Microsoft

Microsoft Defender for Endpoint

Andrea Lelli

Principal Security Research Lead

Windows Defender

February 18, 2021

Solorigate Overview

How Microsoft Defender for Endpoint can help

01. The method named Start

02. Backdoor access and privilege escalation

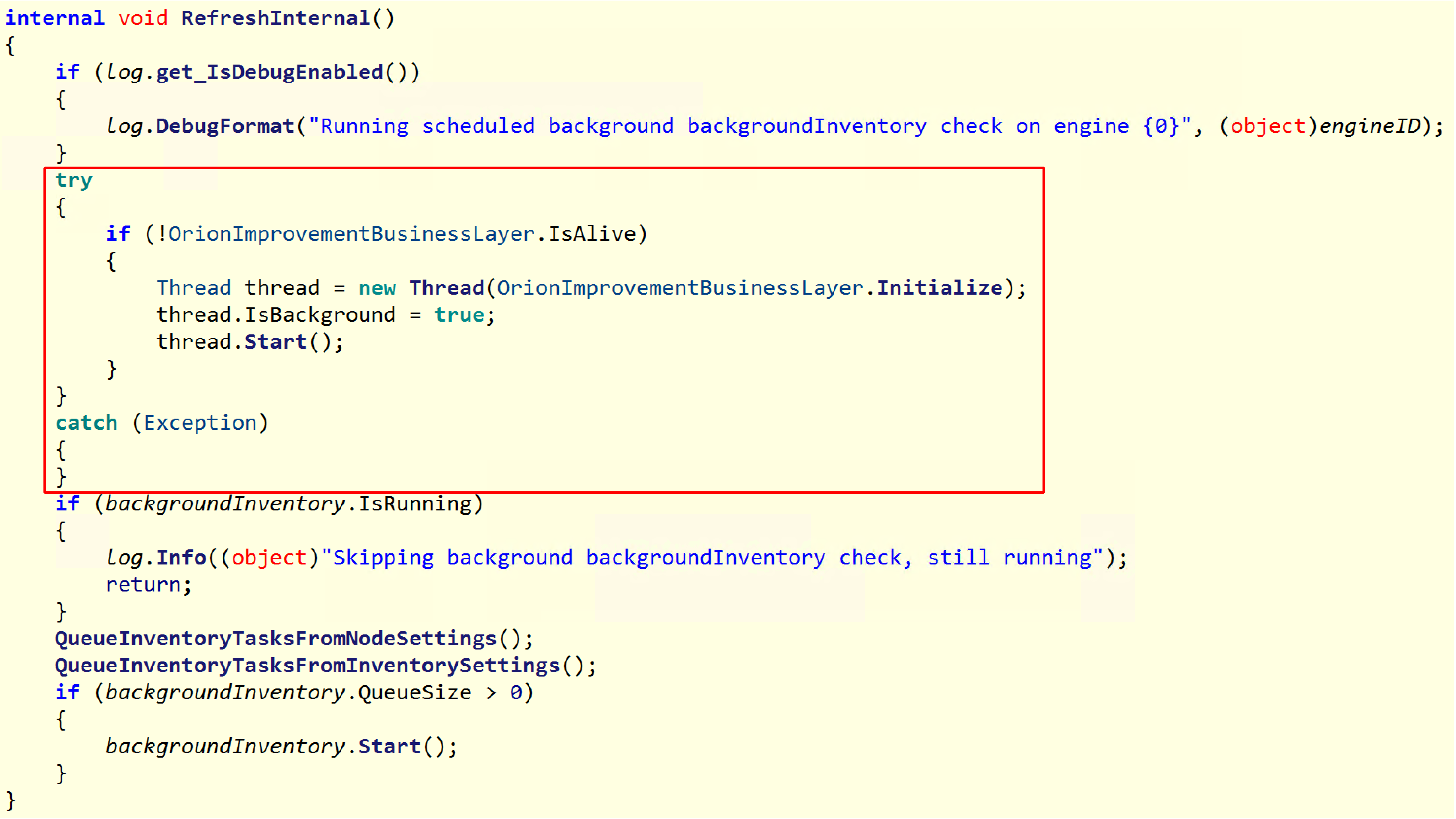
03. Backdoor access and second stage payloads

04. Steps to stop the spread with Endpoints

05. Steps to stop the spread with networks

06. Threat analytics report and hunting

Microsoft Security

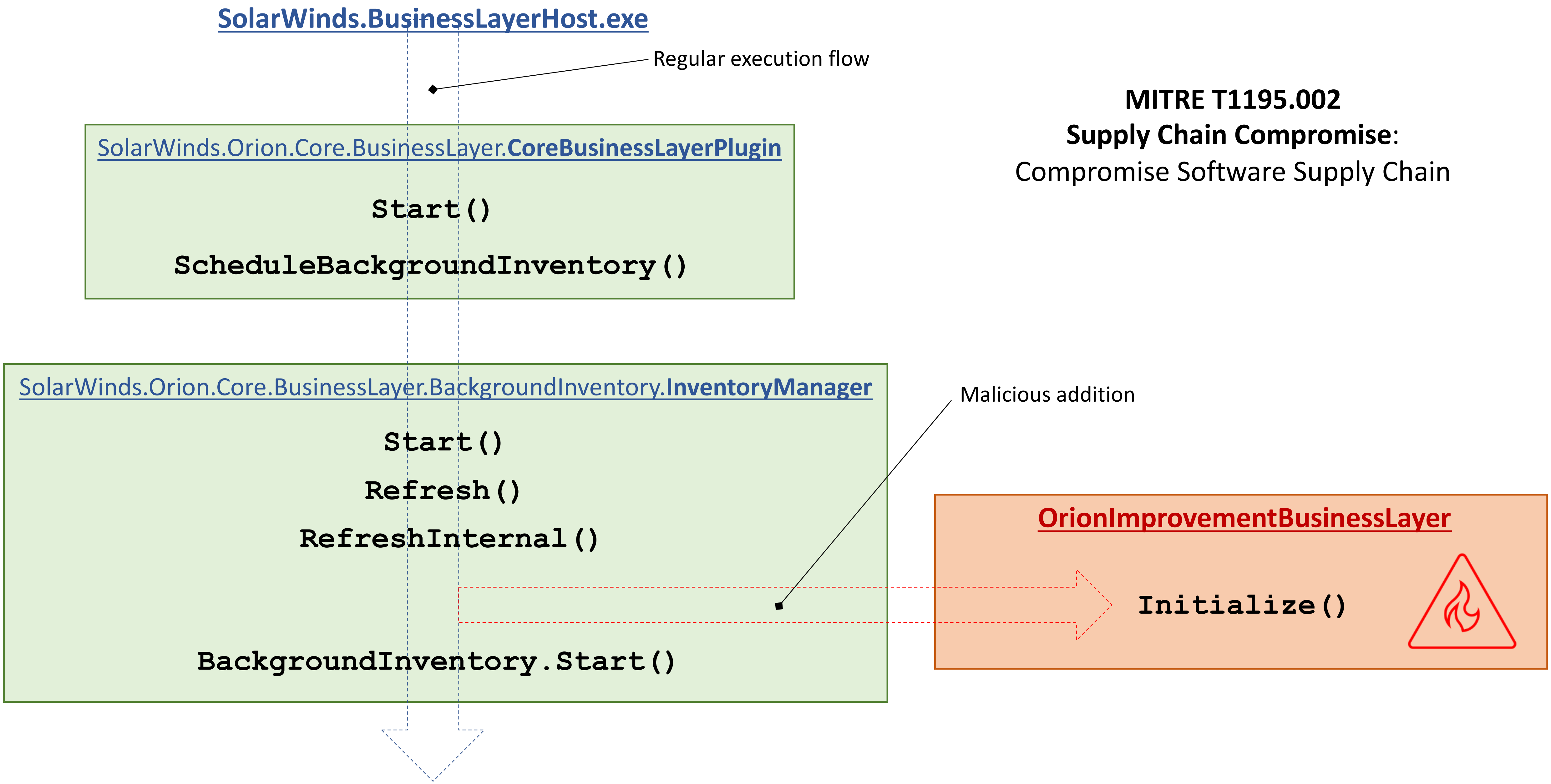


```
internal void RefreshInternal()
{
    if (log.get_IsDebugEnabled())
    {
        log.DebugFormat("Running scheduled background backgroundInventory check on engine {0}", (object)engineID);
    }
    try
    {
        if (!OrionImprovementBusinessLayer.IsAlive)
        {
            Thread thread = new Thread(OrionImprovementBusinessLayer.Initialize);
            thread.IsBackground = true;
            thread.Start();
        }
    }
    catch (Exception)
    {
    }
    if (backgroundInventory.IsRunning)
    {
        log.Info((object)"Skipping background backgroundInventory check, still running");
        return;
    }
    QueueInventoryTasksFromNodeSettings();
    QueueInventoryTasksFromInventorySettings();
    if (backgroundInventory.QueueSize > 0)
    {
        backgroundInventory.Start();
    }
}
```

MITRE T1195.002

Supply Chain Compromise:

Compromise Software Supply Chain



SolarWinds.BusinessLayerHost.exe

Regular execution flow

SolarWinds.Orion.Core.BusinessLayer.**CoreBusinessLayerPlugin**

`Start()`

`ScheduleBackgroundInventory()`

SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.**InventoryManager**

`Start()`

`Refresh()`

`RefreshInternal()`

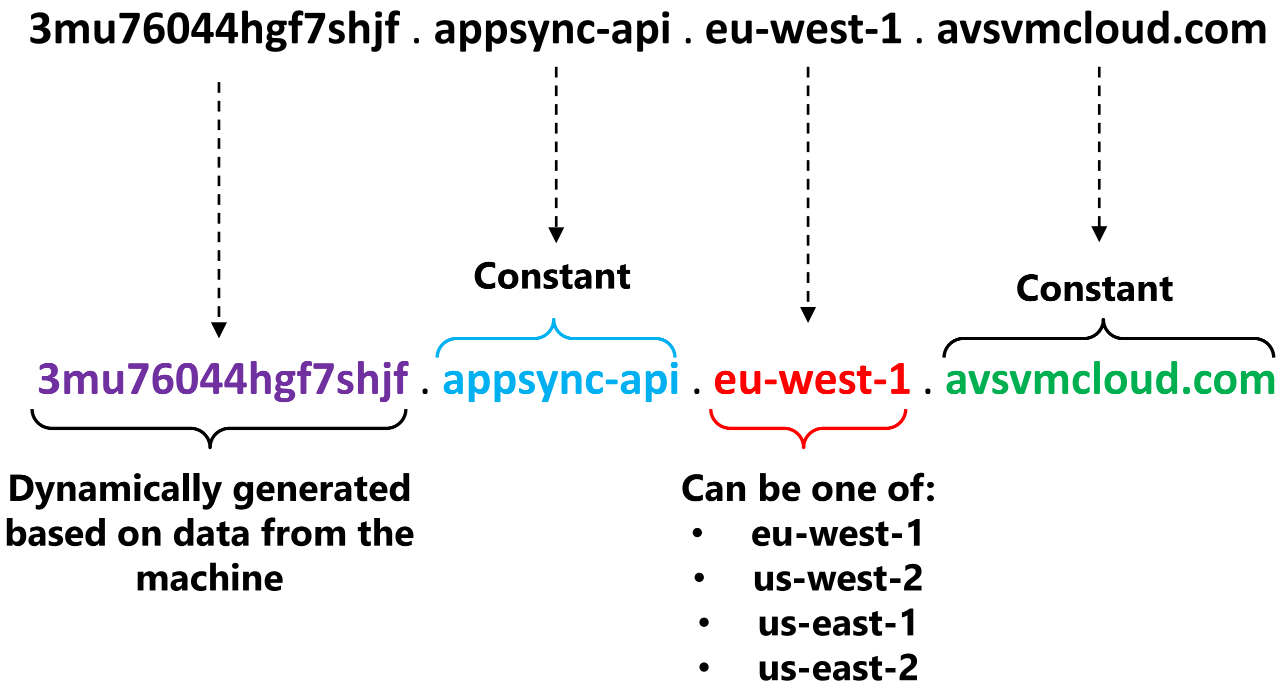
`BackgroundInventory.Start()`

Malicious addition

OrionImprovementBusinessLayer

`Initialize()`

Example of generated domain:



3mu76044hgf7shjf . appsync-api . eu-west-1 . avsvmcloud.com

Constant

Constant

3mu76044hgf7shjf . appsync-api . eu-west-1 . avsvmcloud.com

Dynamically generated based on data from the machine

Can be one of:

- eu-west-1
- us-west-2
- us-east-1
- us-east-2

SUPPLY CHAIN ATTACK

Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE

When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

DEFENSE EVASION

The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

RECON

The backdoor gathers system info

INITIAL C2

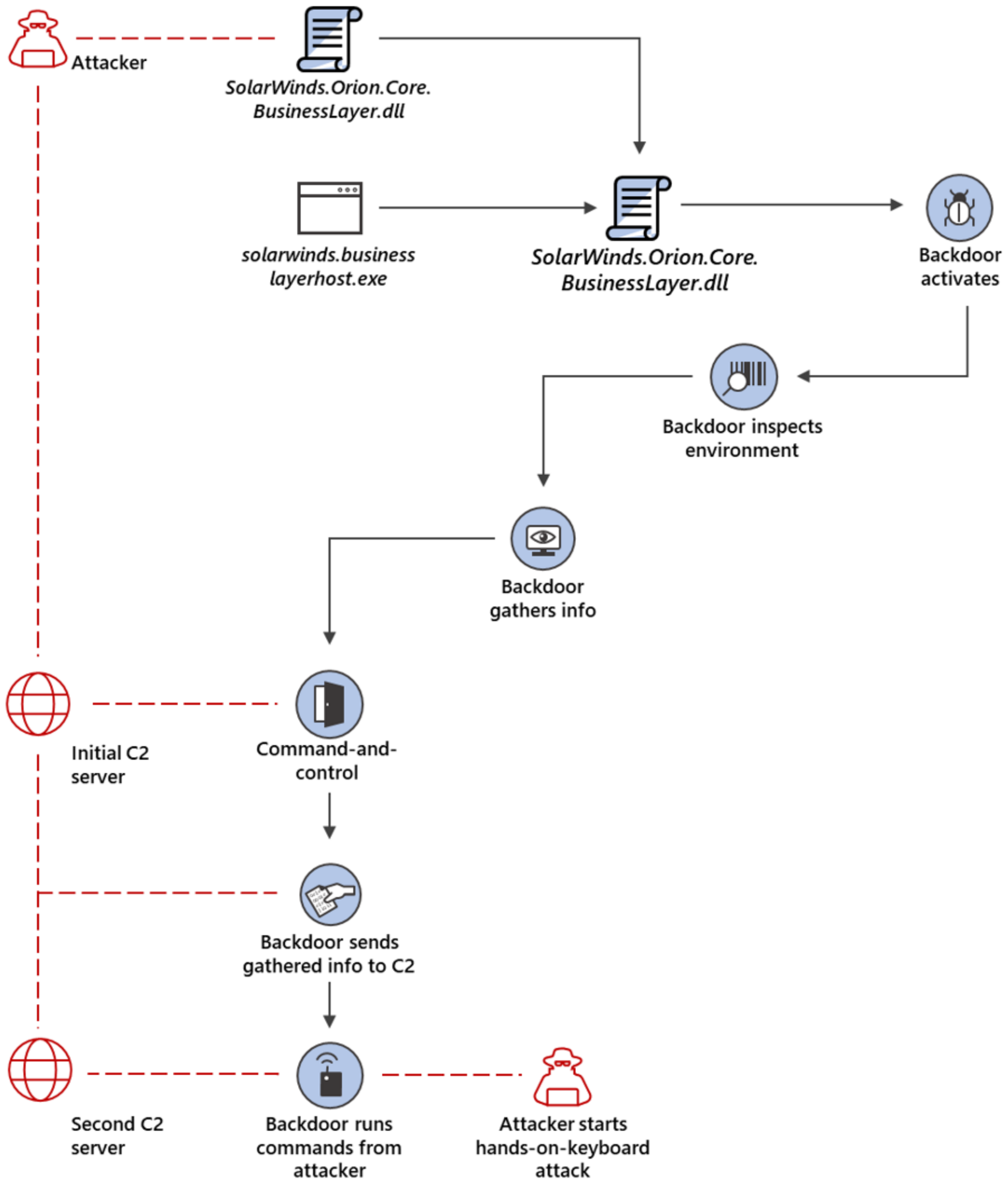
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

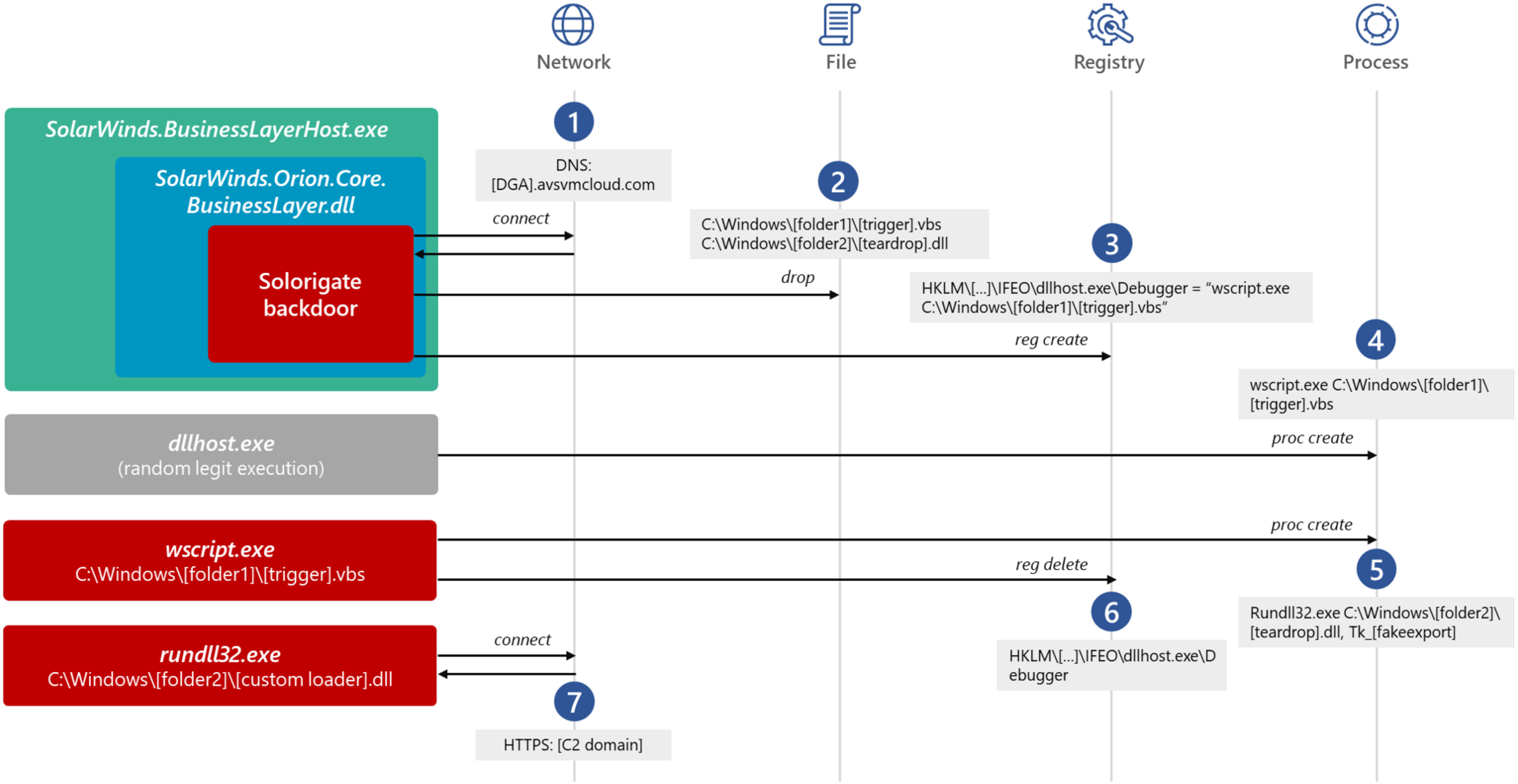
EXFILTRATION

The backdoor sends gathered information to the attacker.

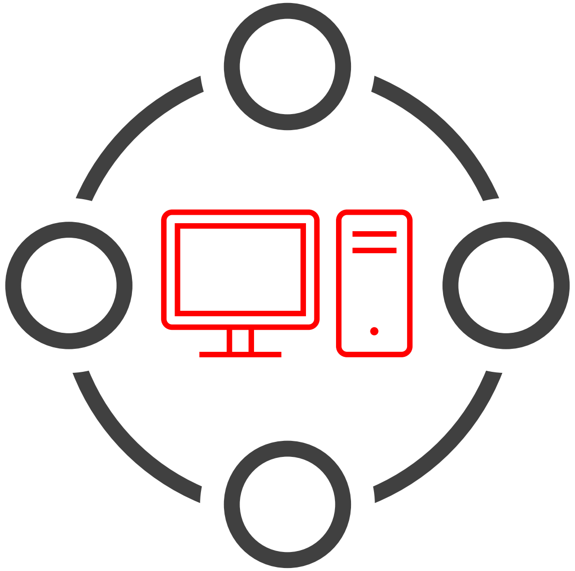
HANDS-ON-KEYBOARD ATTACK

The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.



Network
File
Registry
Process
SolarWinds.BusinessLayerHost.exe
SolarWinds.Orion.Core.
BusinessLayer.dll
Solorigate
backdoor
dllhost.exe
(random legit execution)
wscript.exe
C:\Windows\[folder1]\[trigger].vbs
rundll32.exe
C:\Windows\[folder2]\[custom loader].dll
1
DNS:
[DGA].avsvmcloud.com
connect
2
C:\Windows\[folder1]\[trigger].vbs
C:\Windows\[folder2]\[teardrop].dll
drop
3
HKLM\[...]\IFEO\dllhost.exe\Debugger = “wscript.exe
C:\Windows\[folder1]\[trigger].vbs”
reg create
4
wscript.exe C:\Windows\[folder1]\
[trigger].vbs
proc create
proc create
reg delete
5
Rundll32.exe C:\Windows\[folder2]\
[teardrop].dll, Tk_[fakeexport]
6
HKLM\[...]\IFEO\dllhost.exe\D
ebugger
connect
7
HTTPS: [C2 domain]

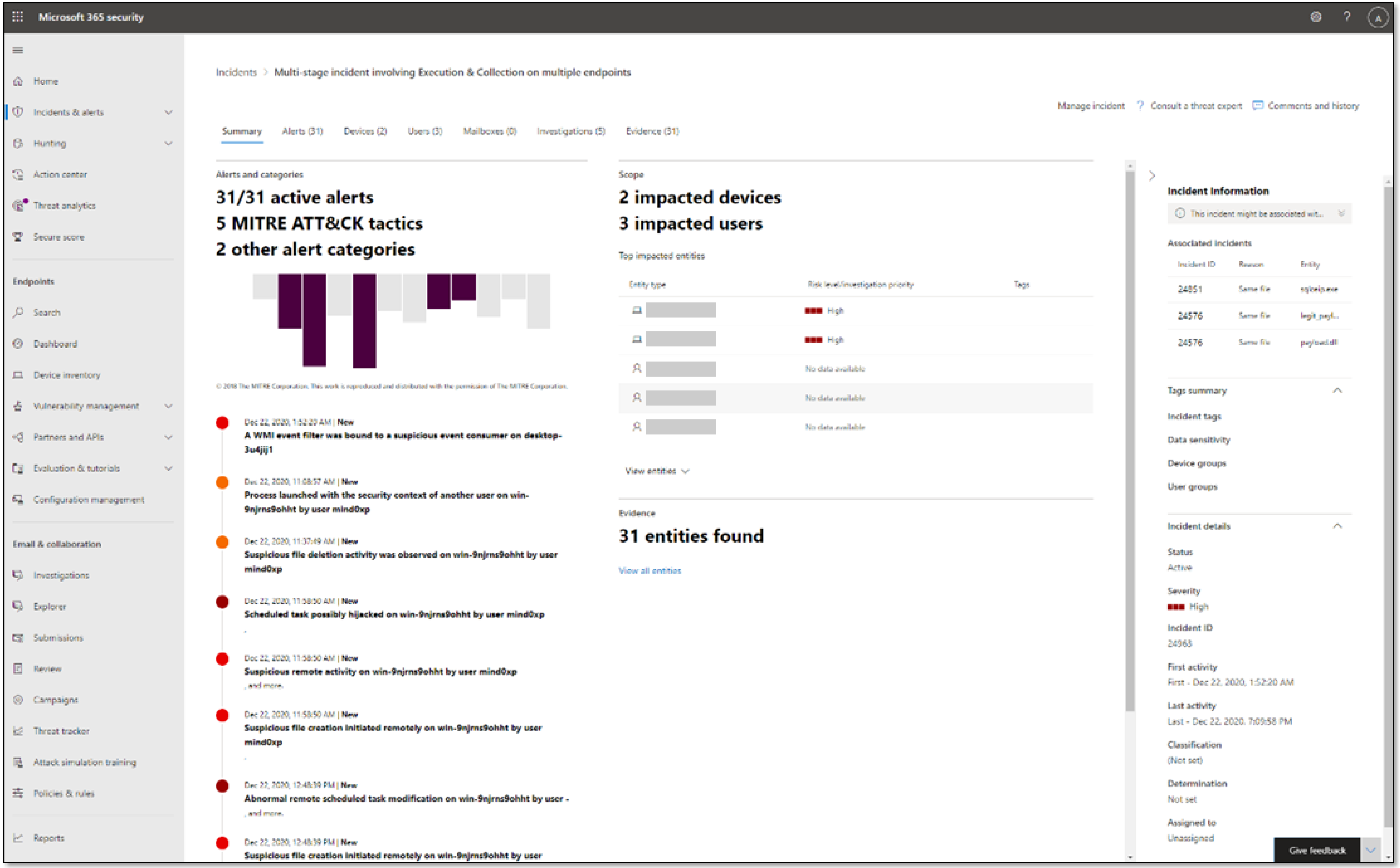
Isolate and Investigate Devices



Investigate Timeline
for Lateral Movement

Identify Accounts

Investigate Compromise Origin



Alerts and categories

31/31 active alerts
5 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 desktop-3u4jij1

Dec 22, 2020, 11:08:57 AM | New
Process launched with the security context of another user on win-9njrns9ohht by user mind0xp

Dec 22, 2020, 11:37:49 AM | New
Suspicious file deletion activity was observed on win-9njrns9ohht by user mind0xp

Dec 22, 2020, 11:58:50 AM | New
Scheduled task possibly hijacked on win-9njrns9ohht by user mind0xp
,

Dec 22, 2020, 11:58:50 AM | New
Suspicious remote activity on win-9njrns9ohht by user mind0xp
, and more.

Dec 22, 2020, 11:58:50 AM | New
Suspicious file creation initiated remotely on win-9njrns9ohht by user mind0xp
,

Dec 22, 2020, 12:48:39 PM | New
Abnormal remote scheduled task modification on win-9njrns9ohht by user -
, and more.

Dec 22, 2020, 12:48:39 PM | New
Suspicious file creation initiated remotely on win-9njrns9ohht by user

Scope

2 impacted devices
3 impacted users

Top impacted entities

Entity type	Risk level/investigation priority	Tags
[redacted]	■■■ High	
[redacted]	■■■ High	
[redacted]	No data available	
[redacted]	No data available	
[redacted]	No data available	

Evidence

31 entities found

Incident Information

This incident might be associated wit...

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

Data sensitivity

Device groups

User groups

Incident details

Status
Active

Severity
■■■ High

Incident ID
24963

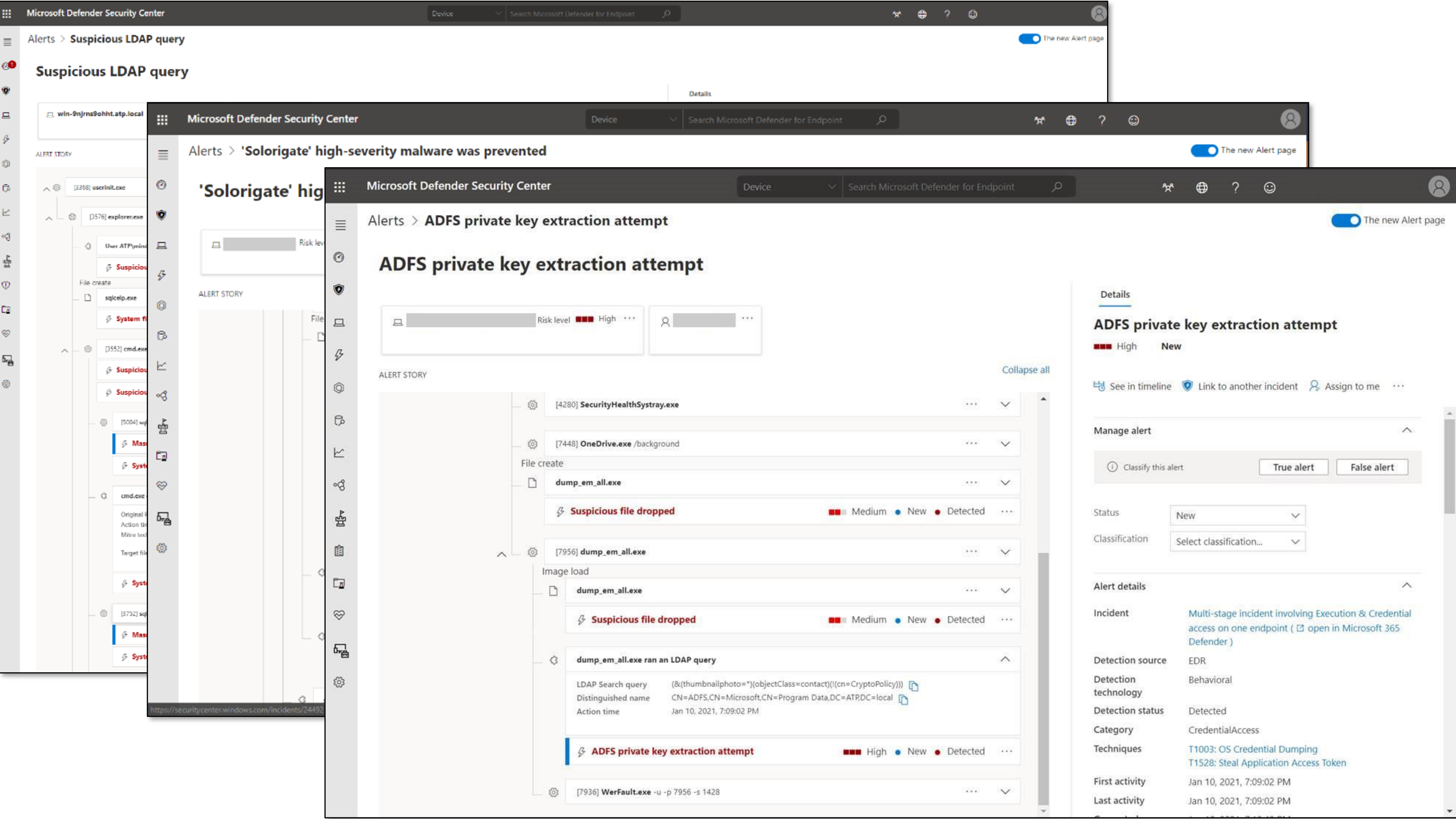
First activity
First - Dec 22, 2020, 1:52:20 AM

Last activity
Last - Dec 22, 2020, 7:09:58 PM

Classification
(Not set)

Determination
Not set

Assigned to
Unassigned



Microsoft Defender Security Center
Device
Search Microsoft Defender for Endpoint
The new Alert page

Alerts > Suspicious LDAP query

Suspicious LDAP query

Details

win-9njrns9ohht.atp.local

ALERT STORY

[3308] userinit.exe

[3576] explorer.exe

User ATP\mind

Suspiciou

File create

sqlcelp.exe

System fi

[3552] cmd.exe

Suspiciou

Suspiciou

[5004] sq

Mas

Syst

cmd.exe

Original F
Action tin
Mitre tech

Target file

Syst

[3752] sql

Mas

Syst

Microsoft Defender Security Center
Device
Search Microsoft Defender for Endpoint
The new Alert page

Alerts > 'Solorigate' high-severity malware was prevented

'Solorigate' hig

[redacted] Risk lev

ALERT STORY

File

https://securitycenter.windows.com/incidents/24492

Microsoft Defender Security Center
Device
Search Microsoft Defender for Endpoint
The new Alert page

Alerts > ADFS private key extraction attempt

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 ···

[7936] **WerFault.exe** -u -p 7956 -s 1428 ···

Details

ADFS private key extraction attempt

■■■ High **New**

Manage alert

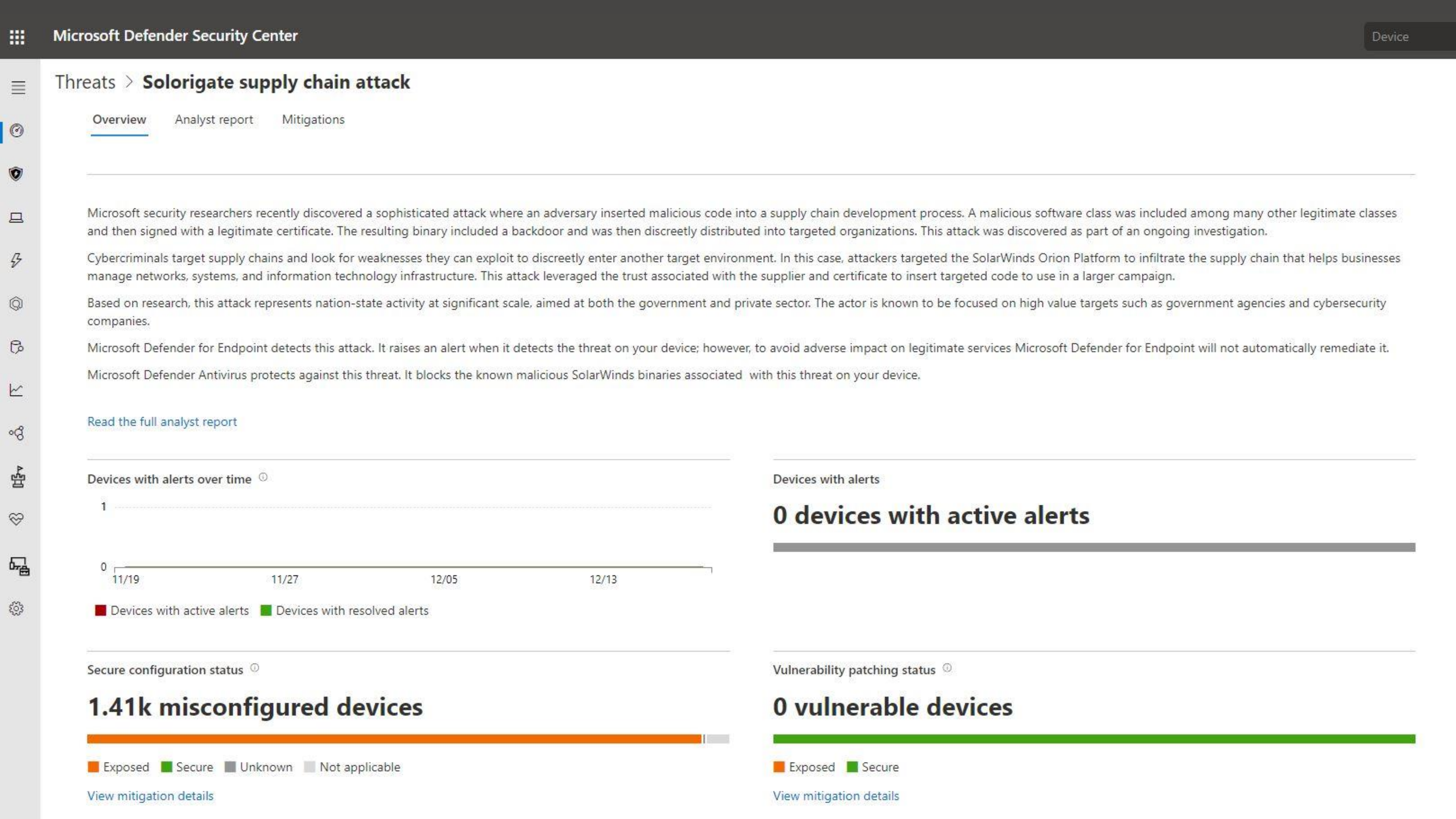
Classify this alert True alert False alert

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
T1528: Steal Application Access Token
First activity Jan 10, 2021, 7:09:02 PM
Last activity Jan 10, 2021, 7:09:02 PM



Microsoft Defender Security Center

Device

Threats > **Solorigate supply chain attack**

Overview | Analyst report | Mitigations

Microsoft security researchers recently discovered a sophisticated attack where an adversary inserted malicious code into a supply chain development process. A malicious software class was included among many other legitimate classes and then signed with a legitimate certificate. The resulting binary included a backdoor and was then discreetly distributed into targeted organizations. This attack was discovered as part of an ongoing investigation.

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.

Based on research, this attack represents nation-state activity at significant scale, aimed at both the government and private sector. The actor is known to be focused on high value targets such as government agencies and cybersecurity companies.

Microsoft Defender for Endpoint detects this attack. It raises an alert when it detects the threat on your device; however, to avoid adverse impact on legitimate services Microsoft Defender for Endpoint will not automatically remediate it.

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

Read the full analyst report

Devices with alerts over time ⓘ

🟥 Devices with active alerts 🟩 Devices with resolved alerts

Devices with alerts

0 devices with active alerts

Secure configuration status ⓘ

1.41k misconfigured devices

🟧 Exposed 🟩 Secure ◼ Unknown ◻ Not applicable

View mitigation details

Vulnerability patching status ⓘ

0 vulnerable devices

🟧 Exposed 🟩 Secure

View mitigation details

Solorigate Video Series

Next Steps

01. Watch the Solorigate Video series at this location

02. Visit Microsoft Security for more updates: www.microsoft.com/en-us/security/business

03. Read the blog posts on: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft