Microsoft

Solorigate Overview

Tim Burrell

Partner Engineering Manager

Microsoft Threat Intelligence Center

February 18, 2021

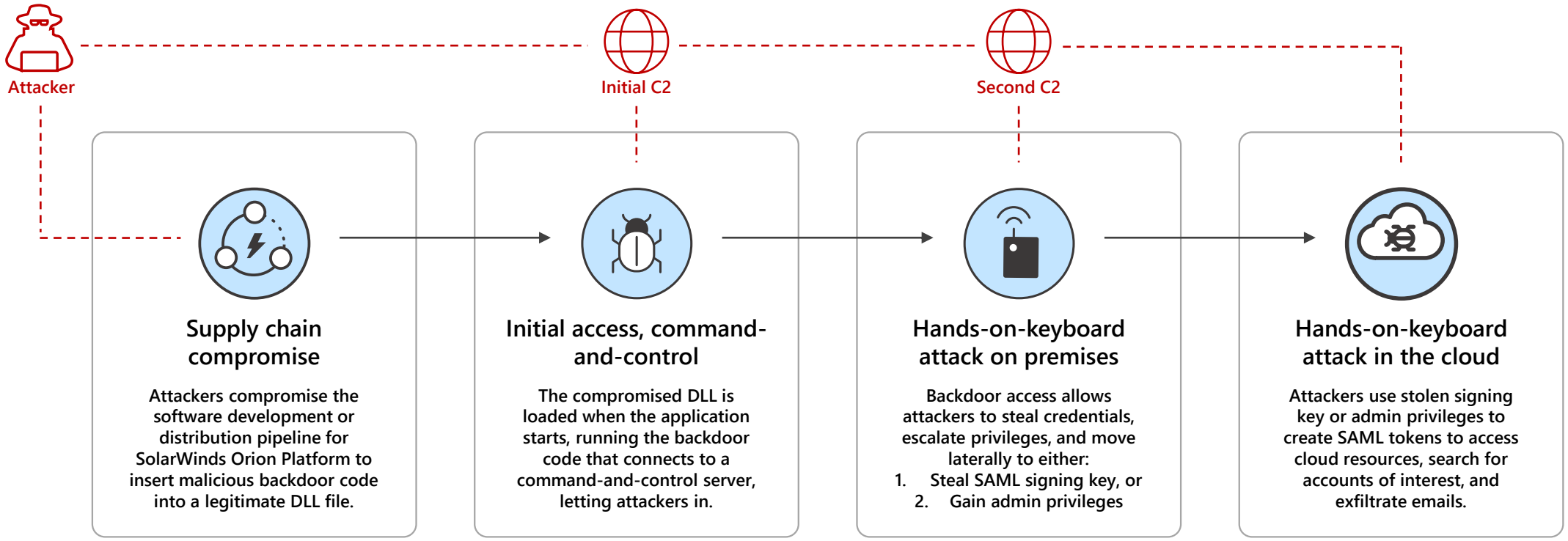
Solorigate Video Series

How to help protect your organization against Solorigate-style attacks.

Microsoft Security

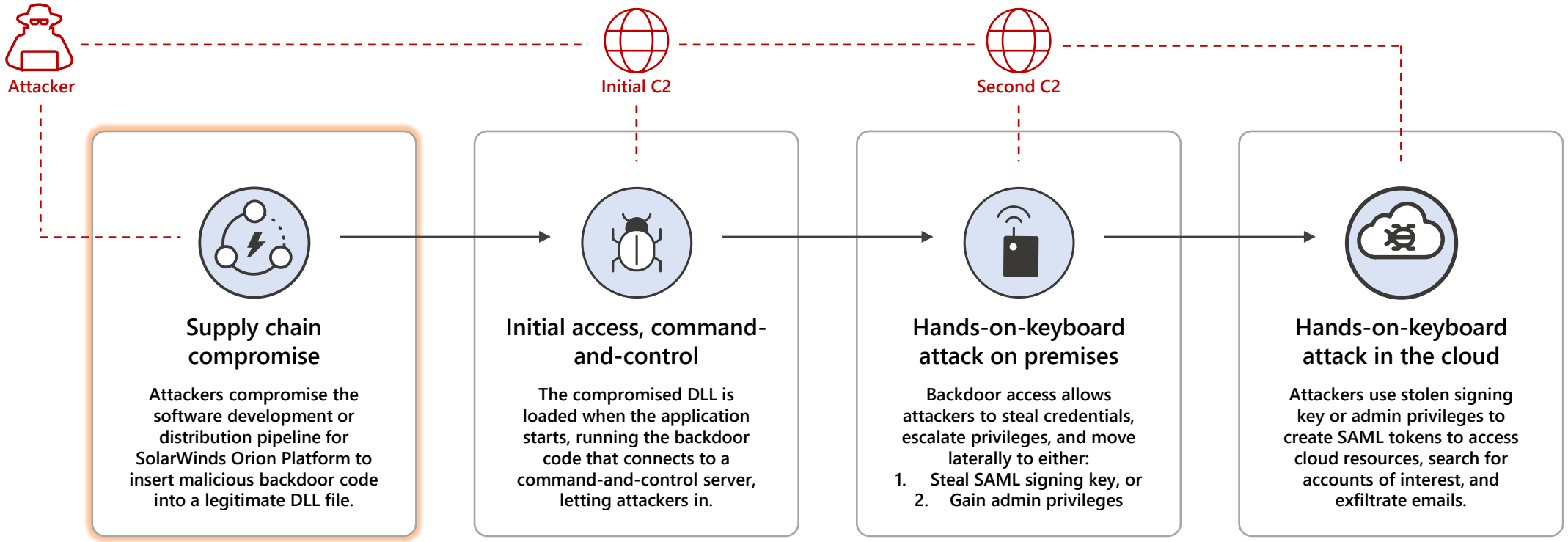
Solorigate Attack

High-level end-to-end attack chain



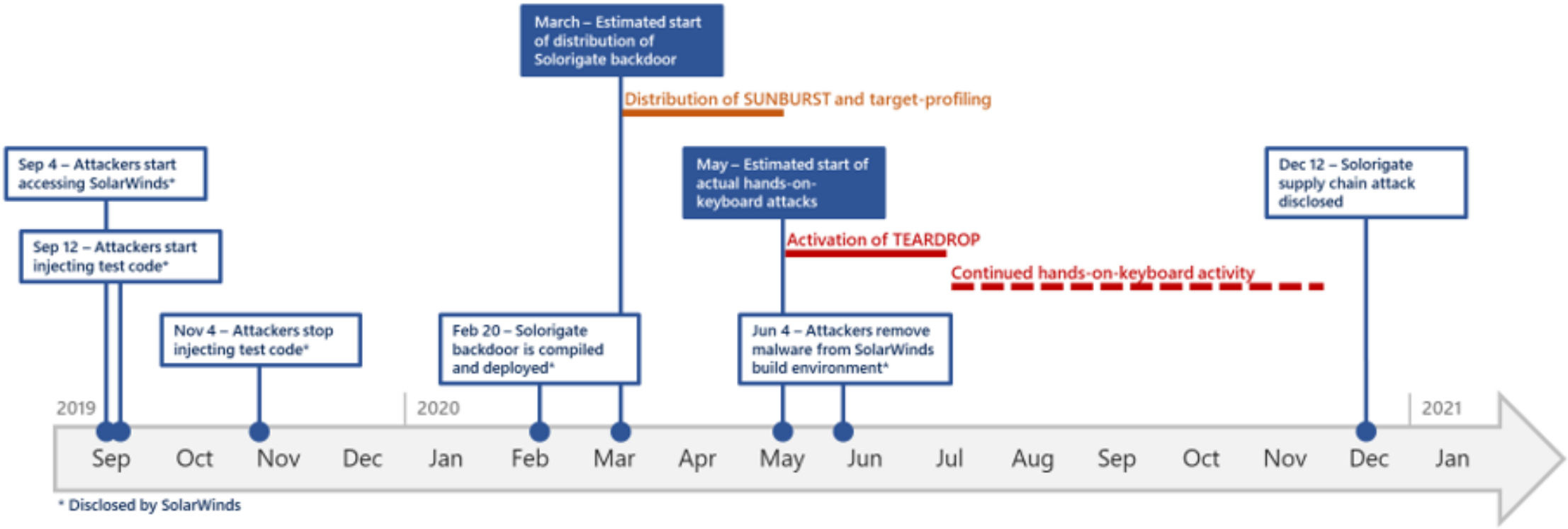
Solorigate Attack

High-level end-to-end attack chain



Solorigate Attack

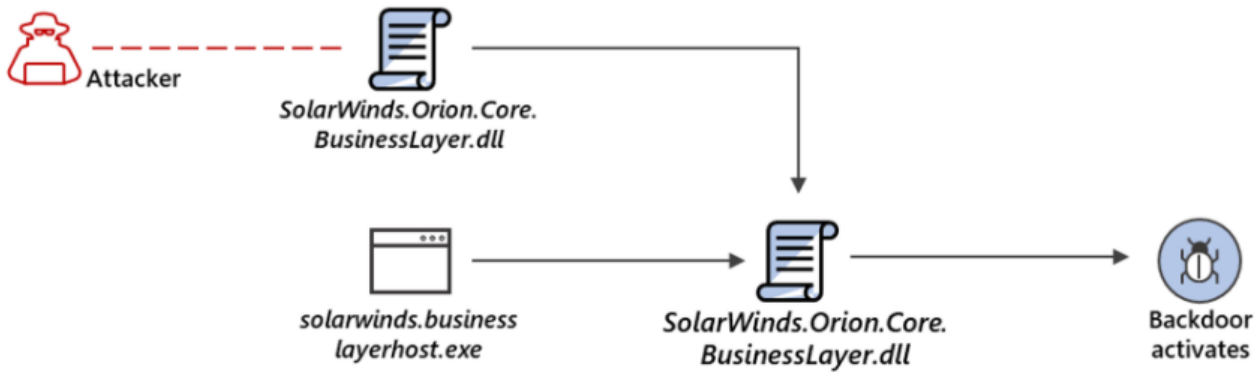
Timeline



Information is correct as of 1/21/2021. please see aka.ms/solorigate for the most recent updates

SUPPLY CHAIN ATTACK
Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

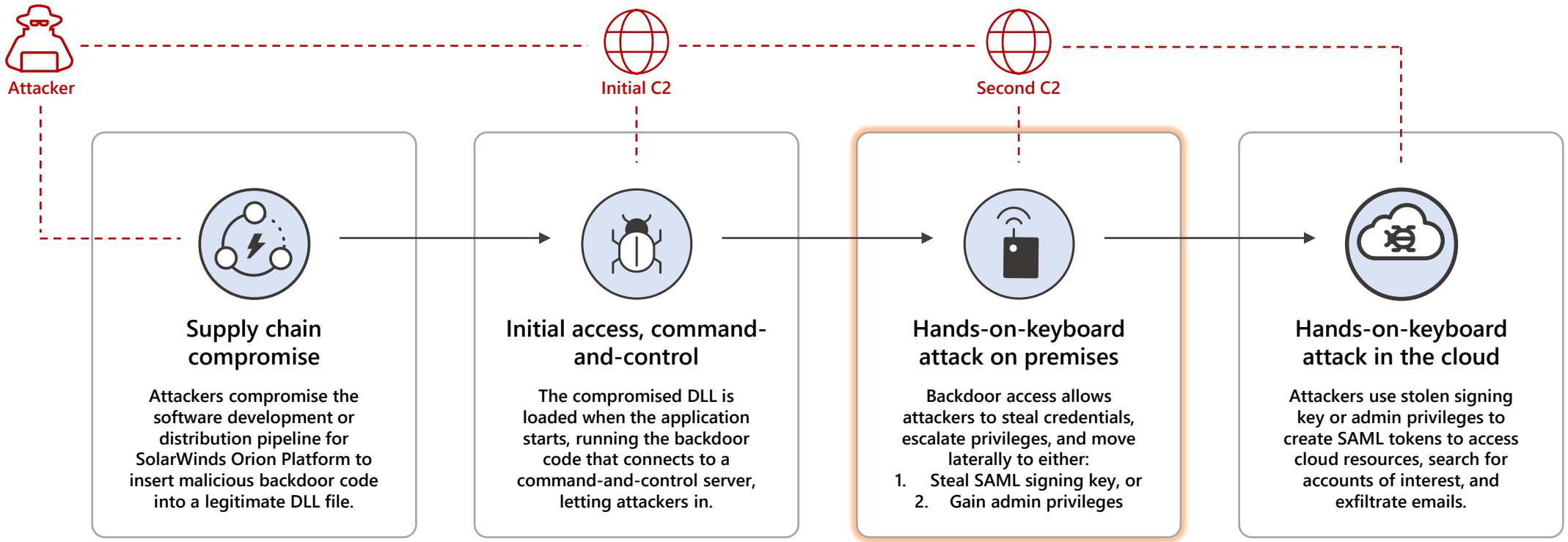
EXECUTION, PERSISTENCE
When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.




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

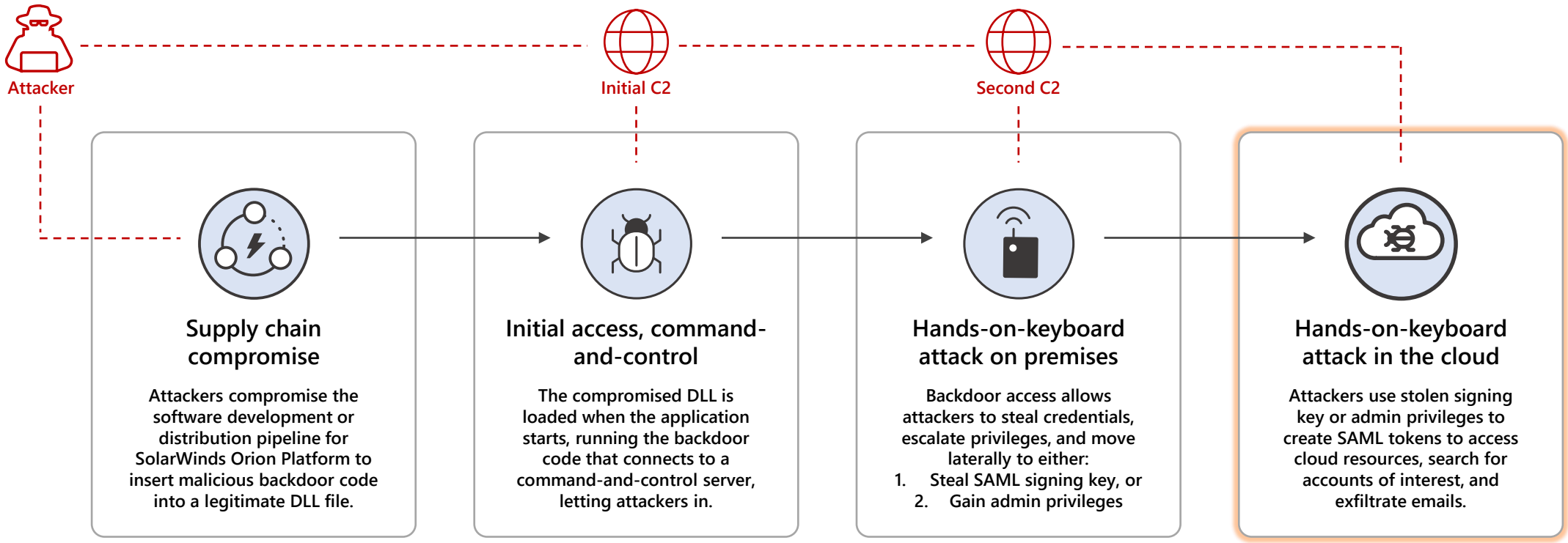
Solorigate Attack

High-level end-to-end attack chain



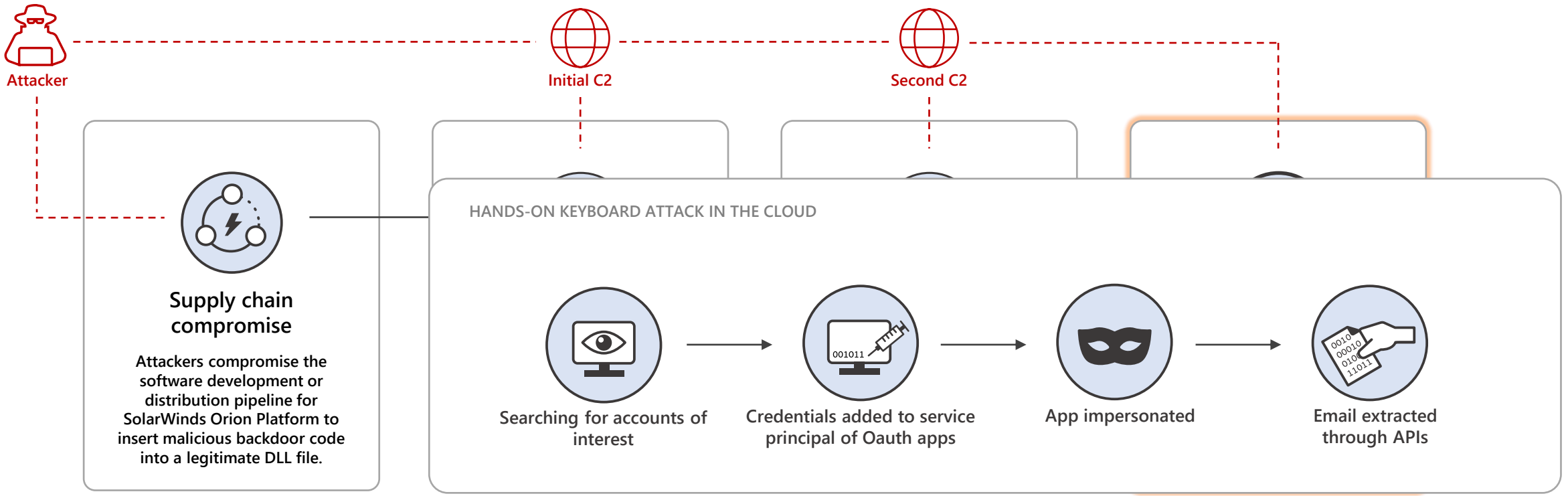
Solorigate Attack

High-level end-to-end attack chain



Solorigate Attack

High-level end-to-end attack chain



Recommended Defenses

7 Steps to help protect against techniques seen in Solorigate

1. Run up-to-date antivirus and EDR products.

2. Block known C2 endpoints using your network infrastructure.

3. Secure your SAML token signing keys, and consider hardware security for your SAML token signing certificates. For Active Directory Federation Services, review Microsoft's best practice recommendations: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs

4. Follow best practices for admin user rights, and reduce the number of users that are members of highly privileged directory roles.

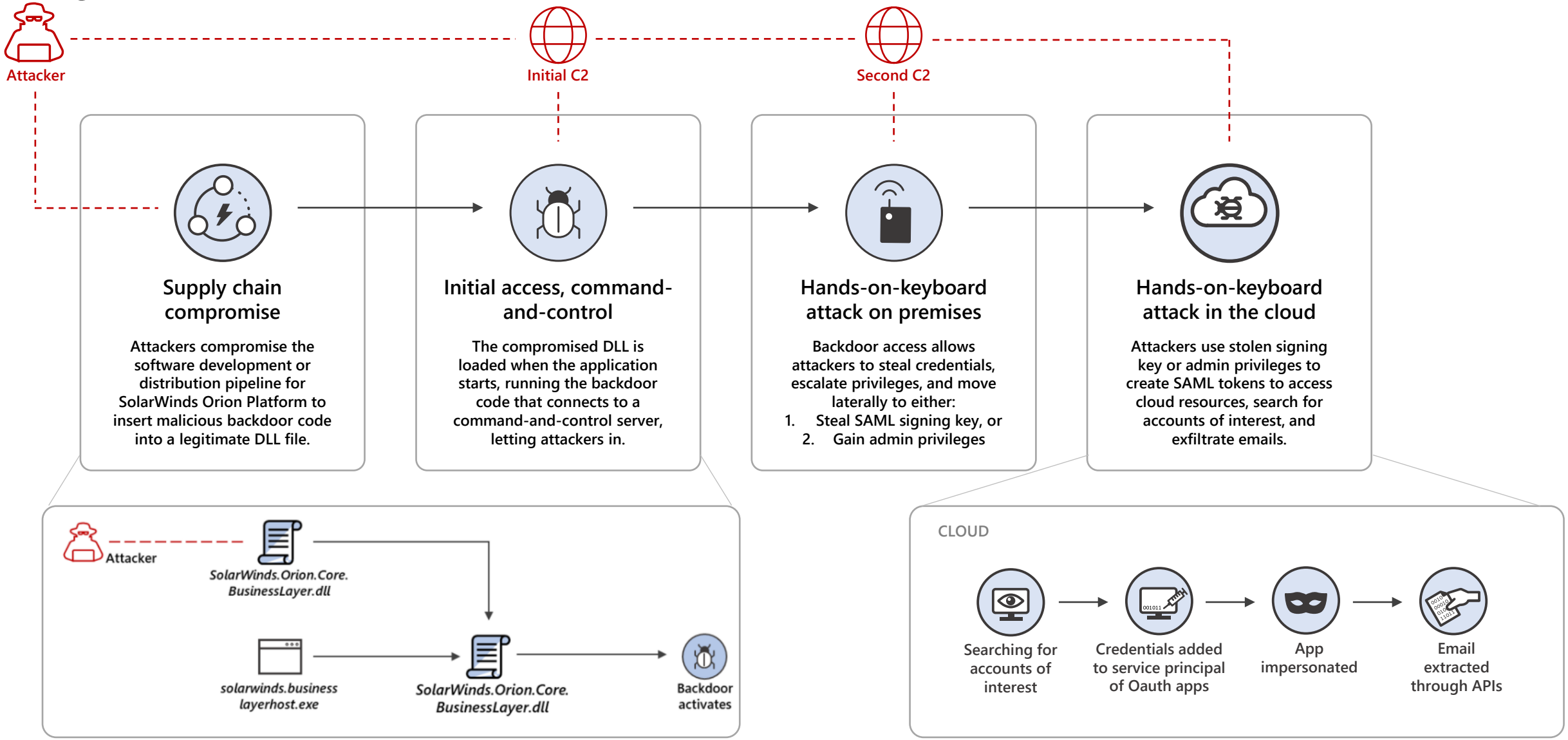
5. Ensure that service accounts with administrative rights use high entropy secrets (i.e. certificates) stored securely. Monitor for changes, sign-ins, and use of anomalous service accounts.

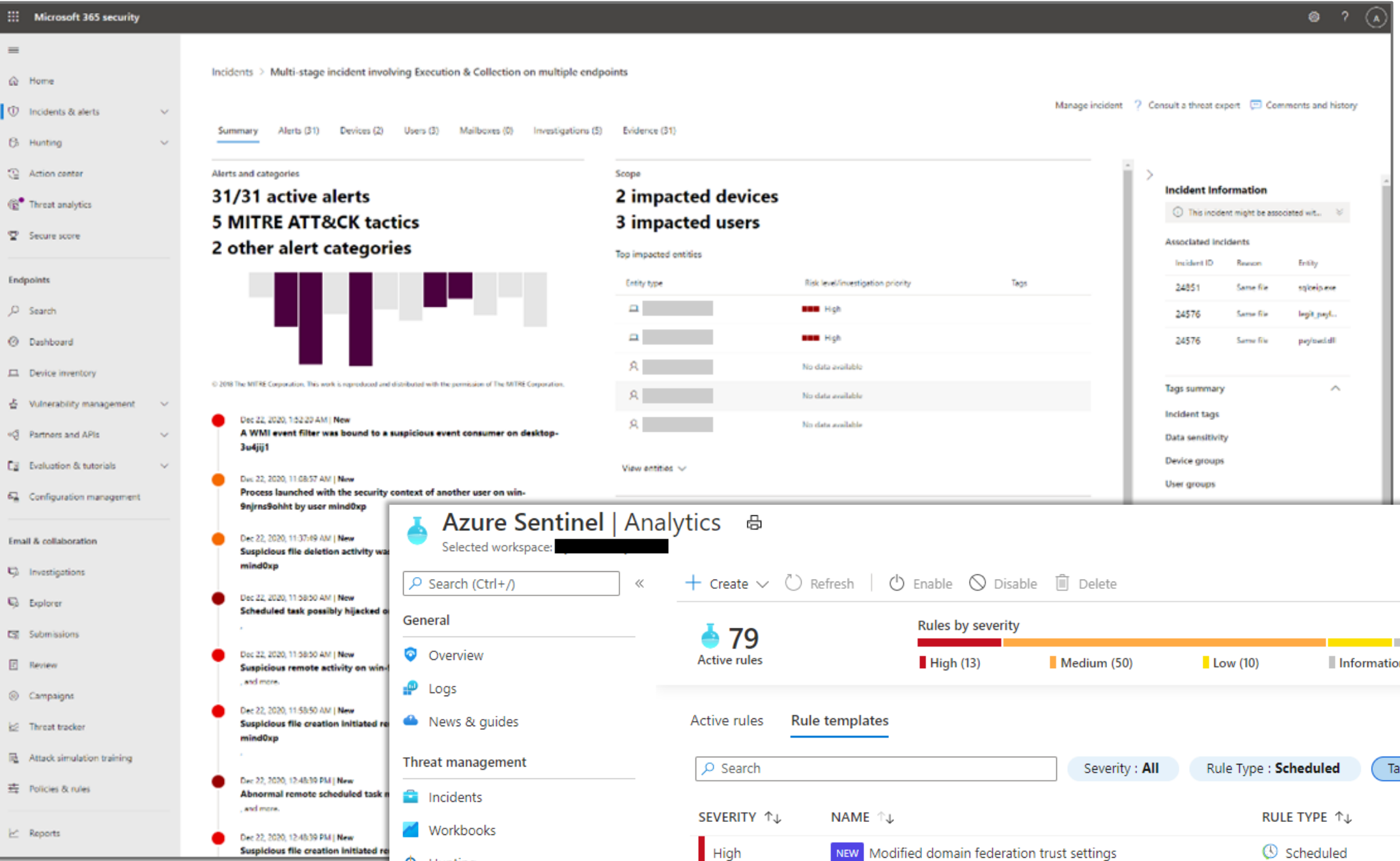
6. Remove or disable unused or unnecessary applications and service principals. Reduce permissions on those you still have.

7. See these additional recommendations to secure your Azure AD identity infrastructure: https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

Solorigate Attack

High-level end-to-end attack chain




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

Solorigate Video Series

Next Steps

01 Watch the Solorigate Video series at this location

02 Visit Microsoft Security for more updates: www.microsoft.com/en-us/security/business

03 Read the blog posts on: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security