Microsoft

Información general de Solorigate

Tim Burrell

Partner Engineering Manager

Microsoft Threat Intelligence Center

18 de febrero de 2021

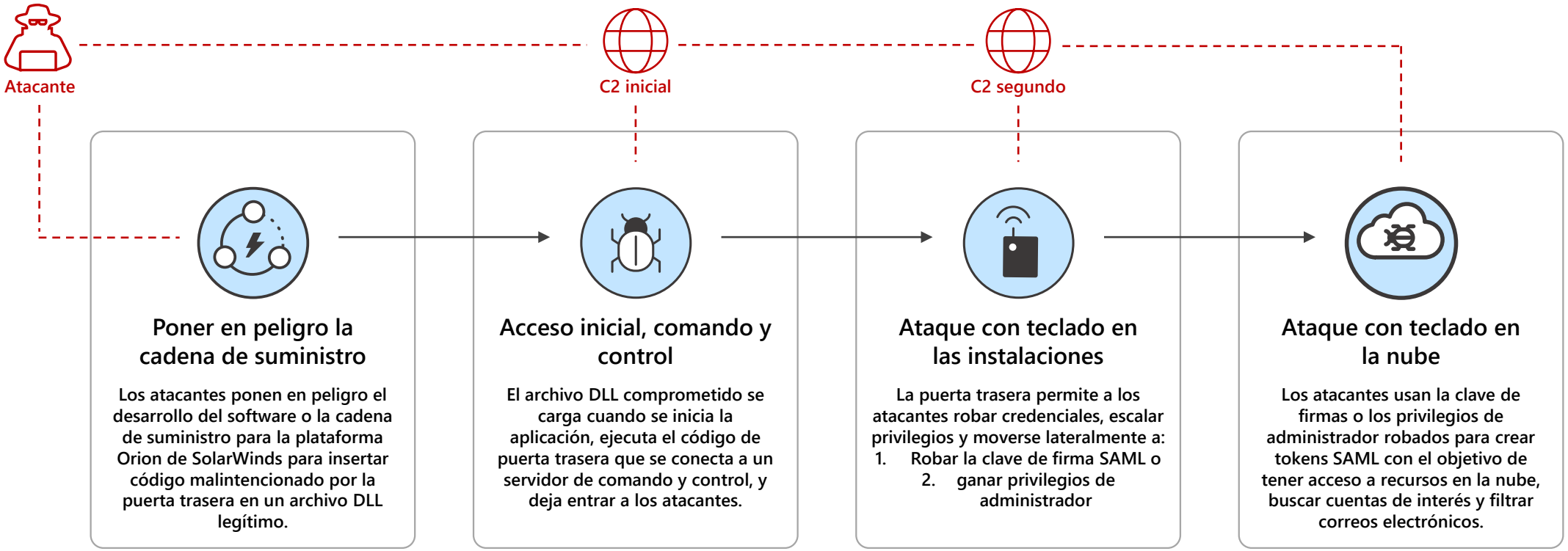
Serie de videos sobre Solorigate

Cómo proteger tu organización contra ataques similares a Solorigate.

Microsoft Security

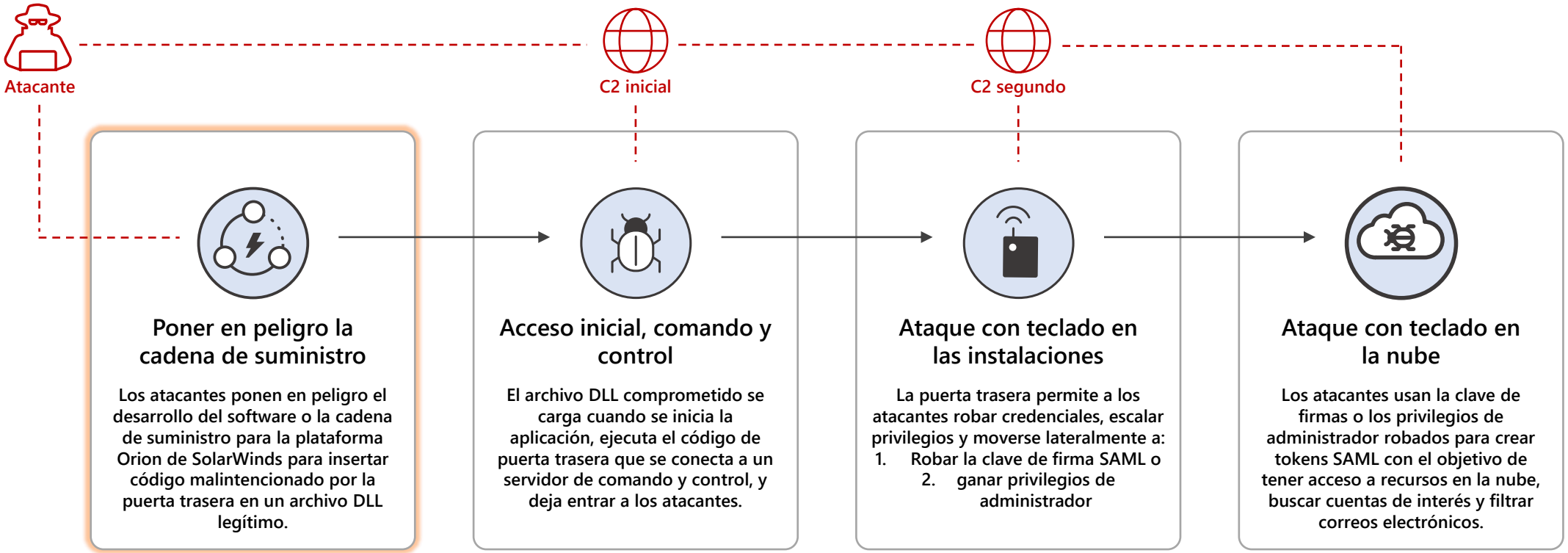
Ataque Solorigate

Cadena de ataques de alto nivel de un extremo a otro



Ataque Solorigate

Cadena de ataques de alto nivel de un extremo a otro



Ataque Solorigate

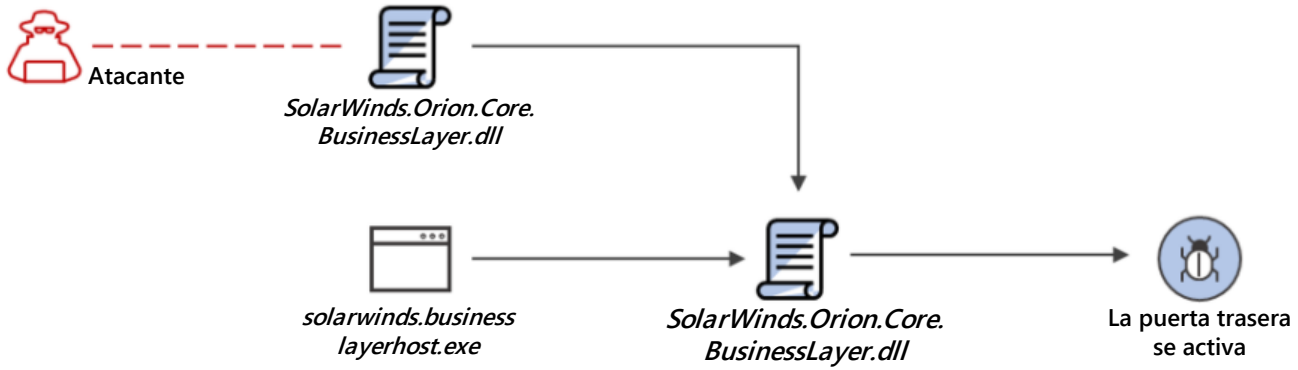
Escala de tiempo

* Divulgado por SolarWinds

A día 21/1/2021 la información es correcta; para obtener la información más reciente, visita aka.ms/solorigate

ATAQUE A LA CADENA DE SUMINISTRO
Los atacantes insertan código malintencionado en un componente DLL de software legítimo. El archivo DLL en peligro se distribuye a las organizaciones que usan el software relacionado.

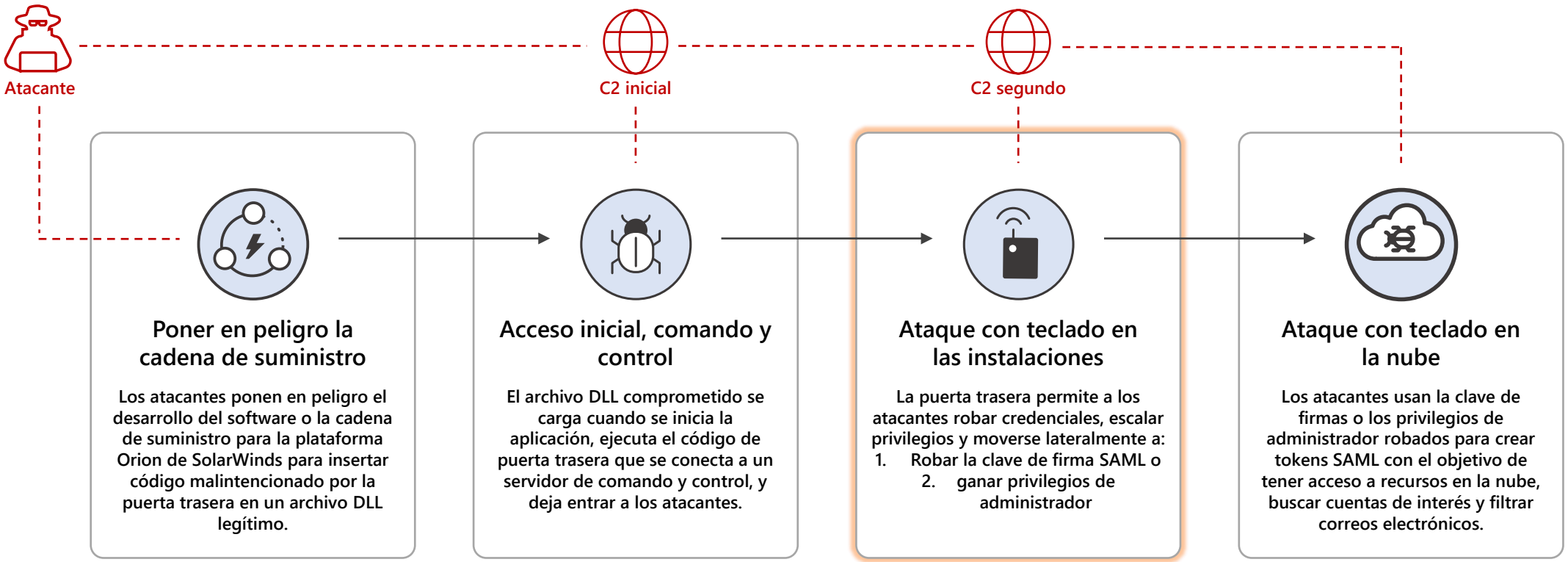
EJECUCIÓN, PERSISTENCIA
Cuando el software se ejecuta, el archivo DLL en peligro se carga y el código malintencionado insertado llama la función que contiene las capacidades de puerta trasera.




```
"Signer": "Solarwinds Worldwide, LLC",
"SignerHash": "47d92d49e6f7f296260da1af355f941eb25360c4",
```

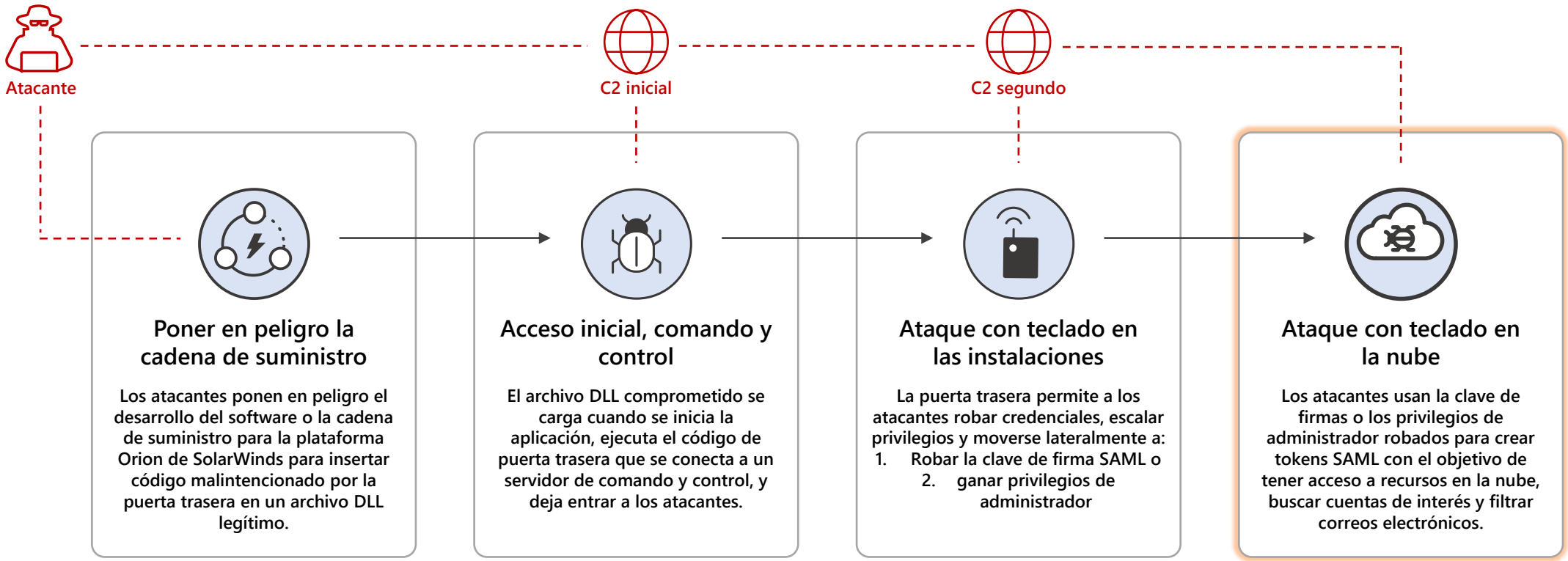
Ataque Solorigate

Cadena de ataques de alto nivel de un extremo a otro



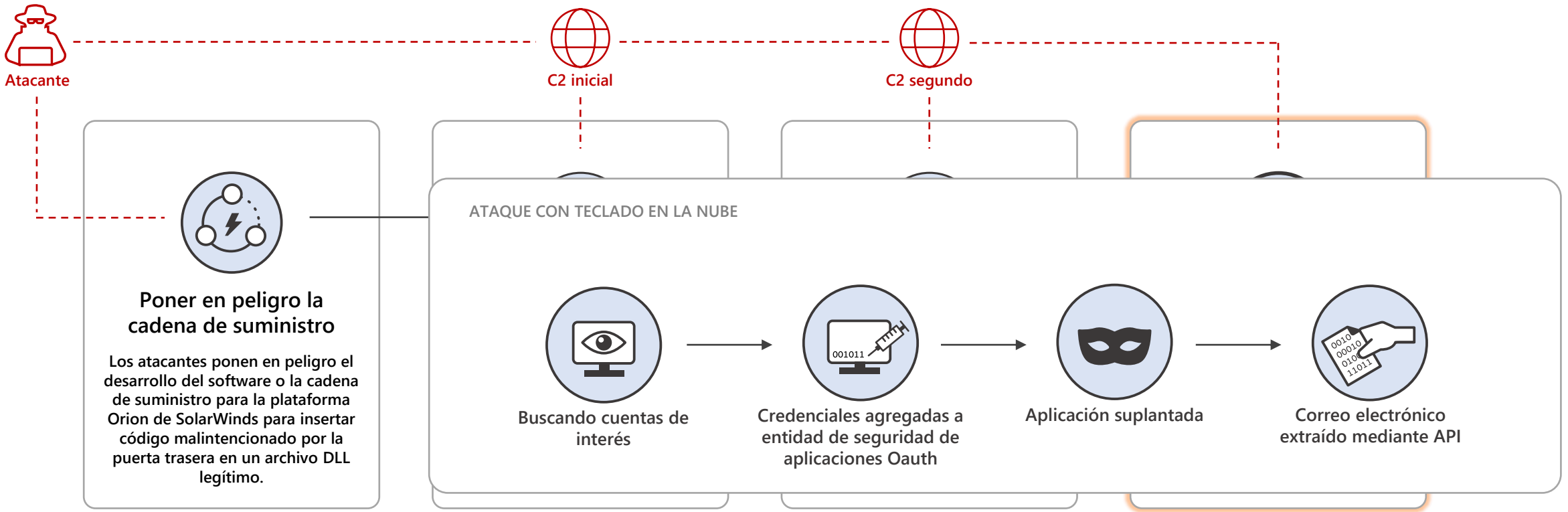
Ataque Solorigate

Cadena de ataques de alto nivel de un extremo a otro



Ataque Solorigate

Cadena de ataques de alto nivel de un extremo a otro



Defensas recomendadas

7 pasos para la protección contra las técnicas vistas en Solorigate

1. Usa un antivirus y productos EDR actualizados.

2. Bloquea los puntos de conexión C2 utilizando la infraestructura de tu red.

3. Asegura el token SAML de las claves de firma y piensa en la seguridad de hardware para tus certificados de firma de token SAML. Para los Servicios de federación de Active Directory (AD FS), revisa las prácticas recomendadas de Microsoft: https://docs.microsoft.com/es-mx/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs

4. Sigue las prácticas recomendadas para los derechos de usuario de administrador y reduce el número de usuarios que son miembros de roles de directorio con privilegios elevados.

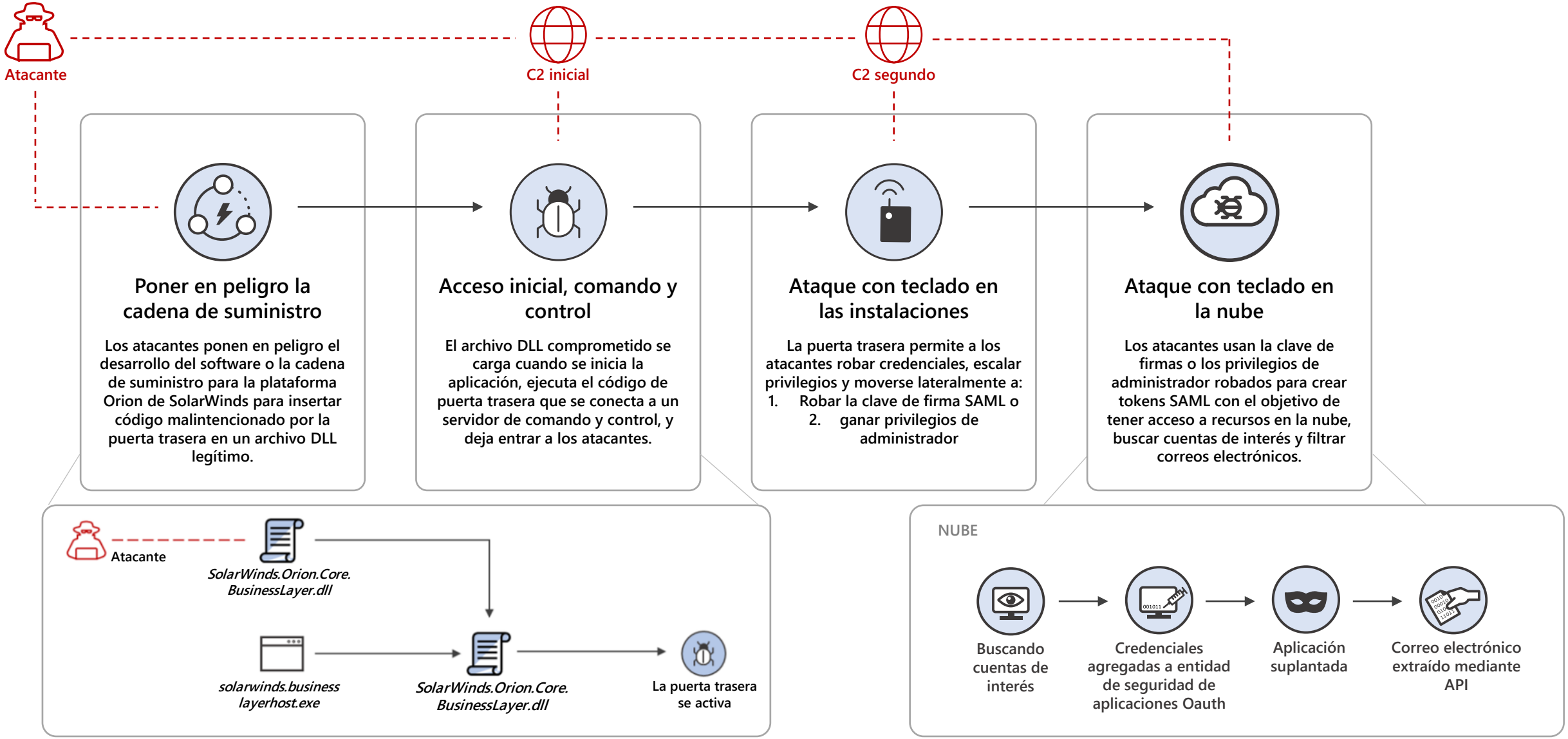
5. Asegúrate de que las cuentas de servicio con derechos de administrador utilizan secretos con un nivel alto de entropía (p. ej., certificados) almacenados de forma segura. Supervisa los cambios, los inicios de sesión y el uso anómalo de cuentas de servicio.

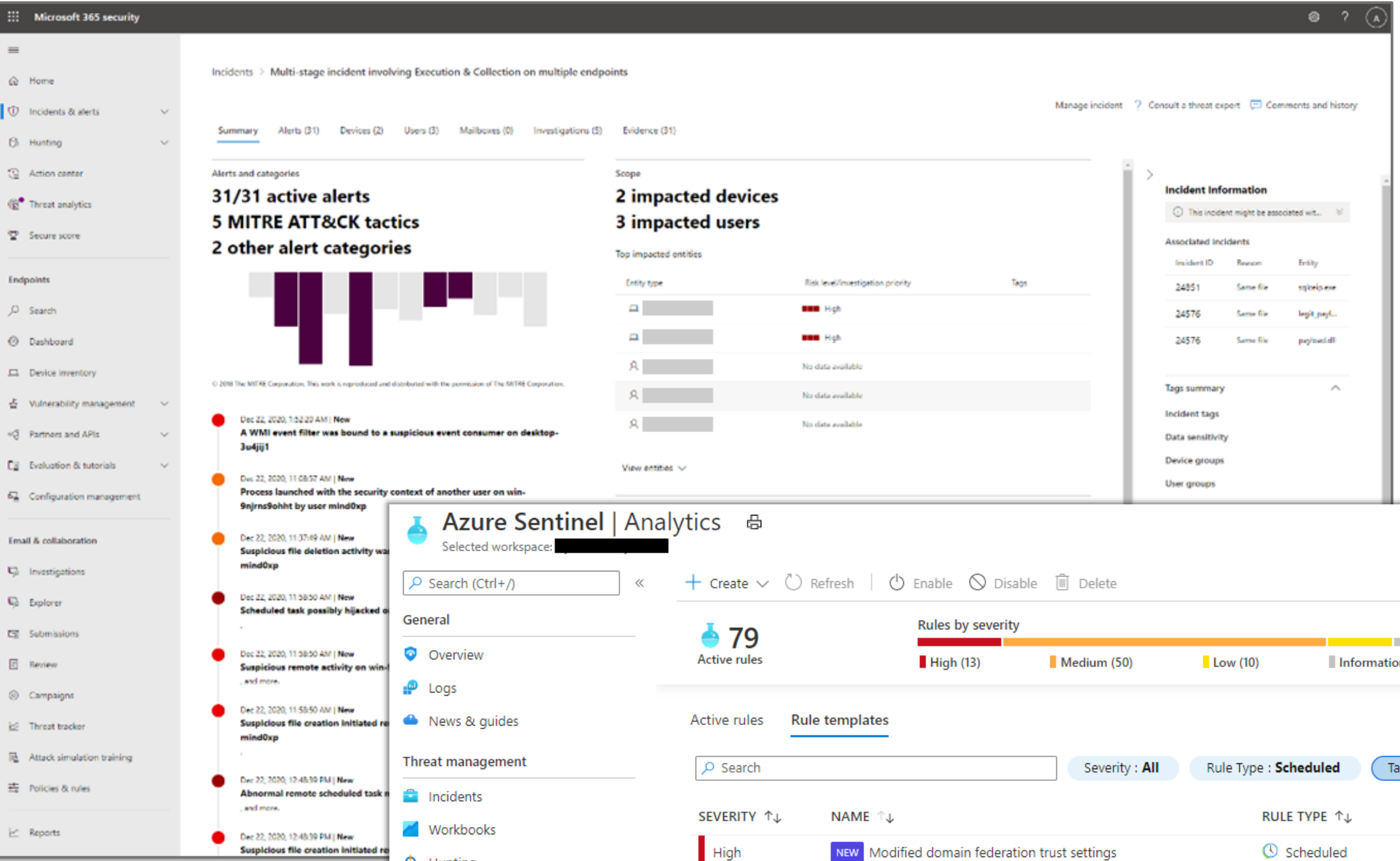
6. Quita o deshabilita las aplicaciones sin usar o innecesarias y las entidades de seguridad. Reduce permisos de acceso en aquellos que aún tengas.

7. Ve estas recomendaciones adicionales para asegurar la infraestructura de identidad de Azure AD: https://docs.microsoft.com/es-mx/azure/security/fundamentals/steps-secure-identity

Ataque Solorigate

Cadena de ataques de alto nivel de un extremo a otro




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
Scope
2 impacted devices
3 impacted users
Top impacted entities
Entity type
Risk level/investigation priority
Tags
High
No data available
View entities
Incident Information
Associated incidents
Tags summary
Incident tags
Data sensitivity
Device groups
User groups
A WMI event filter was bound to a suspicious event consumer on desktop-3u4jij1
Process launched with the security context of another user on win-9njrns9ohht by user mind0xp

Azure Sentinel | Analytics
Selected workspace:
Search (Ctrl+/)
General
Overview
Logs
News & guides
Threat management
Incidents
Workbooks
Hunting
Notebooks (Preview)
Entity behavior
Create
Refresh
Enable
Disable
Delete
79
Active rules
Rules by severity
High (13)
Medium (50)
Low (10)
Informational (6)
Active rules
Rule templates
Search
Severity : All
Rule Type : Scheduled
Tactics : 2 selected
Data Sources : 3 sel
SEVERITY
NAME
RULE TYPE
DATA SOURCES
High
NEW
Modified domain federation trust settings
Scheduled
Azure Active Directory
Low
NEW
Interactive STS refresh token modifications
Scheduled
Azure Active Directory
Low
NEW
Azure Active Directory PowerShell accessing non-AAD resou...
Scheduled
Azure Active Directory

Serie de videos sobre Solorigate

Pasos siguientes

01 Ver la serie de videos de Solorigate en esta ubicación

02 Visita Seguridad de Microsoft para más actualizaciones: www.microsoft.com/es-mx/security/business

03 Lee las publicaciones del blog en: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft