

# M365 Defender

**Corina Feuerstein**

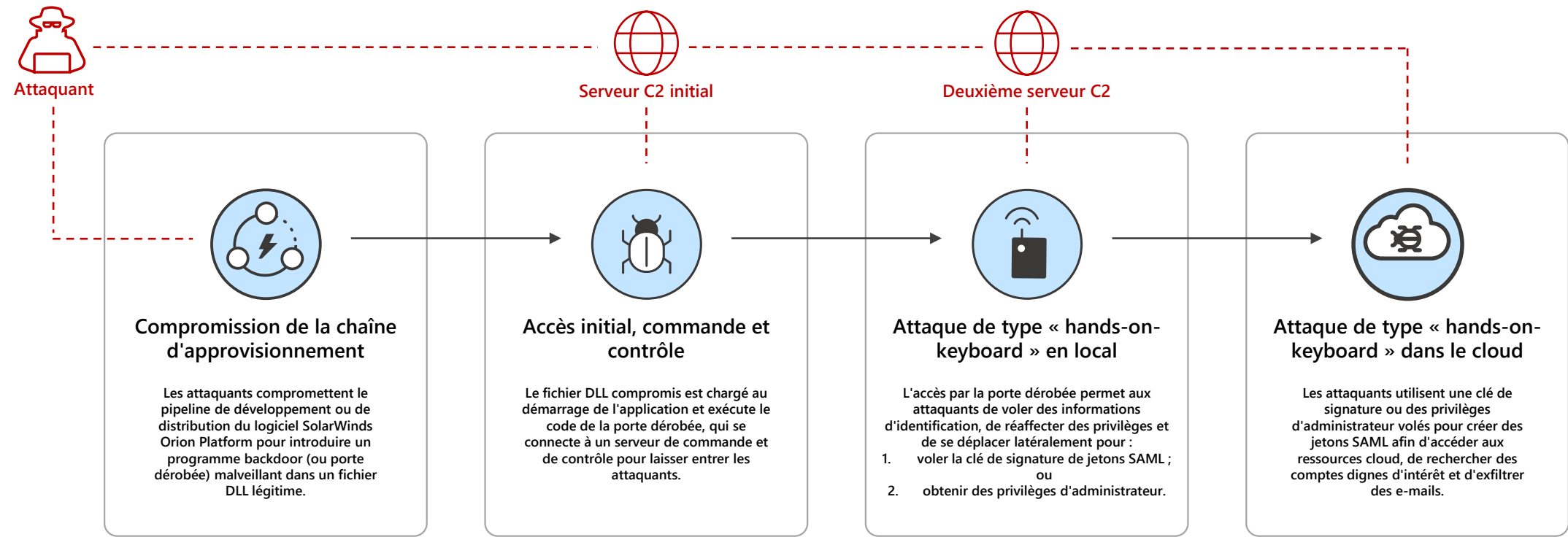
Responsable de la gestion des programmes  
M365 Defender

18 février 2021

# Utiliser Microsoft 365 Defender à des fins de détection, de protection et de correction

1. Apparition de l'attaque Solorigate
2. Détection et blocage de l'activité des points de terminaison locaux
3. Détection de la compromission des identités et basculement vers le cloud
4. Détection et réponse aux activités suspectes des applications cloud
5. Compréhension de l'exposition des organisations et des mesures d'atténuation à l'aide de l'analyse des menaces
6. Repérage dans les domaines à l'aide de Microsoft 365 Defender

# Présentation de Solorigate



# Communication C2 malveillante bloquée par MDE

## Network traffic to domains associated with a supply chain attack

Part of incident: Multi-stage incident involving Execution & Command and control on one endpoint [View incident page](#)

win-9njrns9ohht Risk level High

NT AUTHORITY\SYSTEM

ALERT STORY

Collapse all

9:25:48 AM

[2244] SolarWinds.BusinessLayerHost.exe

Network connect

(oo) Outbound connection from 10.10.50.242:49669 to 10.10.50.199:443

Remote IP address10.10.50.199

Remote port443

Local port49669

Action timeJan 3, 2021 9:25:50 AM

Resolved Domain 3mu76044hgf7shju.appsync-api.eu-west-1.avsvmcloud.com

9:25:50 AM

[2644] cmd.exe /c pause

Network traffic to domains associated with a supply chain attack High Detected New

Process id2644

Creation timeJan 3, 2021 9:25:50 AM

Image file pathC:\Windows\SysWOW64\cmd.exe

Image file SHA1e2ead0993b917e1828a658ada0b87e01d5b8424f

Image file creation timeOct 13, 2020 11:37:56 PM

Execution detailsToken elevation: Default, Integrity level: System

User NT AUTHORITY\SYSTEM

PE metadata cmd.exe

9:25:50 AM

Suspicious process launched using cmd.exe Low Detected New

cmd.exe script interpreter process was created by SolarWinds.BusinessLayerHost.exe

## Network traffic to domains associated with a supply chain attack

High Detected New

Classify this alert

True alert

False alert

Alert state

ClassificationNot Set [Set Classification](#)

Assigned toUnassigned [Assign to me](#)

Alert details

CategoryCommand and control

MITRE ATT&CK Techniques-

Detection sourceEDR

Detection statusDetected

Detection technologyBehavior,Network

Generated onJan 3, 2021 9:28:57 AM

First activityJan 3, 2021 9:25:50 AM

Last activityJan 3, 2021 9:25:50 AM

Alert description

A process has attempted to connect to domains known to serve trojanized versions of auto-update software. Connections to these domains can indicate that the machine has received a malicious update and might be under attacker control.

Recommended actions

A. Validate the alert.  
1. Check the process that initiated the connection

# Mouvement latéral détecté par MDE

Alerts > Suspicious Remote WMI Execution

## Suspicious Remote WMI Execution

 [redacted] Risk level ■ ■ ■ High ...

 [redacted] ...

ALERT STORY

Collapse all

[4284] WmiPrvSE.exe -secured -Embedding ...

[3340] rundll32.exe rundll32 c:\windows\legit\_payload.dll EntryPoint ...

Suspicious behavior by a svchost.exe was observed ■ ■ ■ Medium ● New ● Detected ...

Process launched with the security context of another user ■ ■ ■ Low ● New ● Detected ...

rundll32.exe was invoked remotely

Execution typeWmi

Source machine name[redacted]

Mitre techniquesT1047: Windows Management Instrumentation

Source machine ip a... [redacted] ...

Suspicious Remote WMI Execution ■ ■ ■ Medium ● New ● Detected ...

rundll32.exe process was created from a remote machine 'WINDOWS10-ATP-X' using Windows Management Instrumentation (WMI)

Suspicious WMI process creation ■ ■ ■ Medium ● New ● Detected ...

rundll32.exe process was created from a remote machine 'WINDOWS10-ATP-X' using Windows Management Instrumentation (WMI)

Execution sourceRemote

Remote machine Ne... [redacted]

Remote machine FQ... [redacted]




Action timeDec 22, 2020, 6:14:58 PM



Mitre techniquesT1047: Windows Management Instrumentation

Details


### Suspicious Remote WMI Execution

■ ■ ■ Medium **New**

 See in timeline  Link to another incident  Assign to me ...

 Automated investigation 27604 triggered by this alert is:  No threats found

Manage alert

 Classify this alert

True alert

False alert

Status

New

Classification

Select classification...

Alert details




Incident	Multi-stage incident involving Execution & Collection on multiple endpoints ( <a href="#">open in Microsoft 365 Defender</a> )
Detection source	EDR
Detection technology	Behavioral, Network
Detection status	Detected
Category	LateralMovement
Techniques	T1047: Windows Management Instrumentation
First activity	Dec 22, 2020, 6:14:58 PM
Last activity	Dec 22, 2020, 6:14:58 PM
Generated on	Dec 22, 2020, 6:25:50 PM
Assigned to	Automation



**Compromission d'ADFS  
moyennant le vol de la clé de  
certificat SAML ou la modification  
des approbations de fédération**

# Accès suspect à la clé ADFS

Alerts > ADFS private key extraction attempt



## ADFS private key extraction attempt



  Risk level High 



ALERT STORY


[Collapse all](#)

 [4280] SecurityHealthSystray.exe ... 

 [7448] OneDrive.exe /background ... 

File create

 dump\_em\_all.exe ... 

 Suspicious file dropped Medium New Detected ...








 [7956] dump\_em\_all.exe ... 


Image load

 dump\_em\_all.exe ... 


 Suspicious file dropped Medium New Detected ...

 dump\_em\_all.exe ran an LDAP query ^

LDAP Search query ( &(thumbnailphoto=\*)(objectClass=contact)(!(cn=CryptoPolicy))) 

Distinguished name CN=ADFS,CN=Microsoft,CN=Program Data,DC=ATP,DC=local 

Action time Jan 10, 2021, 7:09:02 PM

 ADFS private key extraction attempt High New Detected ...

Details

## ADFS private key extraction attempt

High New

[See in timeline](#) [Link to another incident](#) [Assign to me](#) ...

Manage alert

 Classify this alert

True alert False alert

Status New 

Classification Select classification... 

Alert details

Incident [Multi-stage incident involving Execution & Credential access on one endpoint \( !\[\]\(683dba75afe26e28cd4de5730b776760\_img.jpg\) open in Microsoft 365 Defender \)](#)

Detection source EDR

Detection technology Behavioral

Detection status Detected


Category CredentialAccess

Techniques [T1003: OS Credential Dumping](#)


**Utilisation de jetons SAML falsifiés  
pour persister dans le cloud,  
accéder aux ressources cloud et  
exfiltrer des e-mails.**





# Manipulation inhabituelle de l'application Oauth détectée par MCAS


Alerts >  **Unusual addition of credentials to an O...** 12/28/20 6:32 AM PREVIEW


+36

 MEDIUM SEVERITY

 Unusual addition of credentials to an OAuth app

 Office 365

 User Name

 1.1.1.1

Resolution options: 

User Name

Close alert









### Description

The user User Name (username@domain.com) performed an unusual addition of credentials to App Name. This usage pattern may indicate that an attacker has compromised the app, and is using it for phishing, exfiltration, or lateral movement. The user added a credentials of type Password, where an application is using a clear text password to authenticate.

### Important information

- Administrative activity was performed for the first time in 180 days by this user.
- Office 365 (Default) was used for administrative activity for the first time in 180 days by this user.
- 1.1.1.1 was used for the first time in 180 days by this user.

### Activity log

1 - 3 of 3 activities ⓘ							Investigate in Activity log		
Activity	User	App	IP address	Location	Device	Date			
 Update service principal: application App Name; ...	User Name	 Office 365	 1.1.1.1	 India	—	Dec 28, 2020, ...			
 Update application configuration: application Ap...	User Name	 Office 365	 1.1.1.1	 India	—	Dec 28, 2020, ...			

Microsoft 365 Security



Overview   Analyst report   Related incidents   Impacted assets   Prevented email attempts   Mitigations

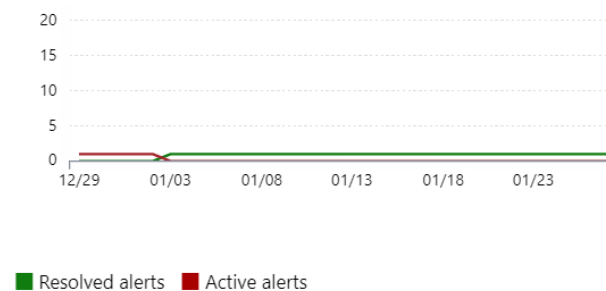
Microsoft Defender Antivirus protects against this threat. It blocks the known malicious SolarWinds binaries associated with this threat on your device.

Related incidents ⓘ

### Incidents severity



### Alerts over time ⓘ



Secure configuration status ⓘ

## Report details

Report type	Published	Last updated
Attack campaigns	12/14/20, 7:59 AM	12/21/20, 9:38 AM

Impacted assets <sup>(1)</sup>

Devices 0 / 1

■ Assets with active alerts   ■ Assets with resolved alerts  
■ Assets with no alerts

Vulnerability patching status ⓘ

## 0 vulnerable devices

# Rapport d'analyse de la menace Solorigate

Threats > Solorigate supply chain attack

Overview Analyst report Related incidents Impacted assets Prevented email attempts Mitigations

Secure configuration status ⓘ

1.43k misconfigured devices



Exposed Secure Unknown Not applicable

Vulnerability patching status ⓘ

0 vulnerable devices



Exposed Secure

Mitigation details

Secure configuration

Vulnerabilities

Product/Component

Vulnerability IDs

Exposed devices

orion\_user\_device\_tracker

TVM-2020-0002

0

highavailability\_orion\_plugin

TVM-2020-0002

0

orion\_netflow\_traffic

orion\_improvement

orion\_core\_services

orion\_network\_performance

orion\_network\_configuration

## Security recommendations

solarwinds orion

Security recommendation	OS platform	Weaknesses	Related component	Threats	Exposed devices	Status	Remediation type
Update Solarwinds Orion Network Performance Monitor	Windows	2	Solarwinds Orion ...	⚠️ ⚠️	7 / 8	Active	Software update
Update Solarwinds Orion Core Services	Windows	1	Solarwinds Orion ...	⚠️ ⚠️	4 / 12	Active	Software update
Update Solarwinds Orion Network Configuration Manager	Windows	1	Solarwinds Orion ...	⚠️ ⚠️	1 / 6	Active	Software update

ID de la vulnérabilité :  
**TVM-2020-0002**

## Update Solarwinds Orion Network Performance Monitor

Open software page Remediation options Exception options

Description  
Update Orion Network Performance Monitor to a later version to mitigate 2 known vulnerabilities affecting your devices.

### Vulnerability details

Number of vulnerabilities  
2

Exploit available  
No

Exposed devices  
7 / 8

Impact  
✔️ <0.01

Exposed operating systems  
Windows Server 2016. Windows Server 2012 R2

# Nouvelles données Azure AD et d'application cloud lors du repérage avancé

## Advanced hunting

### Schema

#### Alerts

- AlertInfo
- AlertEvidence

#### Apps & identities

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- AppFileEvents
- CloudAppEvents
- AADSpnSignInEventsBeta
- AADSignInEventsBeta**

- Timestamp
- Application
- ApplicationId
- LogonType
- ErrorCode
- CorrelationId
- SessionId
- AccountDisplayName
- AccountObjectId
- AccountUpn
- IsExternalUser
- IsGuestUser
- AlternateSignInName
- LastPasswordChangeTimestamp
- ResourceDisplayName
- ResourceId

Get started

Query

Run query

+ New

Save

Share link

```
1 //Look for throttled mailboxes which indicates excessive mail access over a short period of time
2
3 let starttime = 2d;
4 let endtime = 1d;
5 CloudAppEvents
6 | where Timestamp between (startofday(ago(starttime))..startofday(ago(endtime)))
7 | where ActionType == "MailItemsAccessed"
8 | where isnotempty(RawEventData["ClientAppId"]) and RawEventData["OperationProperties"][1] has "True"
9 | project Timestamp, RawEventData["OrganizationId"], AccountObjectId, UserAgent
```

Export

Timestamp RawEventData\_OrganizationId AccountObjectId UserAgent

No results found in the specified time frame.



## AADSignInEventsBeta

### Description

Information about Azure Active Directory (AAD) sign-in events either by a user (interactive) or a client on the user's behalf (non-interactive)

### Columns

Fields in this table:

Timestamp

Date and time when the record was generated

Application

Application that performed the recorded action

ApplicationId

Unique identifier for the application

[View all](#)

### Sample queries

[Sign-ins to disabled accounts](#)

[Users signing in from multiple locations](#)

CloudAppEvents  
/ où Application == « Office 365 »

[See full documentation](#)

Microsoft 365 Security



[Manage incident](#) [? Consult a threat expert](#) [Comments and history](#)

Summary Alerts (50) Devices (2) Users (3) Mailboxes (0) Investigations (6) Evidence (154)

**50/50 active alerts**  
**7 MITRE ATT&CK tactics**  
**2 other alert categories**



Dec 22, 2020, 1:52:20 AM | **New**  
**A WMI event filter was bound to a suspicious event consumer on** [redacted]  
[redacted]

Dec 22, 2020, 11:08:57 AM | **New**  
**Process launched with the security context of another user on** [redacted]  
[redacted] by user [redacted]













Dec 22, 2020, 11:37:49 AM | **New**  
**Suspicious file deletion activity was observed on** [redacted] by user [redacted]

Dec 22, 2020, 11:58:50 AM | **New**  
**Scheduled task possibly hijacked on** [redacted] by user [redacted]

Dec 22, 2020, 11:58:50 AM | **New**  
**Suspicious remote activity on** [redacted] by user [redacted]  
, and more.

Dec 22, 2020, 11:58:50 AM | **New**  
**Suspicious file creation initiated remotely on** [redacted] by user [redacted]

2 impacted devices  
3 impacted users

Entity type	Risk level/investigation priority	Tags
 	 High	
 	 High	
 	No data available	
 	No data available	
 	No data available	

View entities 

## 154 entities found

■ Not Found   ■ Other

[View all entities](#)

### Incident Information

① This incident might be associated with...

### Associated incidents

Incident ID	Reason	Entity
24851	Same file	sqlceip.exe
24576	Same file	legit_payl...
24576	Same file	payload.dll

### Tags summary

Incident tags

### Incident details

Status

Active

Severity

High

Incident ID

24963

### First activity

First - Dec 22, 2020, 1:52:20 AM

Last activity

Last - Dec 28, 2020, 3:04:12 PM

### Classification

Not set

### Determination

Not set

Série de vidéos consacrées à Solorigate

# Étapes suivantes

- 01.** Regardez la série de vidéos consacrées à Solorigate à cet emplacement
- 02.** Visitez le site de Sécurité Microsoft pour plus de mises à jour :  
[www.microsoft.com/en-us/security/business](https://www.microsoft.com/en-us/security/business)
- 03.** Lisez les billets de blog sur :  
[www.microsoft.com/security/blog](https://www.microsoft.com/security/blog)

**<https://aka.ms/solorigate>**

