Microsoft

# Microsoft Defender for Endpoint

**Andrea Lelli**

Principal Security Research Lead

Windows Defender

**18.2.2021**

Solorigate-yleiskatsaus

# Miten Microsoft Defender for Endpoint voi auttaa?

**01.** Menetelmä nimeltä Aloitus

**02.** Takaportin käyttö ja oikeuksien laajentaminen

**03.** Takaportin käyttö ja toisen vaiheen tiedot

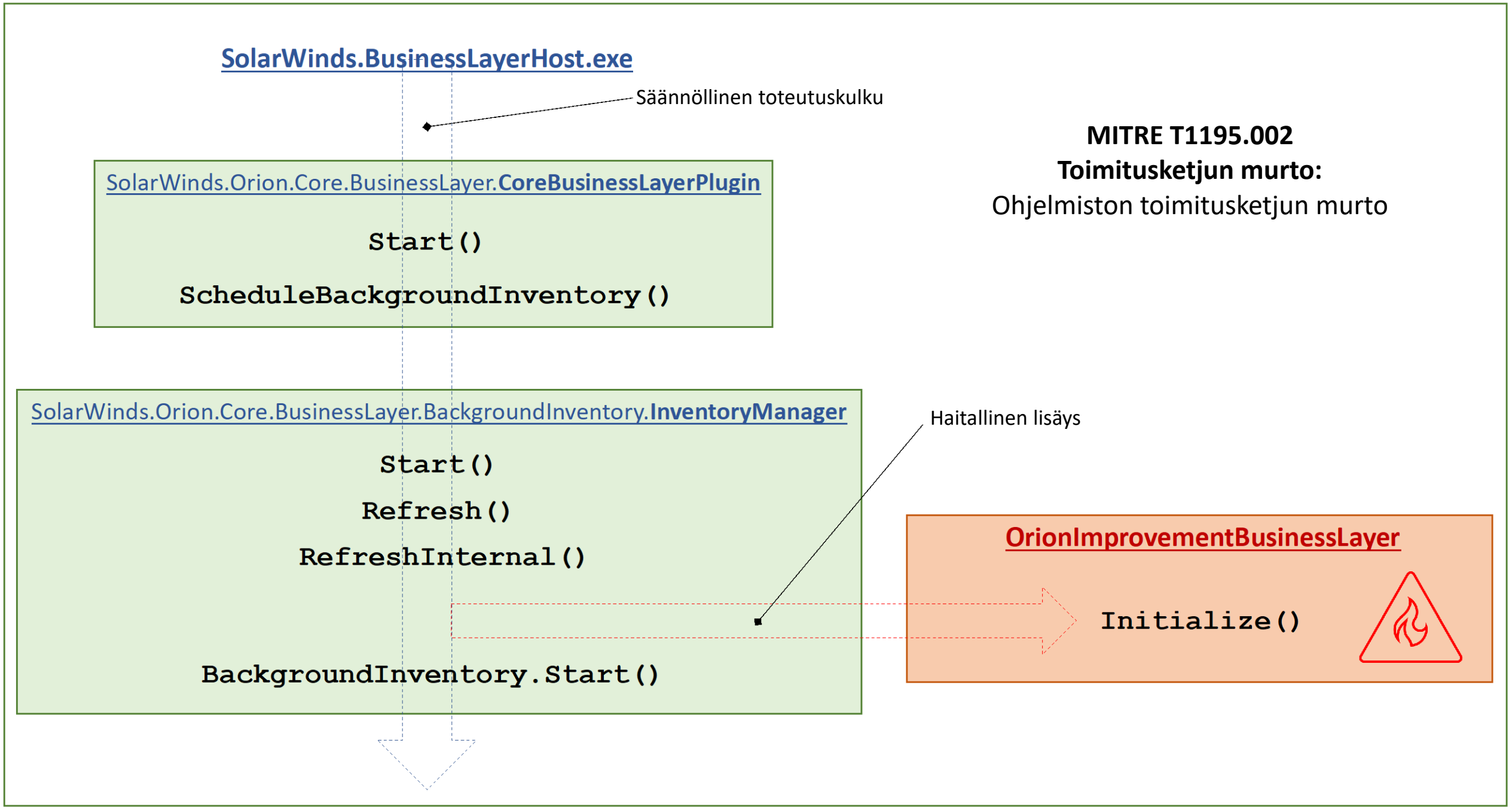
**04.** Vaiheet leviämisen estämiseen päätepisteiden avulla

**05.** Vaiheet leviämisen estämiseen verkkojen avulla

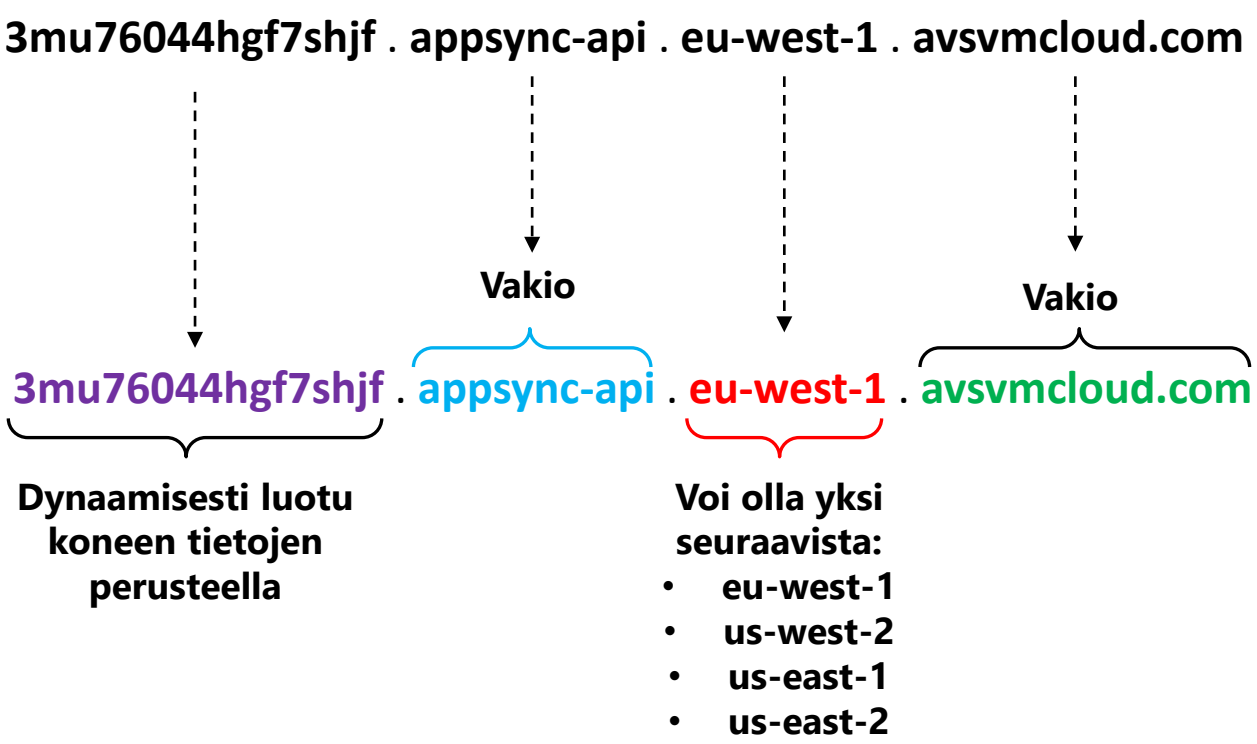
**06.** Uhka-analytiikkaraportti ja etsintä

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();
    }
}
```


SolarWinds.BusinessLayerHost.exe
Säännöllinen toteutuskulku
SolarWinds.Orion.Core.BusinessLayer.CoreBusinessLayerPlugin
Start()
ScheduleBackgroundInventory()
SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager
Start()
Refresh()
RefreshInternal()
BackgroundInventory.Start()
Haitallinen lisäys
OrionImprovementBusinessLayer
Initialize()
MITRE T1195.002
Toimitusketjun murto:
Ohjelmiston toimitusketjun murto

Esimerkki luodusta toimialueesta:



TOIMITUSKETJUN HYÖKKÄYS
Hyökkääjät lisäävät haitallisen koodin oikeutetun ohjelmiston DLL-komponenttiin. Vaarantunut DLL jaetaan organisaatioille, jotka käyttävät siihen liittyvää ohjelmistoa.

TOTEUTUS, PYSYVYYS
Kun ohjelmisto käynnistyy, vaarantunut DLL latautuu ja lisätty haittakoodi kutsuu toimintoa, joka sisältää takaportin ominaisuudet.

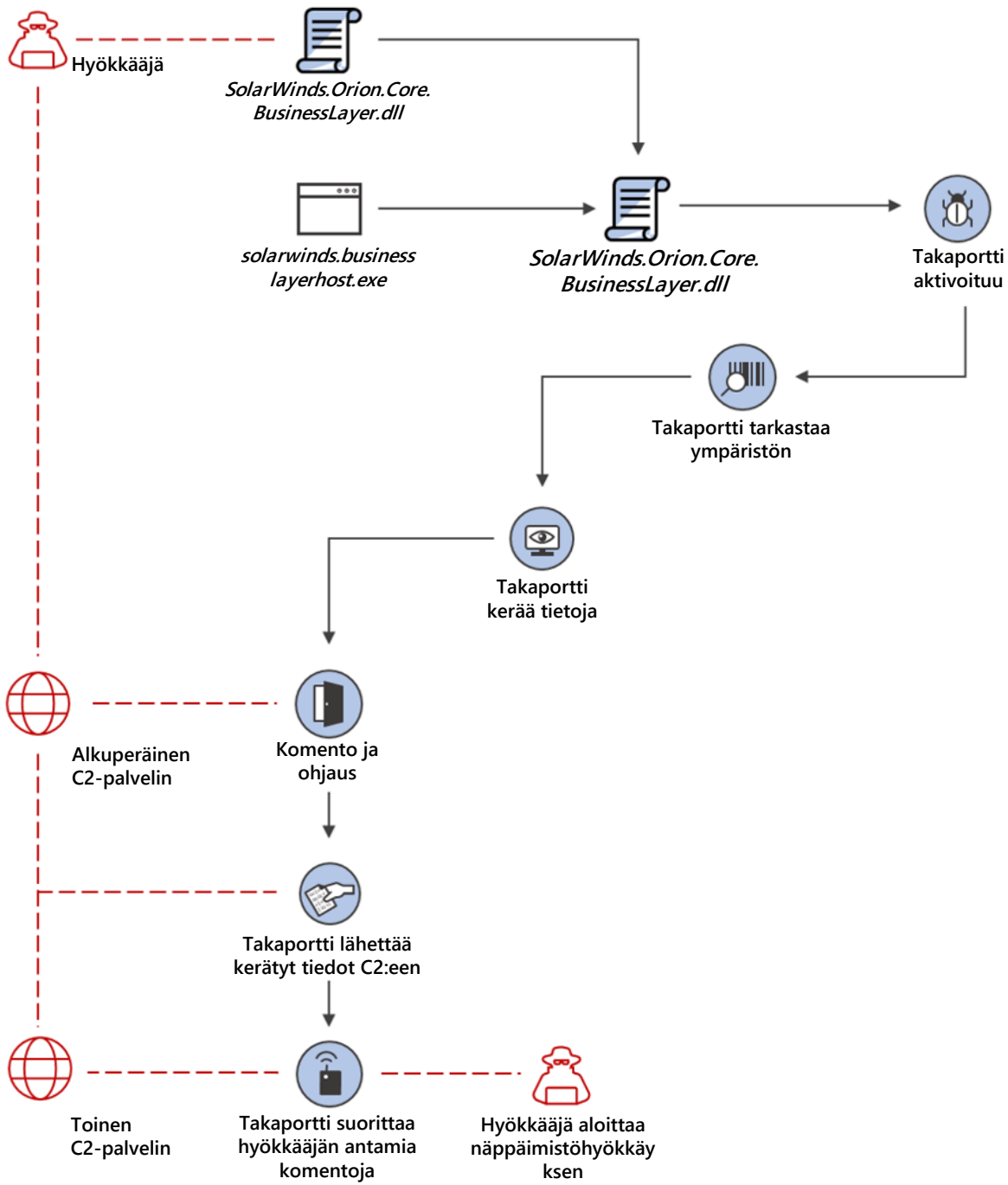
SUOJAUKSEN VÄLTTÄMINEN
Takaportilla on pitkä lista tarkistuksia, joiden avulla se varmistaa, että toimii todellisessa vaarantuneessa verkossa.

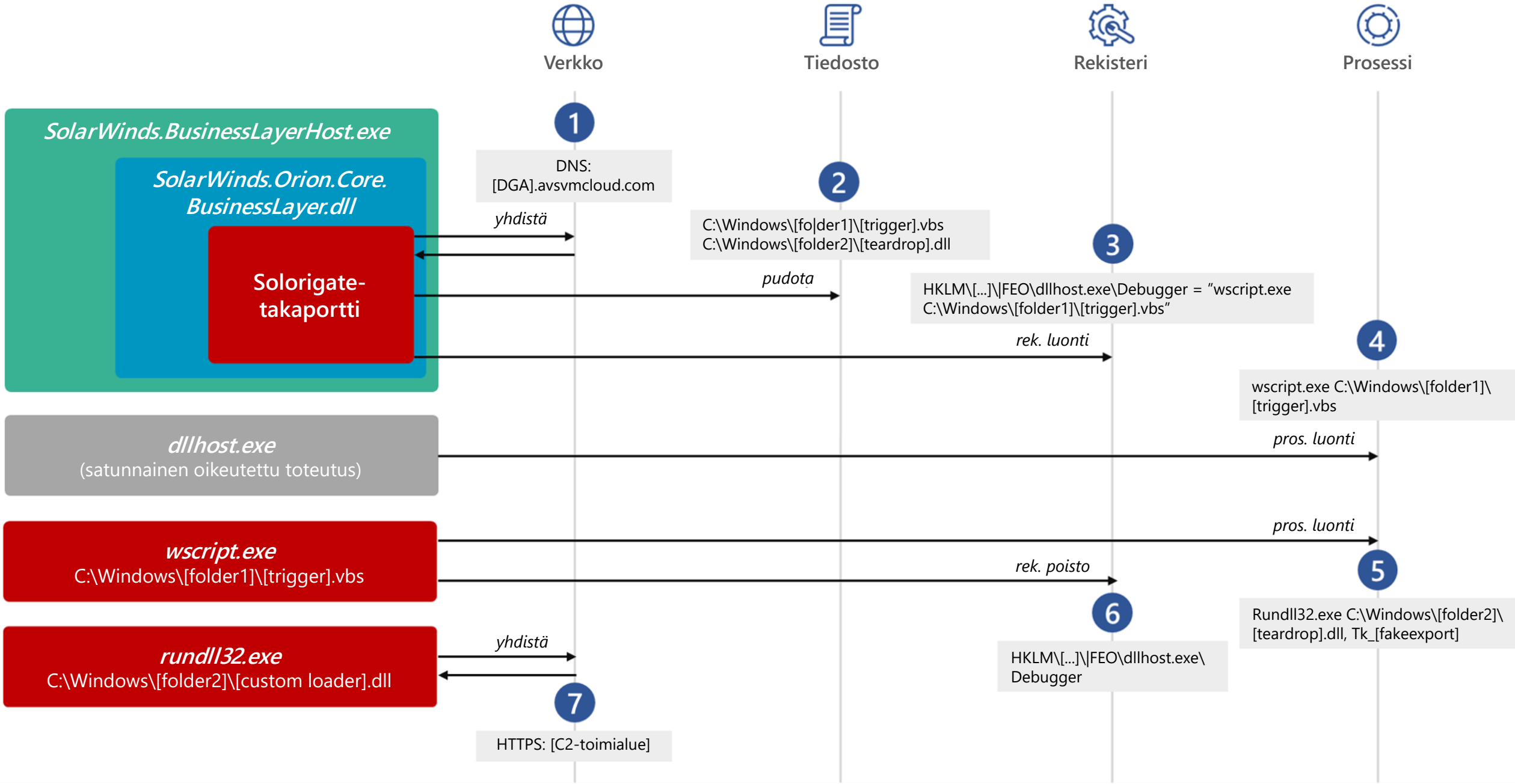
TIEDUSTELU
Takaportti kerää järjestelmätietoja

ALKUPERÄINEN C2
Takaportti muodostaa yhteyden komento- ja ohjauspalvelimeen. Toimialue, johon se muodostaa yhteyden, perustuu osittain järjestelmästä kerättyihin tietoihin, mikä tekee jokaisesta kolmannen tason toimialueesta ainutlaatuisen. Takaportti voi saada ylimääräisen C2-osoitteen, johon se voi muodostaa yhteyden.

LUVATON SIIRTO
Takaportti lähettää kerätyt tiedot hyökkääjälle.

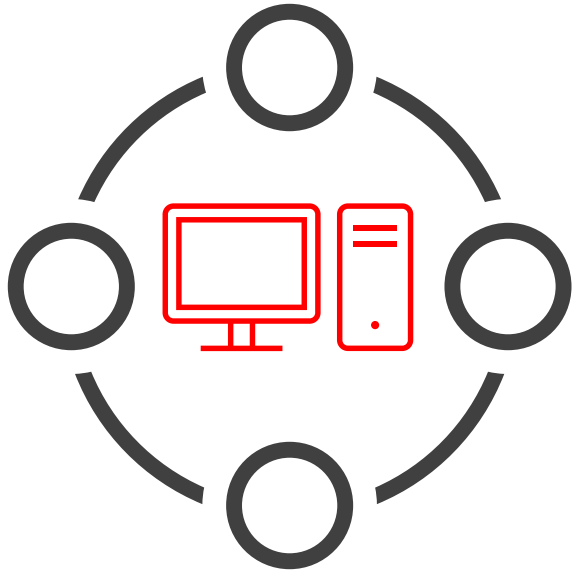
NÄPPÄIMISTÖHYÖKKÄYS
Takaportti suorittaa komentoja, jotka se saa hyökkääjiltä. Takaportin laaja valikoima ominaisuuksia antaa hyökkääjille mahdollisuuden suorittaa lisätoimintoja, kuten tunnistetietojen varastamisen, oikeuksien laajentamisen ja sivuttaissiirtymän.




Verkko
Tiedosto
Rekisteri
Prosessi
SolarWinds.BusinessLayerHost.exe
SolarWinds.Orion.Core.BusinessLayer.dll
Solorigate-takaportti
1
DNS: [DGA].avsvmcloud.com
yhdistä
2
C:\Windows\[fo|der1]\[trigger].vbs
C:\Windows\[folder2]\[teardrop].dll
pudota
3
HKLM\[...]\|FEO\dllhost.exe\Debugger = "wscript.exe C:\Windows\[folder1]\[trigger].vbs"
rek. luonti
4
wscript.exe C:\Windows\[folder1]\[trigger].vbs
dllhost.exe
(satunnainen oikeutettu toteutus)
pros. luonti
wscript.exe
C:\Windows\[folder1]\[trigger].vbs
pros. luonti
rek. poisto
5
Rundll32.exe C:\Windows\[folder2]\[teardrop].dll, Tk_[fakeexport]
6
HKLM\[...]\|FEO\dllhost.exe\Debugger
rundll32.exe
C:\Windows\[folder2]\[custom loader].dll
yhdistä
7
HTTPS: [C2-toimialue]

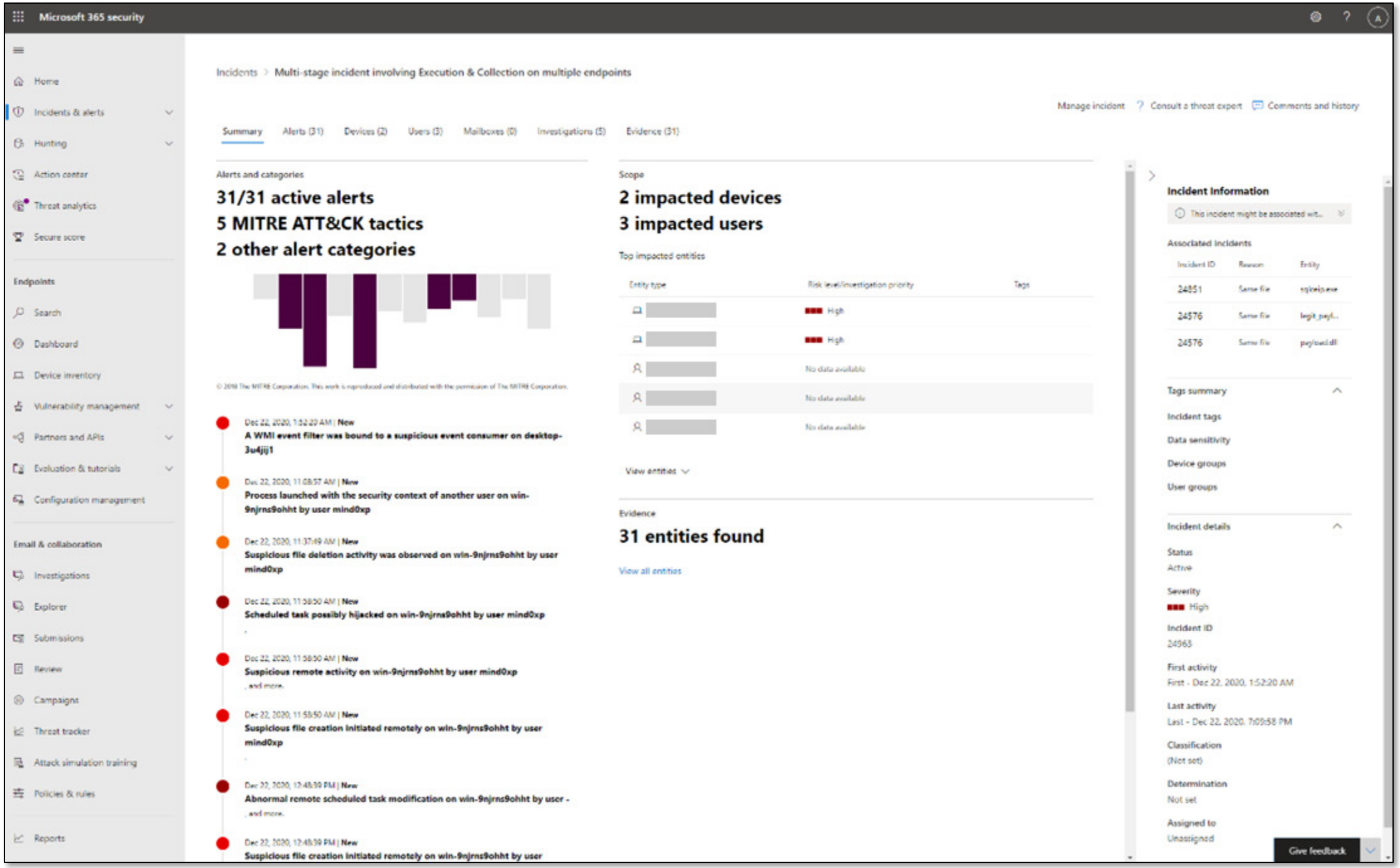
Laitteiden eristäminen ja tutkiminen

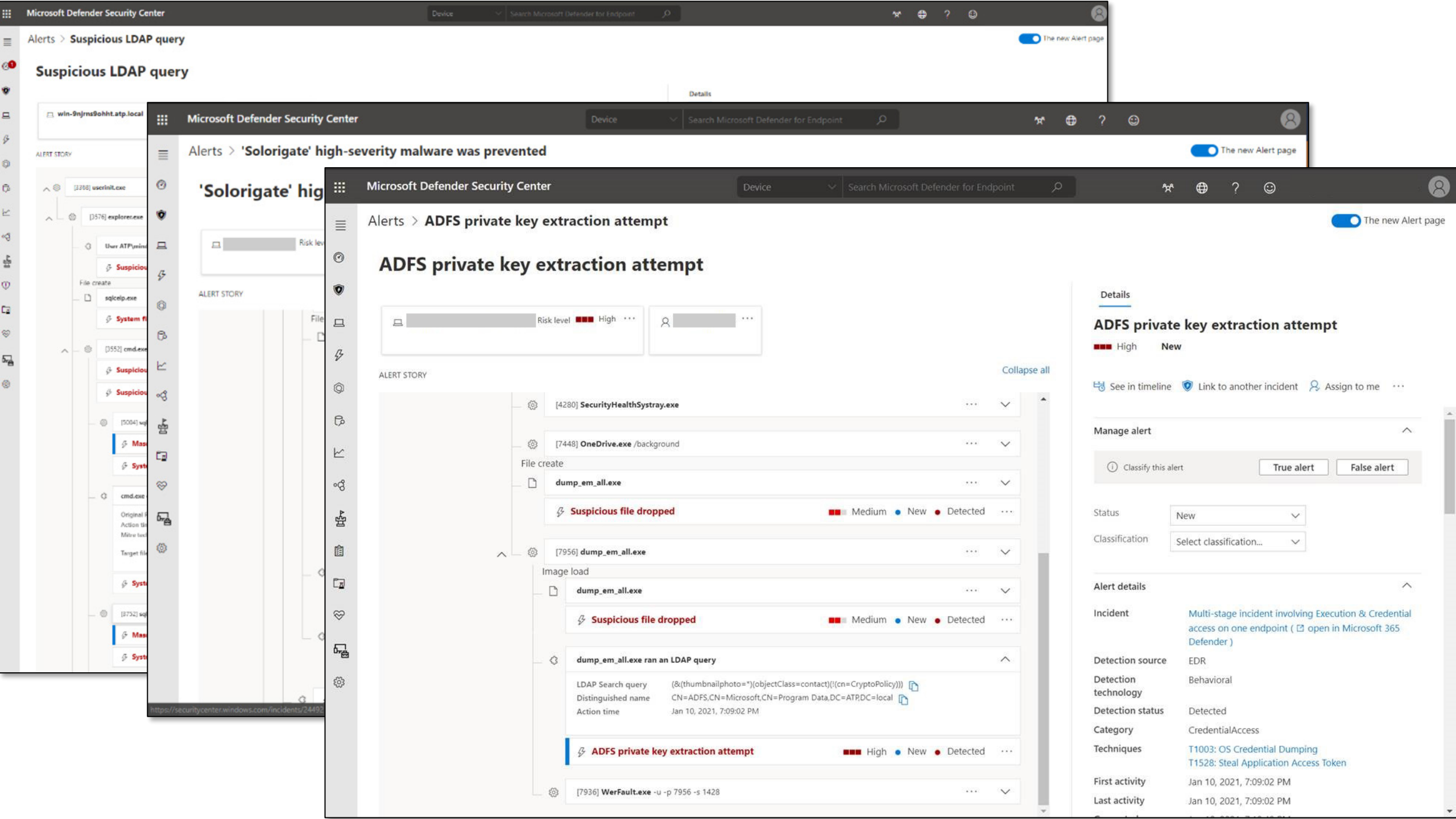
Sivuttaissiirtymän aikajanan tutkiminen



Tilien tunnistaminen

Murron alkuperän tutkiminen


Microsoft 365 security
Home
Incidents & alerts
Hunting
Action center
Threat analytics
Secure score
Endpoints
Search
Dashboard
Device inventory
Vulnerability management
Partners and APIs
Evaluation & tutorials
Configuration management
Email & collaboration
Investigations
Explorer
Submissions
Review
Campaigns
Threat tracker
Attack simulation training
Policies & rules
Reports
Incidents > Multi-stage incident involving Execution & Collection on multiple endpoints
Manage incident
Consult a threat expert
Comments and history
Summary
Alerts (31)
Devices (2)
Users (3)
Mailboxes (0)
Investigations (5)
Evidence (31)
Alerts and categories
31/31 active alerts
5 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 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
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 -
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
High
High
No data available
No data available
No data available
View entities
Evidence
31 entities found
View all entities
Incident Information
Associated incidents
Incident ID
Reason
Entity
24851
24576
24576
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
Give feedback


Microsoft Defender Security Center
Device
Search Microsoft Defender for Endpoint
Alerts > Suspicious LDAP query
The new Alert page
Suspicious LDAP query
Details
win-9njrns9ohht.atp.local
ALERT STORY
Microsoft Defender Security Center
Device
Search Microsoft Defender for Endpoint
Alerts > 'Solorigate' high-severity malware was prevented
The new Alert page
'Solorigate' hig
ALERT STORY
Microsoft Defender Security Center
Device
Search Microsoft Defender for Endpoint
Alerts > ADFS private key extraction attempt
The new Alert page
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
[7936] WerFault.exe -u -p 7956 -s 1428
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
T1528: Steal Application Access Token
First activity
Jan 10, 2021, 7:09:02 PM
Last activity
Jan 10, 2021, 7:09:02 PM

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 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-videosarja

# Seuraavat vaiheet

**01.** Katso Solorigate-videosarja tästä sijainnista

**02.** Saat lisää päivityksiä Microsoft Security -sivustosta: www.microsoft.com/en-us/security/business

**03.** Lue blogitekstit osoitteesta www.microsoft.com/security/blog

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

Microsoft Security

Microsoft