

M365 Defender

Корина Фейерштейн

Руководитель по управлению программами
M365 Defender

18 февраля 2021 года

Использование Microsoft 365 Defender для противостояния угрозам

1. Как произошла атака Solorigate
2. Обнаружение и блокировка локальных действий конечных точек
3. Обнаружение компрометации удостоверений и переход в облако
4. Обнаружение подозрительных действий облачных приложений и реагирование на них
5. Понимание подверженности организации внешнему воздействию и снижение рисков с помощью аналитики угроз
6. Охота на угрозы по доменам с помощью Microsoft 365 Defender

Обзор Solorigate











A vertical sidebar menu featuring 20 distinct icons. From top to bottom, the icons are: a hamburger menu icon, a house icon, a shield with an exclamation mark, two speech bubbles, a circular arrow, a magnifying glass over a document, a trophy, a horizontal separator line, a magnifying glass, a clock face, a laptop, a stack of books, a network diagram with three nodes, a tablet displaying a bar chart, a desktop monitor with a bar chart, another horizontal separator line, an envelope, a document with a checklist, another horizontal separator line, a bar chart with an upward trend line, a heart shape, a key, and finally a gear or settings icon at the bottom.

win-9njrns9ohht Risk level ■■■ High ... NT AUTHORITY\SYSTEM ...

[Collapse all](#)

The image is a screenshot of the Windows Task Manager application, specifically the 'Network' tab. At the top, the process 'SolarWinds.BusinessLayerHost.exe' is selected. Below this, a network connection is highlighted: 'Outbound connection from 10.10.50.242:49669 to 10.10.50.199:443'. A detailed view of this connection is shown below, listing the following information: Remote IP address (10.10.50.199), Remote port (443), Local port (49669), Action time (Jan 3, 2021 9:25:50 AM), and Resolved Domain (3mu76044hg7shju.appsync-api.eu-west-1.avsvmcloud.com). The domain name is enclosed in a light blue box.

Outbound connection from 10.10.50.242:49669 to 10.10.50.199:443	
Remote IP address	10.10.50.199 
Remote port	443
Local port	49669
Action time	Jan 3, 2021 9:25:50 AM
Resolved Domain	 3mu76044hg7fshju.appspot-api.eu-west-1.avsvmcloud.com

[2644] cmd.exe /c pause	
Process id	2644
Creation time	Jan 3, 2021 9:25:50 AM
Image file path	C:\Windows\SysWOW64\cmd.exe
Image file SHA1	e2ead0993b917e1828a658ada0b87e01d5b8424f 
Image file creation time	Oct 13, 2020 11:37:56 PM
Execution details	Token elevation: Default, Integrity level: System 
User	 NT AUTHORITY\SYSTEM 
PE metadata	 cmd.exe 

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

■ ■ ■ High ● Detected ● New

True alert False alert

Classification	Assigned to
Not Set	Unassigned
Set Classification	Assign to me

Category	MITRE ATT&CK Techniques
Command and control	-

Detection source	Detection status
EDR	● Detected

Detection technology	Generated on
Behavior,Network	Jan 3, 2021 9:28:57 AM

First activity	Last activity
Jan 3, 2021 9:25:50 AM	Jan 3, 2021 9:25:50 AM

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.

1. Check the process that initiated the connection.

Microsoft 365 Security



1

1

7

1

II

EDR

Behavioral, Network

Detected

LateralMovement

T1047: Windows Management Instrumentation

Dec 22, 2020, 6:14:58 PM

Dec 22, 2020, 6:14:58 PM


Dec 22, 2020, 6:25:50 PM


Automation

**Компрометация ADFS путем кражи
ключа сертификата SAML или
изменения доверия федерации**

Подозрительный доступ к ключу ADFS


ADFS private key extraction attempt


 [redacted] Risk level High ...

 [redacted]


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 \(open in Microsoft 365 Defender \)](#)

Detection source EDR

Detection technology Behavioral

Detection status Detected

Category CredentialAccess


Techniques [T1003: OS Credential Dumping](#)


**Используйте поддельные
токены SAML для сохранения в
облаке, доступа к облачным
ресурсам и переноса
электронной почты.**


Необычные манипуляции с приложением OAuth, обнаруженные 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

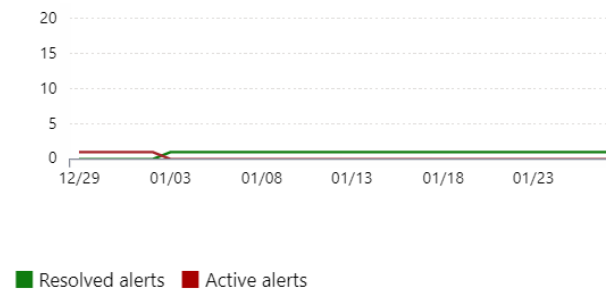
Microsoft Defender Antivirus protects against this threat. It blocks the known malicious SolarWinds binaries associated with this threat on your device.

Related incidents ⓘ

Incidents severity



Alerts over time ^①



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 ⓘ

Devices

0 / 1

** Access needed. Contact a global administrator to access Office 365 data.

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

[View all impacted assets](#)

Vulnerability patching status ⓘ

0 vulnerable devices

Отчет Solorigate об аналитике угроз

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

Идентификатор уязвимости:
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
Exposed devices: 7 / 8
Exploit available: No
Impact: <0.01

Exposed operating systems
Windows Server 2016, Windows Server 2012 R2

Новые данные Azure AD и облачных приложений в расширенной охоте на угрозы

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
/ where Application == "Office 365"

[See full documentation](#)

Изучение оповещений и инцидентов, связанных с Solorigate, в Microsoft 365 Defender

Incidents > Multi-stage incident involving Execution & Collection on multiple endpoints

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

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

Alerts and categories

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















© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

- 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]

Scope

2 impacted devices
3 impacted users

Top impacted entities

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

View entities

Evidence

154 entities found

Evidence remediation status

[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

Серия видео о Solorigate

Дальнейшие действия

- 01.** Посмотрите серию видео о Solorigate по этому адресу
- 02.** Следите за новостями на веб-сайте Microsoft Security:
www.microsoft.com/en-us/security/business
- 03.** Ознакомьтесь с публикациями в блоге:
www.microsoft.com/security/blog

<https://aka.ms/solorigate>

