



Bộ bảo vệ Microsoft dành cho Điểm cuối

Andrea Lelli

Trưởng nhóm Nghiên cứu về Bảo mật

Bộ bảo vệ Windows

18/02/2021

Tổng quan về Solorigate

Cách hỗ trợ của Bộ bảo vệ Microsoft dành cho Điểm cuối

- 01.** Phương pháp có tên Start
- 02.** Truy nhập cửa hậu và leo thang đặc quyền
- 03.** Truy nhập cửa hậu và tải trọng giai đoạn hai
- 04.** Các bước ngừng phát tán với Điểm cuối
- 05.** Các bước ngừng phát tán với mạng
- 06.** Báo cáo phân tích và tìm kiếm mối đe dọa

```
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

Luồng thực thi thông thường

SolarWinds.Orion.Core.BusinessLayer.CoreBusinessLayerPlugin

Start ()

ScheduleBackgroundInventory ()

SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager

Start ()

Refresh ()

RefreshInternal ()

BackgroundInventory.Start ()

Thêm mã độc vào

OrionImprovementBusinessLayer

Initialize ()



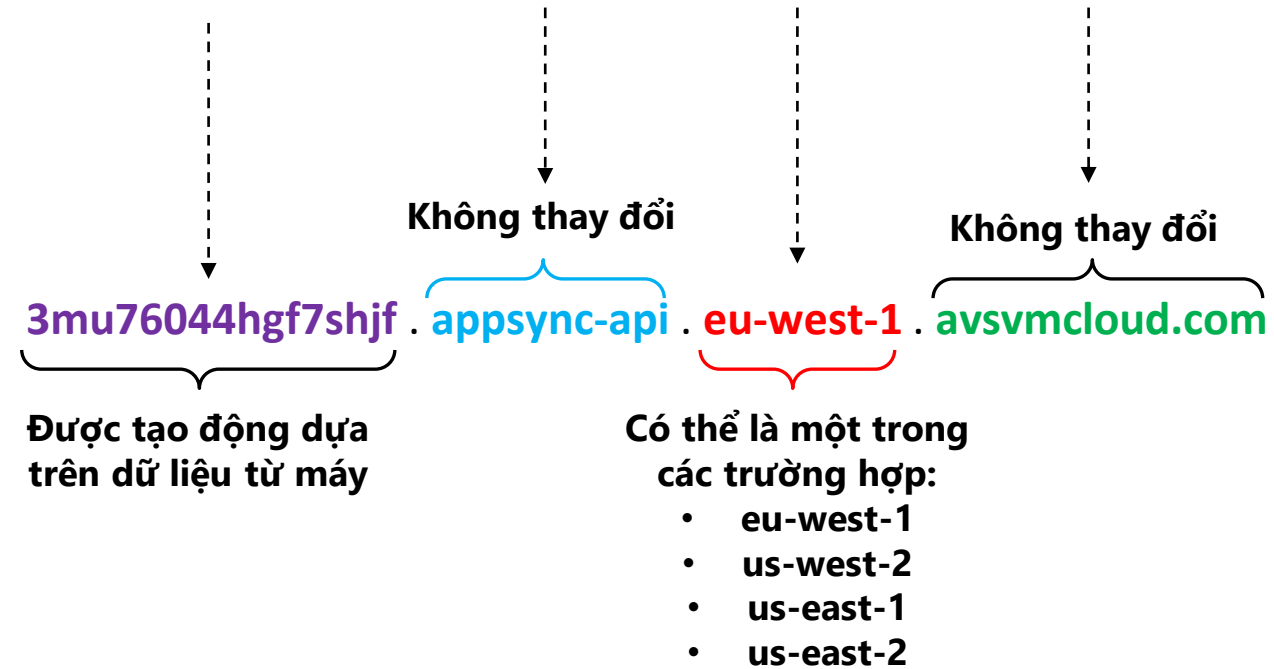
MITRE T1195.002

Xâm phạm chuỗi cung ứng:

Xâm phạm chuỗi cung ứng phần mềm

Ví dụ về miền được tạo:

3mu76044hgf7shjf . appsync-api . eu-west-1 . avsvmcloud.com



CUỘC TẤN CÔNG CHUỖI CUNG ỨNG

Kẻ tấn công chèn mã độc hại vào một cấu phần DLL của phần mềm hợp lệ. DLL bị xâm phạm được phát tán đến các tổ chức sử dụng phần mềm liên quan.

THỰC THI, LIÊN TỤC

Khi phần mềm khởi động, DLL bị xâm phạm sẽ tải và mã độc hại đã chèn sẽ gọi hàm chứa các chức năng cửa hậu.

NÉ TRÁNH LỚP PHÒNG THỦ

Cửa hậu có một danh sách dài các bước kiểm tra để đảm bảo rằng cửa hậu đang chạy trong một mạng bị xâm phạm thực sự.

DO THÁM

Cửa hậu thu thập thông tin hệ thống

C2 BAN ĐẦU

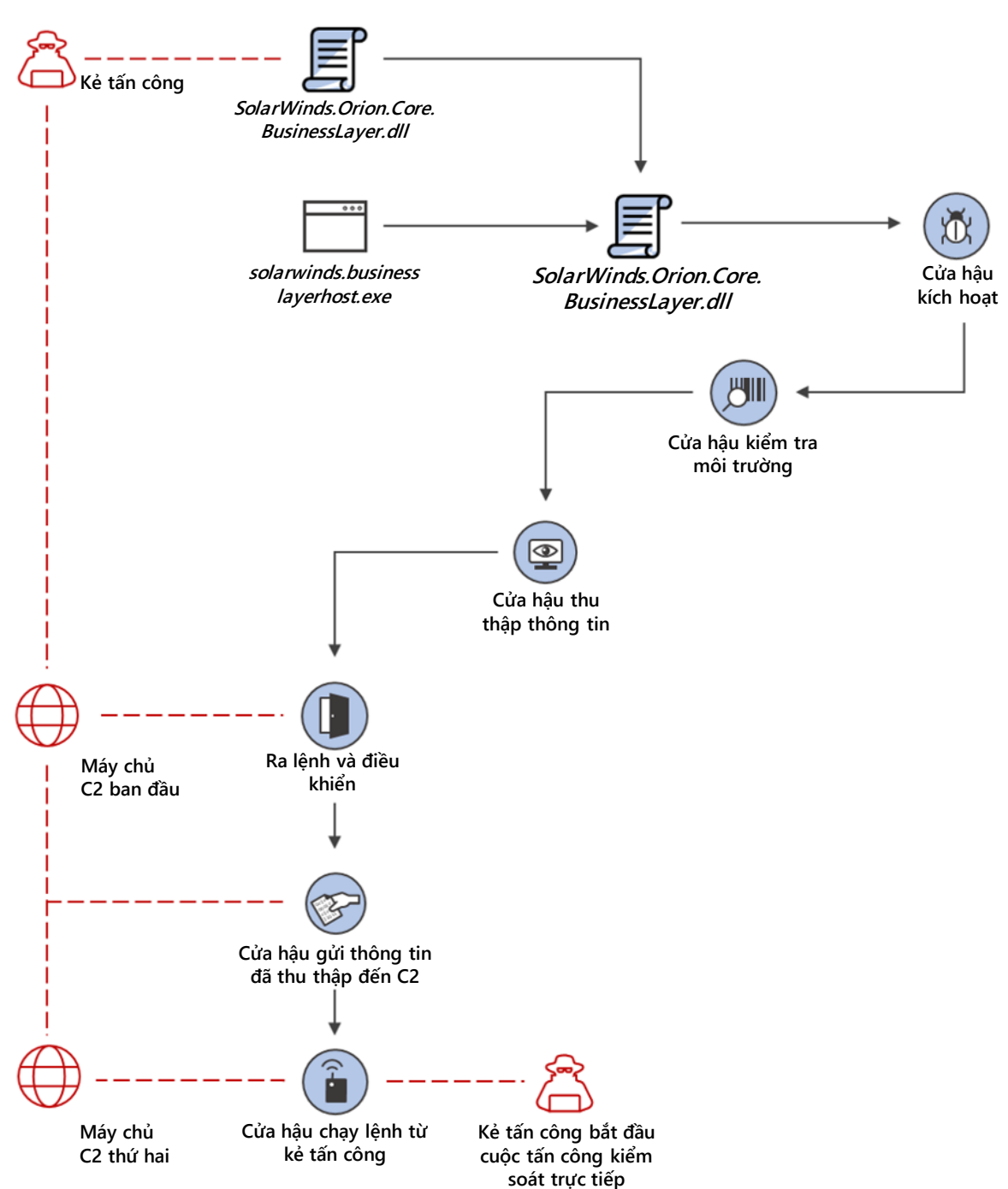
Cửa hậu kết nối với một máy chủ ra lệnh và điều khiển. Miền mà cửa hậu kết nối đến một phần sẽ dựa trên thông tin đã thu thập được từ hệ thống, việc này khiến mỗi miền con là duy nhất. Cửa hậu có thể nhận thêm địa chỉ C2 để kết nối đến.

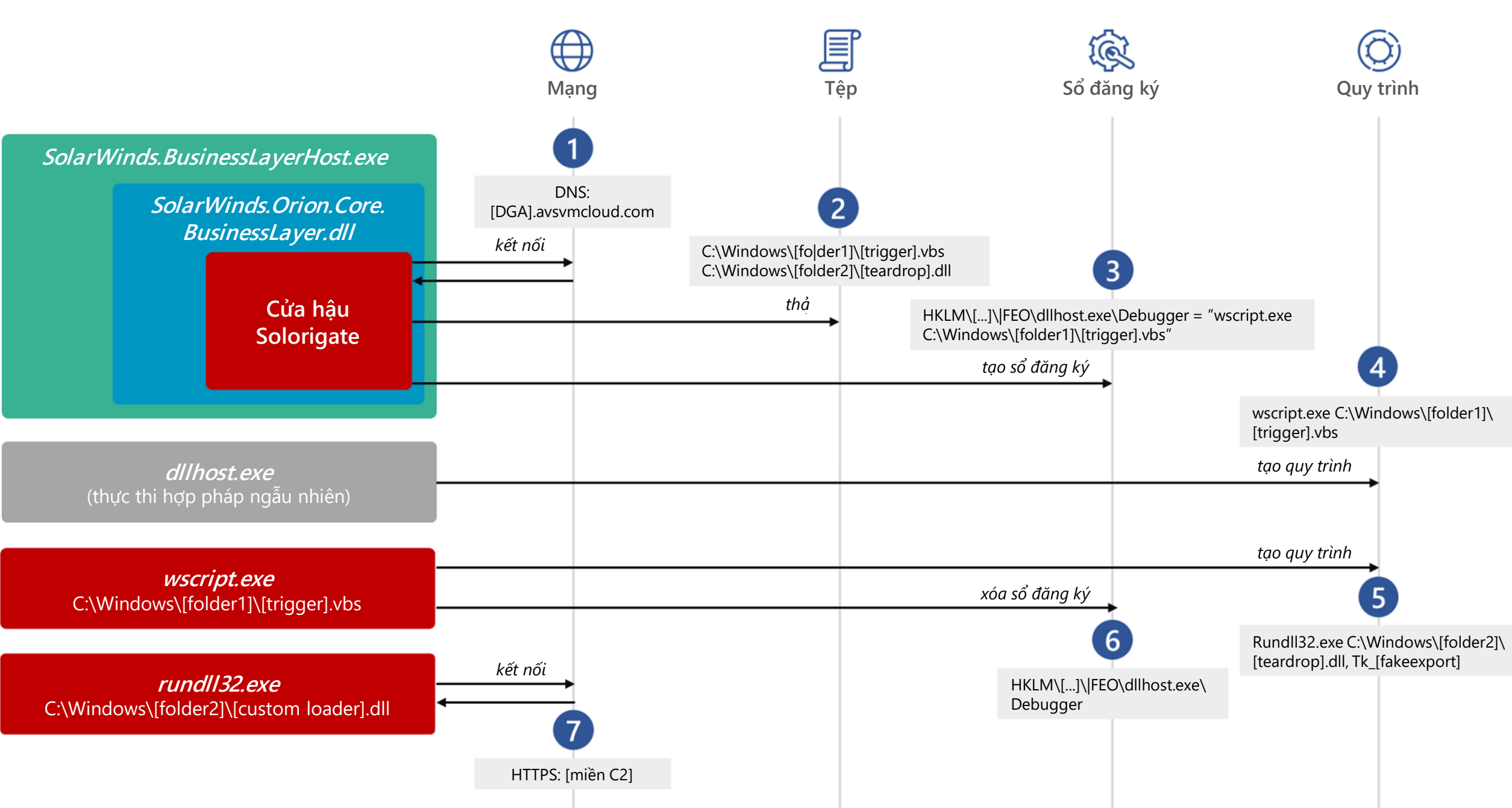
TRÍCH RÚT

Cửa hậu gửi thông tin đã thu thập được cho kẻ tấn công.

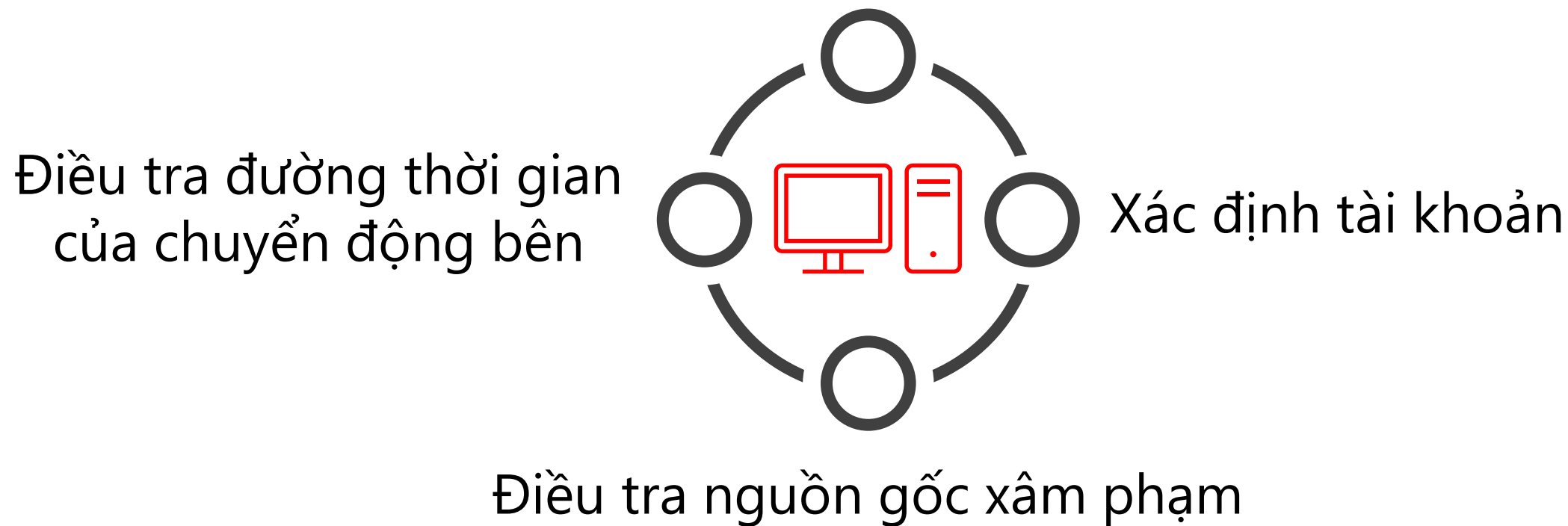
CUỘC TẤN CÔNG KIỂM SOÁT TRỰC TIẾP

Cửa hậu chạy các lệnh nhận được từ những kẻ tấn công. Một loạt các chức năng cửa hậu cho phép kẻ tấn công thực hiện thêm các hoạt động khác, như trộm cắp thông tin xác thực, leo thang đặc quyền lũy tiến và chuyển động bên.





Cách ly và điều tra thiết bị



[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



© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

- 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, 11:58:00 AM | New
Scheduled task possibly hijacked on win-9njrns9ohht by user mind0xp
- Dec 22, 2020, 11:58:00 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
Device	High	
Device	High	
User	No data available	
User	No data available	
User	No data available	

[View entities](#)

Evidence

31 entities found

[View all entities](#)

Incident information

This incident might be associated with...

Associated incidents

Incident ID	Reason	Entity
24851	Same file	sqtwls.exe
24576	Same file	legit_payl...
24576	Same file	paytwid.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)

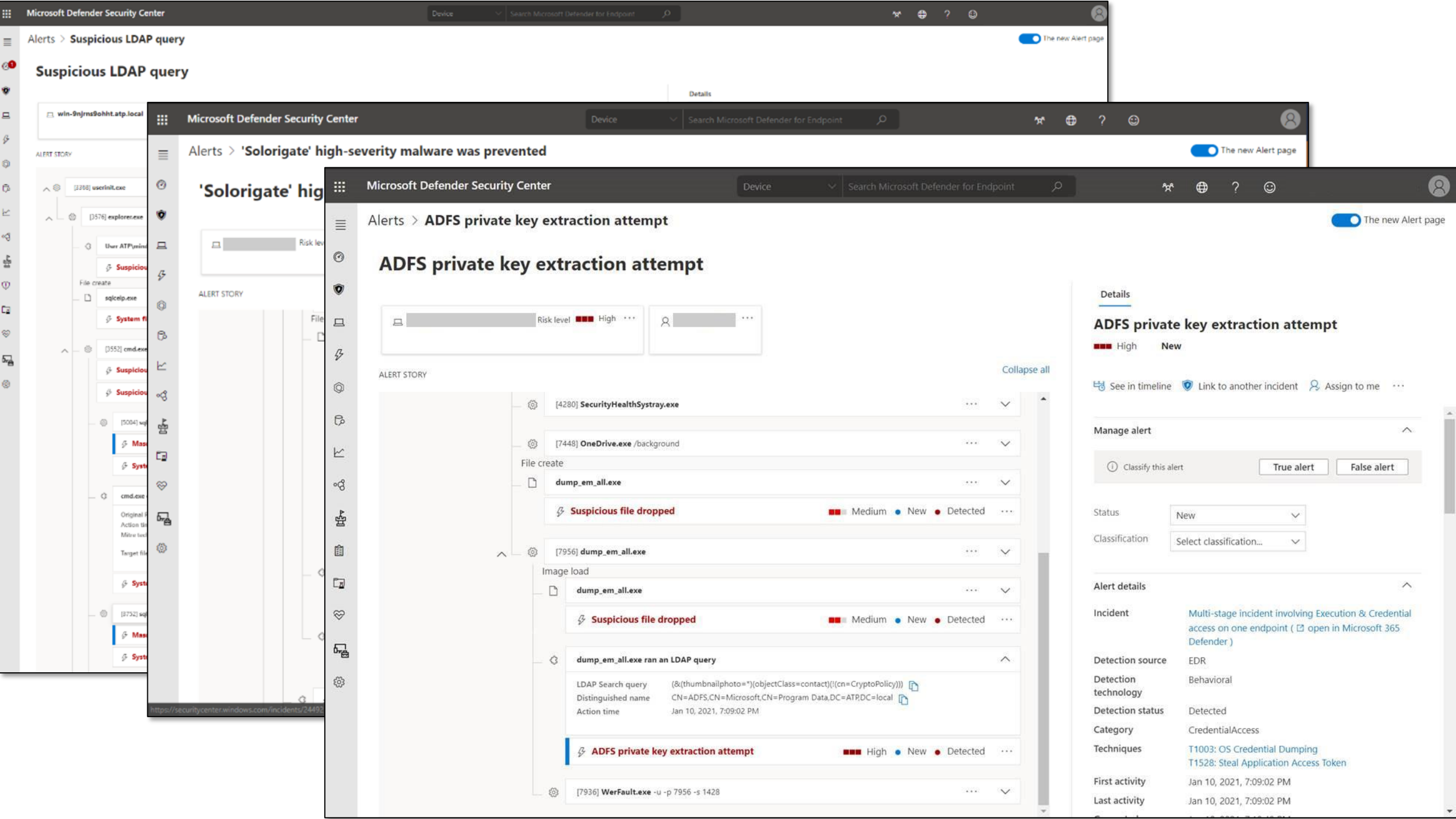
Determination

Not set

Assigned to

Unassigned

[Give feedback](#)



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 ⓘ



Secure configuration status ⓘ

1.41k misconfigured devices



[View mitigation details](#)

Devices with alerts

0 devices with active alerts

Vulnerability patching status ⓘ

0 vulnerable devices



[View mitigation details](#)

Chuỗi video về Solorigate

Bước tiếp theo

- 01.** Xem chuỗi video về Solorigate tại vị trí này
- 02.** Truy nhập Microsoft Security để biết thêm thông tin cập nhật:
<https://www.microsoft.com/vi-vn/security/business>
- 03.** Đọc bài đăng blog trên:
www.microsoft.com/security/blog
<https://aka.ms/solorigate>

