Microsoft

Microsoft Defender for Endpoint

Andrea Lelli

首席安全研究主管

Windows Defender

2021 年 2 月 18 日

Solorigate 概述

Microsoft Defender for Endpoint 如何提供帮助

01. 名为 Start 的方法

02. 后门程序访问权限和特权提升

03. 后门程序访问权限和第二阶段有效负载

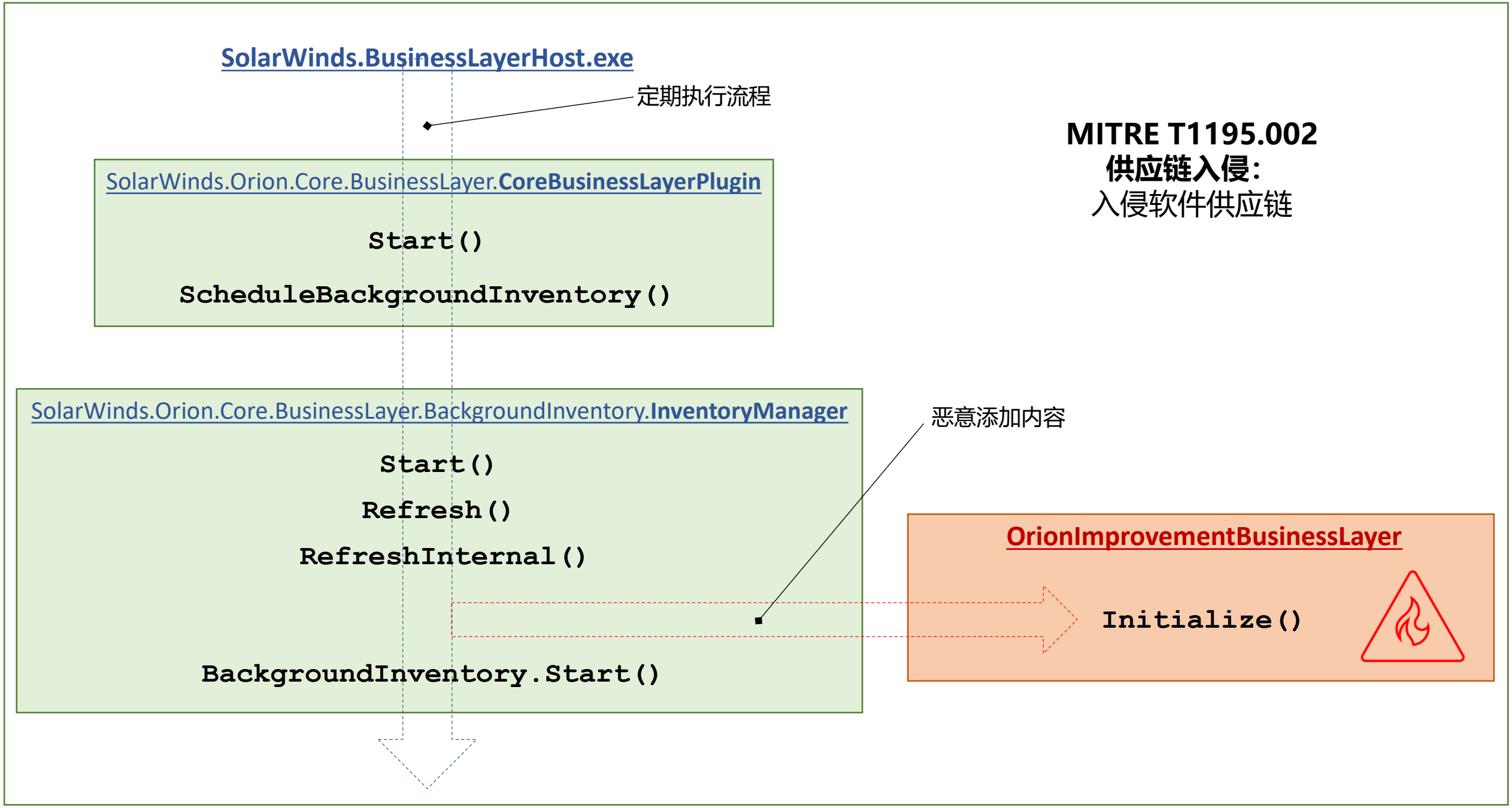
04. 阻止通过端点传播的步骤

05. 阻止通过网络传播的步骤

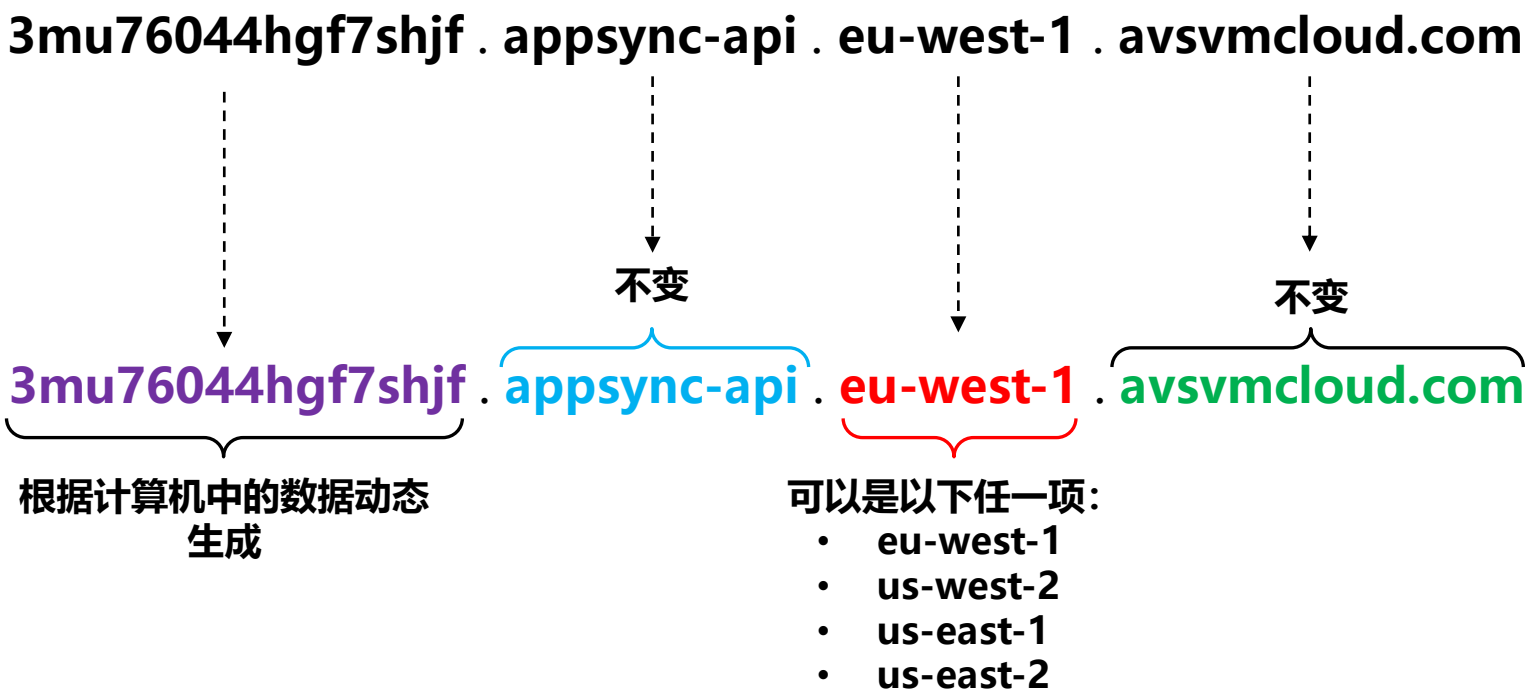
06. 威胁分析报表和搜寻

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
定期执行流程
SolarWinds.Orion.Core.BusinessLayer.CoreBusinessLayerPlugin
Start()
ScheduleBackgroundInventory()
SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager
Start()
Refresh()
RefreshInternal()
BackgroundInventory.Start()
恶意添加内容
OrionImprovementBusinessLayer
Initialize()
MITRE T1195.002
供应链入侵:
入侵软件供应链

生成的域示例：


3mu76044hgf7shjf . appsync-api . eu-west-1 . avsvmcloud.com
不变
不变
3mu76044hgf7shjf . appsync-api . eu-west-1 . avsvmcloud.com
根据计算机中的数据动态生成
可以是以下任一项：
• eu-west-1
• us-west-2
• us-east-1
• us-east-2

供应链攻击
攻击者将恶意代码插入合法软件的 DLL 组件中。将被入侵的 DLL 分发给使用相关软件的组织。

执行，持久性
启动软件时，会加载被入侵的 DLL，并且插入的恶意代码会调用包含后门程序功能的函数。

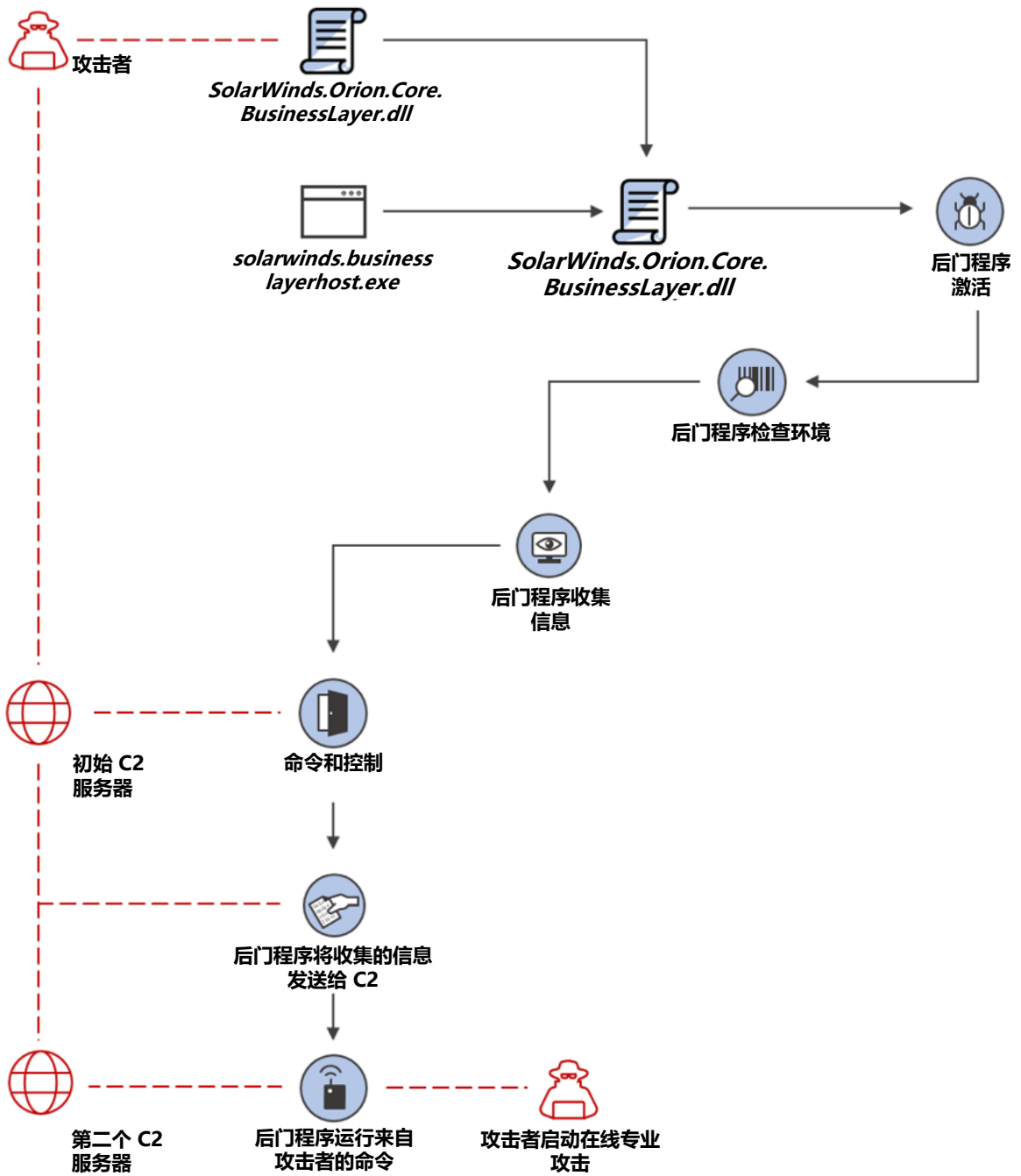
防御规避
后门程序有很长的检查清单，以确保它在实际被入侵的网络中运行。

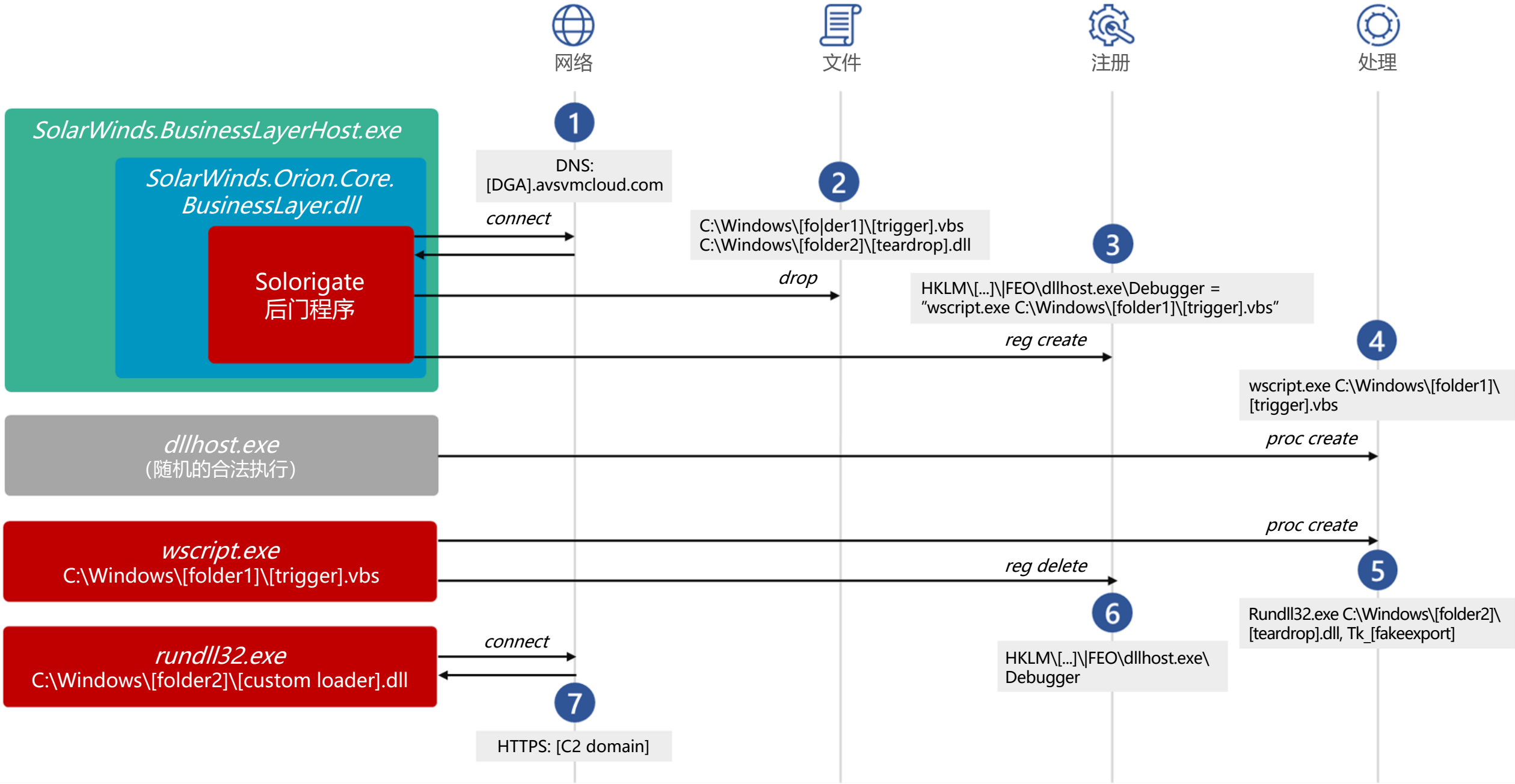
侦察
后门程序收集系统信息

初始 C2
后门程序连接到命令和控制服务器。它所连接到的域部分基于从系统收集的信息，从而使每个子域都是唯一的。后门程序可能会收到一个额外的 C2 地址来进行连接。

泄露
后门程序将收集的信息发送给攻击者。

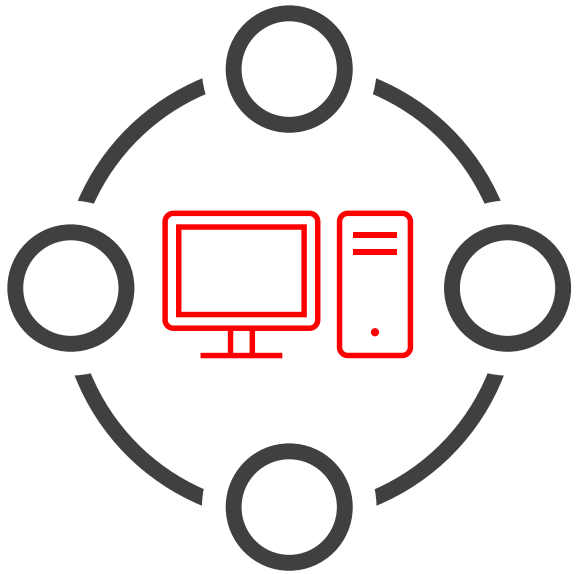
在线专业攻击
后门程序运行它从攻击者那里接收到的命令。借助大量后门程序功能，攻击者可以执行其他活动，例如凭据盗窃、渐进式特权提升和横向移动。




网络
文件
注册
处理
SolarWinds.BusinessLayerHost.exe
SolarWinds.Orion.Core.
BusinessLayer.dll
Solorigate
后门程序
1
DNS:
[DGA].avsvmcloud.com
connect
2
C:\Windows\[fo|der1]\[trigger].vbs
C:\Windows\[folder2]\[teardrop].dll
drop
3
HKLM\[...]\|FEO\dllhost.exe\Debugger =
"wscript.exe C:\Windows\[folder1]\[trigger].vbs"
reg create
4
wscript.exe C:\Windows\[folder1]\
[trigger].vbs
dllhost.exe
(随机的合法执行)
proc create
wscript.exe
C:\Windows\[folder1]\[trigger].vbs
proc create
reg delete
5
Rundll32.exe C:\Windows\[folder2]\
[teardrop].dll, Tk_[fakeexport]
6
HKLM\[...]\|FEO\dllhost.exe\
Debugger
rundll32.exe
C:\Windows\[folder2]\[custom loader].dll
connect
7
HTTPS: [C2 domain]

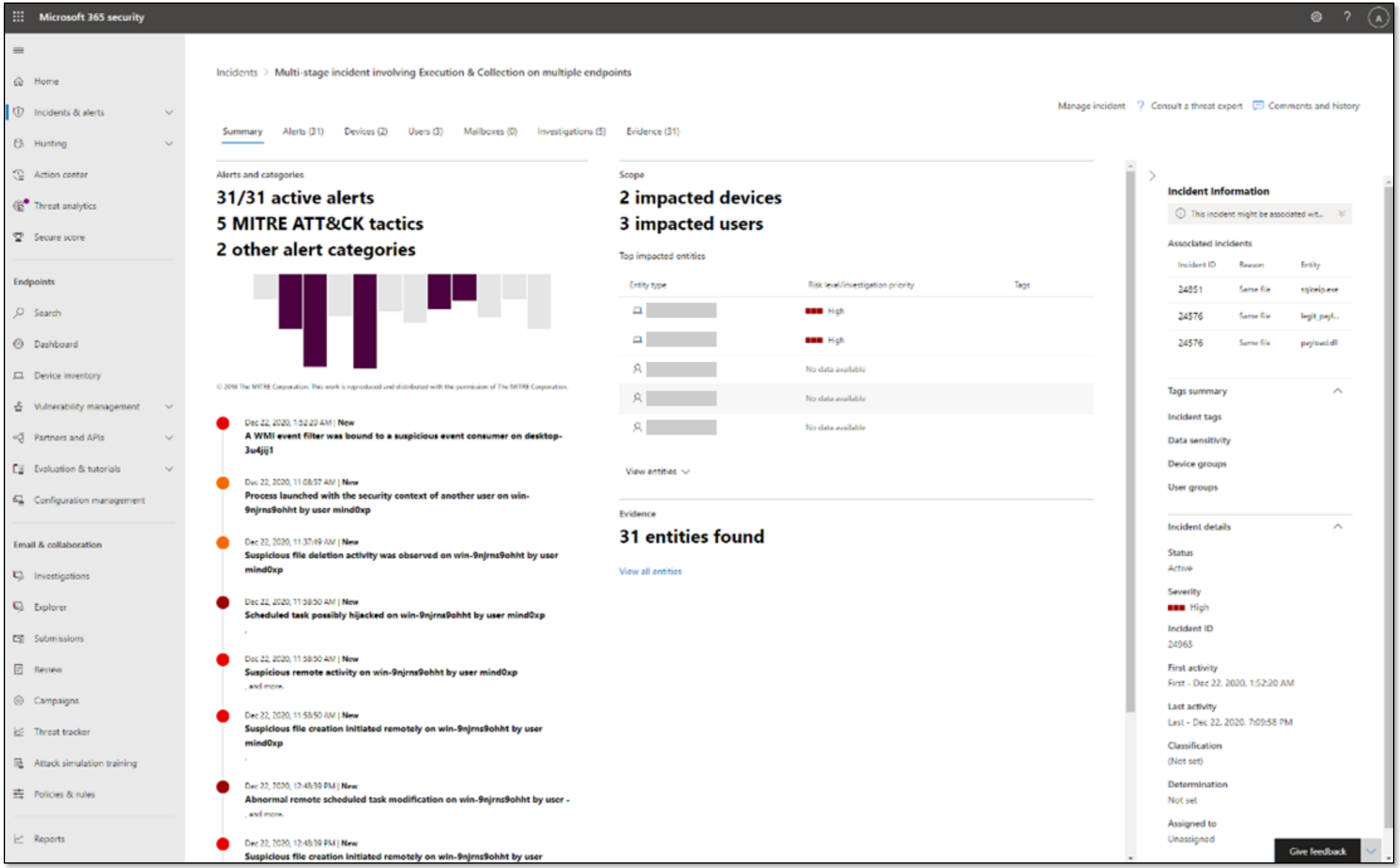
隔离和调查设备

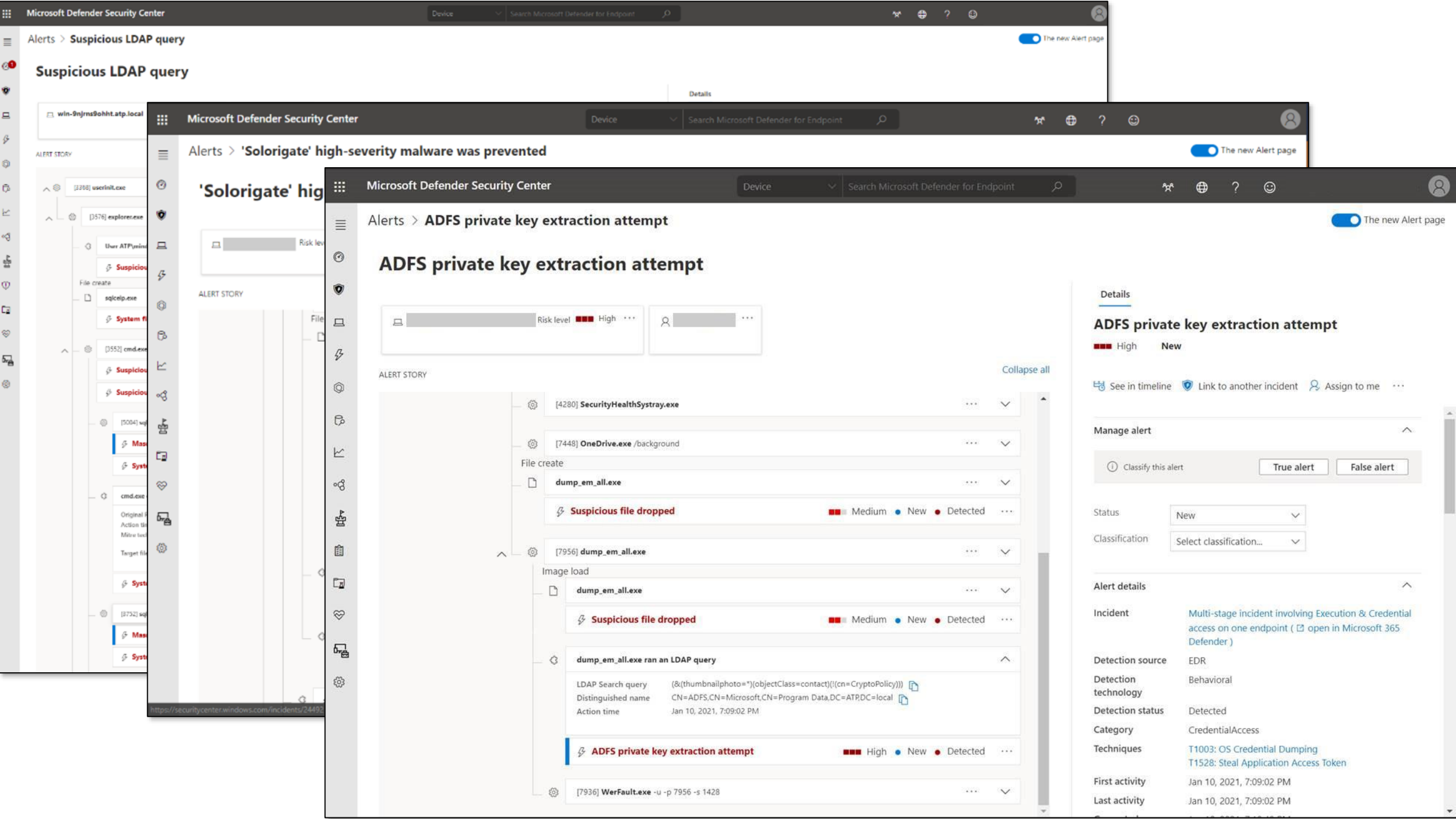
调查横向移动的时间线



识别帐户

调查入侵源


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
Alerts > Suspicious LDAP query
Suspicious LDAP query
Microsoft Defender Security Center
Alerts > 'Solorigate' high-severity malware was prevented
Microsoft Defender Security Center
Alerts > ADFS private key extraction attempt
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 视频系列

后续步骤

01. 在此位置观看 Solorigate 视频系列
02. 请访问 Microsoft 安全以获取更多更新：www.microsoft.com/zh-cn/security/business
03. 阅读博客文章：www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft