Microsoft

Ochrona punktu końcowego w usłudze Microsoft Defender

Andrea Lelli

Główny kierownik badań nad bezpieczeństwem

Windows Defender

18 lutego 2021 r.

Omówienie ataku Solorigate

Jak platforma Ochrona punktu końcowego w usłudze Microsoft Defender może pomóc

Microsoft Security

01. Metoda o nazwie Start

02. Dostęp backdoor i eskalacja uprawnień

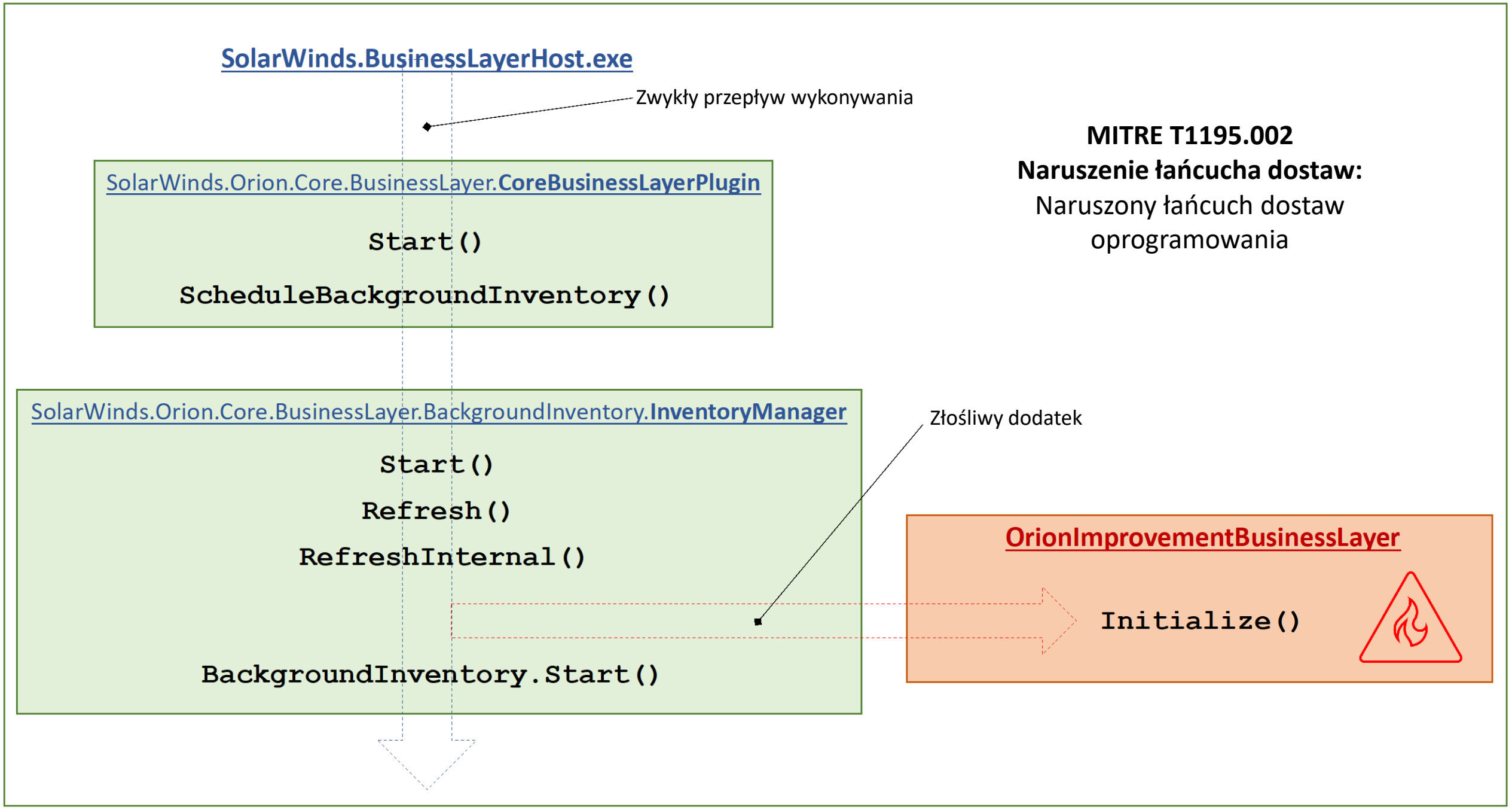
03. Dostęp backdoor i obciążenia drugiego stopnia

04. Kroki do zatrzymania rozpowszechniania za pomocą punktów końcowych

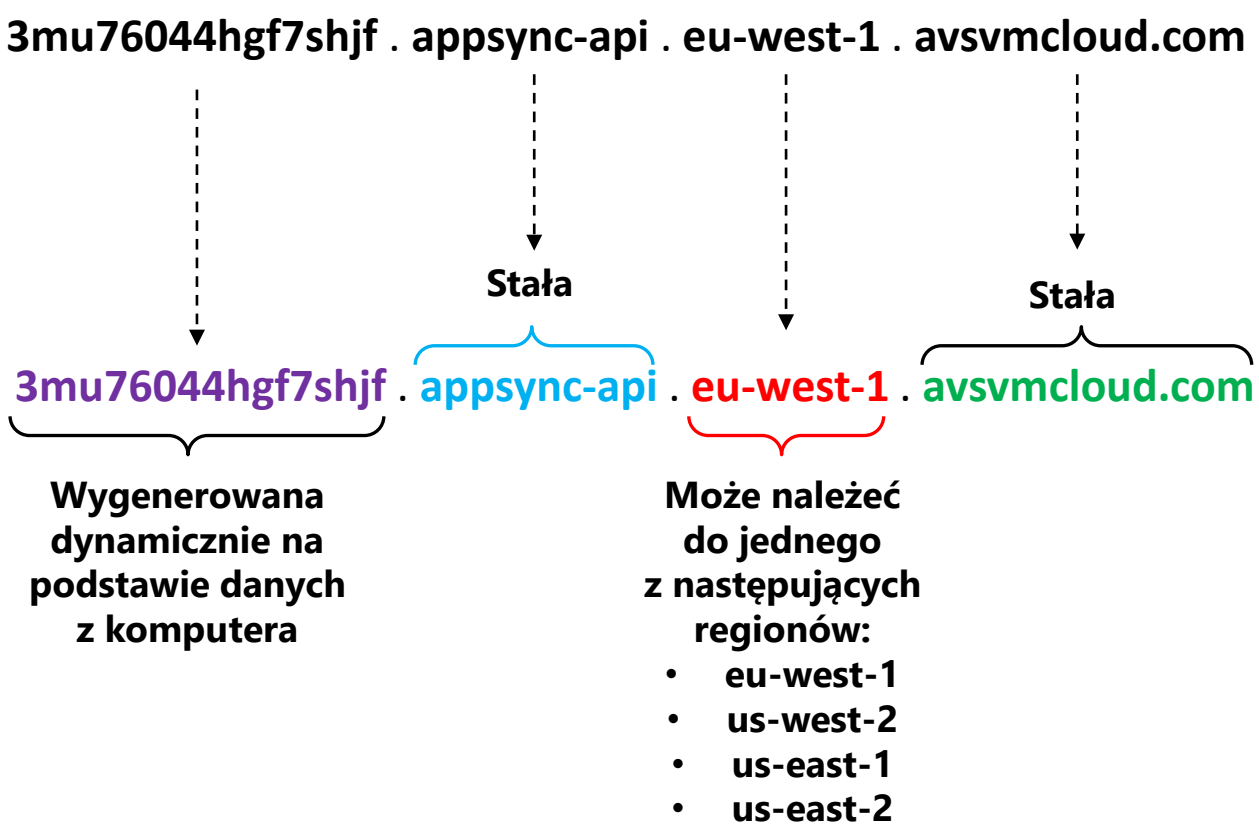
05. Kroki do zatrzymania rozpowszechniania za pomocą sieci

06. Raport analityczny dotyczący zagrożeń i wyszukiwanie zagrożeń

```
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
Zwykły przepływ wykonywania
SolarWinds.Orion.Core.BusinessLayer.CoreBusinessLayerPlugin
Start()
ScheduleBackgroundInventory()
SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager
Start()
Refresh()
RefreshInternal()
BackgroundInventory.Start()
Złośliwy dodatek
OrionImprovementBusinessLayer
Initialize()
MITRE T1195.002
Naruszenie łańcucha dostaw:
Naruszony łańcuch dostaw oprogramowania

Przykład wygenerowanej domeny:



ATAK NA ŁAŃCUCH DOSTAW
Napastnicy wstawiają złośliwy kod do składnika DLL legalnego oprogramowania. Biblioteka DLL z naruszonymi zabezpieczeniami jest dystrybuowana do organizacji korzystających z powiązanego oprogramowania.

WYKONYWANIE, TRWAŁOŚĆ
Po uruchomieniu oprogramowania ładuje się biblioteka DLL, a wstawiony złośliwy kod wywołuje funkcję zawierającą możliwości ataku backdoor.

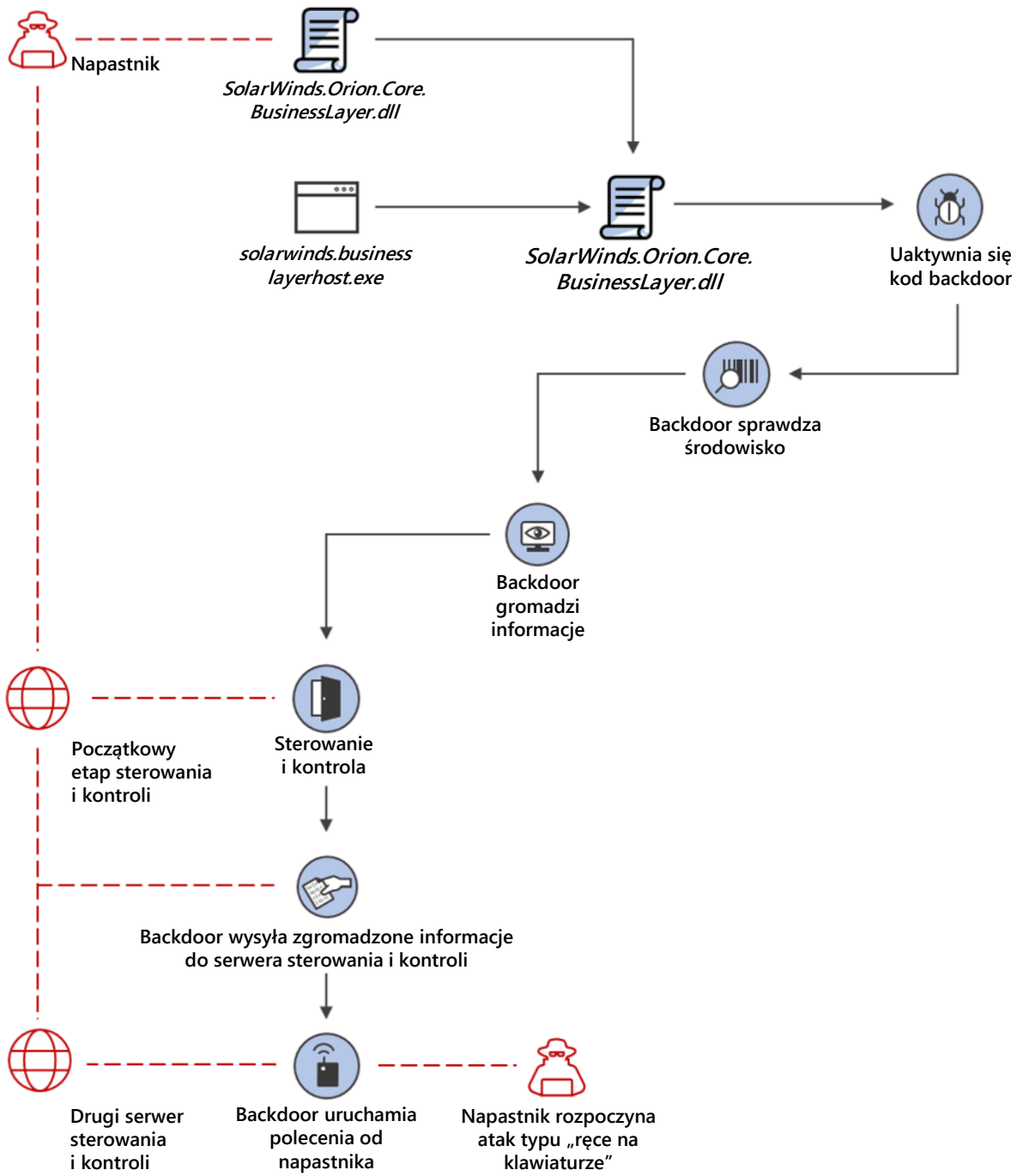
UNIKANIE OBRONY
Atak backdoor zawiera długą listę testów, które pozwalają upewnić się, że jest przeprowadzany w sieci z rzeczywiście naruszonymi zabezpieczeniami.

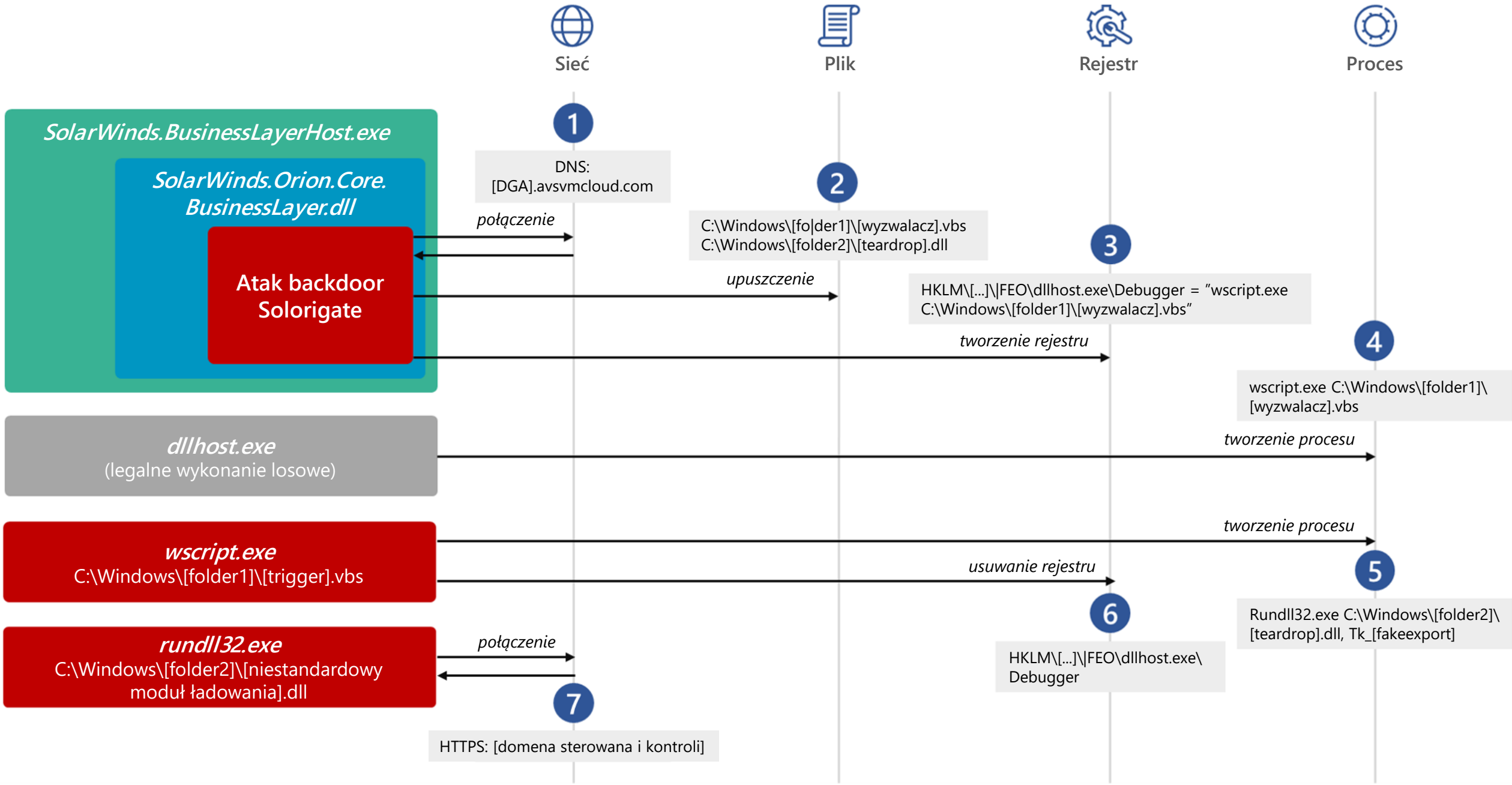
ZWIAD
Backdoor gromadzi informacje o systemie

POCZĄTKOWY ETAP STEROWANIA I KONTROLI
Backdoor łączy się z serwerem sterowania i kontroli. Domena, z którą się łączy, jest częściowo oparta na informacjach zgromadzonych z systemu, dzięki czemu każda domena trzeciego poziomu jest unikatowa. Backdoor może otrzymać dodatkowy adres sterowania i kontroli do nawiązywania połączeń.

FILTROWANIE
Backdoor wysyła zgromadzone informacje do napastnika.

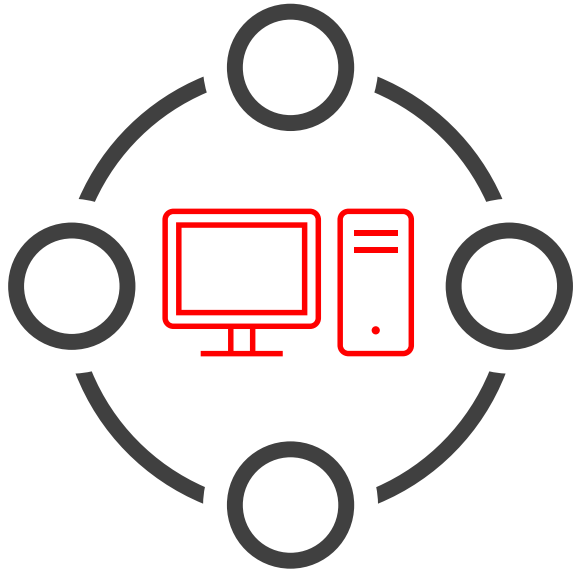
ATAK TYPU „RĘCE NA KLAWIATURZE”
Backdoor uruchamia polecenia, które otrzymuje od napastników. Szeroka gama możliwości ataku backdoor pozwala napastnikom na wykonywanie dodatkowych działań, takich jak przejęcie poświadczeń, postępująca eskalacja uprawnień i penetracja sieci.




Sieć
Plik
Rejestr
Proces
SolarWinds.BusinessLayerHost.exe
SolarWinds.Orion.Core.BusinessLayer.dll
Atak backdoor Solorigate
1
DNS: [DGA].avsvmcloud.com
połączenie
2
C:\Windows\[fo|der1]\[wyzwalacz].vbs
C:\Windows\[folder2]\[teardrop].dll
upuszczenie
3
HKLM\[...]\|FEO\dllhost.exe\Debugger = "wscript.exe C:\Windows\[folder1]\[wyzwalacz].vbs"
tworzenie rejestru
4
wscript.exe C:\Windows\[folder1]\[wyzwalacz].vbs
dllhost.exe
(legalne wykonanie losowe)
tworzenie procesu
wscript.exe
C:\Windows\[folder1]\[trigger].vbs
tworzenie procesu
usuwanie rejestru
5
Rundll32.exe C:\Windows\[folder2]\[teardrop].dll, Tk_[fakeexport]
6
HKLM\[...]\|FEO\dllhost.exe\Debugger
rundll32.exe
C:\Windows\[folder2]\[niestandardowy moduł ładowania].dll
połączenie
7
HTTPS: [domena sterowana i kontroli]

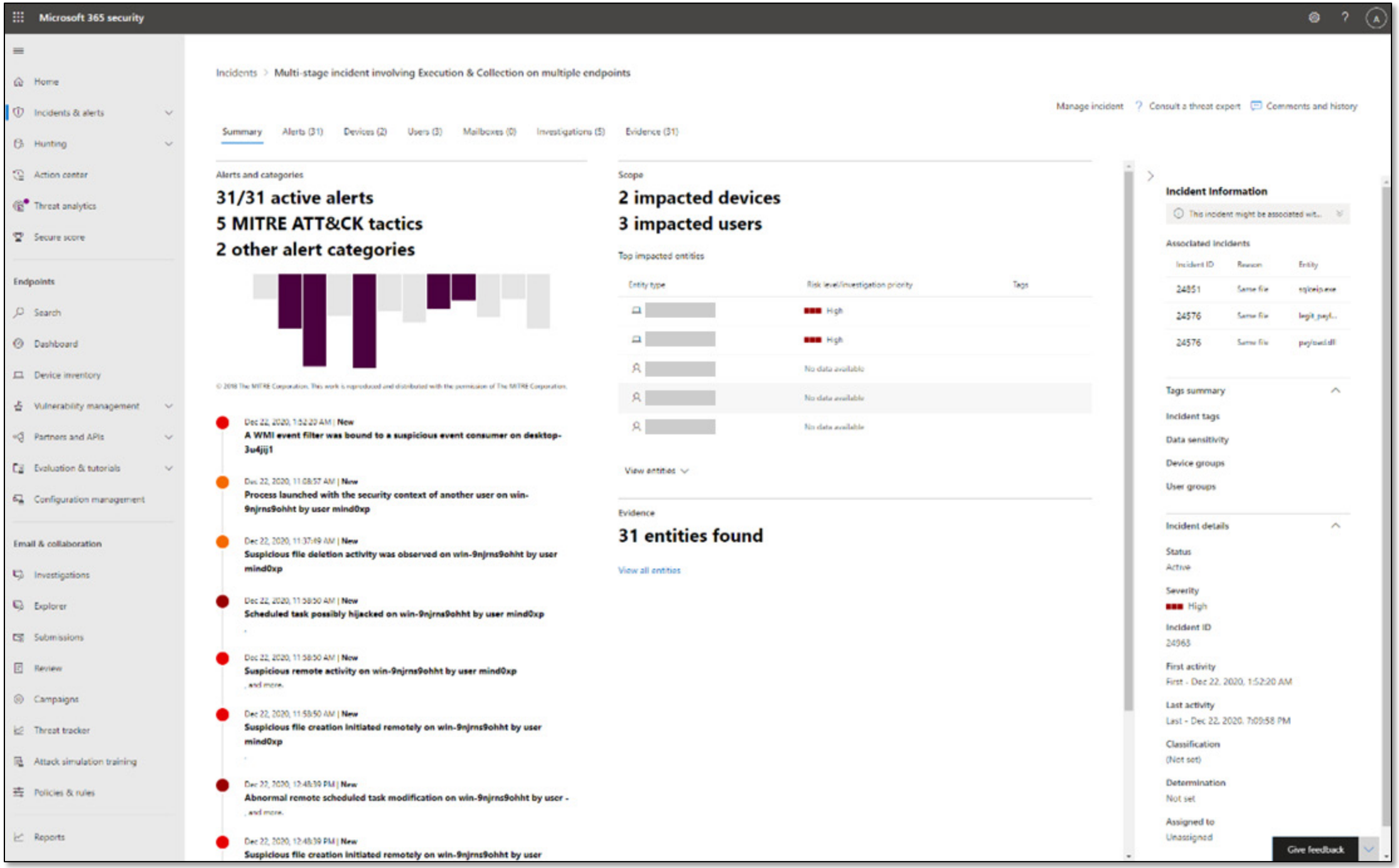
Izolowanie i badanie urządzeń

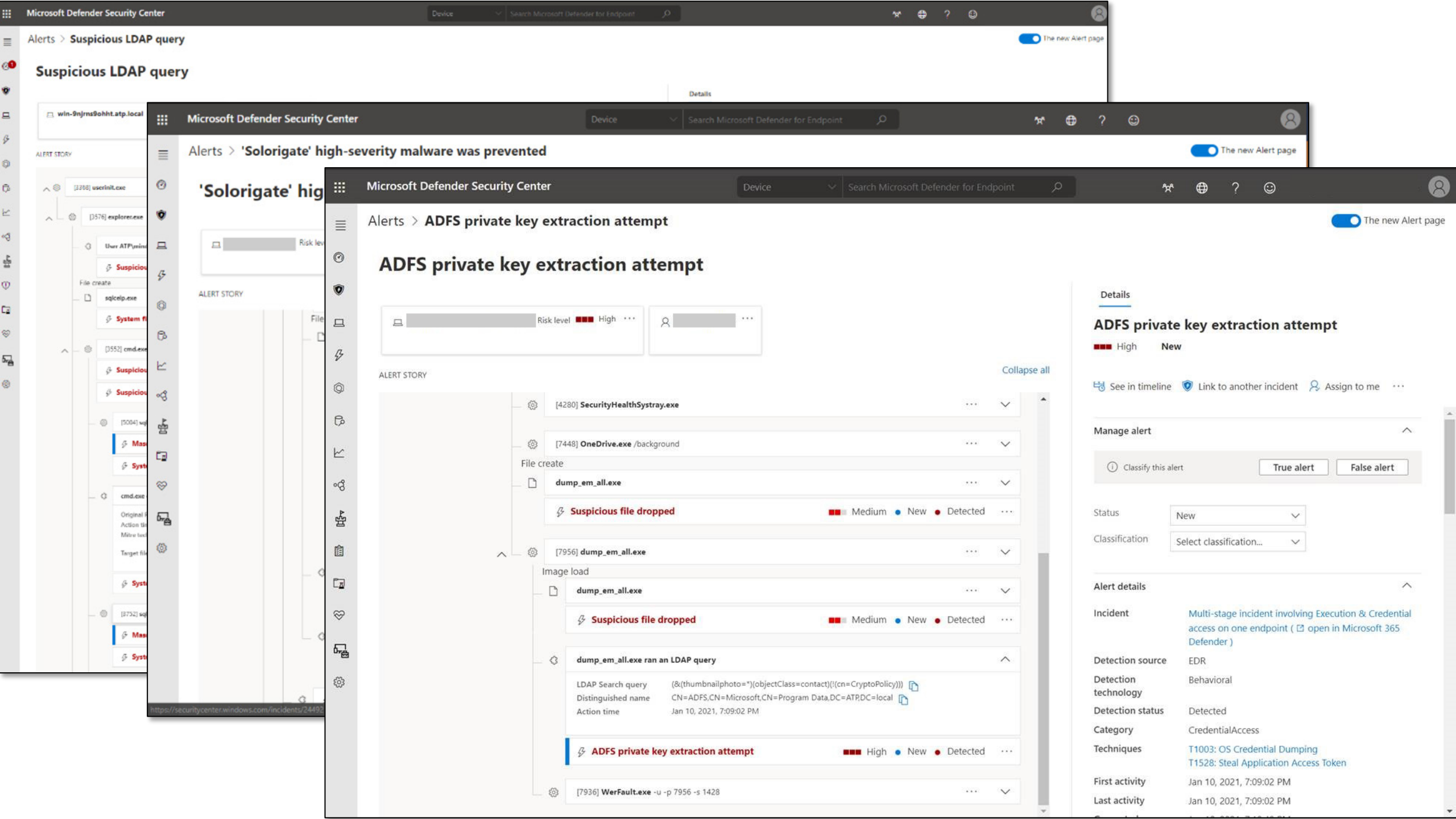
Badanie osi czasu penetracji sieci



Identyfikowanie kont

Identyfikowanie źródła naruszeń zabezpieczeń


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
, 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
High
High
No data available
No data available
No data available
View entities
Evidence
31 entities found
View all entities
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
Give feedback


Microsoft Defender Security Center
Alerts > Suspicious LDAP query
Suspicious LDAP query
Microsoft Defender Security Center
Alerts > 'Solorigate' high-severity malware was prevented
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

Seria filmów wideo o ataku Solorigate

Następne kroki

01. Obejrzyj serię filmów wideo o ataku Solorigate w tej lokalizacji

02. Zobacz rozwiązania zabezpieczające firmy Microsoft, aby uzyskać najnowsze informacje: www.microsoft.com/en-us/security/business

03. Przeczytaj wpisy w blogu: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft