Microsoft

Microsoft Defender para Ponto de Extremidade

Andrea Lelli

Líder principal de Pesquisas sobre Segurança

Windows Defender

18 de fevereiro de 2021

Visão geral sobre o Solorigate

Como o Microsoft Defender para Ponto de Extremidade pode ajudar

01. O método chamado Início

02. Acesso de backdoor e elevação de privilégio

03. Acesso de backdoor e payloads de segundo estágio

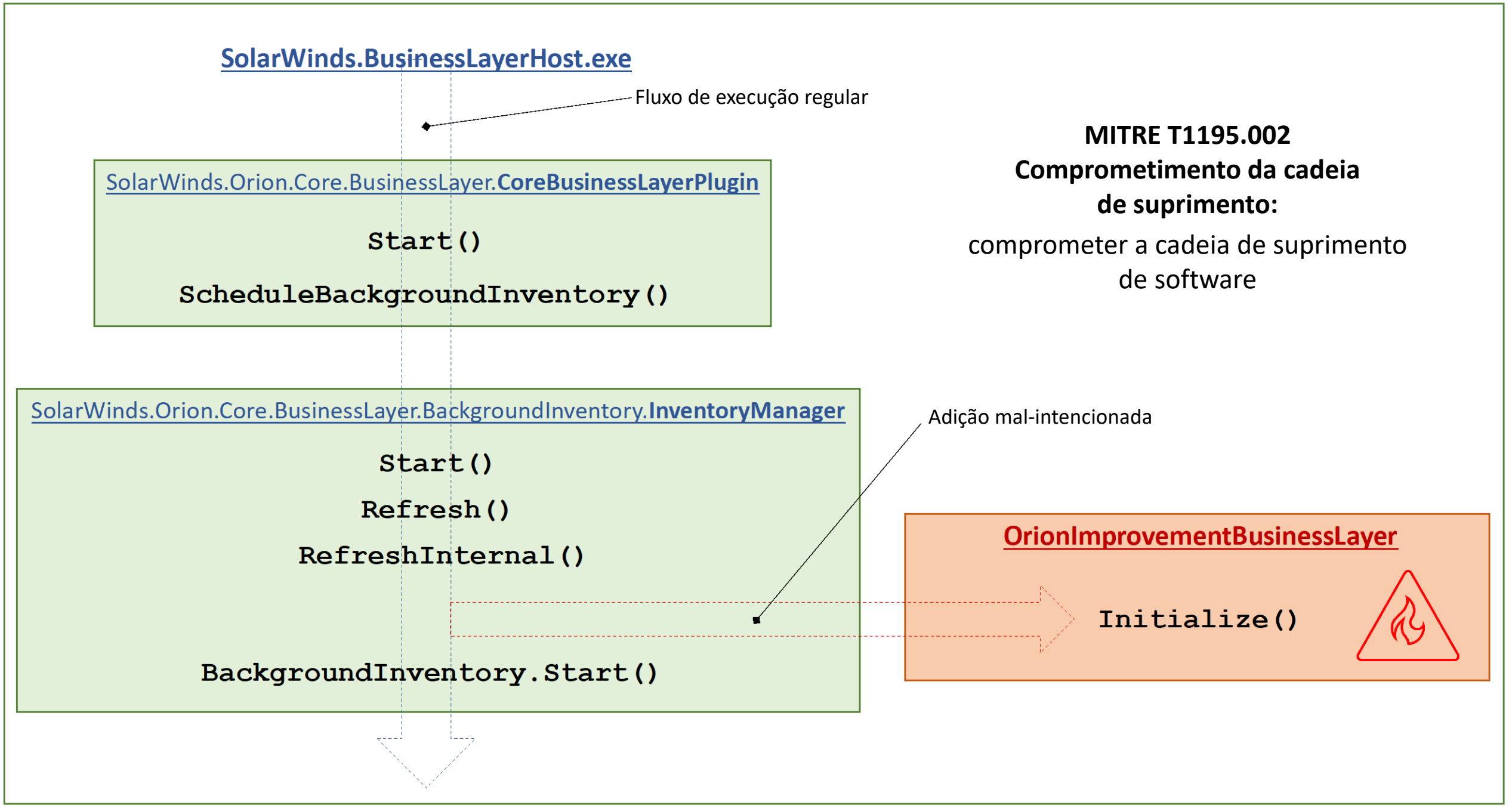
04. Etapas para interromper a disseminação com pontos de extremidade

05. Etapas para interromper a disseminação com redes

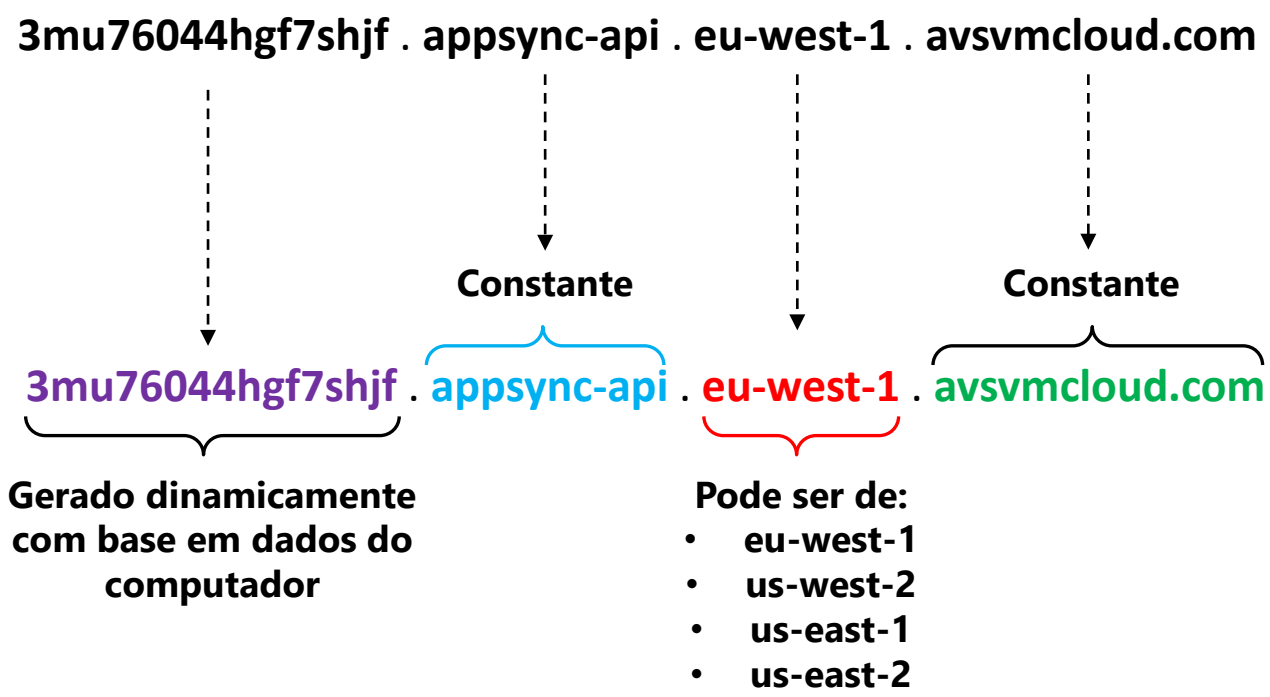
06. Busca e relatório de análise de ameaças

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
Fluxo de execução regular
SolarWinds.Orion.Core.BusinessLayer.CoreBusinessLayerPlugin
Start()
ScheduleBackgroundInventory()
SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager
Start()
Refresh()
RefreshInternal()
BackgroundInventory.Start()
Adição mal-intencionada
OrionImprovementBusinessLayer
Initialize()
MITRE T1195.002
Comprometimento da cadeia de suprimento:
comprometer a cadeia de suprimento de software

Exemplo de domínio gerado:



ATAQUE À CADEIA DE SUPRIMENTO
Os invasores inserem código mal-intencionado em um componente DLL de um software legítimo. A DLL comprometida é distribuída às organizações que usam esse software.

EXECUÇÃO, PERSISTÊNCIA
Quando o software é iniciado, a DLL comprometida é carregada, e o código mal-intencionado inserido chama a função que contém as funcionalidades de backdoor.

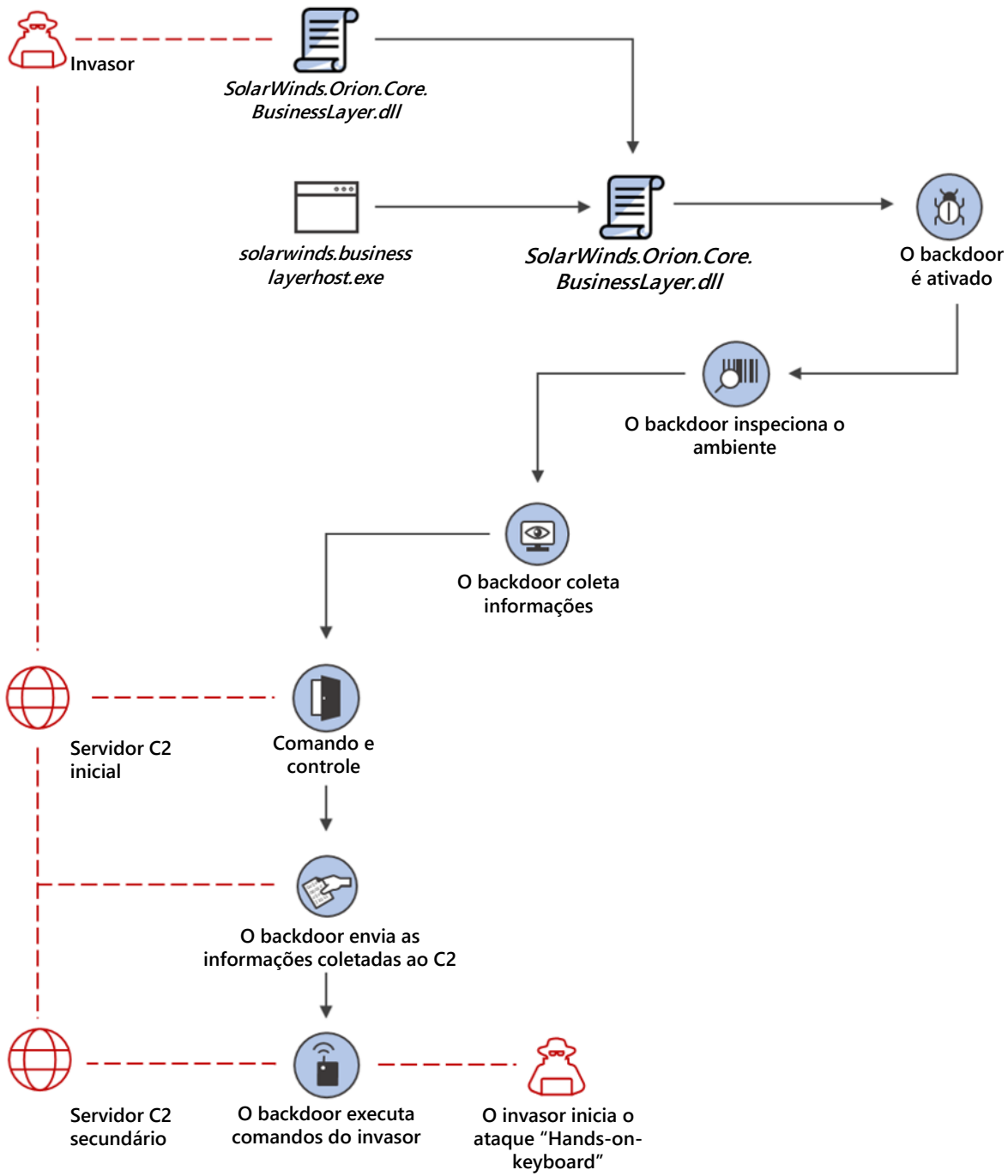
EVASÃO DE DEFESA
O backdoor tem uma longa lista de verificações para confirmar que está sendo executado em uma rede comprometida de fato.

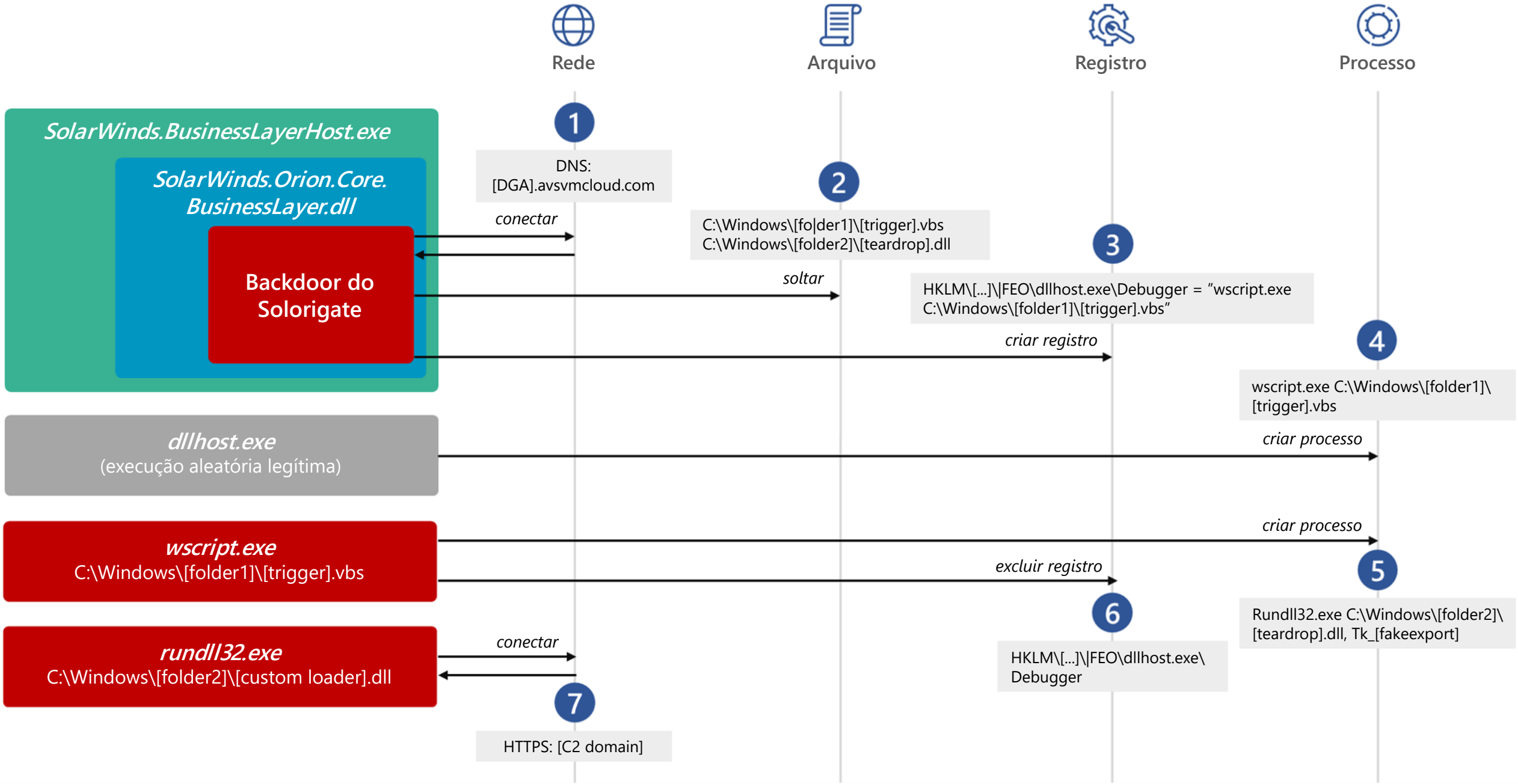
RECONHECIMENTO
O backdoor coleta informações do sistema

C2 INICIAL
O backdoor se conecta a um servidor de comando e controle. O domínio ao qual ele se conecta se baseia, em parte, nas informações coletadas do sistema, tornando cada subdomínio único. O backdoor pode receber um endereço adicional de C2 para se conectar.

EXFILTRAÇÃO
O backdoor envia as informações coletadas ao invasor.

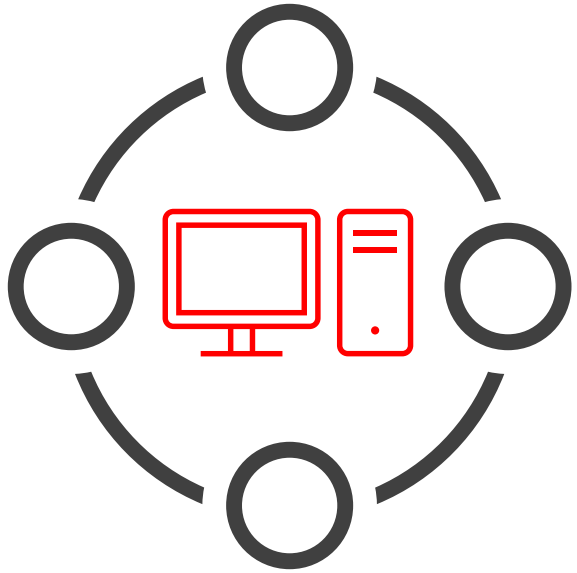
ATAQUE "HANDS-ON-KEYBOARD"
O backdoor executa comandos recebidos dos invasores. O vasto leque de funcionalidades do backdoor permite que os invasores realizem atividades adicionais, como roubo de credencial, elevação progressiva de privilégios e movimentação lateral.




Rede
Arquivo
Registro
Processo
SolarWinds.BusinessLayerHost.exe
SolarWinds.Orion.Core.BusinessLayer.dll
Backdoor do Solorigate
dllhost.exe
(execução aleatória legítima)
wscript.exe
C:\Windows\[folder1]\[trigger].vbs
rundll32.exe
C:\Windows\[folder2]\[custom loader].dll
1
DNS:
[DGA].avsvmcloud.com
conectar
2
C:\Windows\[fo|der1]\[trigger].vbs
C:\Windows\[folder2]\[teardrop].dll
soltar
3
HKLM\[...]\|FEO\dllhost.exe\Debugger = "wscript.exe C:\Windows\[folder1]\[trigger].vbs"
criar registro
4
wscript.exe C:\Windows\[folder1]\[trigger].vbs
criar processo
criar processo
excluir registro
5
Rundll32.exe C:\Windows\[folder2]\[teardrop].dll, Tk_[fakeexport]
6
HKLM\[...]\|FEO\dllhost.exe\Debugger
conectar
7
HTTPS: [C2 domain]

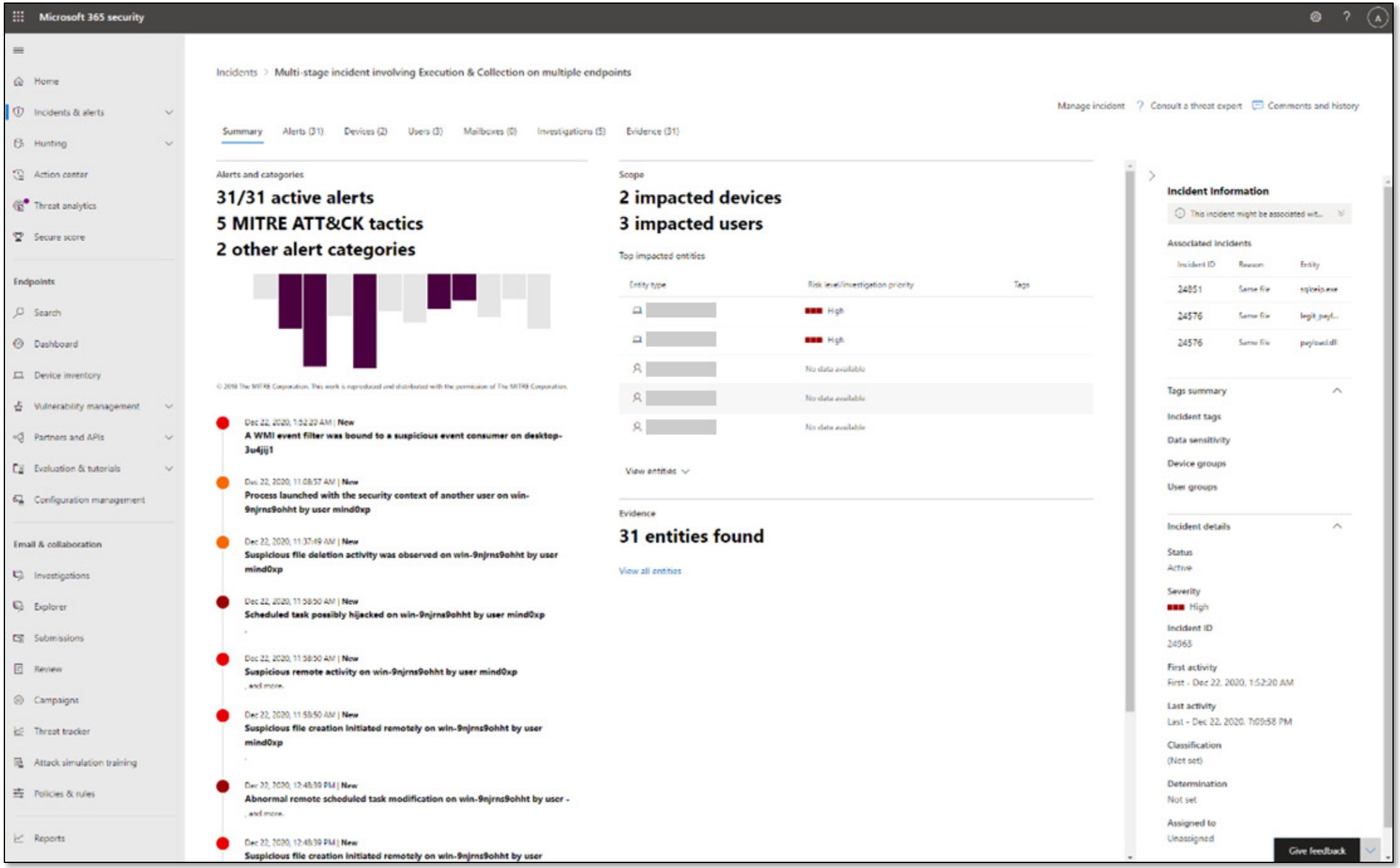
Isolar e investigar dispositivos

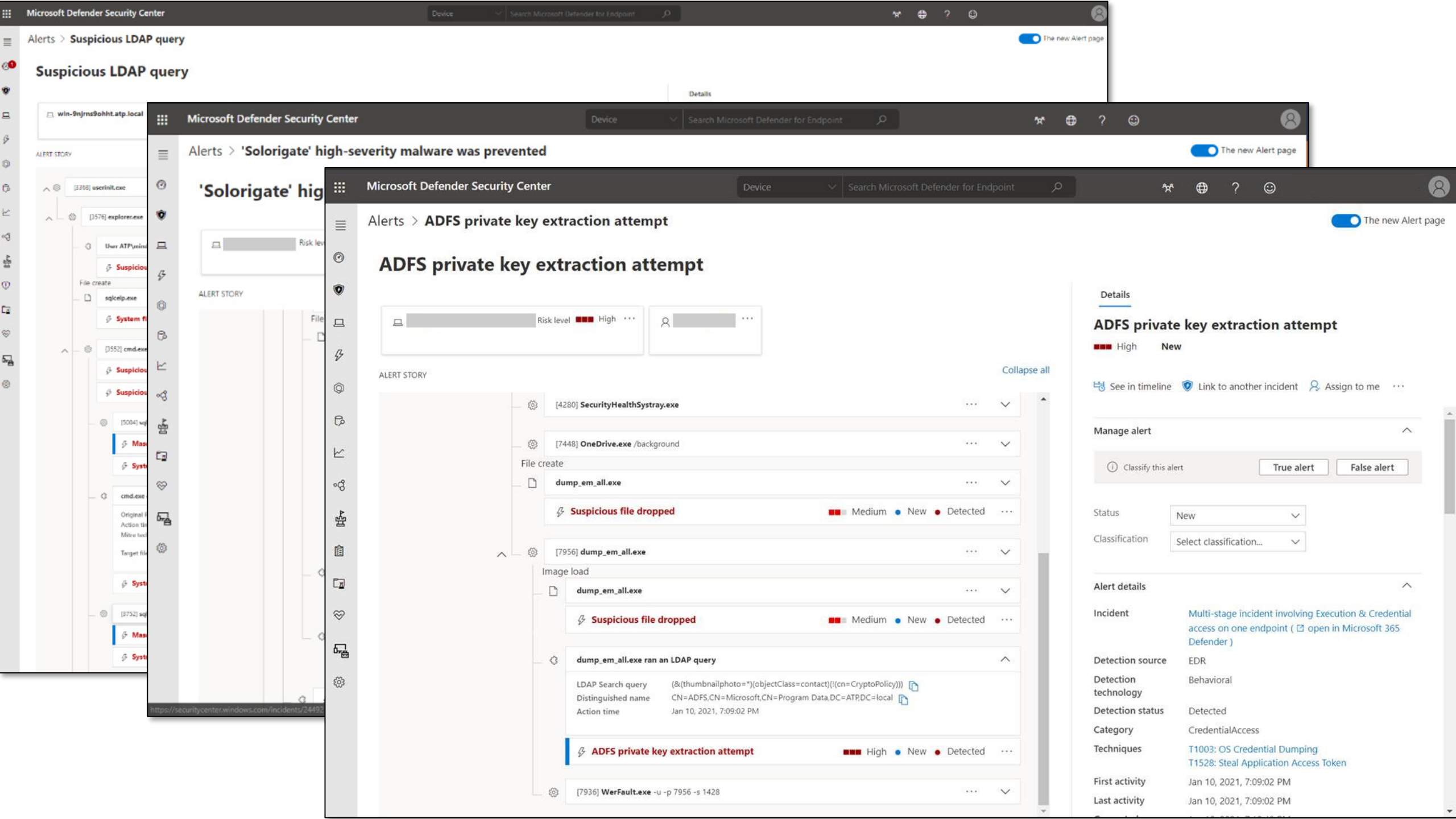
Investigar a linha do tempo em busca de movimentos laterais



Identificar contas

Investigar a origem do comprometimento


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 vídeos sobre o Solorigate

Próximas Etapas

01. Assista à série de vídeos sobre o Solorigate neste local

02. Confira mais atualizações na Segurança da Microsoft: www.microsoft.com/pt-br/security/business

03. Leia as postagens no blog em: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security