Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Streaming Edition 2021

ASTREA Advanced Security, Training Research, Events Agency

Atelier tecnologico

Contrastare Solorigate

Patrizio Rinaldi, Senior Technical Specialist, Microsoft Italia

16 marzo 2021 orario 15.00-15.40 - StreamingEdition

#securitysummit #streamingedition

Streaming Edition

Patrizio Rinaldi

SENIOR TECHNICAL SPECIALIST

SECURITY AND COMPLIANCE

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Streaming Edition

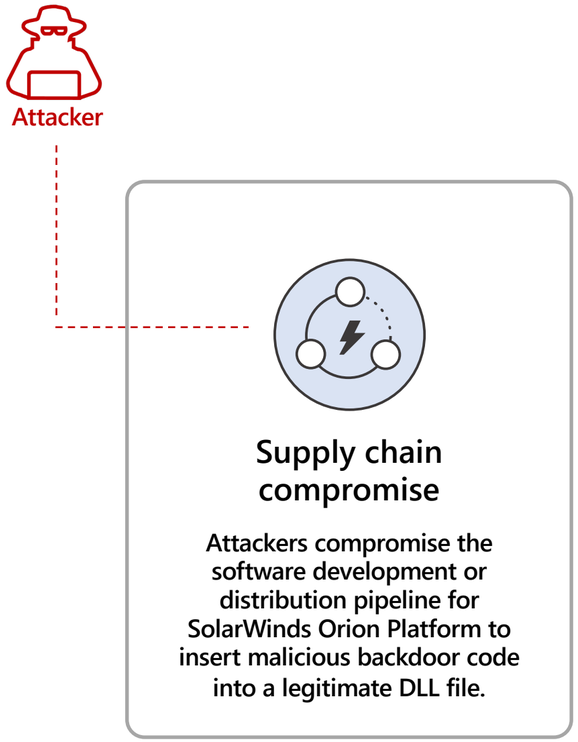
16-17-18 marzo 2021

Microsoft

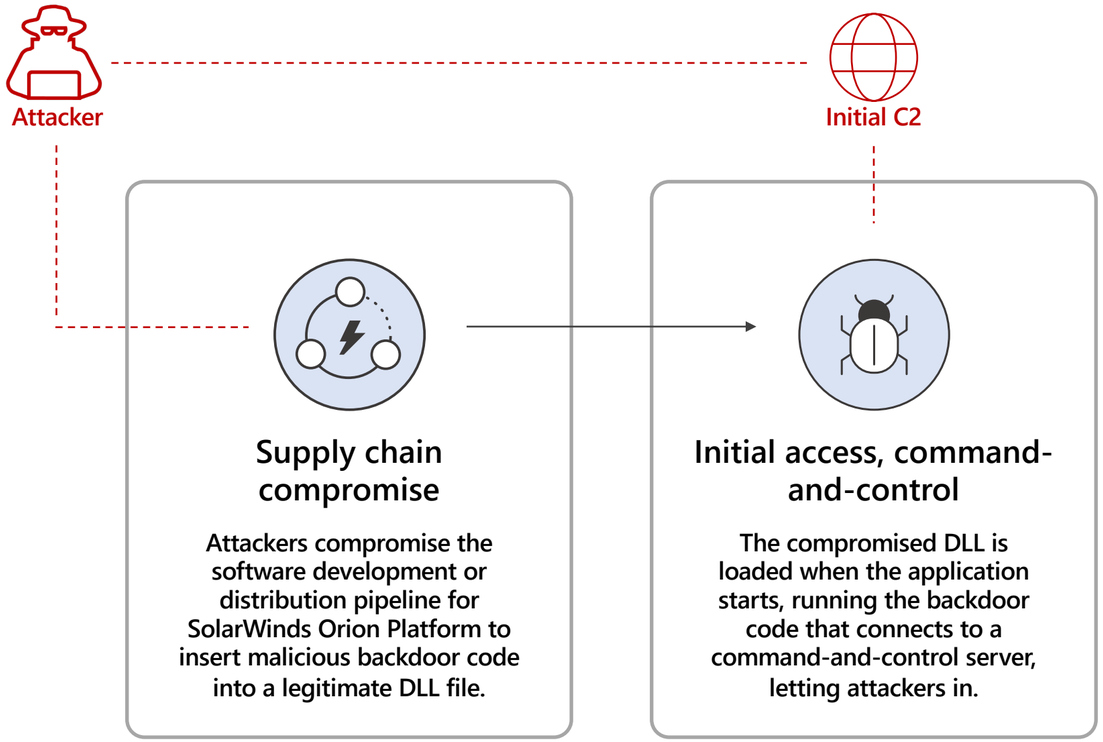
Un attacco alla Supply Chain

Rivolto a fornitori e sviluppatori di software, l'obiettivo è accedere ai codici sorgente, creare processi o aggiornare i meccanismi infettando applicazioni legittime e ***considerate trusted*** per distribuire malware.

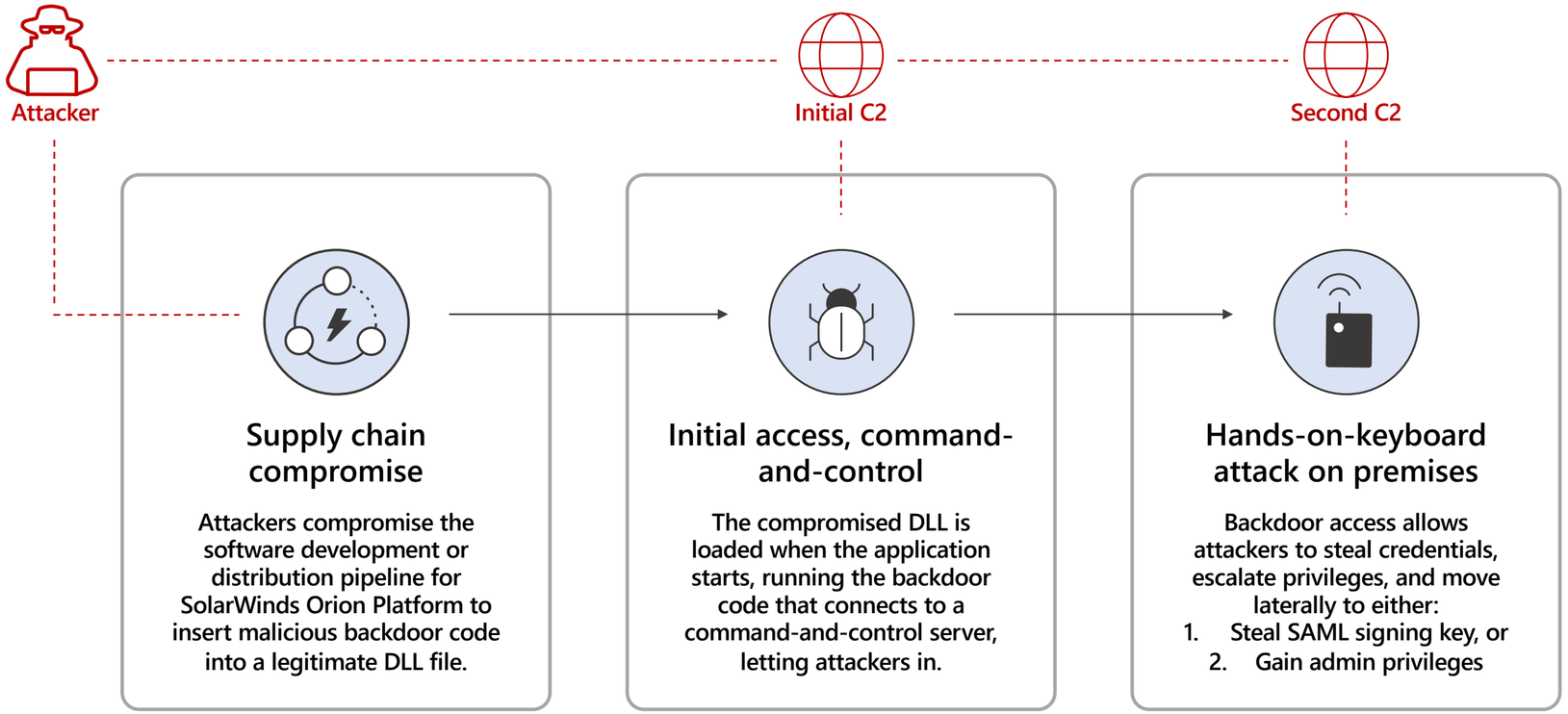
SOLORIGATE ATTACK
High-level end-to-end attack chain



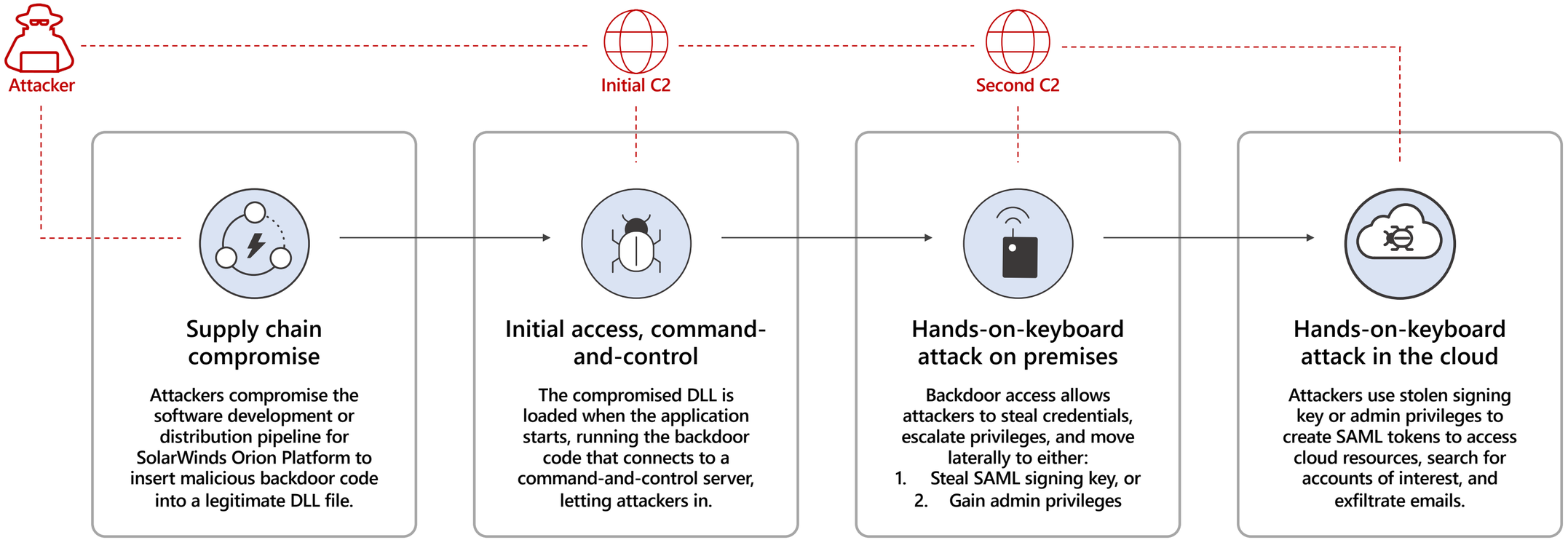
SOLORIGATE ATTACK
High-level end-to-end attack chain



SOLORIGATE ATTACK
High-level end-to-end attack chain



SOLORIGATE ATTACK
High-level end-to-end attack chain



Solorigate (aka Sunburst aka UNC2452)

Solorigate è un attacco complesso, che sfrutta il coinvolgimento di molteplici sistemi legati alla catena produttiva (supply-chain) multi-stadio e multi-dominio, che ha mostrato l'uso di tecniche di attacco avanzate per compromettere obiettivi di alto profilo.

Identities Domain

Endpoints Domain

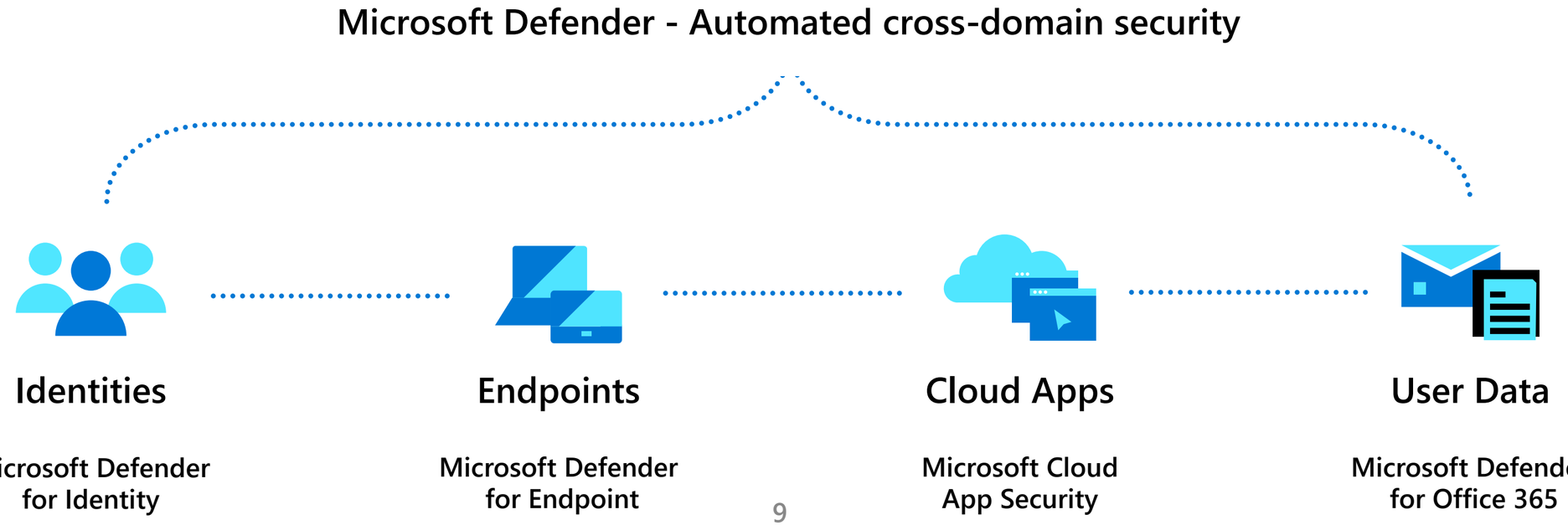
Cloud Domain

Data Domain

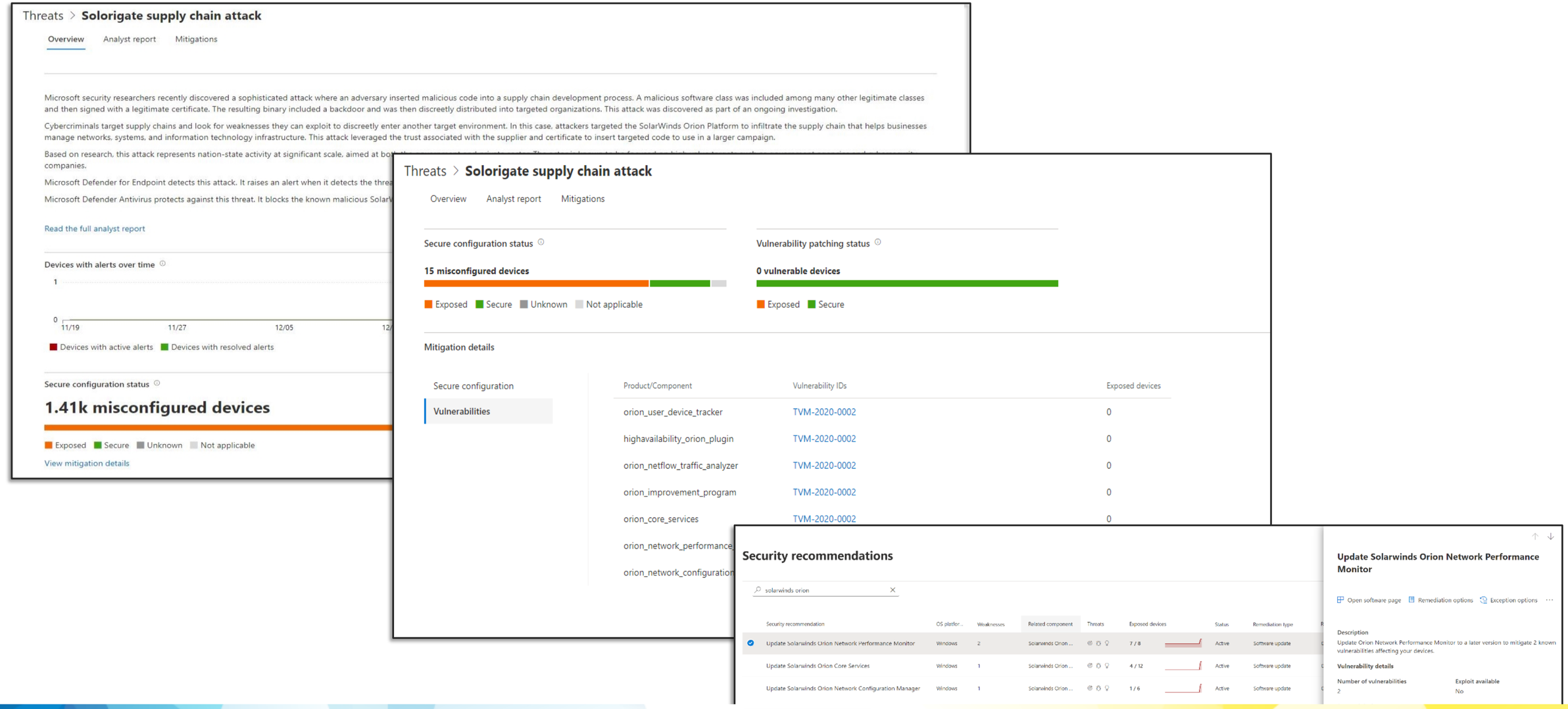
Più di 17000 organizzazioni colpite, l'anatomia dell'attacco è ormai nota, questo ci permette di definire buone pratica di risposta ma soprattutto di prevenzione.

Serve proteggere i domini IT attraverso un approccio Olistico

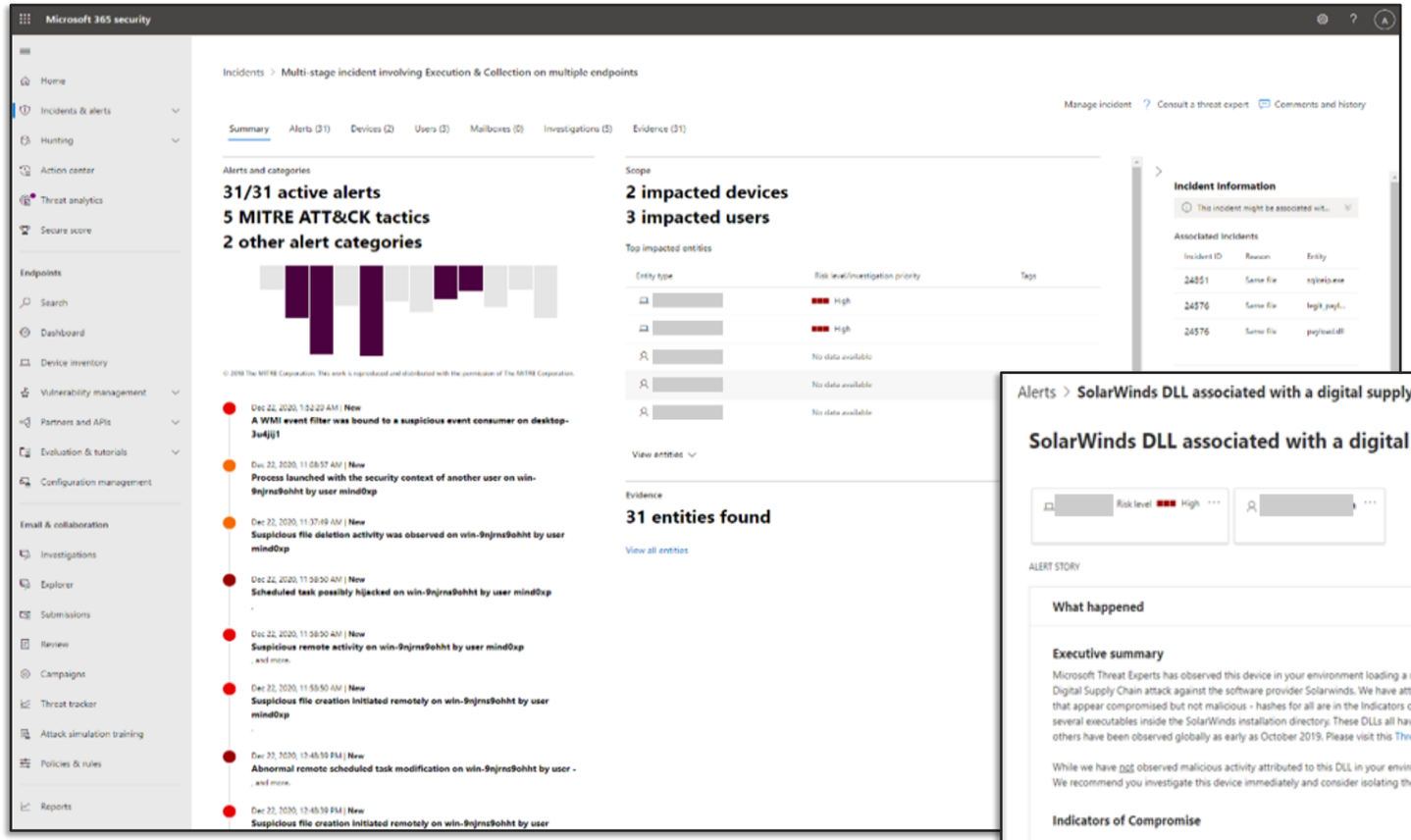
Passare dai singoli silos ad un modello di sicurezza coordinata tra domini che permetta di sfruttare, a scopo preventivo e di risposta, segnali provenienti dai vari strati della nostra dell'infrastruttura

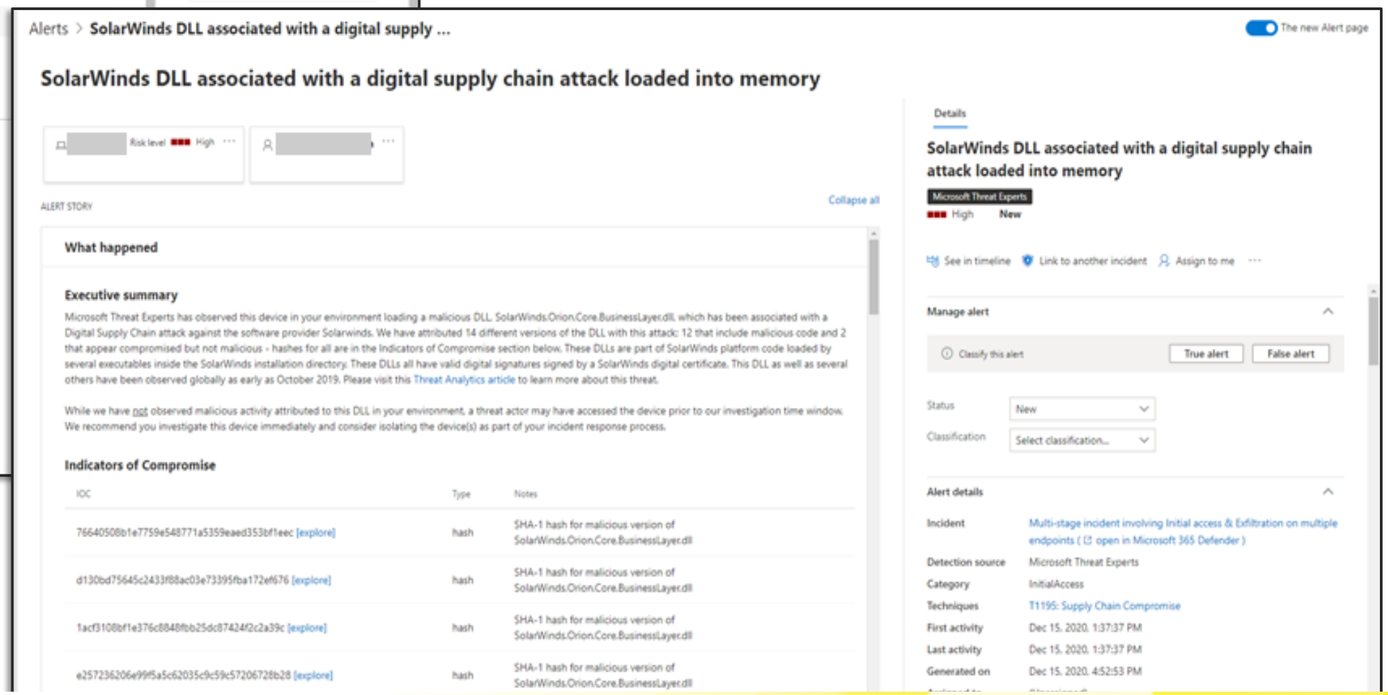


L'attacco Solorigate in M365 Defender Threat Analytics



Analisi di avvisi e incidenti correlati in M365 Defender





Nuovi dati di Azure AD in M365 Defender Advanced Hunting

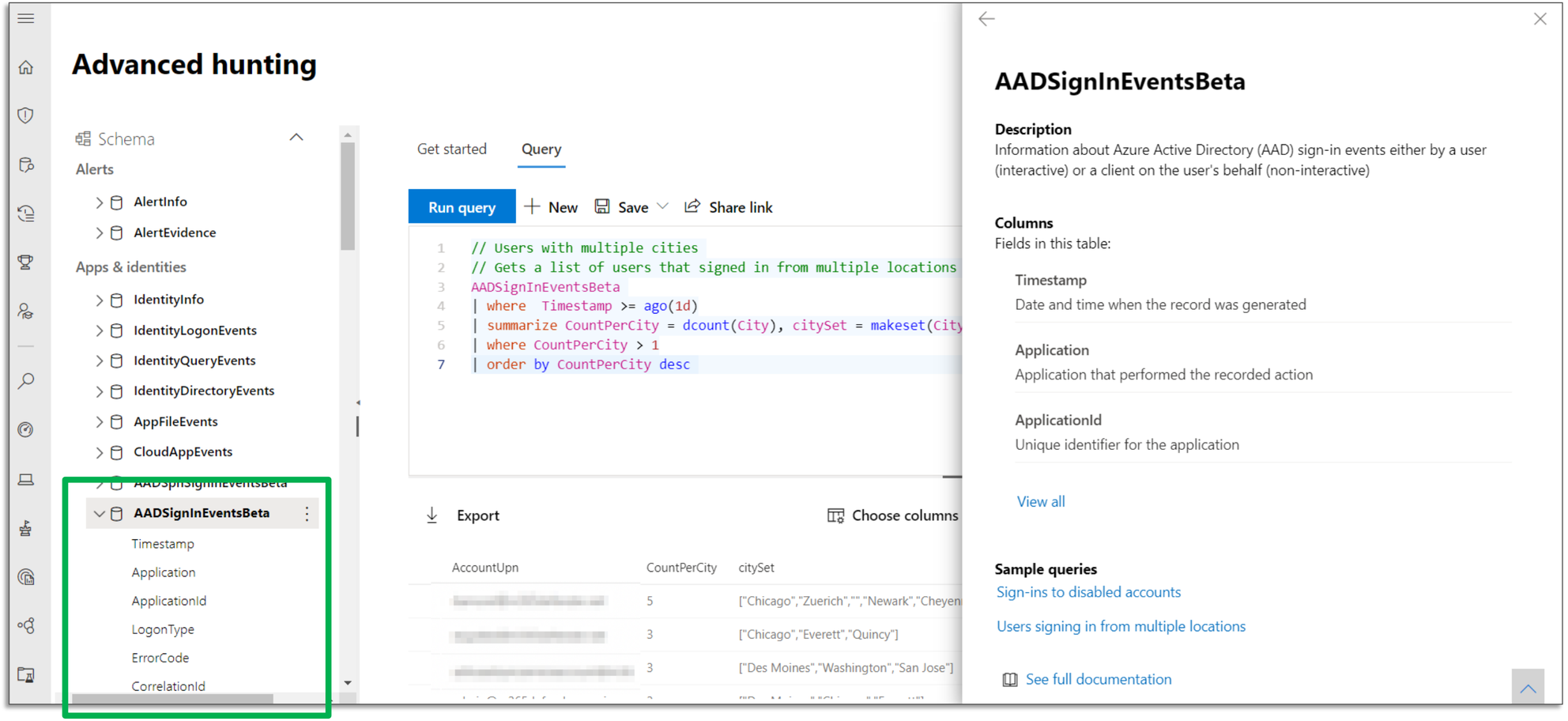
- **Azure Active Directory audit log**
  - Provide traceability for all changes done by various features within Azure AD.
  - Available in CloudAppEvents table:

```
CloudAppEvents
| where Application == "Office 365"
```

- **Azure Active Directory sign-ins**
  - **AADSpnSignInEventsBeta** – includes service principal and managed identities sign-in events
  - **AADSignInEventsBeta** – includes interactive and non-interactive sign-in events

Nuove query sono disponibili online, identificate dal suffisso [Solorigate], GitHub repo.

Nuovi dati di Azure AD in M365 Defender Advanced Hunting



SOLORIGATE ATTACK
Stage 1: Initial access and command-and-control

Streaming Edition

SOLORIGATE ATTACK
Stage 1: Initial access and command-and-control

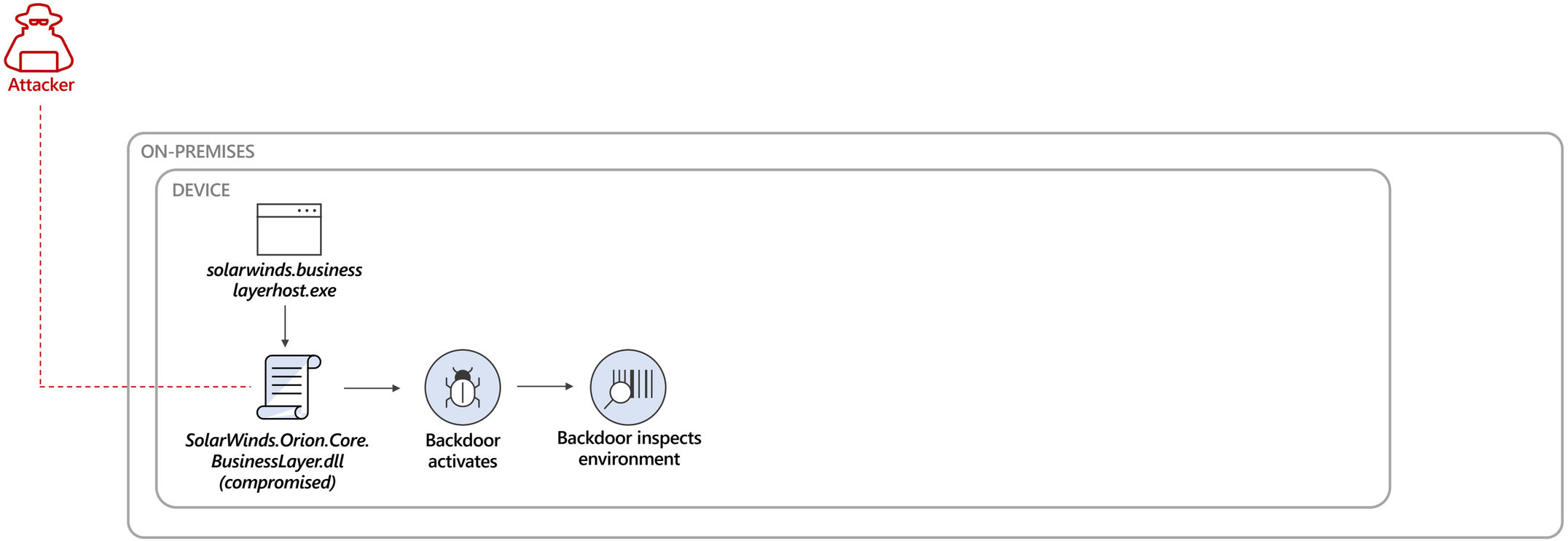
ON-PREMISES

Streaming Edition

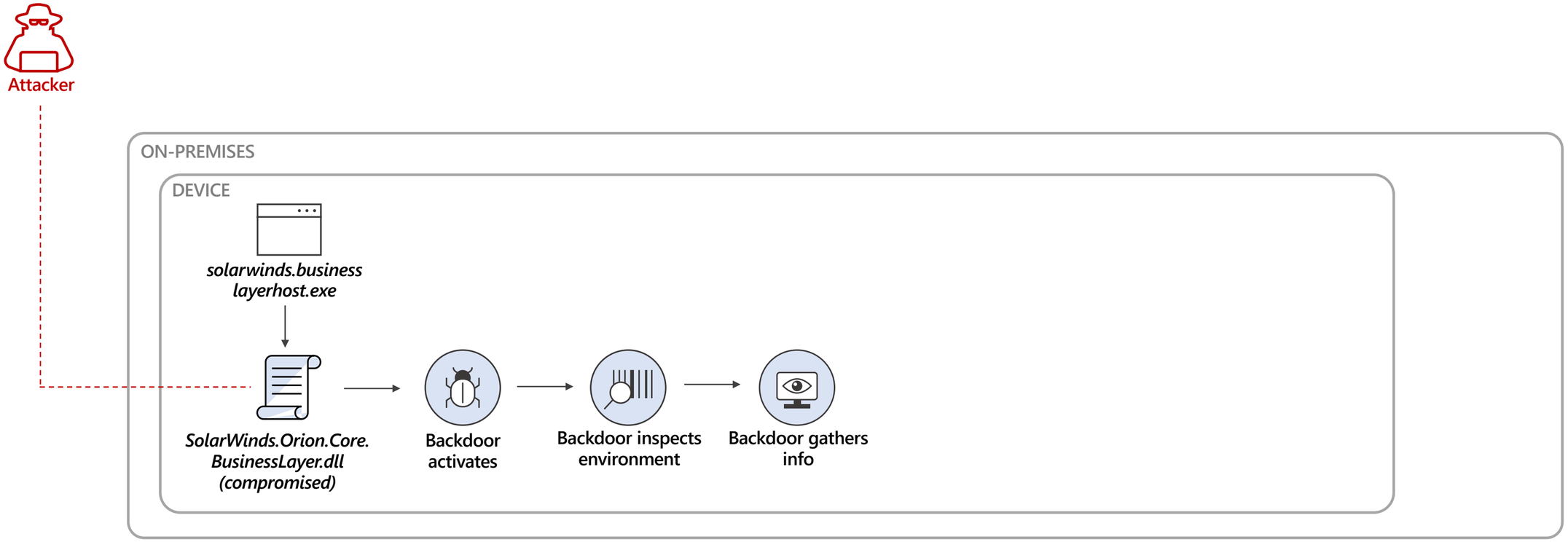
SOLORIGATE ATTACK
Stage 1: Initial access and command-and-control

SOLORIGATE ATTACK
Stage 1: Initial access and command-and-control

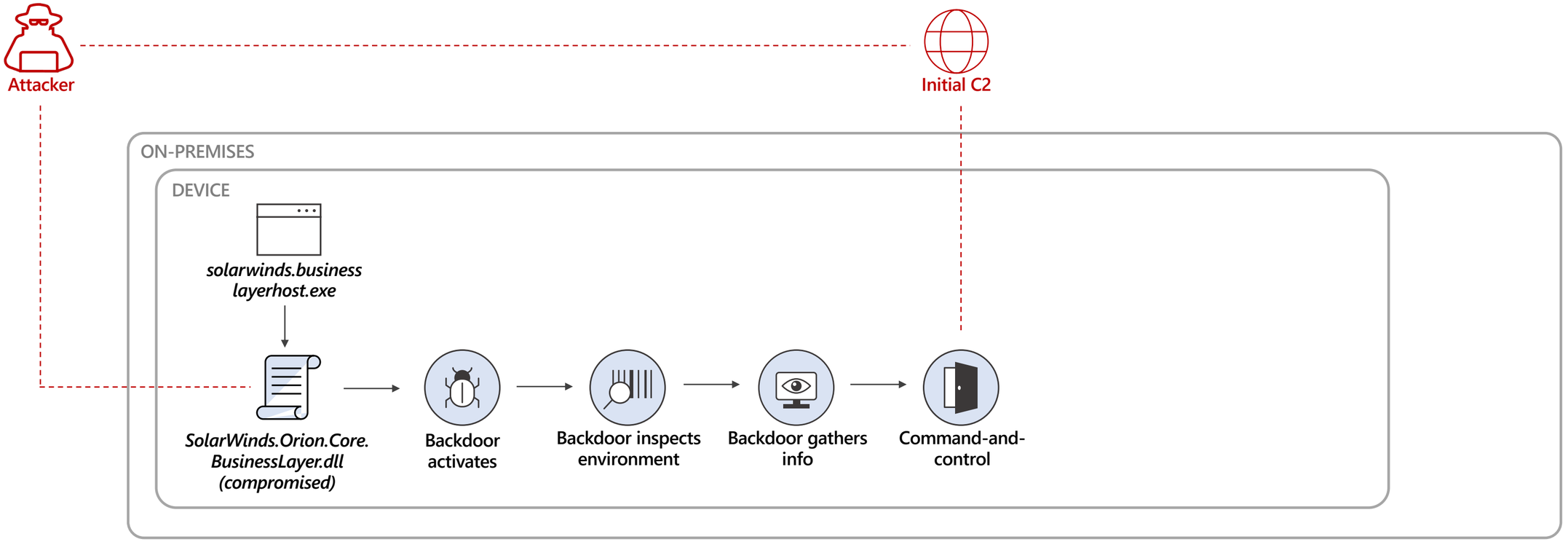
SOLORIGATE ATTACK
Stage 1: Initial access and command-and-control



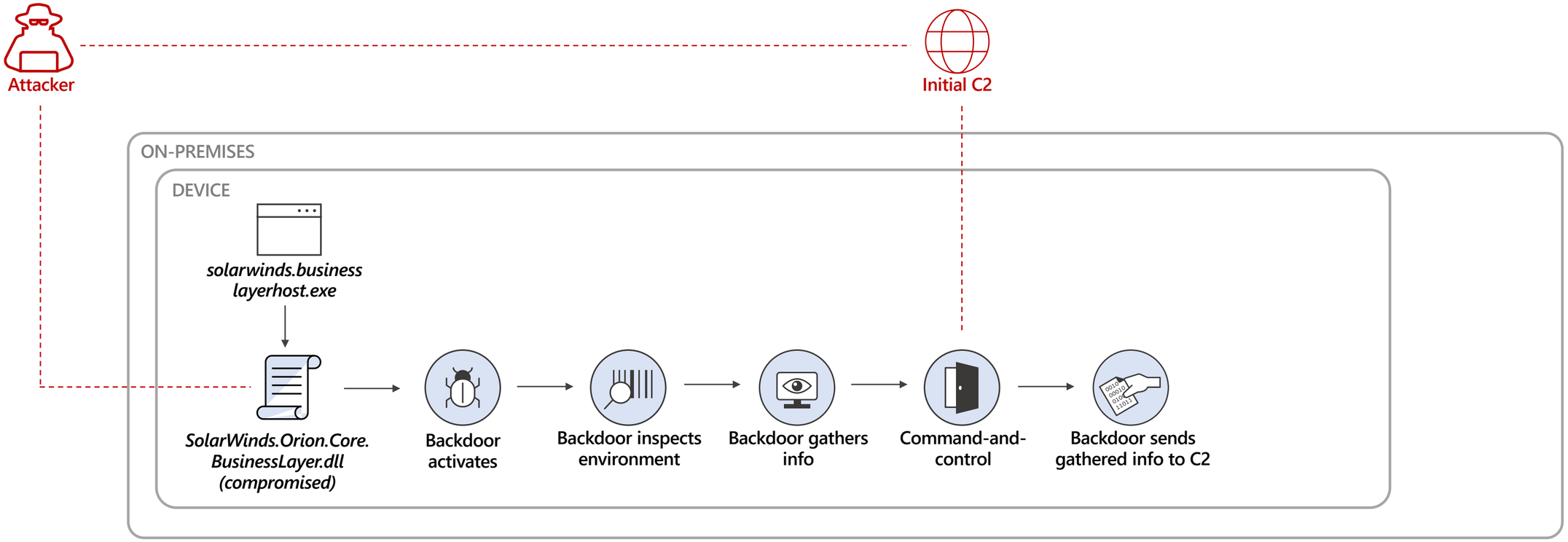
SOLORIGATE ATTACK
Stage 1: Initial access and command-and-control



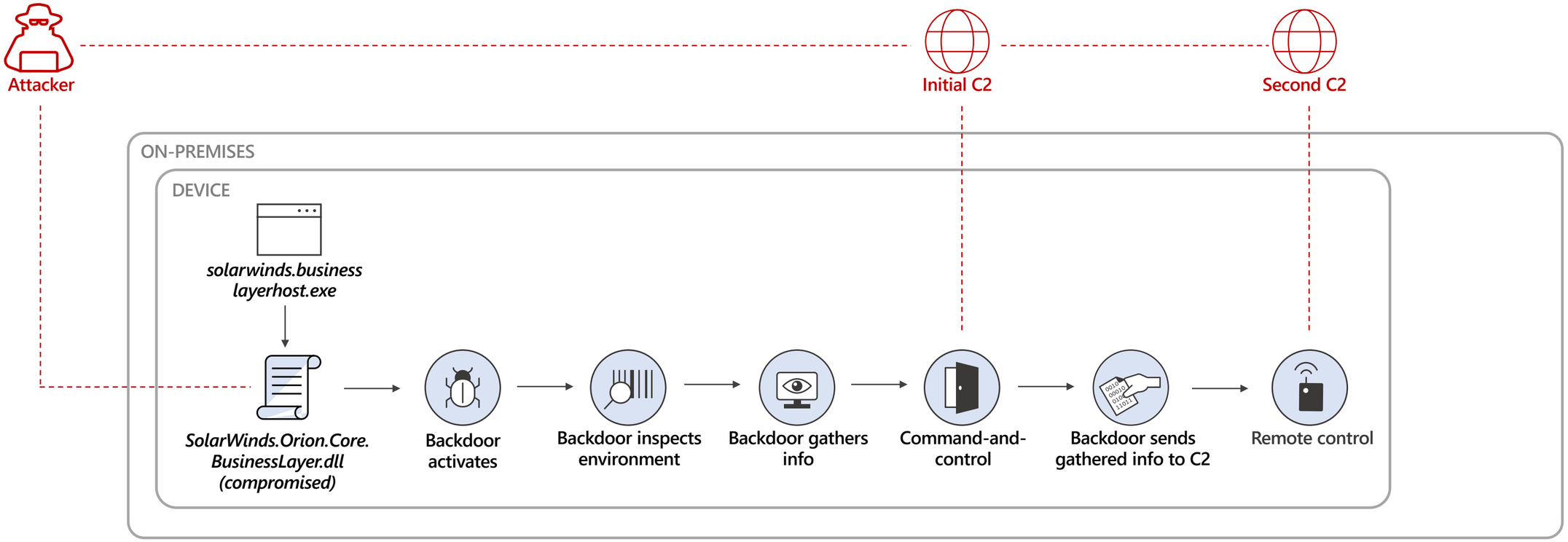
SOLORIGATE ATTACK
Stage 1: Initial access and command-and-control



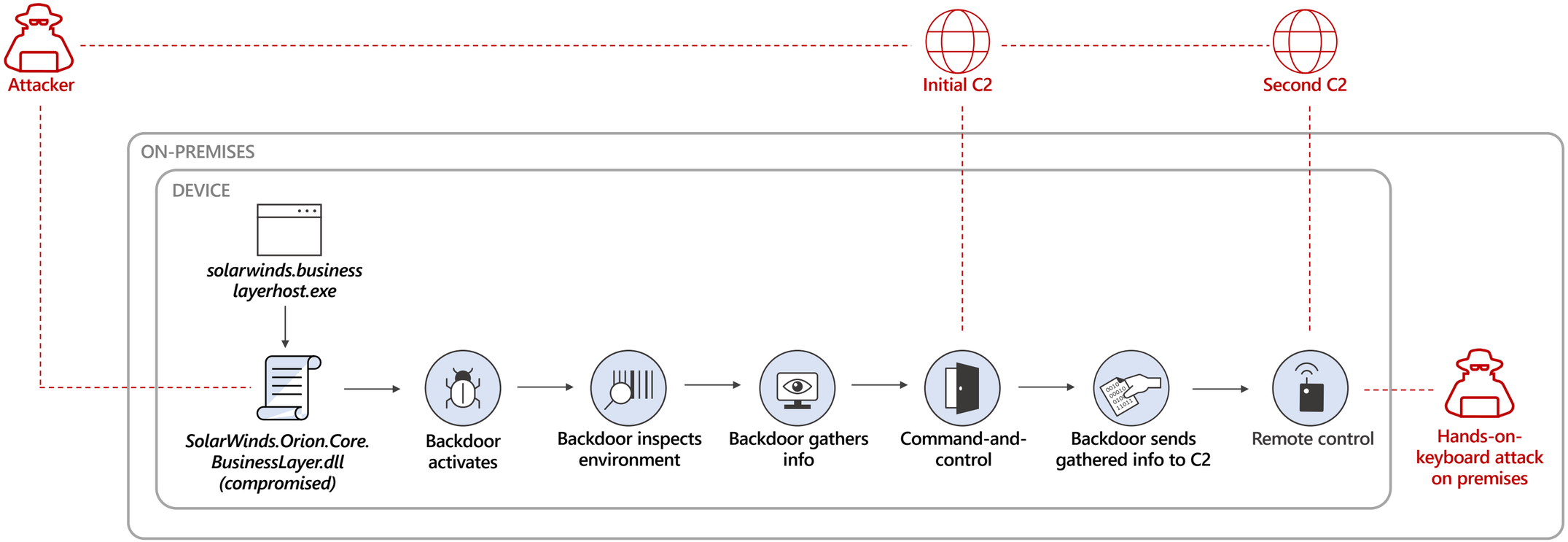
SOLORIGATE ATTACK
Stage 1: Initial access and command-and-control



SOLORIGATE ATTACK
Stage 1: Initial access and command-and-control



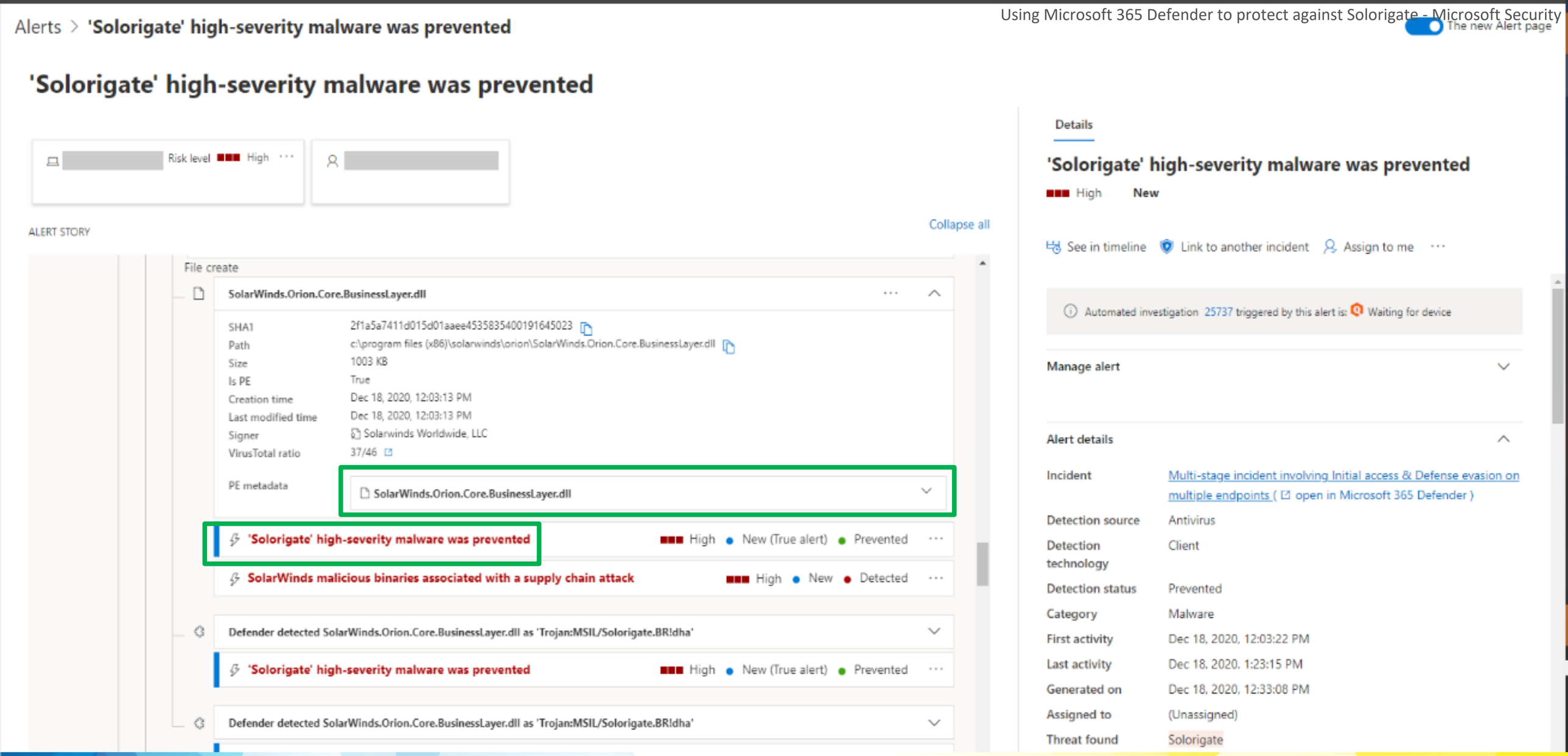
SOLORIGATE ATTACK
Stage 1: Initial access and command-and-control



Serve gestire e proteggere i SO

- Gestire e mantenere aggiornati i SO e gli strumenti di detection e response
- Passare da sistemi tradizionali di detection a sistemi avanzati che permettano l'utilizzo diffuso di tecniche di behavioral analysis (EDR)
- Bloccare gli Endpoint C2 noti e monitorare le attività di rete dei SO
- Ricostruire i sistemi identificati come compromessi dall'aggressore durante l'indagine

Streaming Edition


Alerts > 'Solorigate' high-severity malware was prevented
The new Alert page
'Solorigate' high-severity malware was prevented
Risk level High
ALERT STORY
Collapse all
File create
SolarWinds.Orion.Core.BusinessLayer.dll
SHA1 2f1a5a7411d015d01aaee4535835400191645023
Path c:\program files (x86)\solarwinds\orion\SolarWinds.Orion.Core.BusinessLayer.dll
Size 1003 KB
Is PE True
Creation time Dec 18, 2020, 12:03:13 PM
Last modified time Dec 18, 2020, 12:03:13 PM
Signer Solarwinds Worldwide, LLC
VirusTotal ratio 37/46
PE metadata
SolarWinds.Orion.Core.BusinessLayer.dll
'Solorigate' high-severity malware was prevented High New (True alert) Prevented
SolarWinds malicious binaries associated with a supply chain attack High New Detected
Defender detected SolarWinds.Orion.Core.BusinessLayer.dll as 'Trojan:MSIL/Solorigate.BR!dha'
'Solorigate' high-severity malware was prevented High New (True alert) Prevented
Defender detected SolarWinds.Orion.Core.BusinessLayer.dll as 'Trojan:MSIL/Solorigate.BR!dha'
Details
'Solorigate' high-severity malware was prevented
High New
See in timeline
Link to another incident
Assign to me
Automated investigation 25737 triggered by this alert is: Waiting for device
Manage alert
Alert details
Incident Multi-stage incident involving Initial access & Defense evasion on multiple endpoints (open in Microsoft 365 Defender)
Detection source Antivirus
Detection technology Client
Detection status Prevented
Category Malware
First activity Dec 18, 2020, 12:03:22 PM
Last activity Dec 18, 2020, 1:23:15 PM
Generated on Dec 18, 2020, 12:33:08 PM
Assigned to (Unassigned)
Threat found Solorigate

Alerts > **Network traffic to domains associated with a sup...**

Network traffic to domains associated with a supply chain attack

[redacted] Risk level High ··· [redacted] ···

ALERT STORY

Collapse all

[4984] **SolarWinds.BusinessLayerHost.exe** ···

Suspicious file launch Low New Detected ···

SolarWinds.BusinessLayerHost.exe was dropped remotely from 10.10.50.1 and executed

Source ip	10.10.50.1
Remote share	C$
Action time	Dec 28, 2020, 5:56:20 PM
Mitre techniques	T1021.002: SMB/Windows Admin Shares ; T1570: Lateral Tool Transfer
Copied file	SolarWinds.BusinessLayerHost.exe

File dropped and launched from remote location Medium New Detected ···

Network connect

Outbound connection from 10.10.50.242:49823 to 10.10.50.199:443 ···

Remote IP address	10.10.50.199
Remote port	443
Local port	49823
Action time	Dec 28, 2020, 6:11:38 PM
Resolved Domain	3mu76044hgf7shjq.appsync-api.eu-west-1.avsvmcloud.com

Network traffic to domains associated with a supply chain attack High New Detected ···

[1272] **cmd.exe** /c pause ···

Suspicious process launched using cmd.exe Low New Detected ···

cmd.exe script interpreter process was created by SolarWinds.BusinessLayerHost.exe

Suspicious process launched using cmd.exe Low New Detected ···

Details

Network traffic to domains associated with a supply chain attack

High **New**

See in timeline | Link to another incident | Assign to me | Create a suppression rule ···

Manage alert

Classify this alert — True alert | False alert

Status: New

Classification: Select classification...

Alert details

Incident	Multi-stage incident involving Execution & Command and control on one endpoint (open in Microsoft 365 Defender)
Detection source	EDR
Detection technology	Behavioral, Network
Detection status	Detected
Category	CommandAndControl
First activity	Dec 28, 2020, 6:11:38 PM
Last activity	Dec 28, 2020, 6:11:38 PM
Generated on	Dec 28, 2020, 6:14:15 PM
Assigned to	(Unassigned)

Alert description

A process has attempted to connect to domains known to serve trojanized versions of auto-update software. Connections to these domains can indicate that the machine has received a malicious update and might be under attacker control.

Discovering potentially tampered devices using Advanced Hunting

```
let timeAgo=1d;
let silenceTime=8h;
```

Imposta il lookback per durare 24 ore e i dispositivi non raggiunti per almeno 8 ore

```
let allNetwork=materialize(DeviceNetworkEvents
| where Timestamp > ago(timeAgo)
and isnotempty(LocalIP)
and isnotempty(RemoteIP)
and ActionType in ("ConnectionSuccess", "InboundConnectionAccepted")
and LocalIP !in ("127.0.0.1", "::1")
| project DeviceId, Timestamp, LocalIP, RemoteIP, ReportId);
```

Raccogliere dispositivi con attività di rete

```
let nonSilentDevices=allNetwork
| where Timestamp > ago(silenceTime)
| union (DeviceProcessEvents | where Timestamp > ago(silenceTime))
| summarize by DeviceId;
```

Acquisire dispositivi con attività di processo nelle ultime 8 ore

```
let nonSilentIPs=allNetwork
| where Timestamp > ago(silenceTime)
| summarize by LocalIP;
```

Acquisire gli IP dei dispositivi con l'attività di rete nelle ultime 8 ore

```
let silentDevices=allNetwork
| where DeviceId !in (nonSilentDevices)
and LocalIP !in (nonSilentIPs)
| project DeviceId, LocalIP, Timestamp, ReportId;
```

Acquisire dispositivi senza traffico di rete

```
let addressesDuringSilence=allNetwork
| where Timestamp > ago(silenceTime)
| summarize by RemoteIP;
```

Ottenere tutti gli IP remoti visti di recente come attivi da altri dispositivi

```
silentDevices
| where LocalIP in (addressesDuringSilence)
| summarize ReportId=arg_max(Timestamp, ReportId), Timestamp=max(Timestamp),
LocalIP=arg_max(Timestamp, LocalIP) by DeviceId
| project DeviceId, ReportId=ReportId1, Timestamp, LocalIP=LocalIP1
```

Dispositivi potenzialmente in rete ma che non inviavano dati a Defender

**Information is correct as of Jan 15, 2021. please see aka.ms/solorigate for the most recent updates*

SOLORIGATE ATTACK
Stage 2: Hands-on-keyboard attack on premises

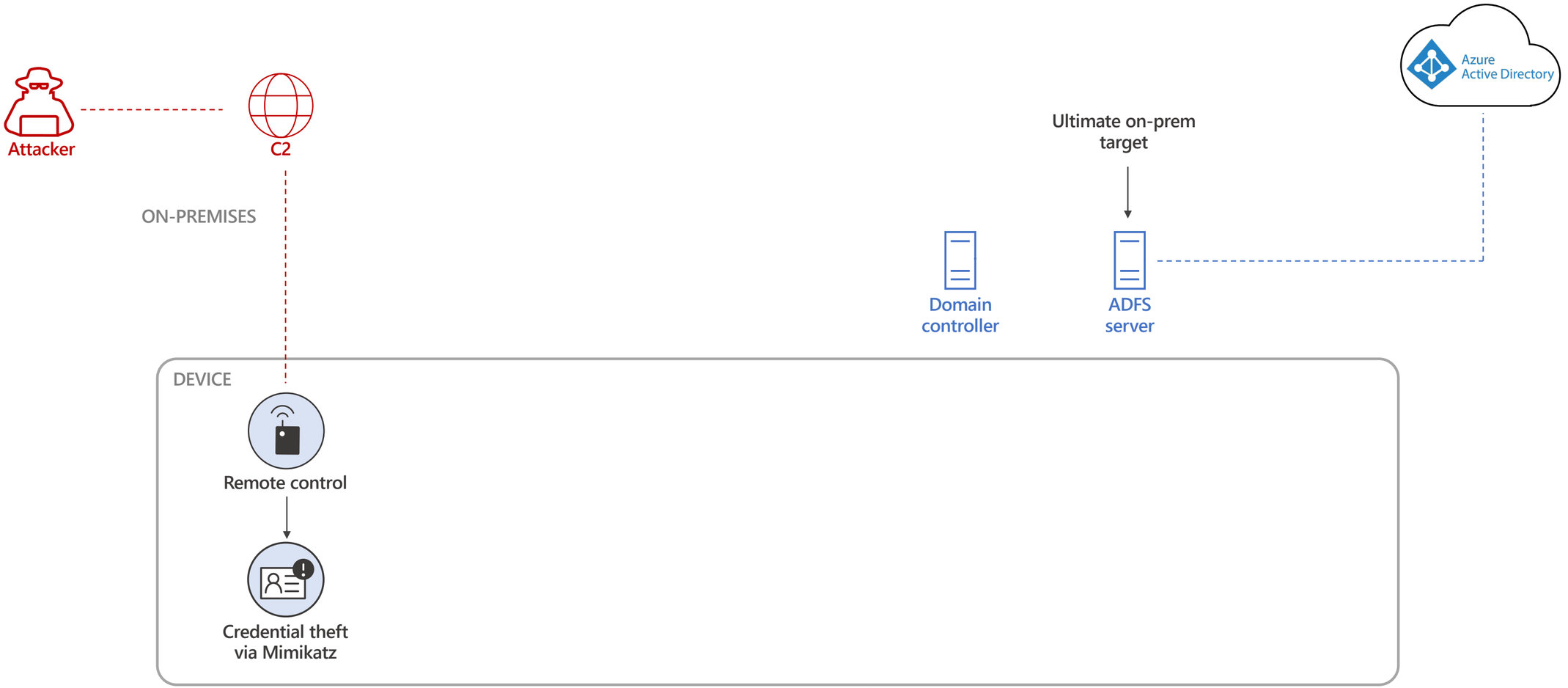
Streaming Edition

SOLORIGATE ATTACK
Stage 2: Hands-on-keyboard attack on premises

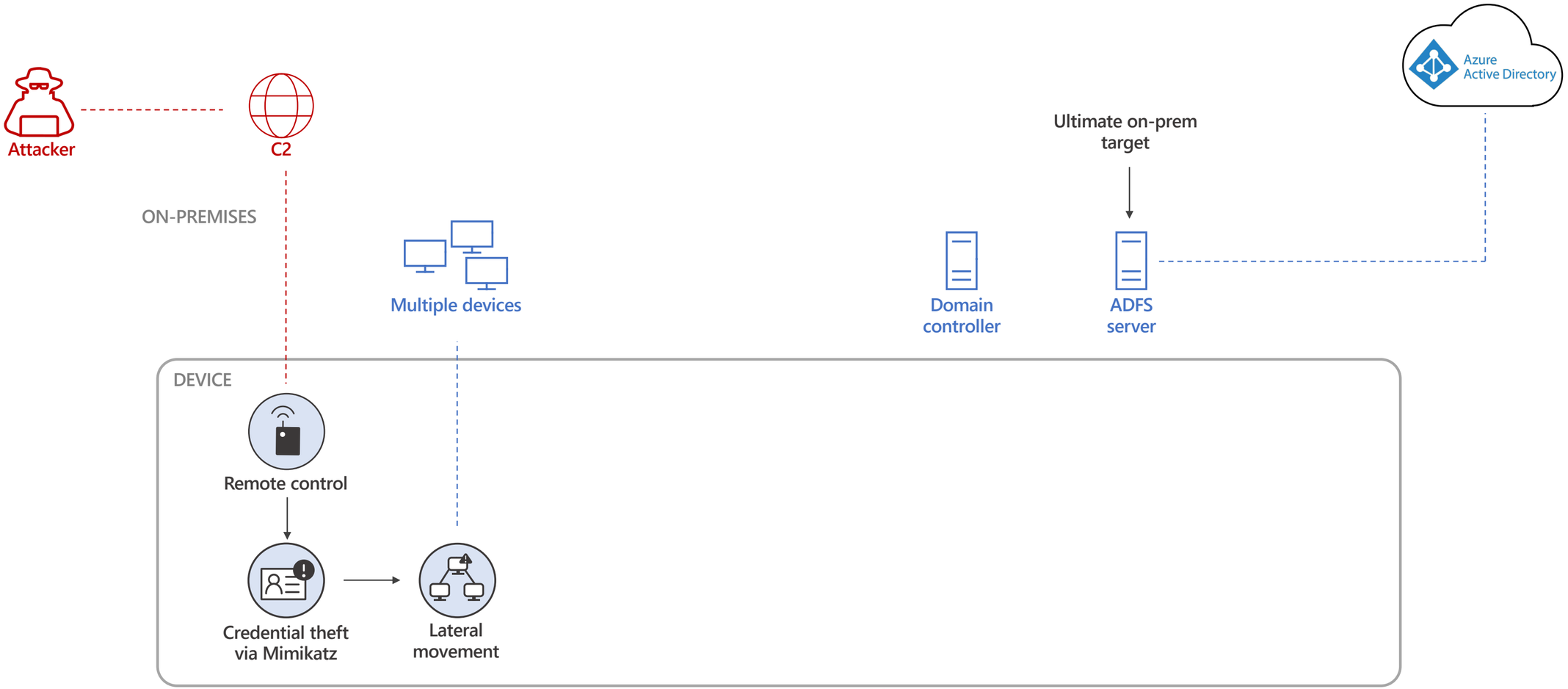
Streaming Edition
SECURITY
SUMMIT
Streaming Edition

SOLORIGATE ATTACK
Stage 2: Hands-on-keyboard attack on premises

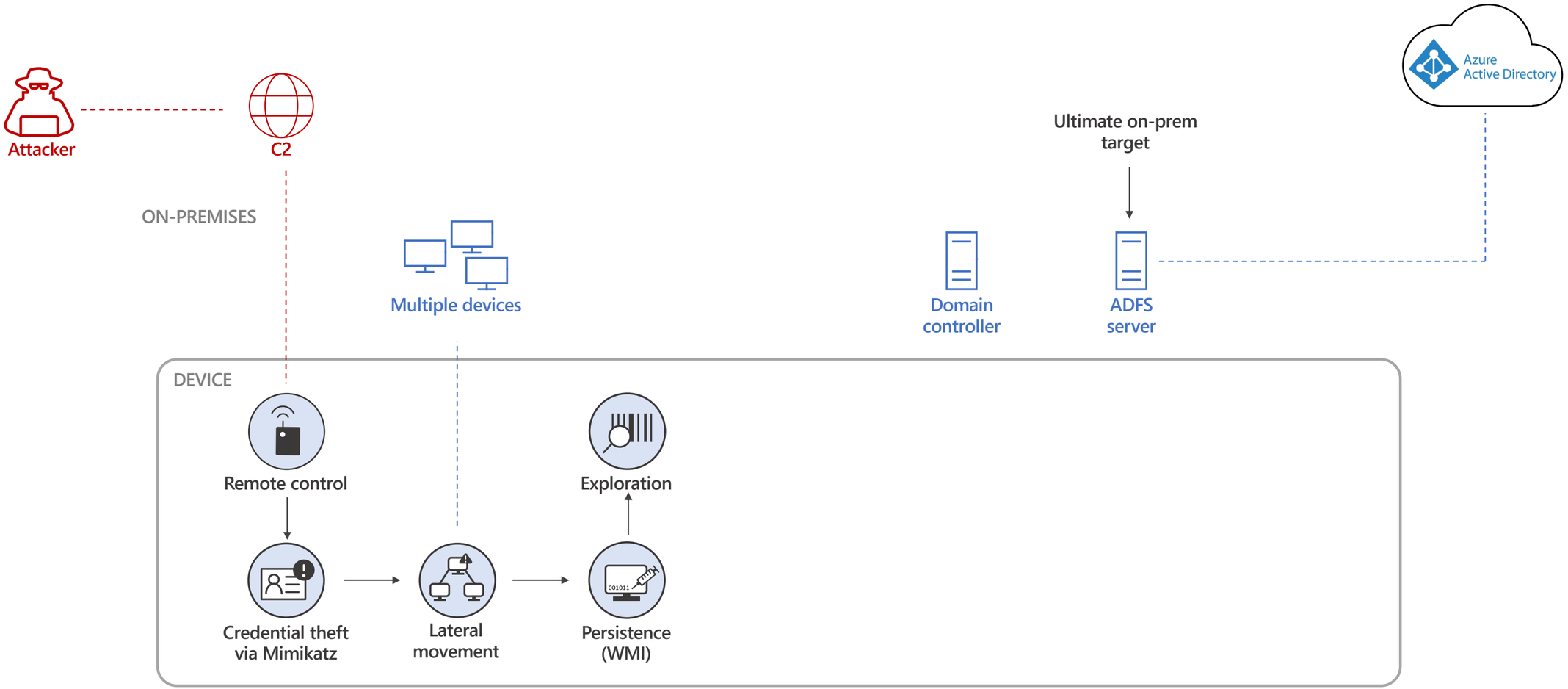
SOLORIGATE ATTACK
Stage 2: Hands-on-keyboard attack on premises



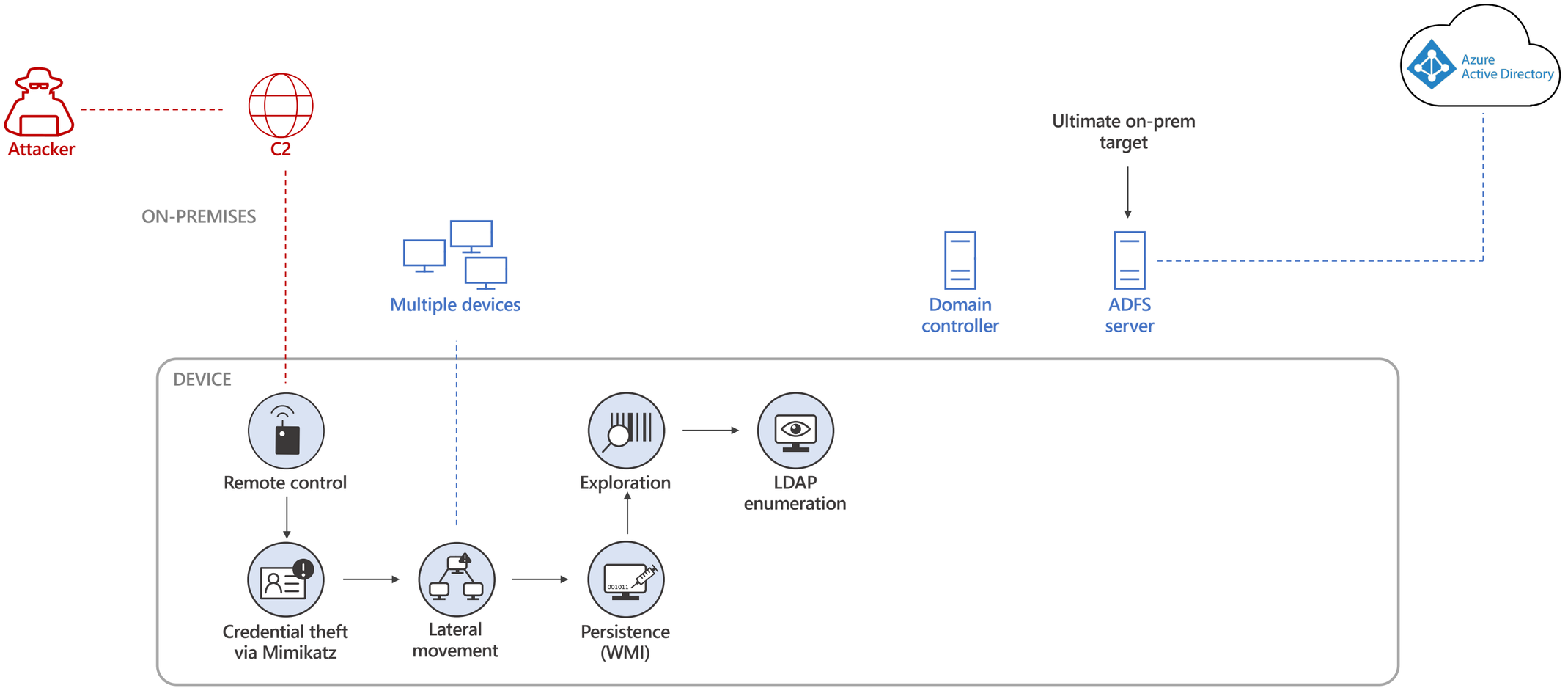
SOLORIGATE ATTACK
Stage 2: Hands-on-keyboard attack on premises



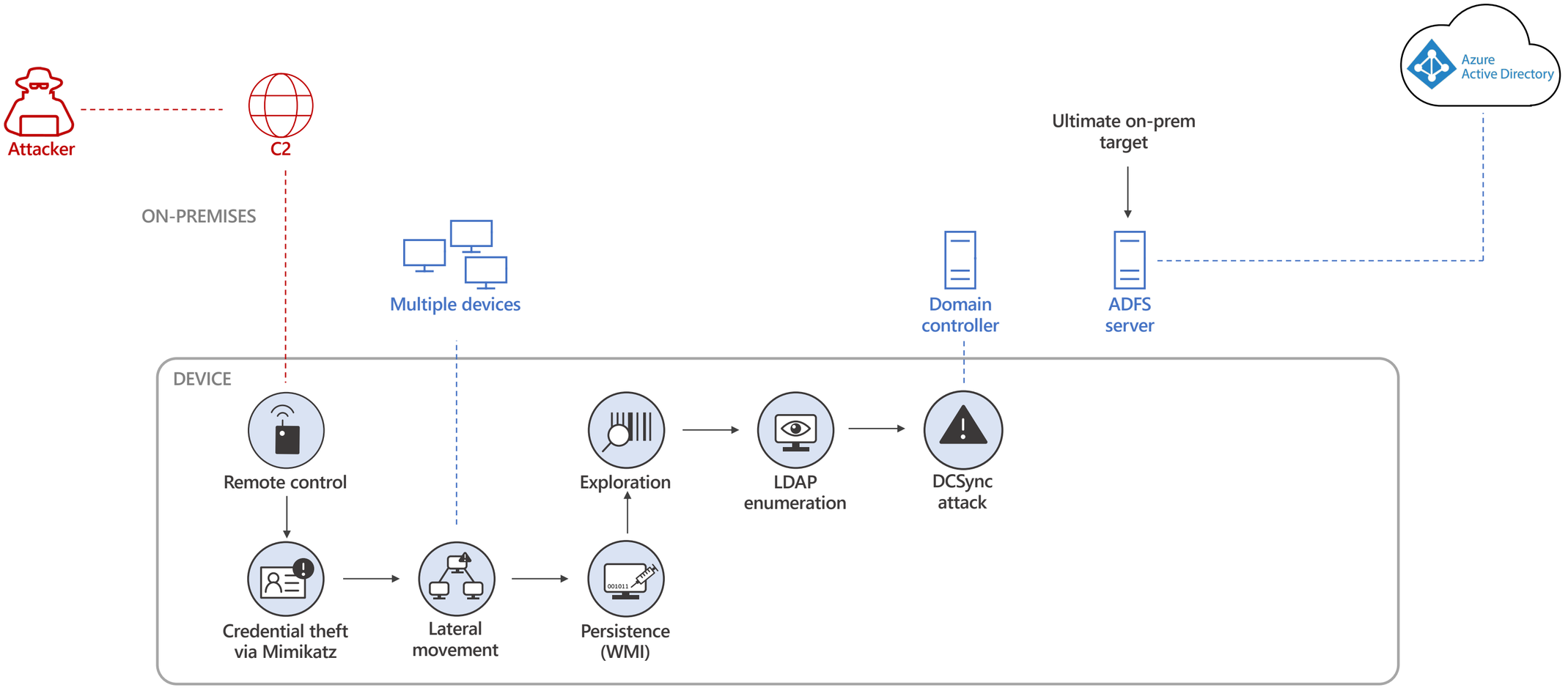
SOLORIGATE ATTACK
Stage 2: Hands-on-keyboard attack on premises



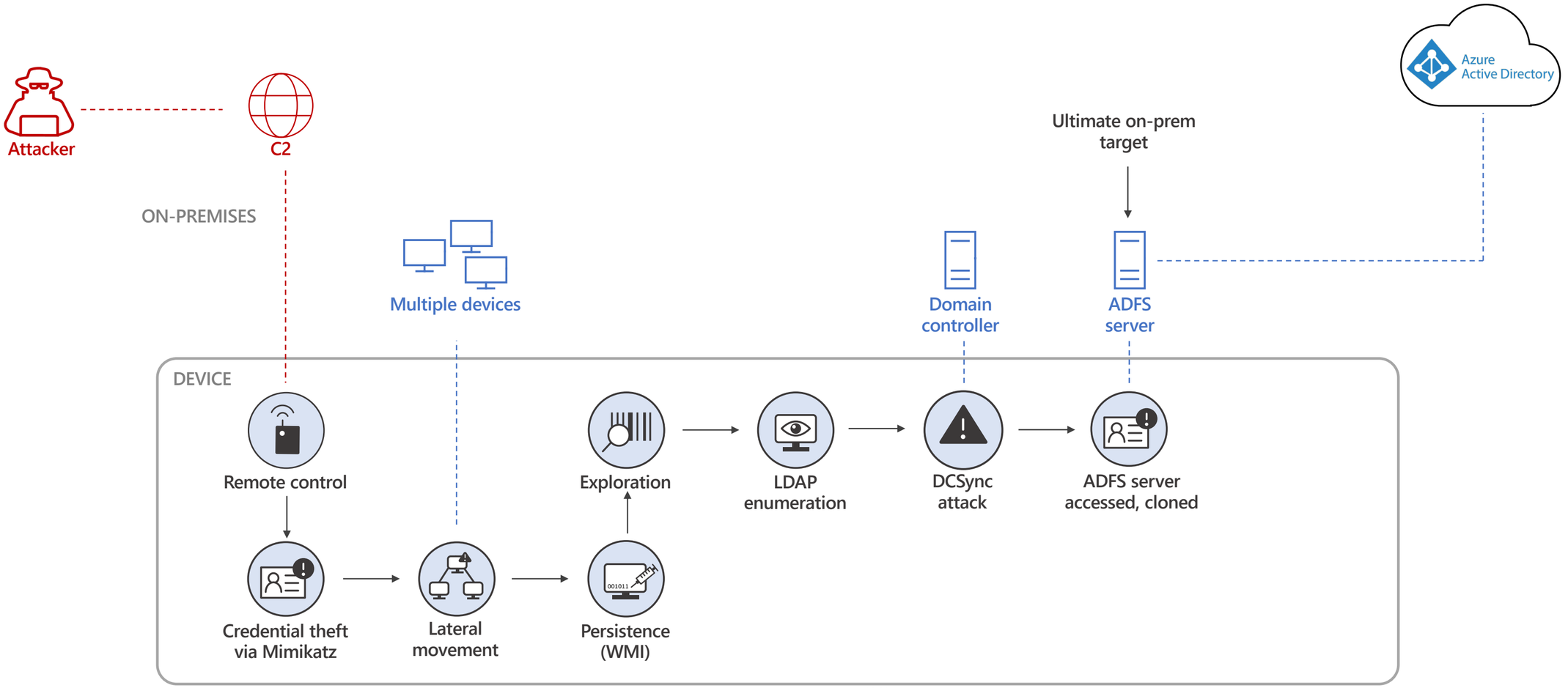
SOLORIGATE ATTACK
Stage 2: Hands-on-keyboard attack on premises



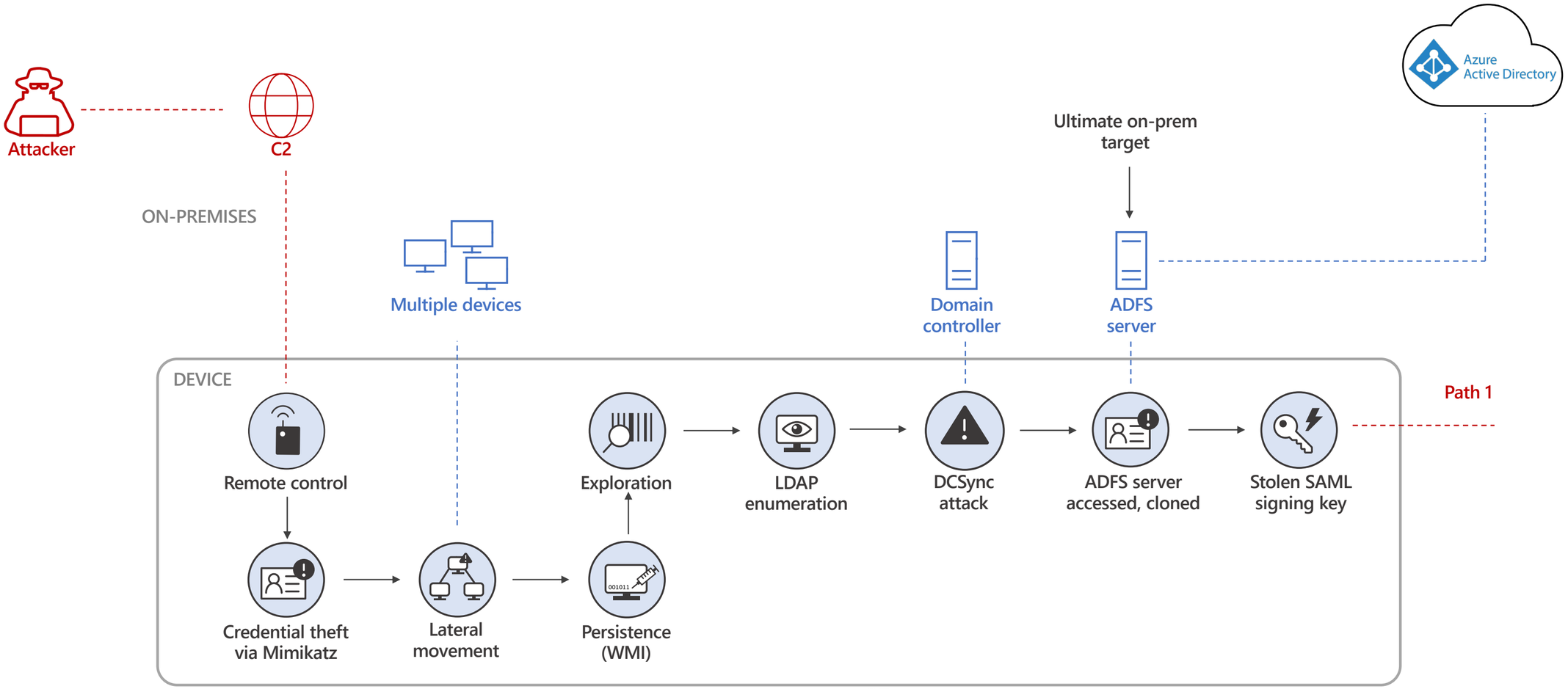
SOLORIGATE ATTACK
Stage 2: Hands-on-keyboard attack on premises



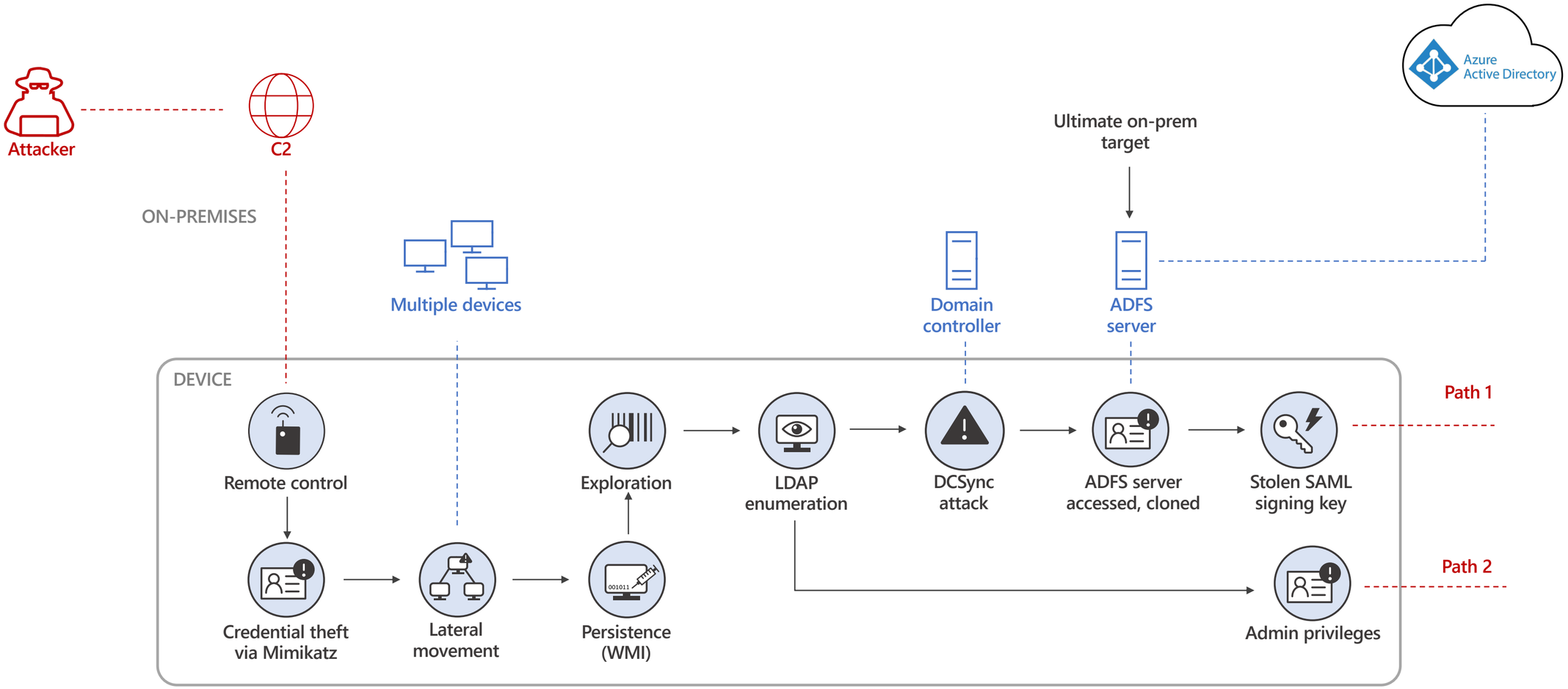
SOLORIGATE ATTACK
Stage 2: Hands-on-keyboard attack on premises



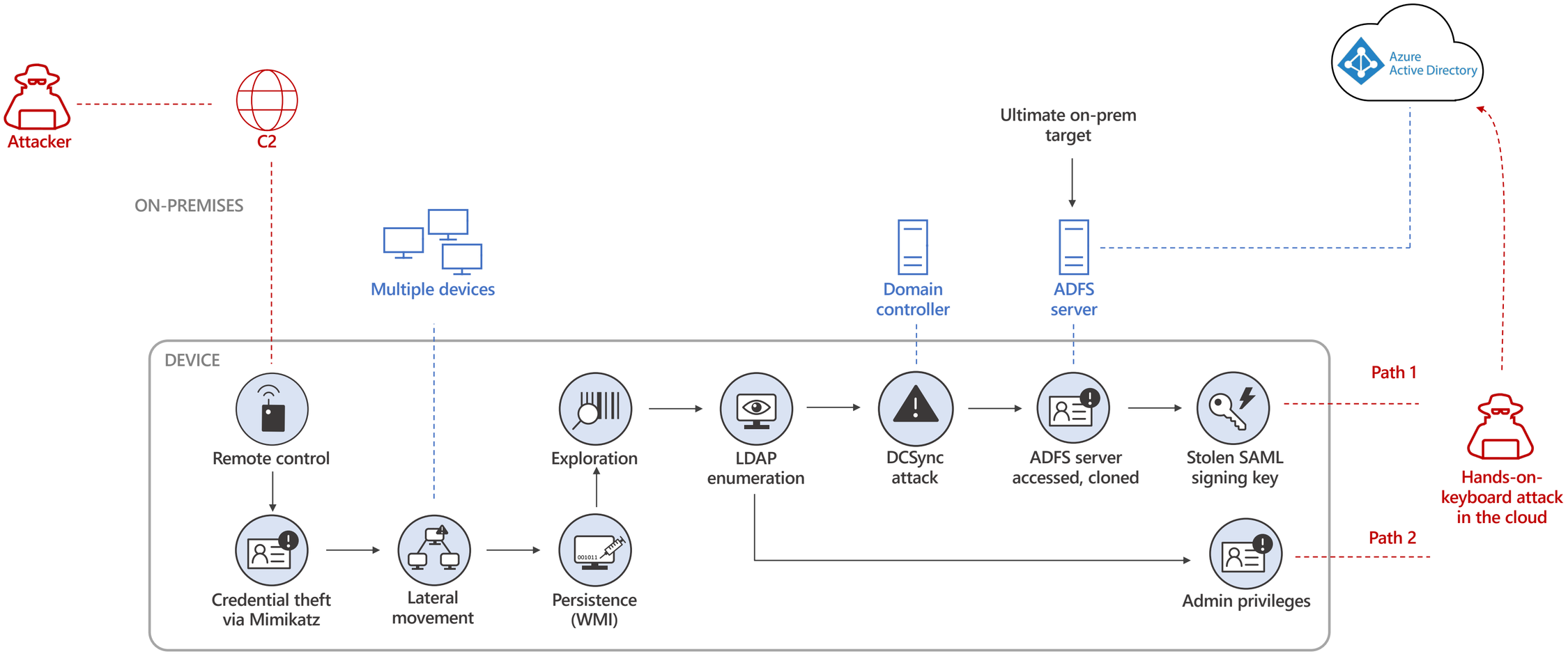
SOLORIGATE ATTACK
Stage 2: Hands-on-keyboard attack on premises



SOLORIGATE ATTACK
Stage 2: Hands-on-keyboard attack on premises



SOLORIGATE ATTACK
Stage 2: Hands-on-keyboard attack on premises

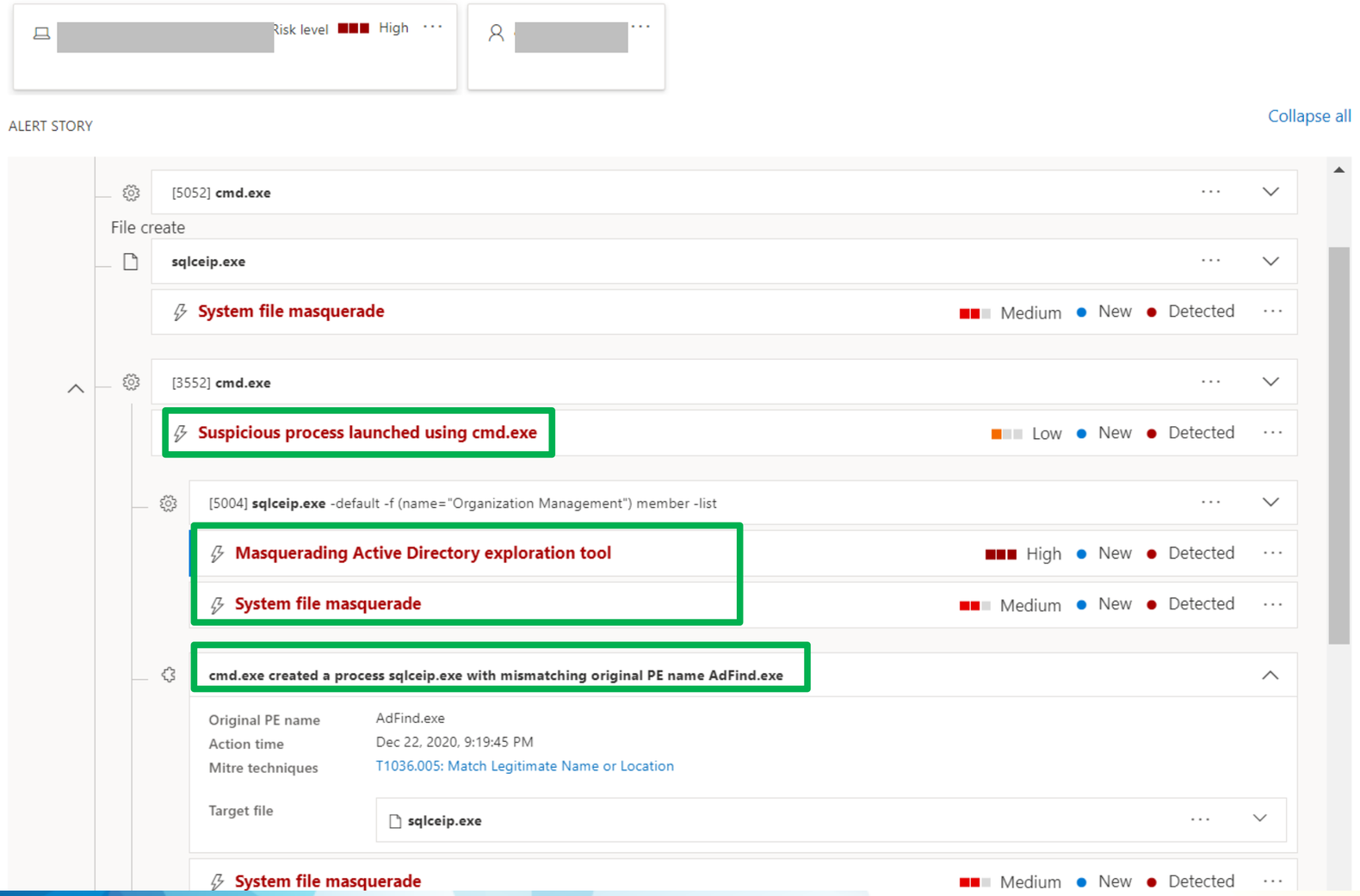


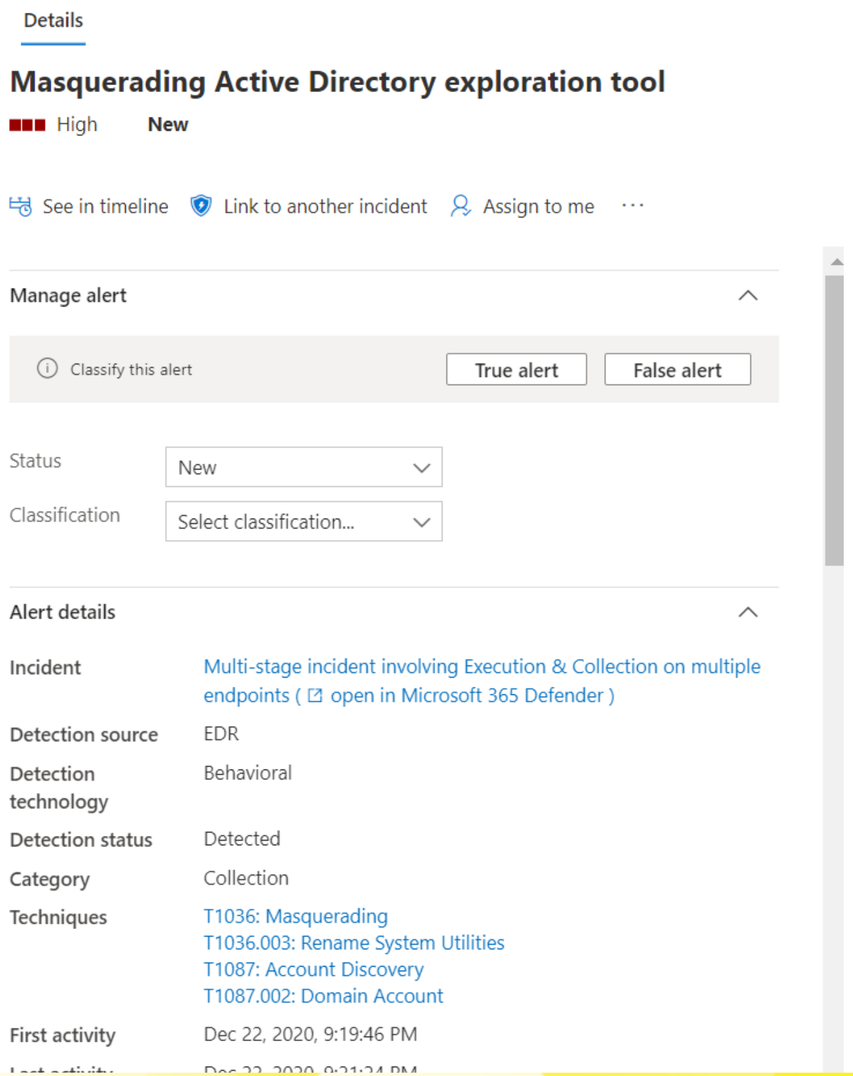
Serve gestire e proteggere le identità privilegiate e i servizi di autenticazione

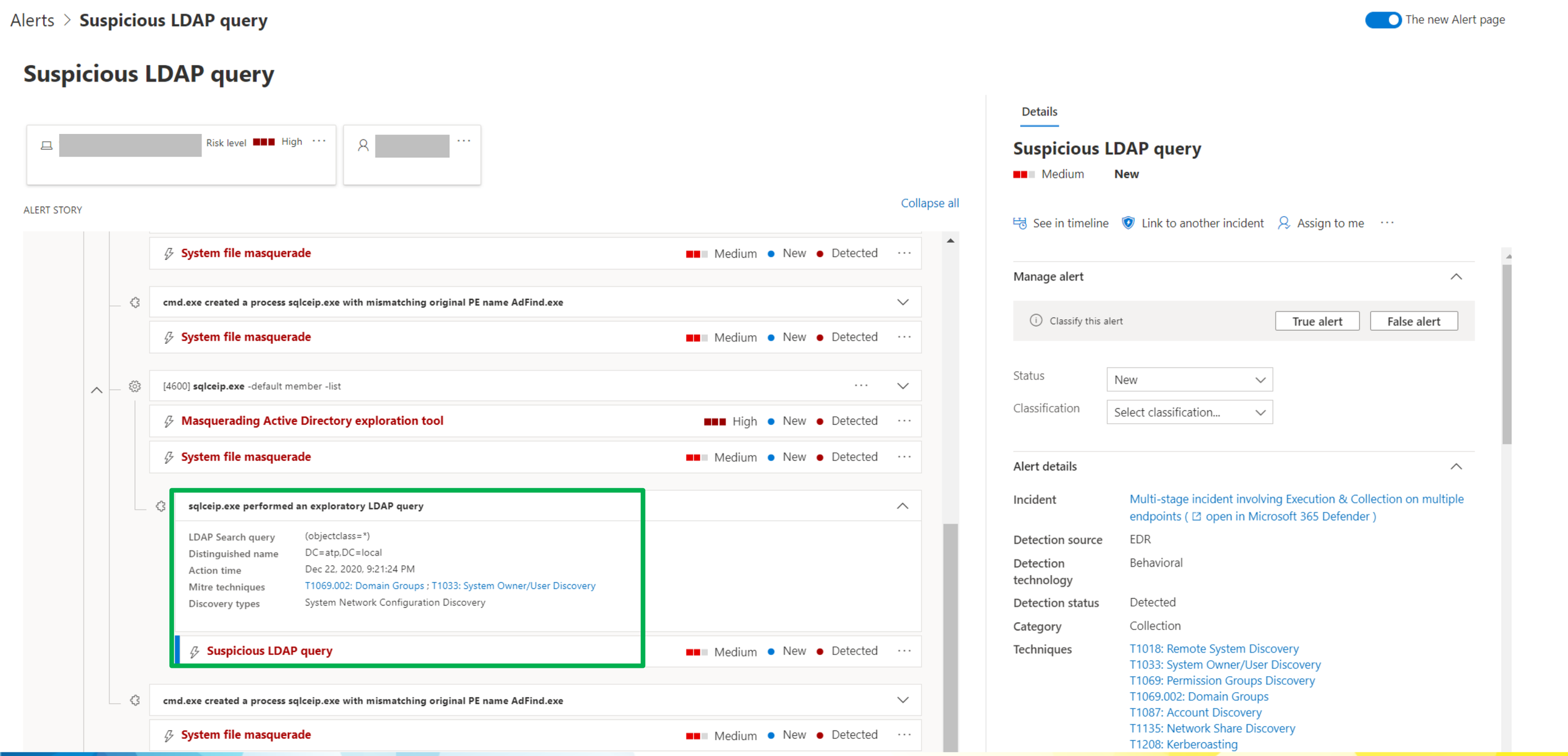
- Abilitare strumenti di detection dei path di attacco sul dominio Active Directory
- Mettere in sicurezza le chiavi di firma dei token SAML
- Utilizzare strumenti di gestione e monitoraggio delle utenze privilegate JIT/JEA, PAW eliminando le membership permanenti ai gruppi amministrativi
- Abilitare soluzioni di strong authentication per tutti gli utenti
- Valutare l'impiego di autenticazione su Azure Active Directory

Streaming Edition

Masquerading Active Directory exploration tool







Streaming Edition
SECURITY SUMMIT
Streaming Edition

Discovering high-volume LDAP queries using Advanced Hunting in M365 Defender

```
let Threshold = 12;
let BinTime = 1m;
```

```
let listDC=IdentityDirectoryEvents
| where Application == "Active Directory"
| where ActionType == "Directory Services replication"
| summarize by DestinationDeviceName;
```

```
IdentityQueryEvents
| where Timestamp > ago(30d)
| where DeviceName !in (listDC)
| where ActionType == "LDAP query"
| parse Query with * "Search Scope: " SearchScope ", Base Object:" BaseObject ", Search Filter: " SearchFilter
| summarize NumberOfDistinctLdapQueries = dcount(SearchFilter) by DeviceName, bin(Timestamp, BinTime)
| where NumberOfDistinctLdapQueries > Threshold
```

Impostare finestre di 1 minuto e una soglia di 12 query LDAP distinte

Creare un elenco di controller di dominio

Escludere il traffico da controller di dominio a cc

Contare query LDAP distinte al minuto su tutti i dispositivi. Mostrami i dispositivi che hanno superato le 12 query distinte al minuto

E adesso?

Utilizzare l'elenco risultante per analizzare e isolare i dispositivi e bloccare il payload eseguito. Contrassegnare gli utenti connessi come compromessi.

**Information is correct as of Jan 15, 2021. please see aka.ms/solorigate for the most recent updates*

Suspicious Remote WMI Execution

Risk level High

at

ALERT STORY

Collapse all

[4284] **WmiPrvSE.exe** -secured -Embedding

[3340] **rundll32.exe** rundll32 c:\windows\legit_payload.dll EntryPoint

Suspicious behavior by a svchost.exe was observed Medium New Detected

Process launched with the security context of another user Low New Detected

rundll32.exe was invoked remotely

Execution type Wmi
Source machine name WINDOWS10-ATP-X
Mitre techniques T ement Instrumentation

Source machine ip a... 10.10.50.110

Suspicious Remote WMI Execution Medium New Detected

rundll32.exe process was created from a remote machine 'WINDOWS10-ATP-X' using Windows Management Instrumentation (WMI)

Suspicious WMI process creation Medium New Detected

rundll32.exe process was created from a remote machine 'WINDOWS10-ATP-X' using Windows Management Instrumentation (WMI)

Execution source Remote
Remote machine Ne... WINDOWS10-ATP-X
Remote machine FQ... W local
Action time D
Mitre techniques T1047: Windows Management Instrumentation

Details

Suspicious Remote WMI Execution

Medium **New**

See in timeline | Link to another incident | Assign to me ...

Automated investigation 27604 triggered by this alert is: No threats found

Manage alert

Classify this alert True alert False alert

Status New

Classification Select classification...

Alert details

Incident	Multi-stage incident involving Execution & Collection on multiple endpoints (open in Microsoft 365 Defender)
Detection source	EDR
Detection technology	Behavioral, Network
Detection status	Detected
Category	LateralMovement
Techniques	T1047: Windows Management Instrumentation
First activity	Dec 22, 2020, 6:14:58 PM
Last activity	Dec 22, 2020, 6:14:58 PM
Generated on	Dec 22, 2020, 6:25:50 PM
Assigned to	Automation

Streaming Edition

SECURITY SUMMIT

Streaming Edition

Alerts > **A WMI event filter was bound to a suspicious ev...**

The new Alert page

A WMI event filter was bound to a suspicious event consumer

Risk level High ···

ALERT STORY

Collapse all

Windows Management Instrumentation (WMI) binding event filter to consumer

Consumer	CommandLineEventConsumer="OfficeLauncherConsumer"
Ess	OfficeLauncherEvent
Namespace	//./root/subscription
Possible cause	Binding EventFilter: instance of __EventFilter { Creat...
Mitre techniques	T1546.003: Windows Management Instrumentatic

A WMI event filter was bound to a suspicious event consu

dium New Detected ···

```
Binding EventFilter:
instance of __EventFilter
{
CreatorSID = {1, 5, 0, 0, 0, 0, 0, 5, 21, 0, 0, 0, 117, 61, 61, 178,
179, 75, 246, 184, 181, 65, 166, 61, 233, 3, 0, 0};
EventNamespace = "root\\cimv2";
Name = "OfficeLauncherEvent";
Query = "SELECT * FROM __InstanceModificationEvent
WITHIN 60 WHERE TargetInstance ISA
'Win32_PerfFormattedData_PerfOS_System' AND
TargetInstance.SystemUpTime >= 200 AND
TargetInstance.SystemUpTime < 320";
QueryLanguage = "WQL";
};
Perm. Consumer:
instance of CommandLineEventConsumer
{
CommandLineTemplate = "rundll32.exe
c:\\windows\\temp\\error.dll,MainFunc";
CreatorSID = {1, 5, 0, 0, 0, 0, 0, 5, 21, 0, 0, 0, 117, 61, 61, 178,
179, 75, 246, 184, 181, 65, 166, 61, 233, 3, 0, 0};
Name = "OfficeLauncherConsumer";
};
```

45

Details

A WMI event filter was bound to a suspicious event consumer

Medium **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 & Collection on multiple endpoints (open in Microsoft 365 Defender)
Detection source	EDR
Detection technology	Behavioral
Detection status	Detected
Category	Persistence
Techniques	T1084: Windows Management Instrumentation Event Subscription T1546.003: Windows Management Instrumentation Event Subscription

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

Defender for Identity Alert

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

ADFS private key extraction attempt

The new Alert page

Defender for Identity Alert

Risk level High

ALERT STORY

[4280] SecurityHealthSystray.exe

[7448] OneDrive.exe /background

File create

dump_em_all.exe

Suspicious file dropped

[7956] dump_em_all.exe

Image load

dump_em_all.exe

Suspicious file dropped

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

Active Directory attributes Reconnaissance using LDAP

An actor on [redacted] sent a suspicious LDAP query, searching for ADFS_Key on [redacted]

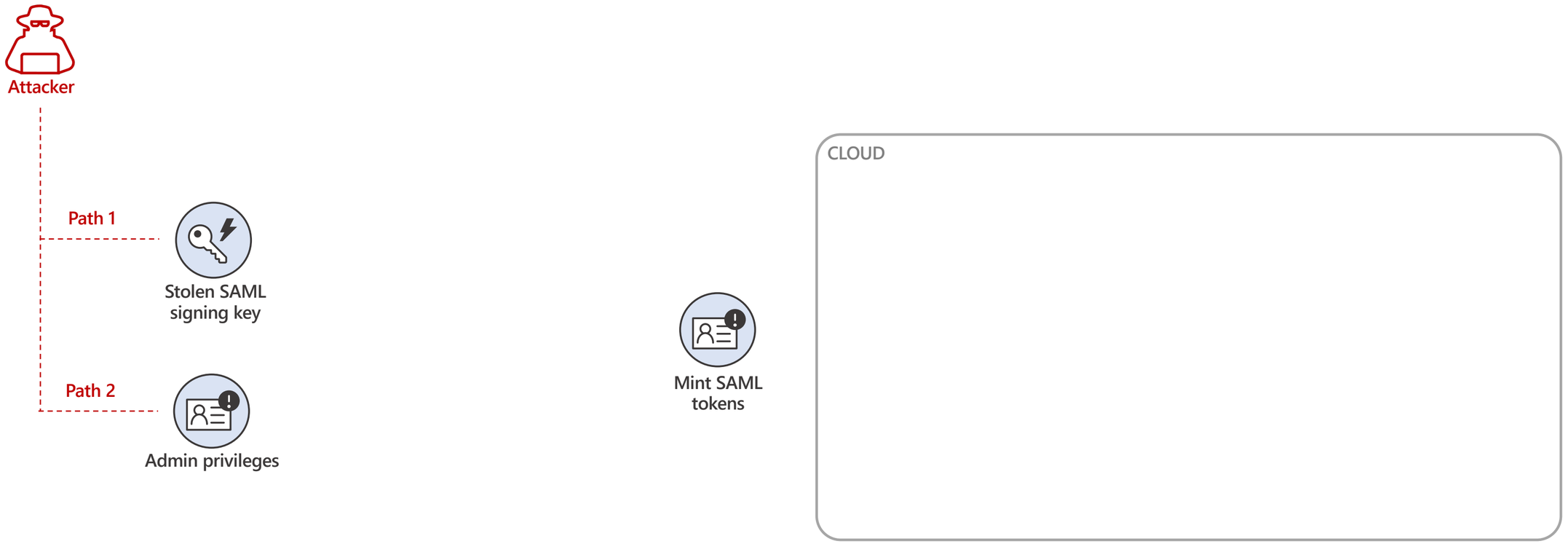
3:50 PM Dec 21, 2020

Detection technology	Behavioral
Detection status	Detected
Category	CredentialAccess
Techniques	T1003: OS Credential Dumping

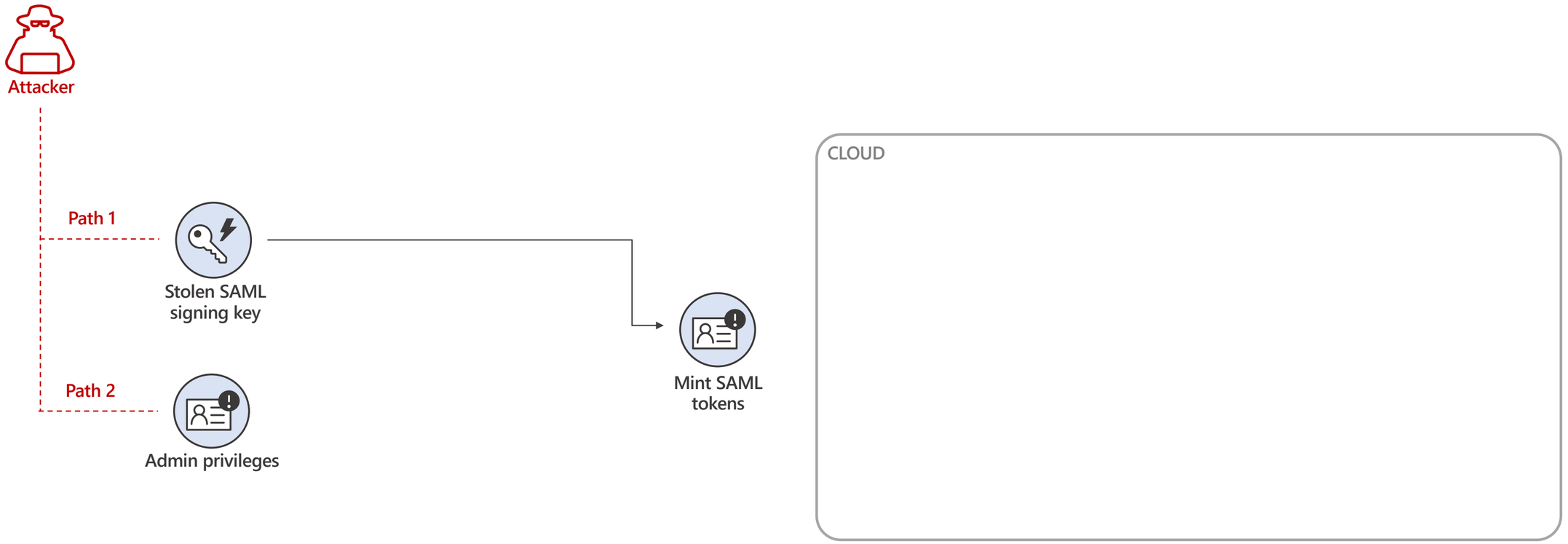
SOLORIGATE ATTACK
Stage 3: Hands-on-keyboard attack in the cloud

Streaming Edition

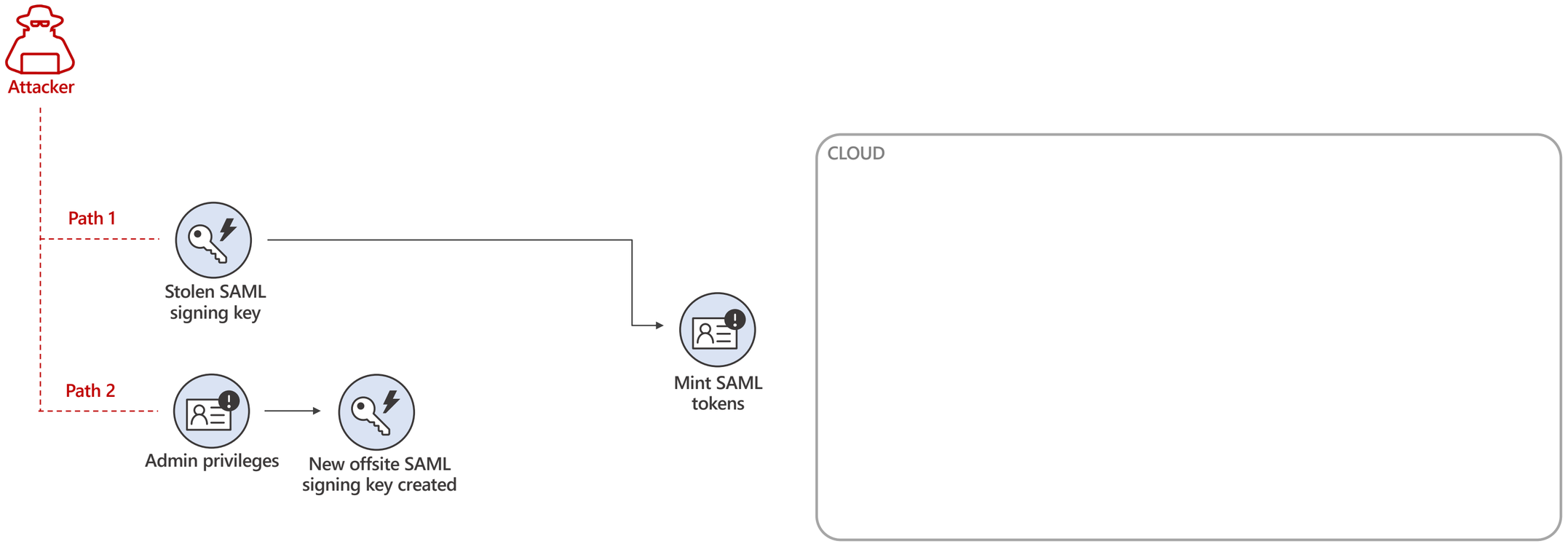
SOLORIGATE ATTACK
Stage 3: Hands-on-keyboard attack in the cloud



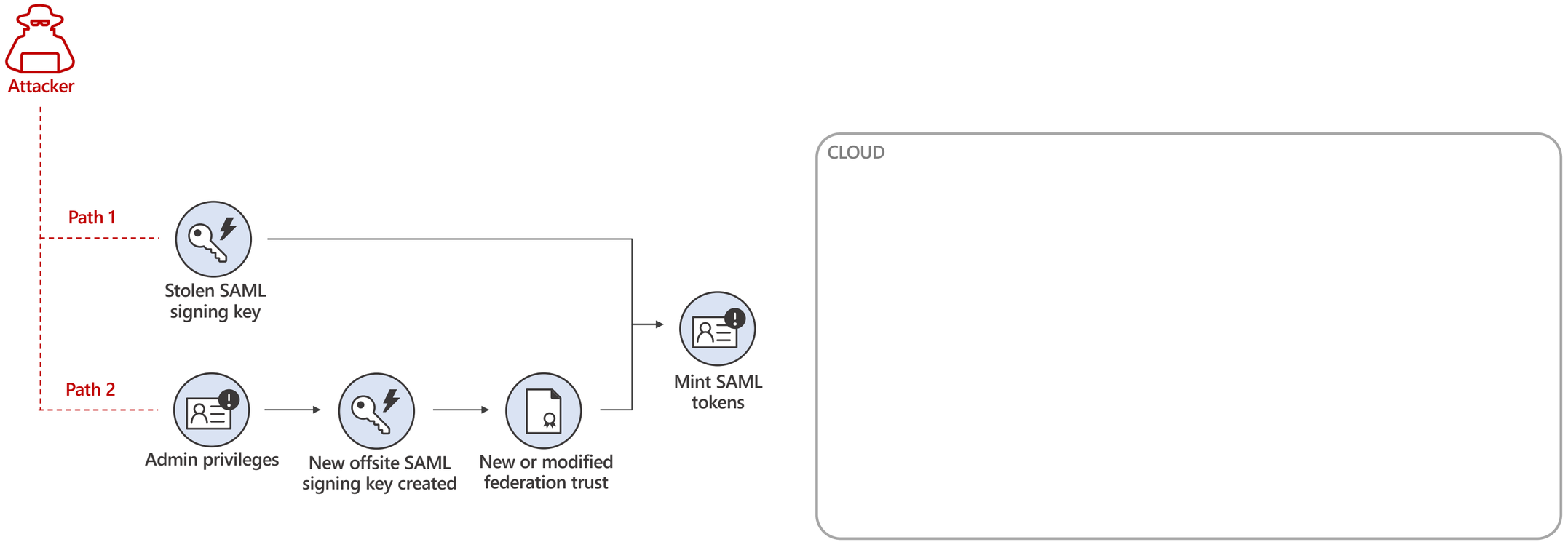
SOLORIGATE ATTACK
Stage 3: Hands-on-keyboard attack in the cloud



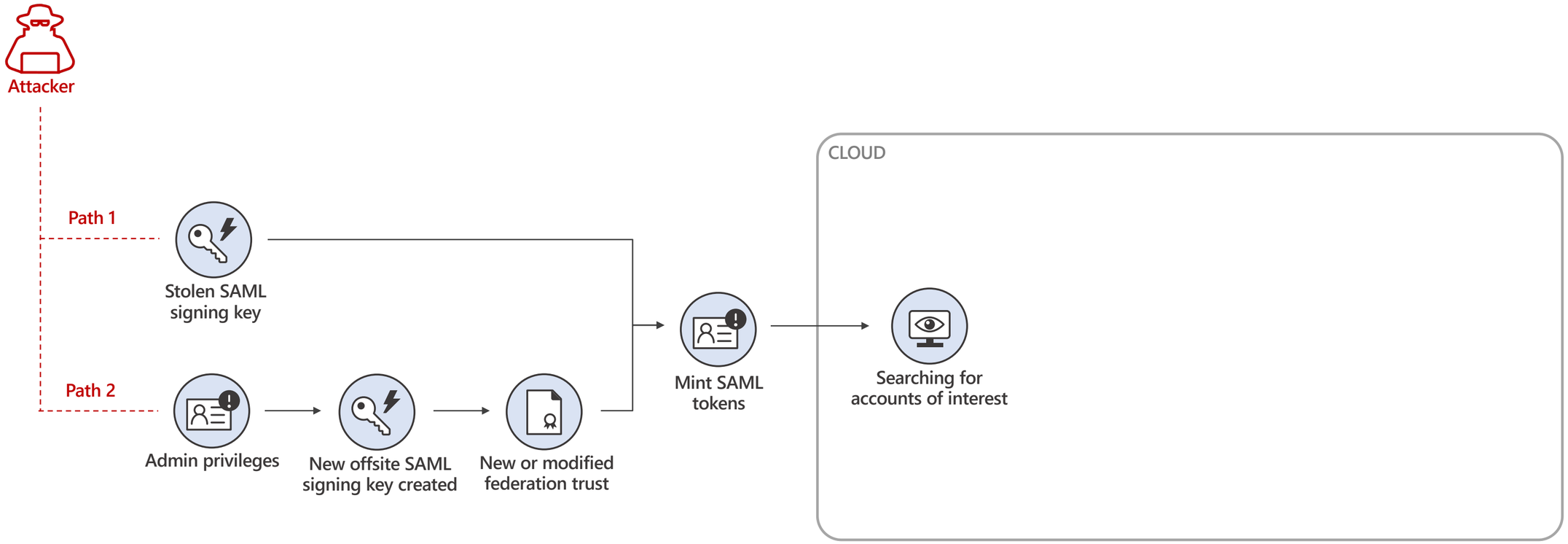
SOLORIGATE ATTACK
Stage 3: Hands-on-keyboard attack in the cloud



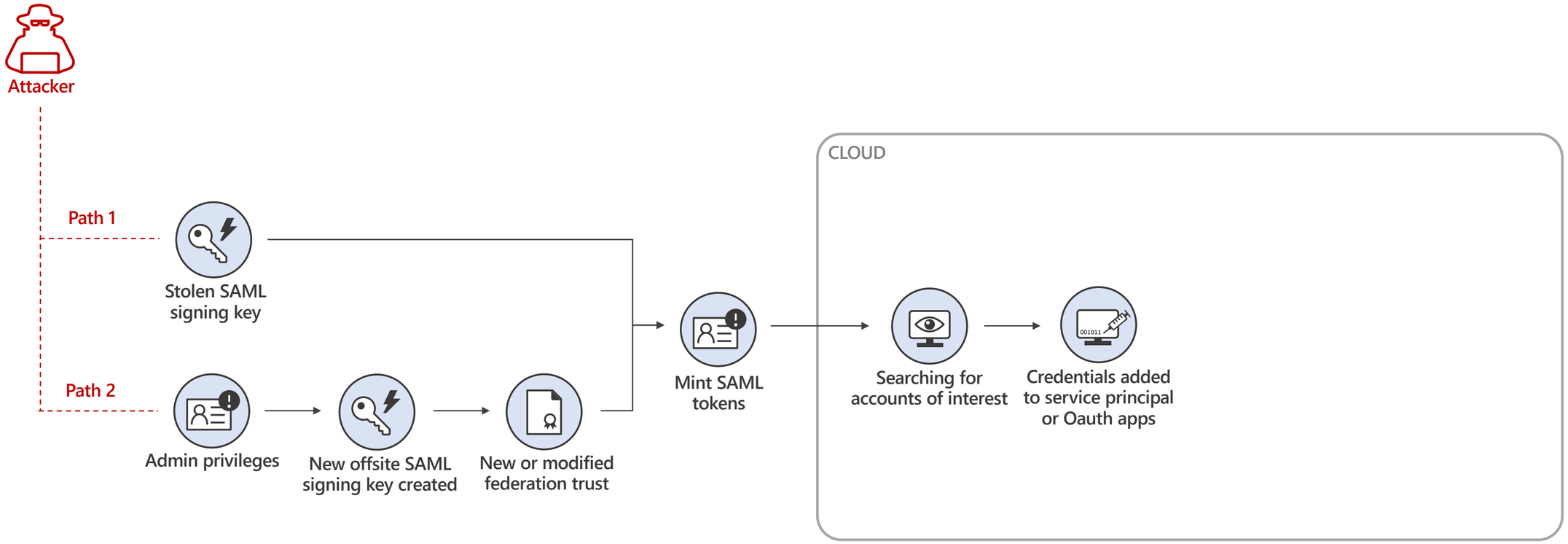
SOLORIGATE ATTACK
Stage 3: Hands-on-keyboard attack in the cloud



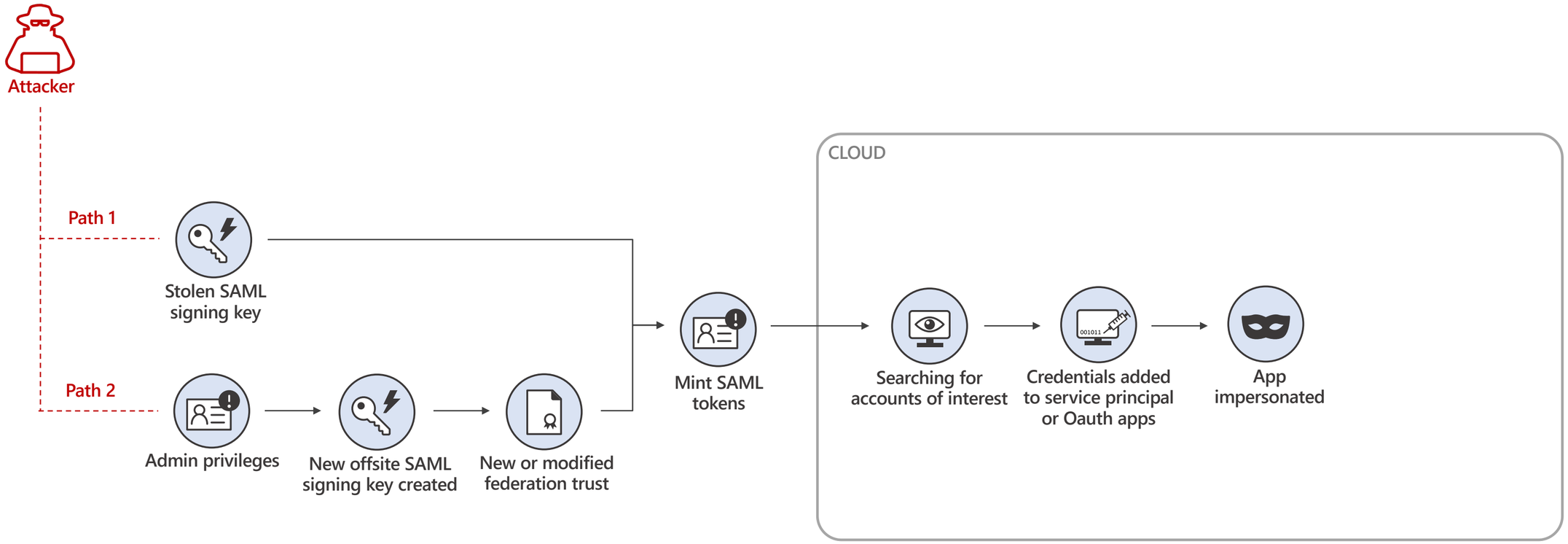
SOLORIGATE ATTACK
Stage 3: Hands-on-keyboard attack in the cloud



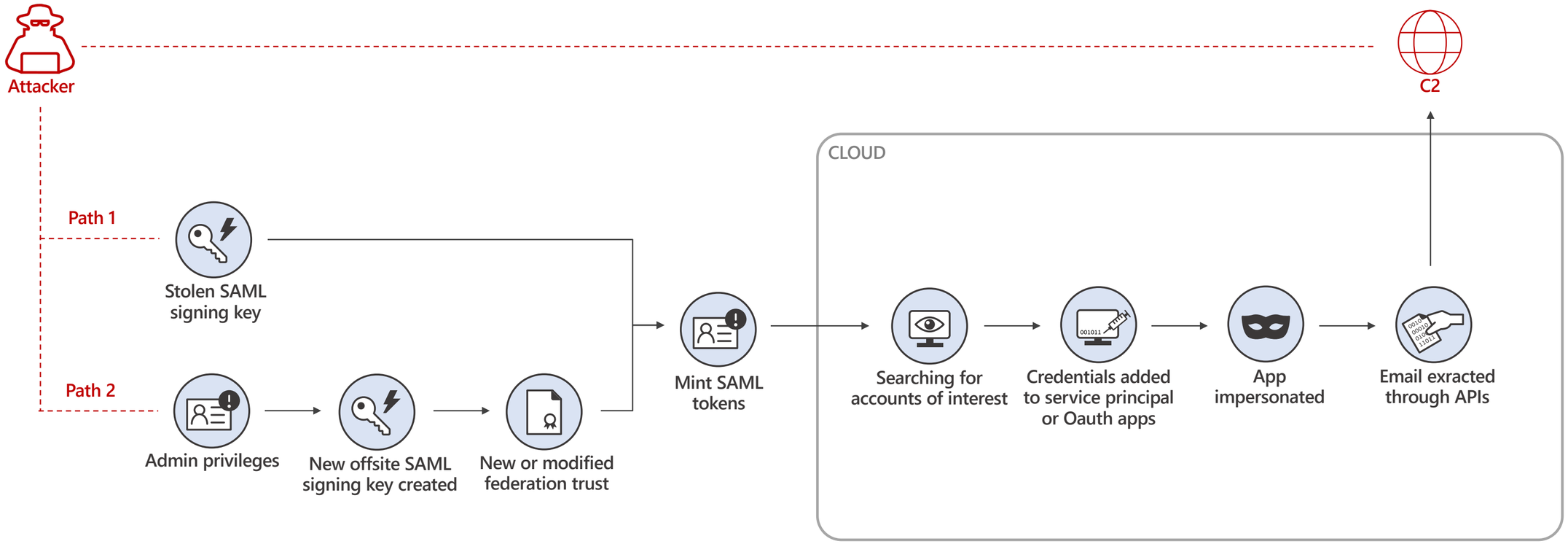
SOLORIGATE ATTACK
Stage 3: Hands-on-keyboard attack in the cloud



SOLORIGATE ATTACK
Stage 3: Hands-on-keyboard attack in the cloud



SOLORIGATE ATTACK
Stage 3: Hands-on-keyboard attack in the cloud



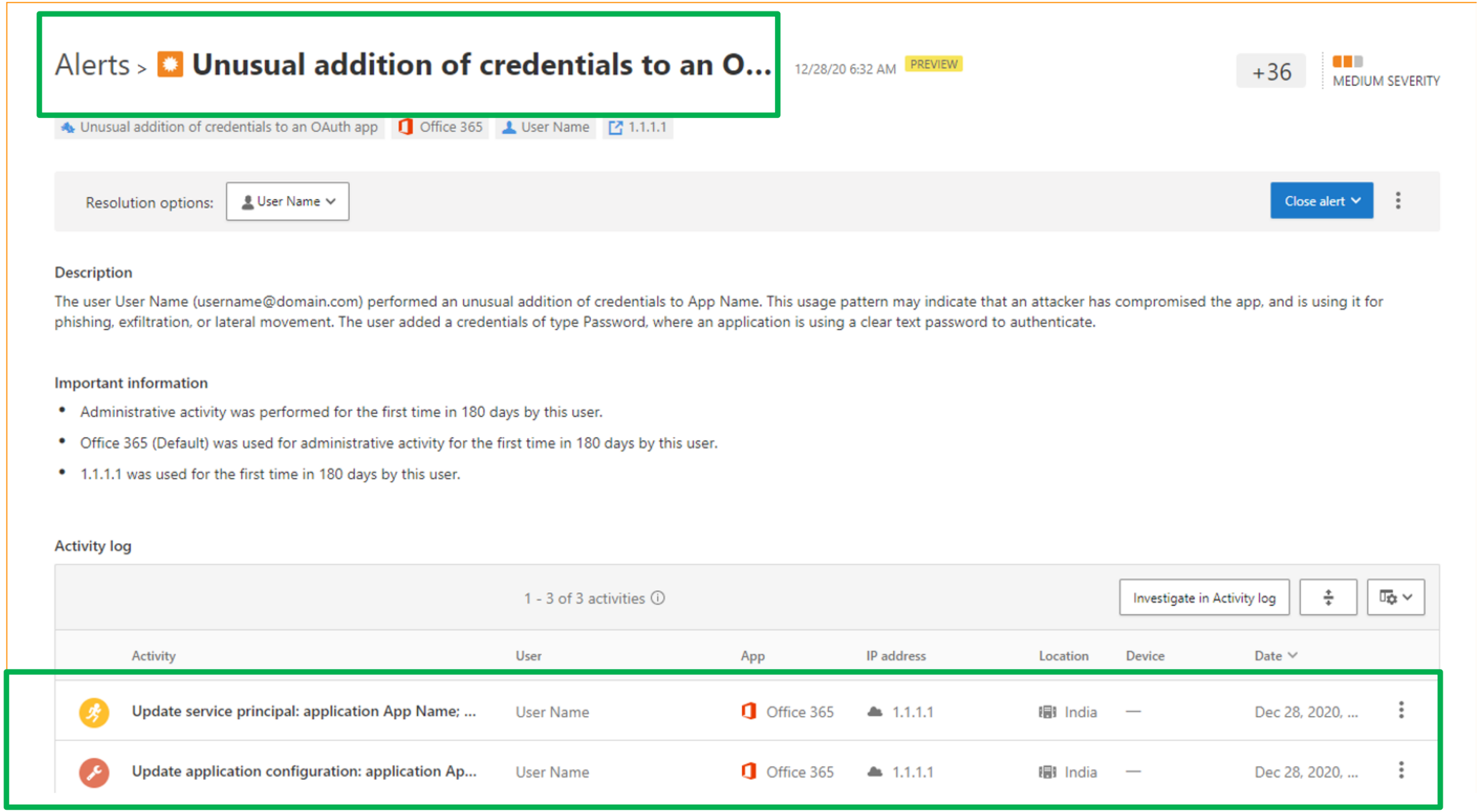
Serve ridurre la superficie d'attacco e monitorare costantemente

- Monitorare e proteggere gli account di servizio e i service principals con diritti amministrativi

- Ridurre l'area di esposizione rimuovendo utenze e service principals non usati

- Adottare strumenti di collezionamento e analisi relazionata dei log
  - Unified Audit Logs (UAL)
  - Azure Active Directory (Azure AD) logs
  - Active Directory Logs
  - Exchange on-prem logs
  - VPN logs
  - Engineering systems logging
  - Antivirus and endpoint detection logging
  - Group membership changes
  - New user account creation
  - Delegation within Active Directory
  - Review administrative rights in environment

Streaming Edition


Alerts > Unusual addition of credentials to an O...
12/28/20 6:32 AM
PREVIEW
+36
MEDIUM SEVERITY
Unusual addition of credentials to an OAuth app
Office 365
User Name
1.1.1.1
Resolution options:
User Name
Close alert
Description
The user User Name (username@domain.com) performed an unusual addition of credentials to App Name. This usage pattern may indicate that an attacker has compromised the app, and is using it for phishing, exfiltration, or lateral movement. The user added a credentials of type Password, where an application is using a clear text password to authenticate.
Important information
Administrative activity was performed for the first time in 180 days by this user.
Office 365 (Default) was used for administrative activity for the first time in 180 days by this user.
1.1.1.1 was used for the first time in 180 days by this user.
Activity log
1 - 3 of 3 activities
Investigate in Activity log
Activity
User
App
IP address
Location
Device
Date
Update service principal: application App Name; ...
User Name
Office 365
1.1.1.1
India
—
Dec 28, 2020, ...
Update application configuration: application Ap...
User Name
Office 365
1.1.1.1
India
—
Dec 28, 2020, ...

Discovering addition of uncommon credential types to application through Advanced Hunting

```
CloudAppEvents
| where Application == "Office 365"
| where ActionType in ("Add service principal credentials.", "Update application – Certificates and secrets management ")
| project Timestamp, RawEventData, AccountDisplayName, ActionType, AccountObjectId
| extend ModifiedProperties = RawEventData.ModifiedProperties[0]
| extend NewValue = ModifiedProperties.NewValue, OldValue = ModifiedProperties.OldValue, Name = ModifiedProperties.Name
| project Timestamp, AccountDisplayName, ActionType, NewValue, OldValue, RawEventData, AccountObjectId
| where (NewValue has "KeyType=Password" and OldValue !has "KeyType=Password" and OldValue has "AsymmetricX509Cert") or (NewValue has "AsymmetricX509Cert" and OldValue !has "AsymmetricX509Cert" and OldValue has "KeyType=Password")
| extend NewSecret = set_difference(todynamic(parse_json(tostring(NewValue))), todynamic(parse_json(tostring(OldValue))))
| project Timestamp,ActionType,ActorType = RawEventData.Actor[-1].ID, ObjectId = RawEventData.Actor[-2].ID, AccountDisplayName, AccountObjectId, AppnName = RawEventData.Target[3].ID, AppObjectId = RawEventData.Target[1].ID, NewSecret = NewSecret[0], RawEventData
```

Cercare gli eventi nelle app O365 , in cui sono state aggiunte/aggiornate le credenziali dell'entità servizio o i certificati/segreti

Cercare gli eventi in cui una credenziale basata su password ha sostituito un certificato o un certificato ha sostituito una credenziale basata su password

Visualizzare le applicazioni interessate insieme alla differenza nel set di credenziali precedente e nuovo.

**Information is correct as of Jan 15, 2021. please see aka.ms/solorigate for the most recent updates*

Discovering anomalies on O365 mailbox access with Advanced Hunting

MailItemsAccessedThrottling

```
let starttime = 2d;
let endtime = 1d;
CloudAppEvents
| where Timestamp between (startofday(ago(starttime))..startofday(ago(endtime)))
| where ActionType == “MailItemsAccessed”
| where isnotempty(RawEventData[‘ClientAppId’]) and
    RawEventData[‘OperationProperties’][1] has “True”
| project Timestamp, RawEventData[‘OrganizationId’],AccountObjectId,UserAgent
```

Cerca gli eventi che si sono verificati tra 48h e 24h precedenti

Cercare l'attività di accesso alla posta dalle app Oauth o dalle entità servizio in cui il controllo è stato limitato.

OAuthGraphAPIAnomalies

```
//Look for OAuth App reading mail via GraphAPI – that did not read mail via graph API in prior week
let appMailReadActivity = (timeframeStart:datetime, timeframeEnd:datetime) {
CloudAppEvents
| where Timestamp between (timeframeStart .. timeframeEnd)
| where ActionType == “MailItemsAccessed”
| where RawEventData has “00000003-0000-0000-c000-000000000000” // Graph API
| extend rawData = parse_json(RawEventData)
| extend AppId = tostring(parse_json(rawData.AppId))
| extend OAuthAppId = tostring(parse_json(rawData.ClientAppId)) // extract OAuthAppId
| summarize by OAuthAppId
};
appMailReadActivity(ago(1d),now()) // detection period
| join kind = leftanti appMailReadActivity(ago(7d),ago(2d)) // baseline period
on OAuthAppId
```

Crea una funzione che elenca tutte le app che hanno usato GraphAPI per accedere ai messaggi di posta elettronica in un determinato intervallo di tempo

Confronta l'attività tra le ultime 24 ore e 5 giorni prima ed elenca le app che sono nuove alla lettura di e-mail tramite GraphAPI

**Information is correct as of Jan 15, 2021. please see aka.ms/solorigate for the most recent updates*

SOLORIGATE ATTACK
Conclusioni

Streaming Edition

Nessun «salvatore» eliminerà tutti i rischi per la sicurezza, avere una corretta postura può fare la differenza

Adottare una filosofia «*Assume Breach*»

Gli aggressori ci provano sempre, quindi bisogna presumere che avranno un certo successo. Bisogna adottare un approccio "di difesa in profondità" che migliora continuamente la sicurezza di persone, processi e tecnologia e crea livelli di prevenzione e rilevamento su e-mail, dispositivi, server, identità e servizi cloud.

Ridurre l'area di superficie per l'accesso privilegiato

Ridurre rapidamente i rischi concentrandosi sull'autenticazione senza password e multi-fattore (MFA), su una rigorosa manutenzione del software (aggiornamenti/patch di sicurezza) e sulla protezione degli account più sensibili

Strategia di sicurezza olistica e pragmatica

Microsoft consiglia un approccio olistico alla sicurezza che si adatti pragmaticamente alle nuove minacce. Ogni aspetto della nostra infrastruttura va considerato e relazionato per arrivare ad una visione d’insieme. Bisogna di dotarsi di strumenti adatti!

Resta aggiornato

Controlla https://aka.ms/solorigate per le informazioni più recenti.

Zero trust

Assume Breach, Explicit Verification, Least Privilege

Q&A

prinaldi@microsoft.com
https://www.linkedin.com/in/patrizio-rinaldi-9168002/

Vieni a trovarci al nostro virtual desk!