</u> • <u>SolarWinds processes launching CMD with echo</u> • ADFS adapter process spawning: <i>DeviceProcessEvents</i> <i>where InitiatingProcessFileName</i> =~" <i>Microsoft.IdentityServer.ServiceHost.exe</i> " <i>where FileName in~("werfault.exe", "csc.exe"</i>) <i>where ProcessCommandLine !contains ("nameId"</i>)
Command and Control	Microsoft Defender for Endpoint <u>C2 communications</u> <u>C2 lookup</u>
Credential access	 Azure Active Directory (Microsoft Cloud App Security): Credentials added to AAD app after admin consent New access credential added to application or service principal Domain federation trust settings modified Add uncommon credential type to application Service Principal Added To Role
Exfiltration	 Exchange Online (Microsoft Cloud App Security): Mail Items Accessed Throttling Analytic Mail Items Accessed Anomaly Analytic OAuth Apps reading mail via GraphAPI anomaly OAuth Apps reading mail both via GraphAPI and directly