Microsoft

# Microsoft Defender pour point de terminaison

**Andrea Lelli**

Responsable principal de la recherche sur la sécurité

Windows Defender

**18 février 2021**

Présentation de Solorigate

# Aide apportée par Microsoft Defender pour point de terminaison

Microsoft Security

**01.** Méthode Start

**02.** Accès par porte dérobée et élévation des privilèges

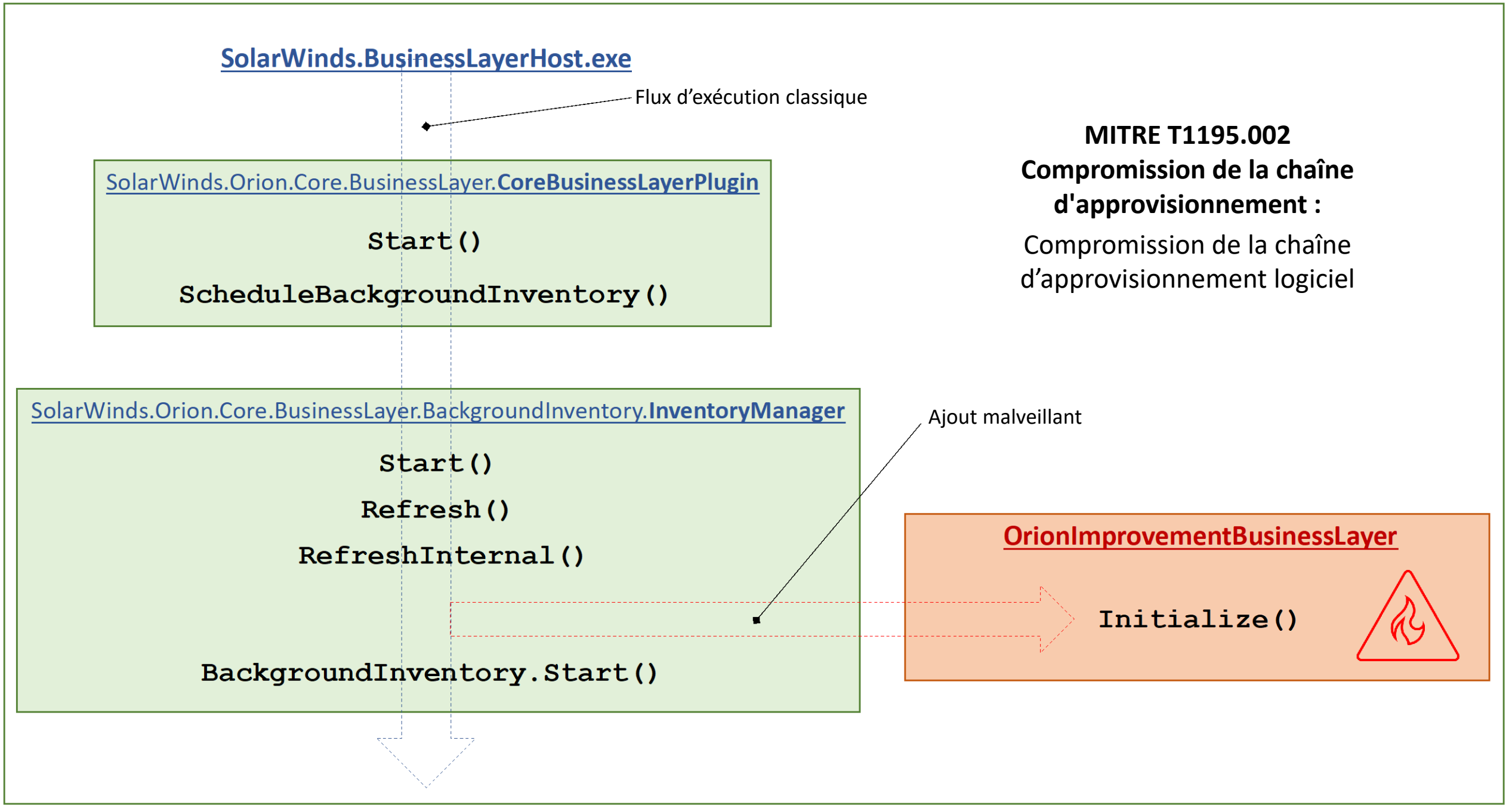
**03.** Accès par porte dérobée et charges utiles de deuxième phase

**04.** Étapes pour arrêter la propagation avec les points de terminaison

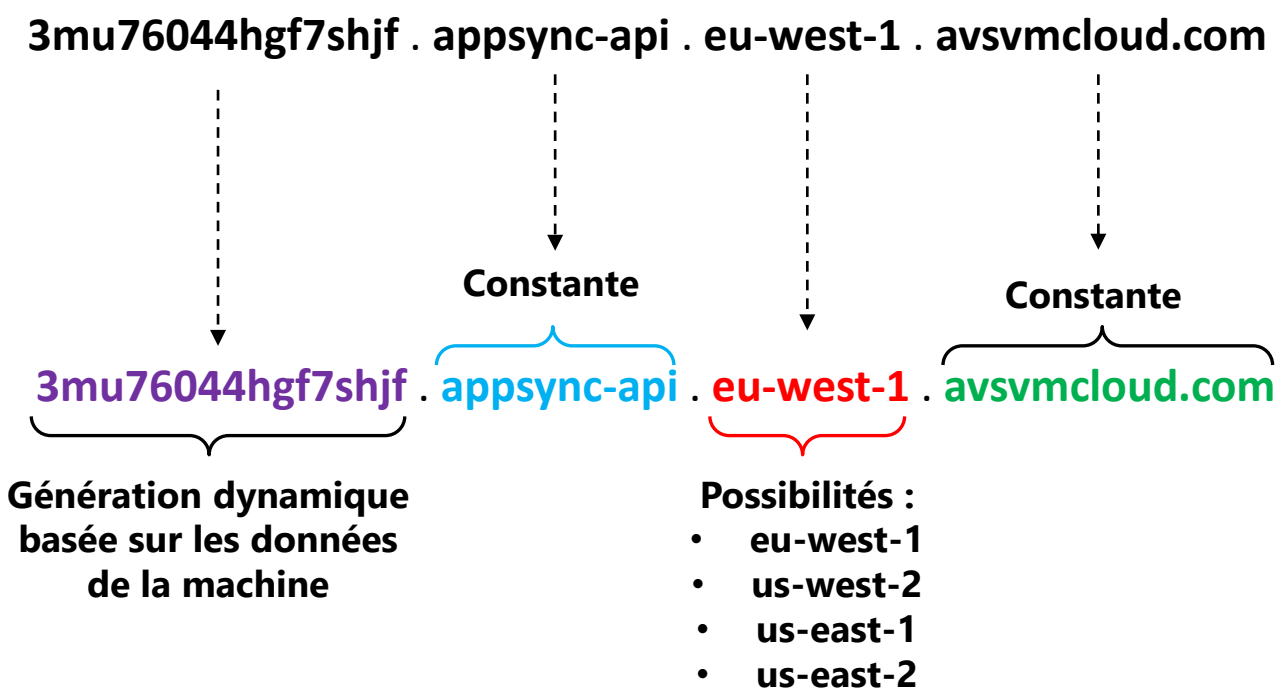
**05.** Étapes pour arrêter la propagation avec les réseaux

**06.** Rapport d'analyse de menaces et repérage

```
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
Flux d’exécution classique
SolarWinds.Orion.Core.BusinessLayer.CoreBusinessLayerPlugin
Start()
ScheduleBackgroundInventory()
SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager
Start()
Refresh()
RefreshInternal()
BackgroundInventory.Start()
Ajout malveillant
OrionImprovementBusinessLayer
Initialize()
MITRE T1195.002
Compromission de la chaîne d'approvisionnement :
Compromission de la chaîne d’approvisionnement logiciel

Exemple de domaine généré :



ATTAQUE PAR LA CHAÎNE D'APPROVISIONNEMENT
Les attaquants introduisent du code malveillant dans un composant DLL d'un logiciel légitime. Le fichier DLL compromis est distribué aux organisations qui utilisent le logiciel correspondant.

EXÉCUTION, PERSISTANCE
Au démarrage du logiciel, le fichier DLL compromis se charge et le code malveillant inséré appelle la fonction qui contient les fonctionnalités de la porte dérobée.

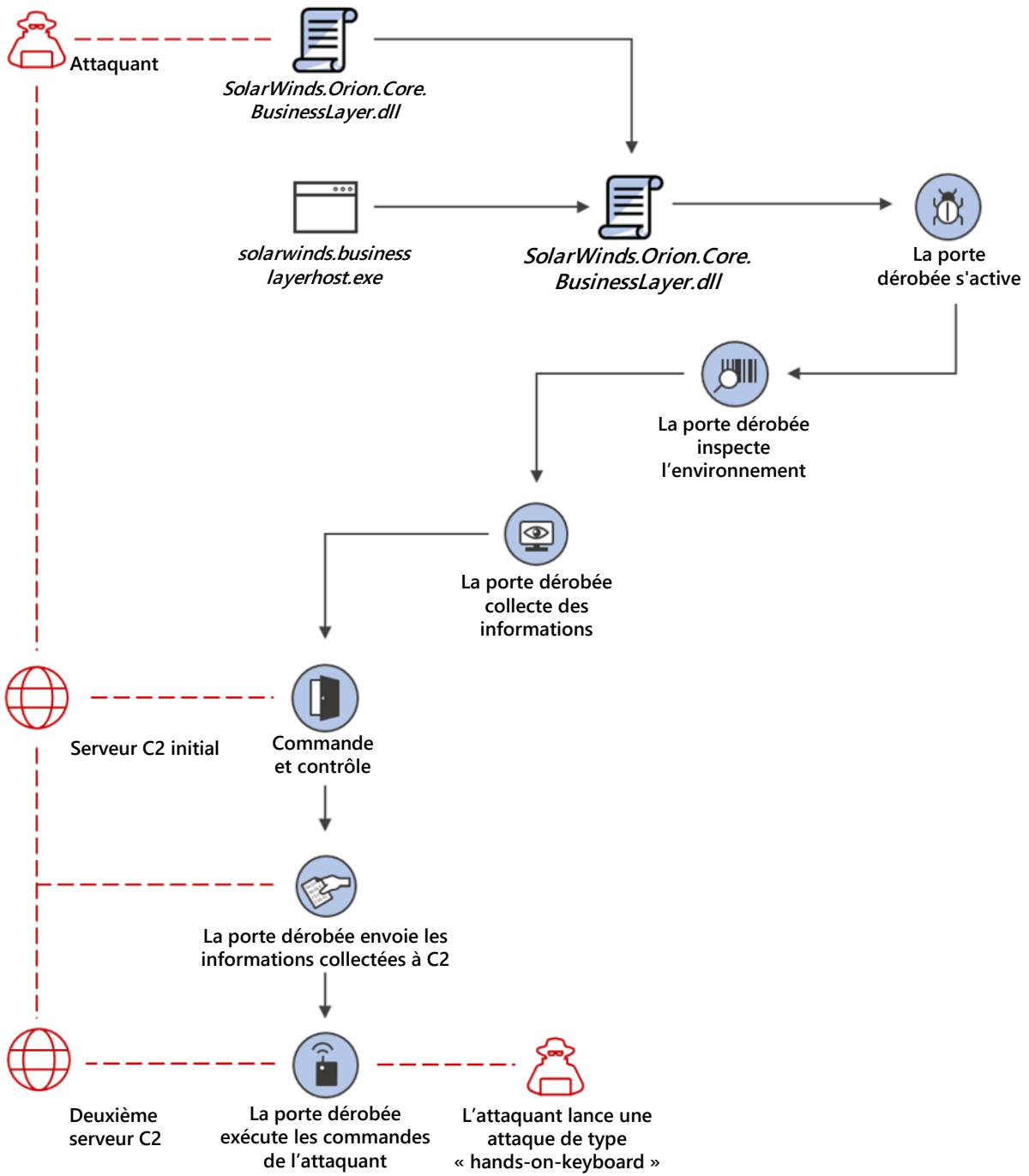
ÉVASION DÉFENSIVE
La porte dérobée s'accompagne d'une longue liste de vérifications pour assurer son fonctionnement dans un réseau réellement compromis.

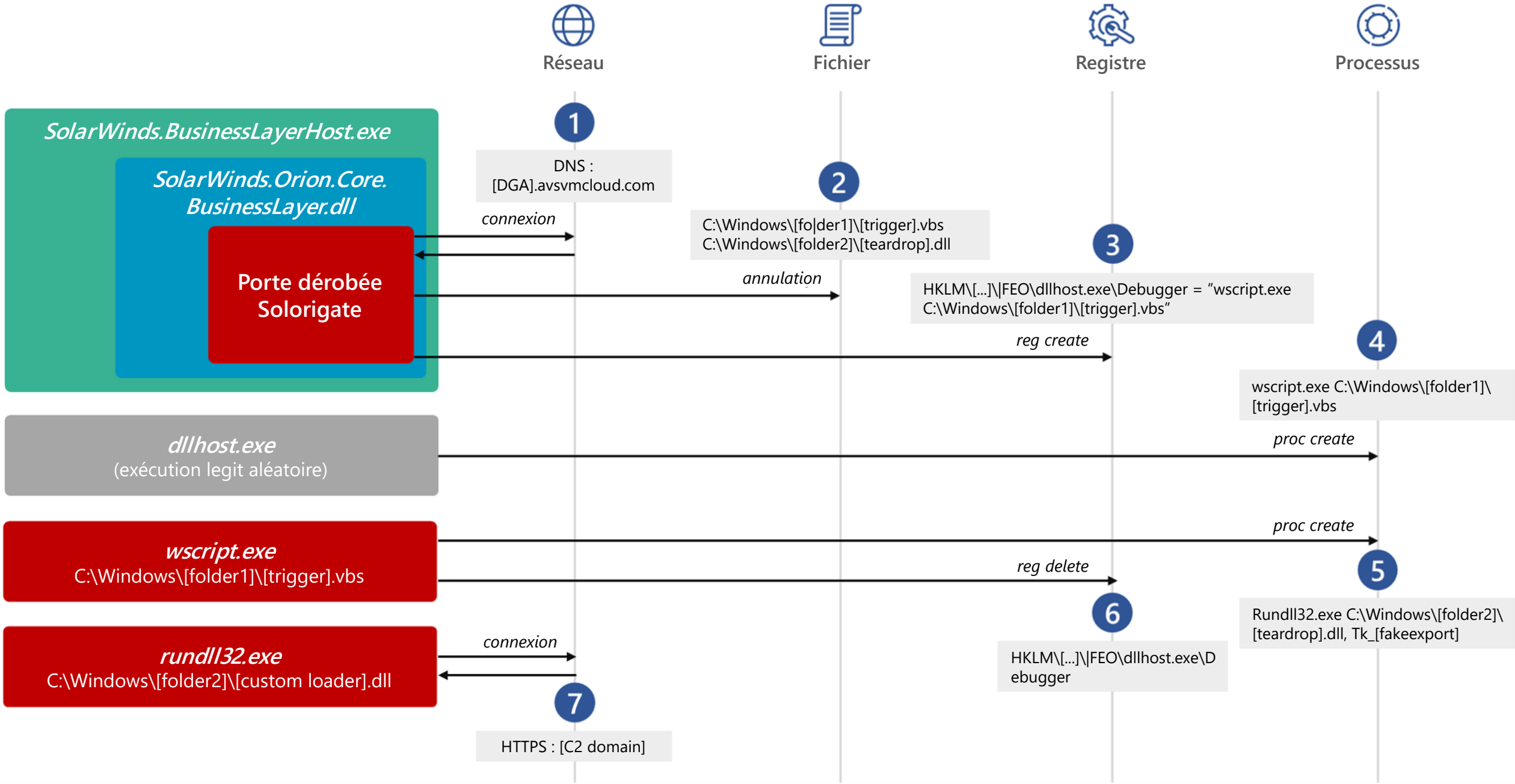
RECON
La porte dérobée collecte des informations système

INITIAL C2
La porte dérobée se connecte à un serveur commande et contrôle. Le domaine auquel elle se connecte repose partiellement sur les informations collectées à partir du système, ce qui rend chaque sous-domaine unique. La porte dérobée peut recevoir une adresse C2 supplémentaire à laquelle se connecter.

EXFILTRATION
La porte dérobée envoie les informations collectées à l'attaquant.

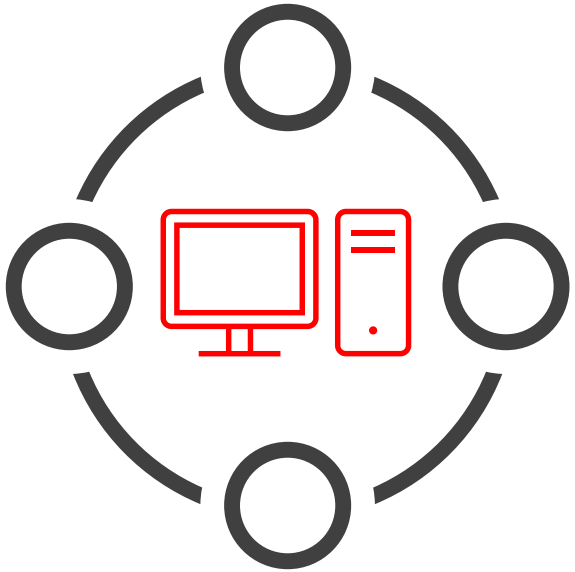
ATTAQUE DE TYPE « HANDS-ON-KEYBOARD »
La porte dérobée exécute les commandes qu'elle reçoit des attaquants. Le large éventail de fonctionnalités de porte dérobée permet aux attaquants d'effectuer des activités supplémentaires, telles que le vol d'informations d'identification, l'élévation progressive des privilèges et le mouvement latéral.




Réseau
Fichier
Registre
Processus
SolarWinds.BusinessLayerHost.exe
SolarWinds.Orion.Core.BusinessLayer.dll
Porte dérobée Solorigate
dllhost.exe
(exécution legit aléatoire)
wscript.exe
C:\Windows\[folder1]\[trigger].vbs
rundll32.exe
C:\Windows\[folder2]\[custom loader].dll
1
DNS : [DGA].avsvmcloud.com
connexion
2
C:\Windows\[fo|der1]\[trigger].vbs
C:\Windows\[folder2]\[teardrop].dll
annulation
3
HKLM\[...]\|FEO\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\[...]\|FEO\dllhost.exe\Debugger
connexion
7
HTTPS : [C2 domain]

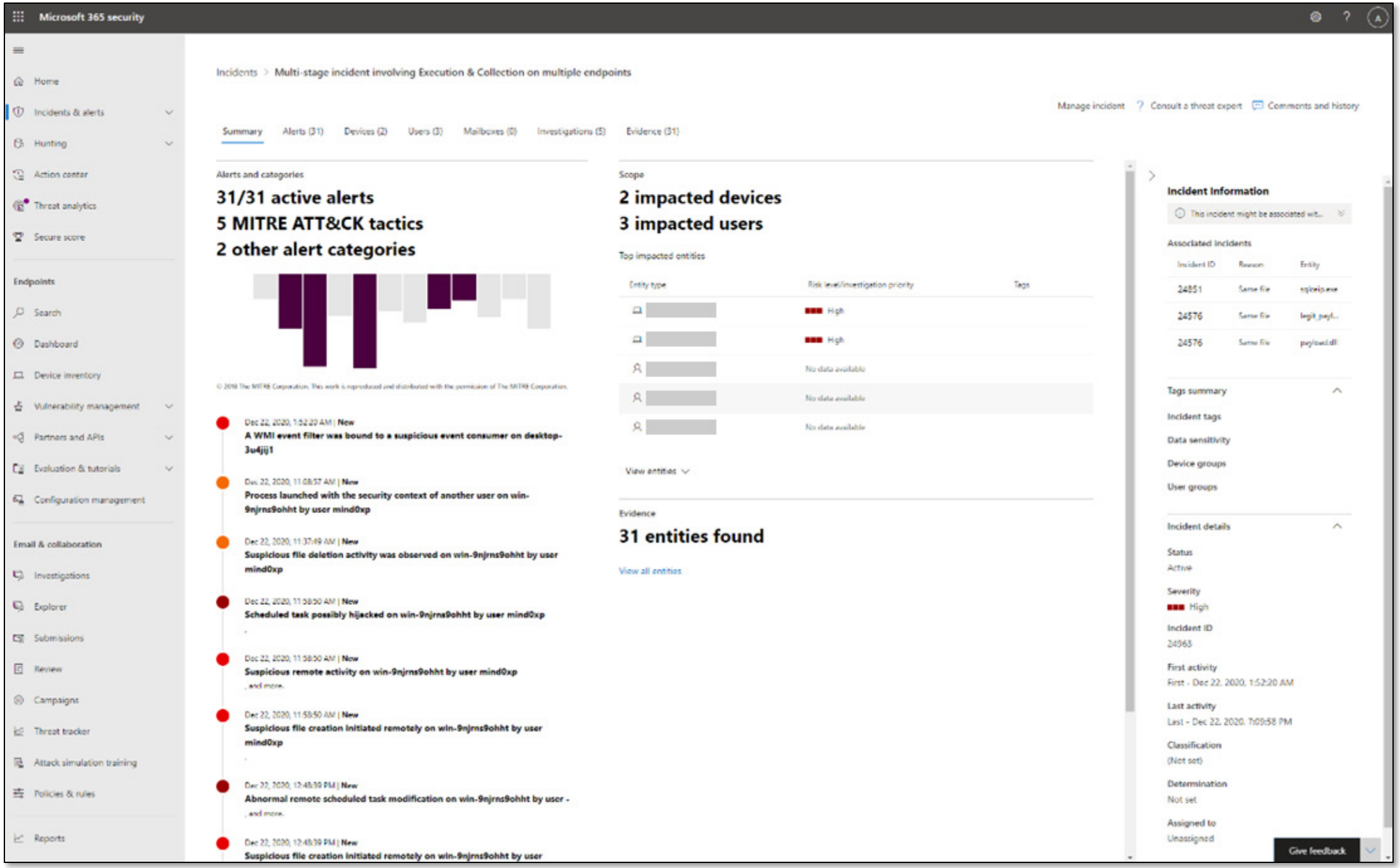
Isoler et examiner les appareils

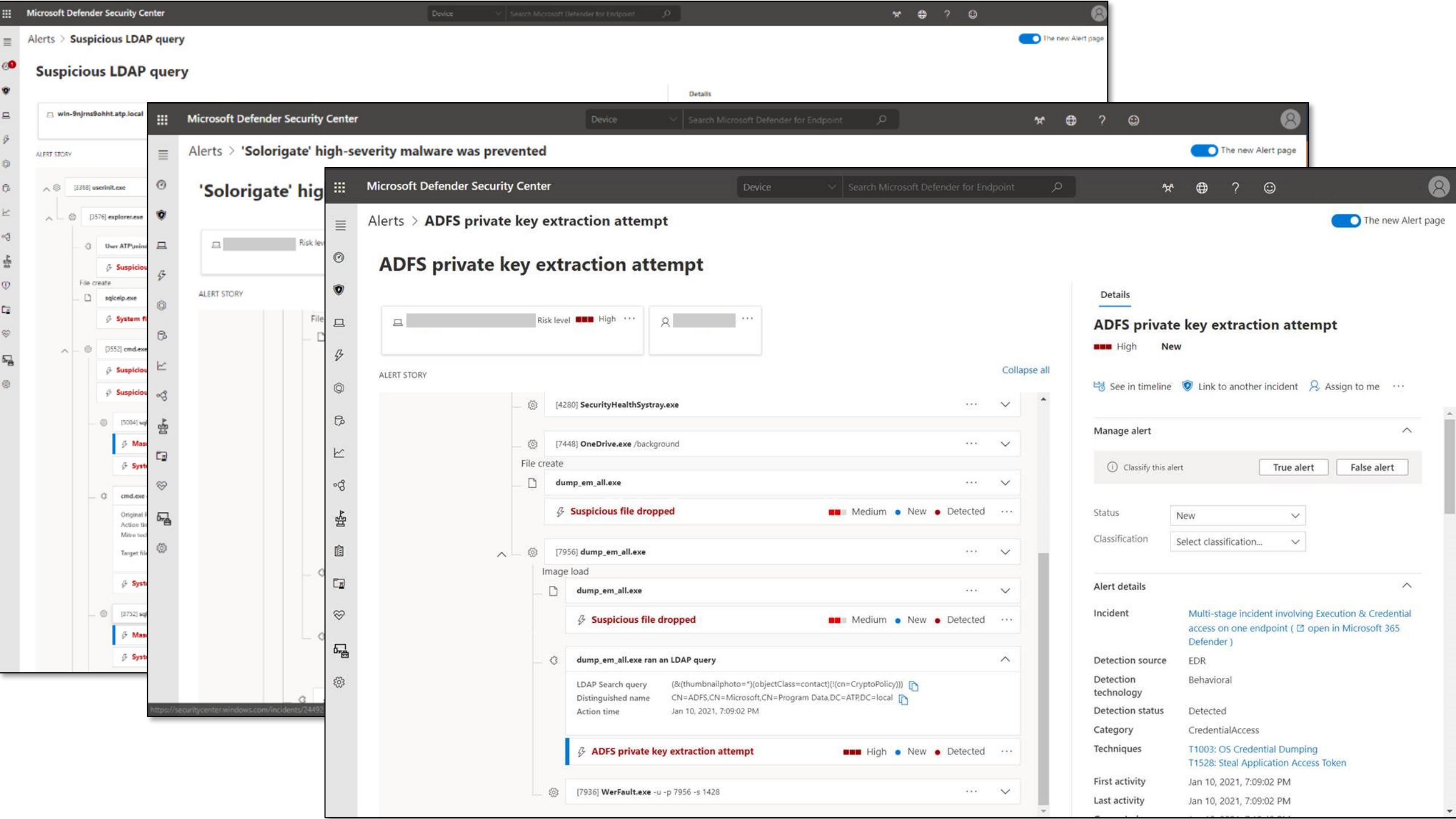
Examiner la chronologie du mouvement latéral



Identifier les comptes

Examiner l’origine de la compromission


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

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

**03.** Lisez les billets de blog sur : www.microsoft.com/security/blog

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

Microsoft Security