Microsoft

Solorigate の概要

Tim Burrell
パートナー エンジニアリング マネージャー
Microsoft Threat Intelligence Center

2021 年 2 月 18 日

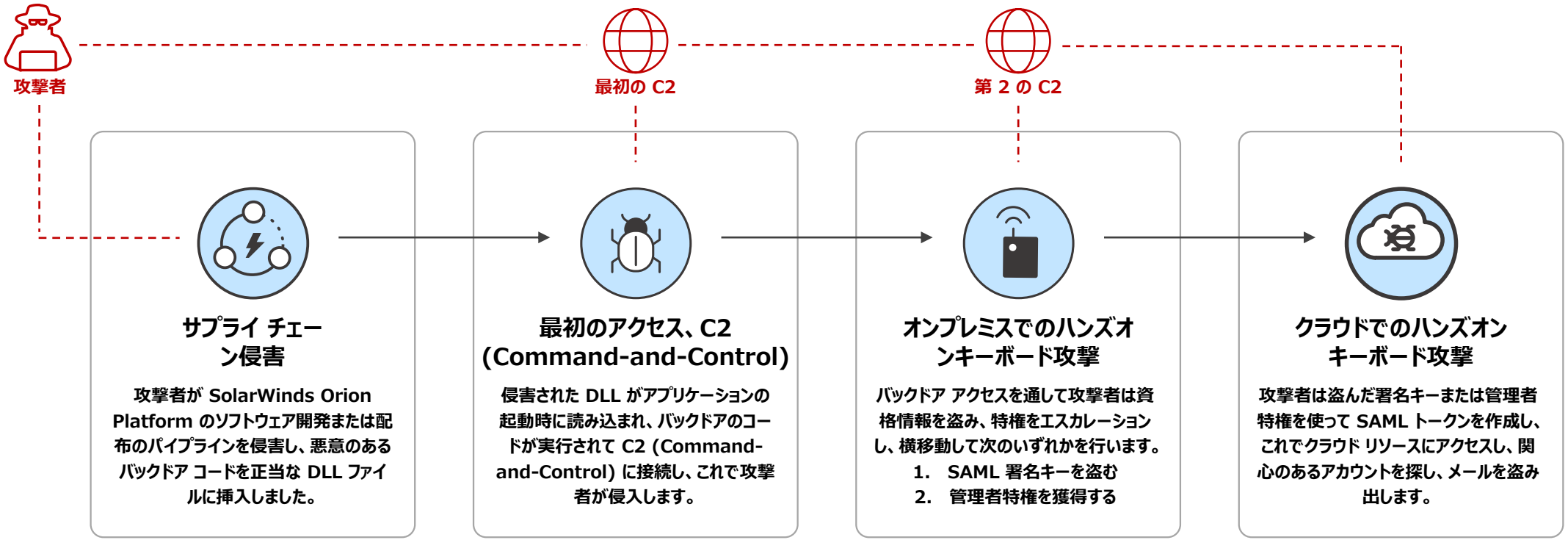
Solorigate ビデオ シリーズ

Solorigate スタイルの攻撃から組織を守るのに役立つ方法とは。

Microsoft Security

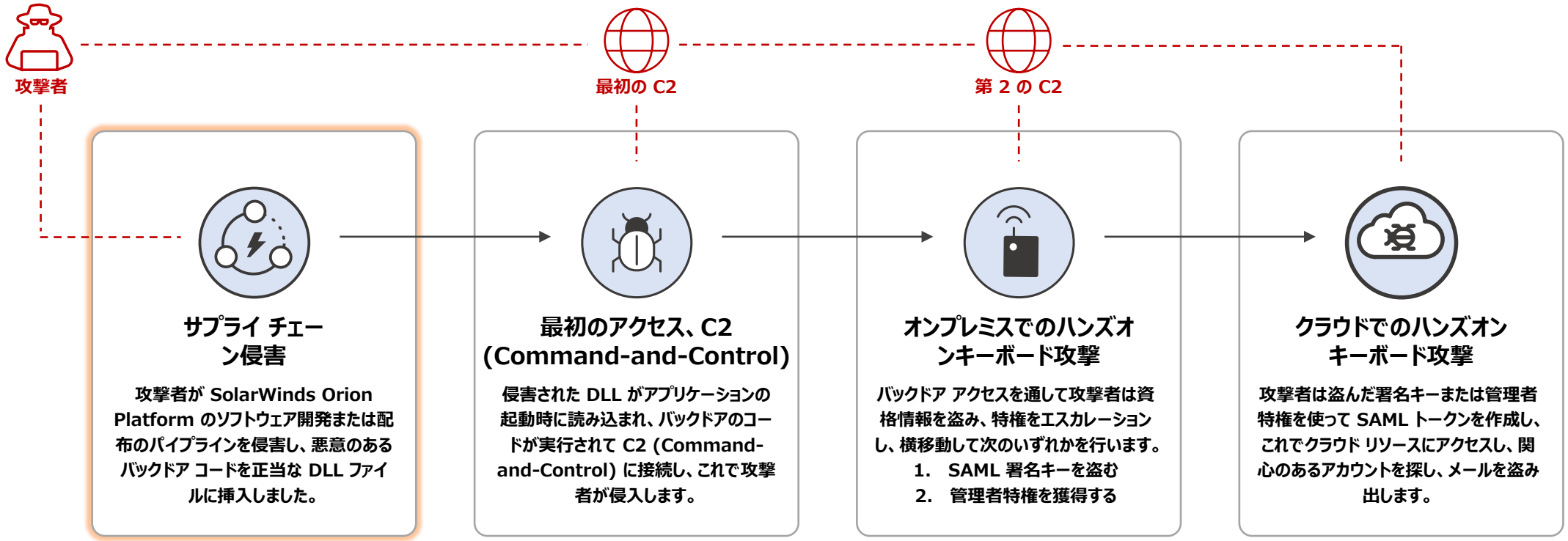
Solorigate 攻撃

攻撃チェーン全体の概要

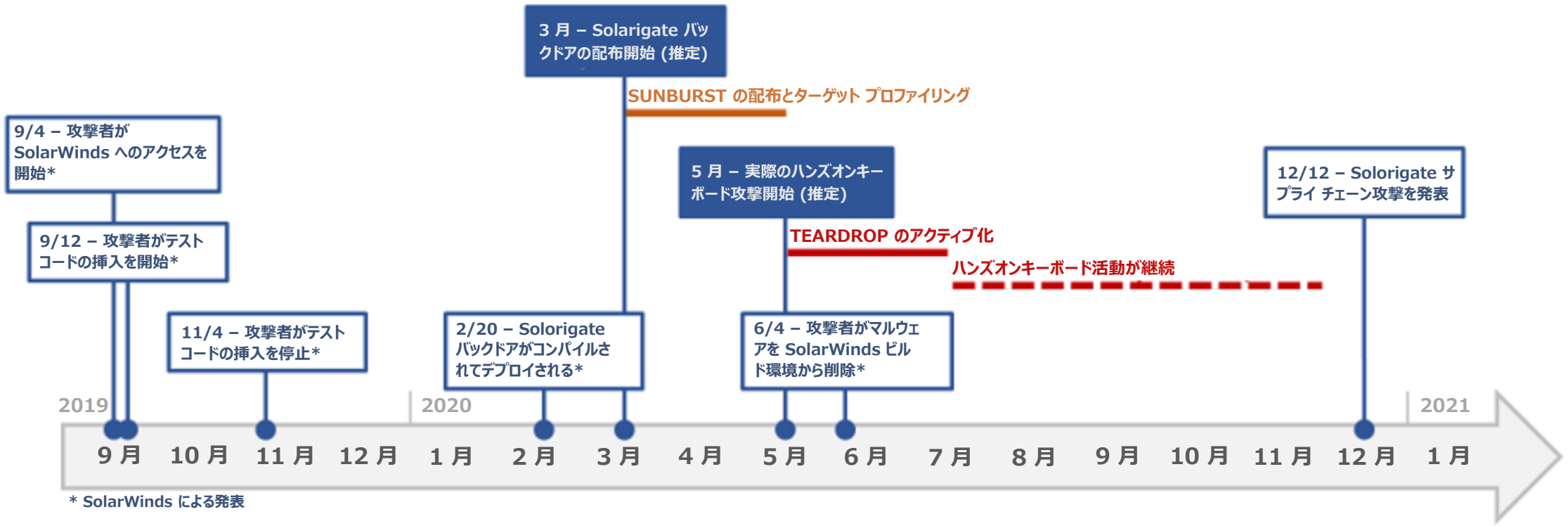


Solorigate 攻撃

攻撃チェーン全体の概要



Solorigate 攻撃
タイムライン

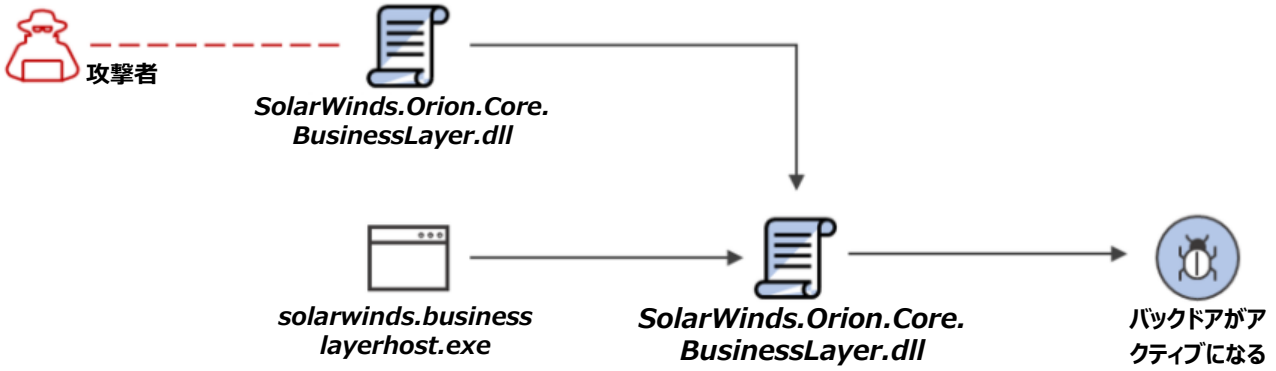


* SolarWinds による発表

情報は *2021/1/21* の時点で正確です。最新の情報については *aka.ms/solorigate* をご覧ください。

サプライ チェーン攻撃
攻撃者が、正当なソフトウェアの DLL コンポーネントに悪意のあるコードを挿入します。侵害された DLL が、関連ソフトウェアを使用する組織に配布されます。

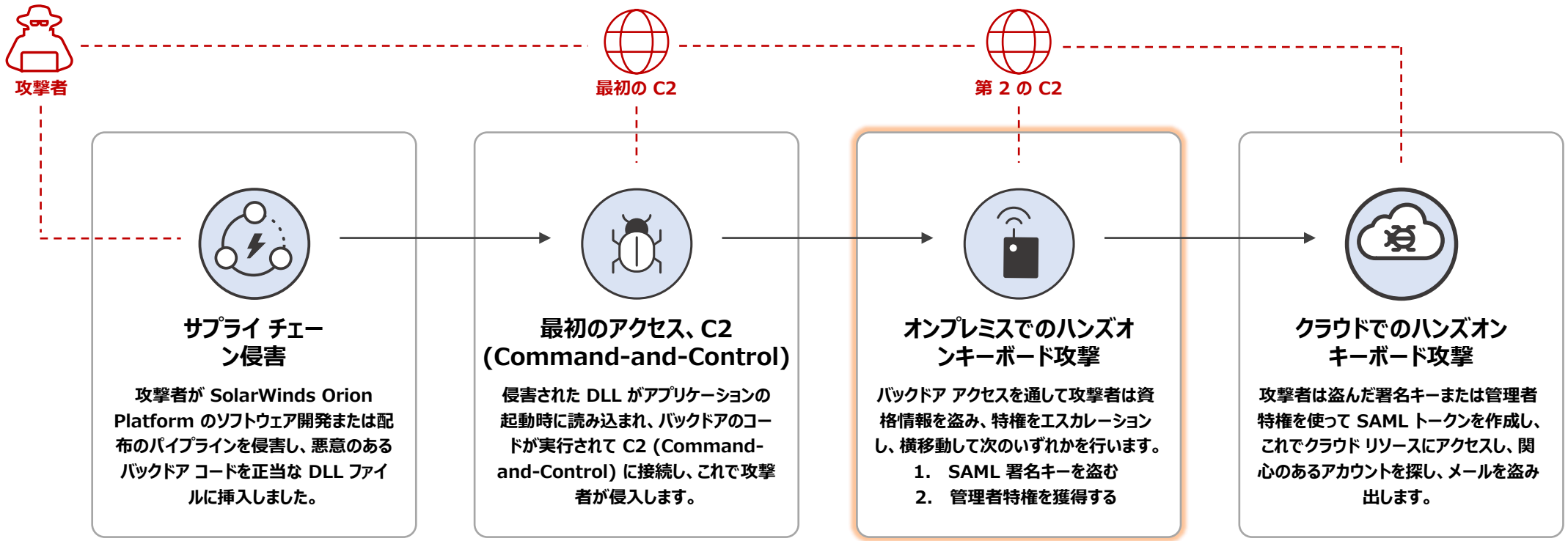
実行、永続化
ソフトウェアが起動すると、侵害された DLL が読み込まれます。この中に挿入された、悪意のあるコードが呼び出す関数の中にバックドア機能があります。




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

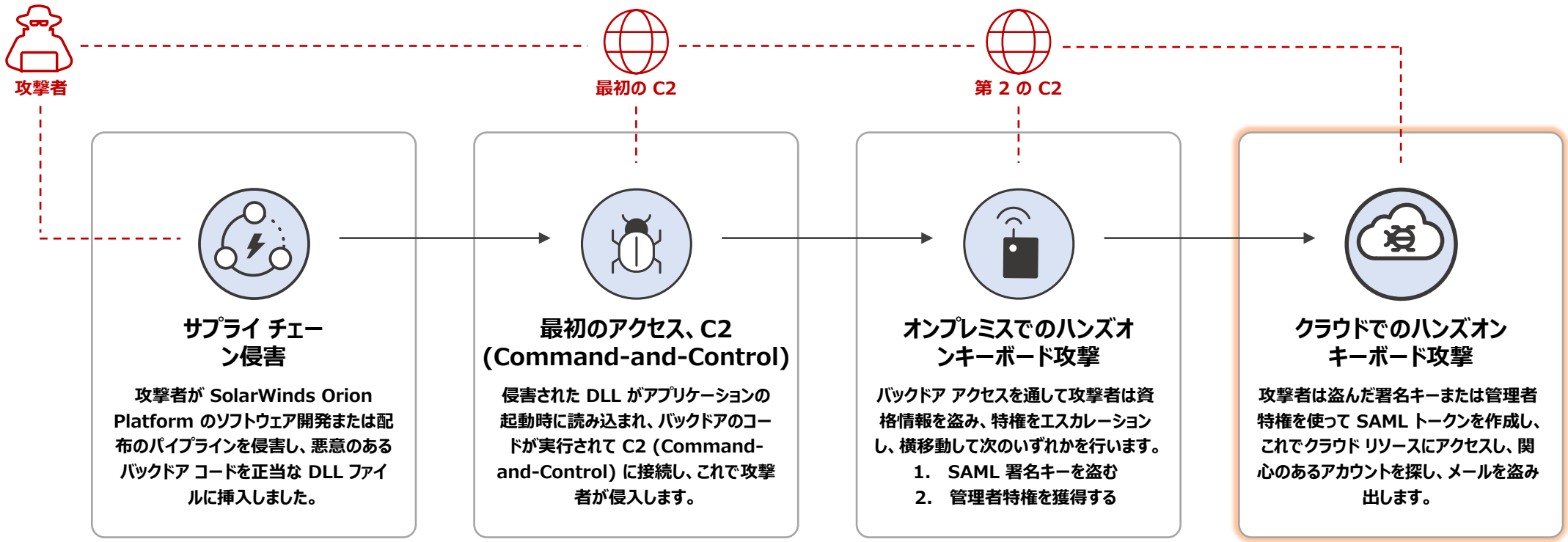
Solorigate 攻撃

攻撃チェーン全体の概要



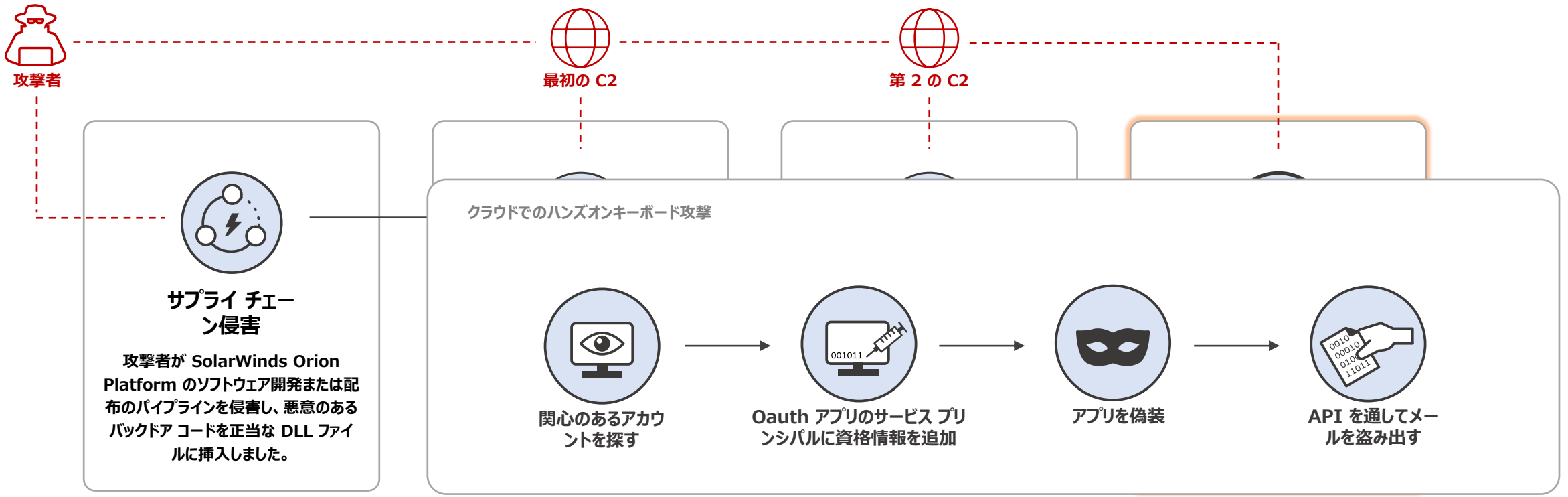
Solorigate 攻撃

攻撃チェーン全体の概要



Solorigate 攻撃

攻撃チェーン全体の概要



推奨される防御

Solorigate での手口に対する防御に役立つ 7 つのステップ

1. 最新のウイルス対策と EDR の製品を実行します。

2. 自社のネットワーク インフラストラクチャを使う既知の C2 エンドポイントをブロックします。

3. SAML トークン署名キーをセキュリティ保護するとともに、ハードウェア セキュリティを SAML トークン署名証明書に使用することを検討します。Active Directory フェデレーション サービス (AD FS) については、Microsoft のベスト プラクティス推奨事項を確認します。
https://docs.microsoft.com/ja-jp/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs

4. 管理者ユーザー権利についてのベスト プラクティスに従い、高い特権を持つディレクトリ ロールのメンバーであるユーザーの数を減らします。

5. 管理者権限を持つサービス アカウントには、安全に保管されている高エントロピー シークレット (つまり証明書) を使用します。監視を行って、通常とは異なるサービス アカウントの変更、サインイン、使用を見つけます。

6. 未使用または不要のアプリケーションとサービス プリンシパルを削除するか無効化します。まだ残っているものに対するアクセス許可を減らします。

7. Azure AD アイデンティティ インフラストラクチャをセキュリティで保護するためのその他の推奨事項を参照します。
https://docs.microsoft.com/ja-jp/azure/security/fundamentals/steps-secure-identity

Solorigate 攻撃

攻撃チェーン全体の概要

攻撃者

最初の C2

第 2 の C2

サプライ チェーン侵害

攻撃者が SolarWinds Orion Platform のソフトウェア開発または配布のパイプラインを侵害し、悪意のあるバックドア コードを正当な DLL ファイルに挿入しました。

最初のアクセス、C2 (Command-and-Control)

侵害された DLL がアプリケーションの起動時に読み込まれ、バックドアのコードが実行されて C2 (Command-and-Control) に接続し、これで攻撃者が侵入します。

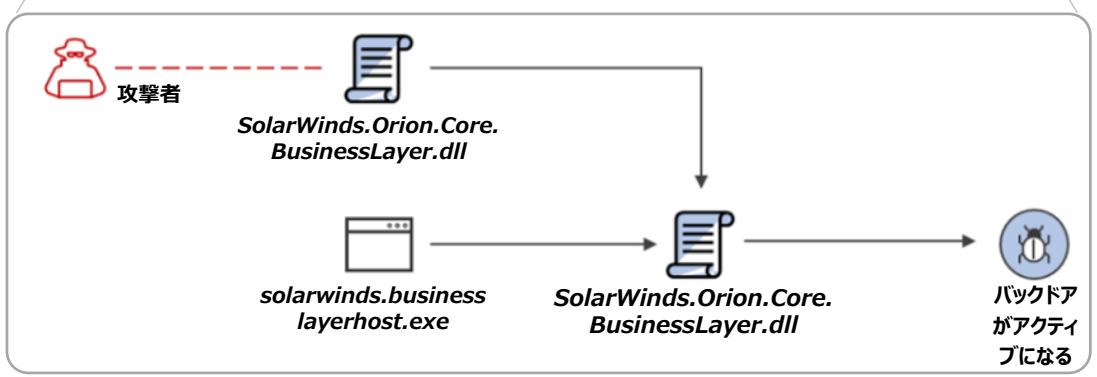
オンプレミスでのハンズオンキーボード攻撃

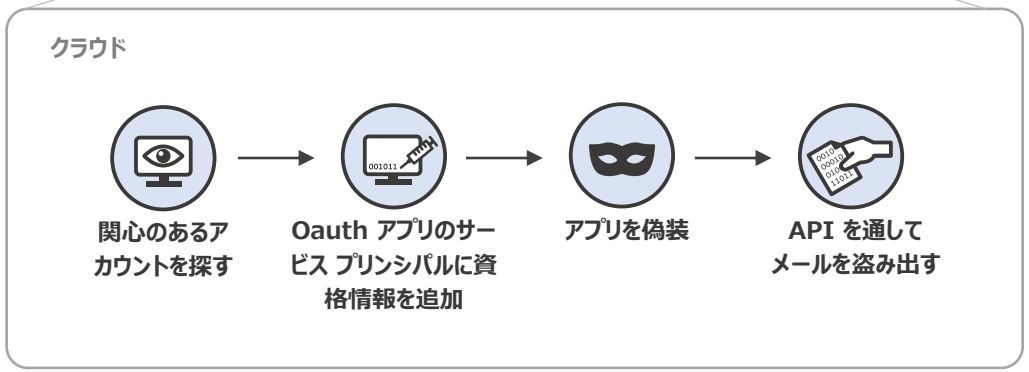
バックドア アクセスを通して攻撃者は資格情報を盗み、特権をエスカレーションし、横移動して次のいずれかを行います。

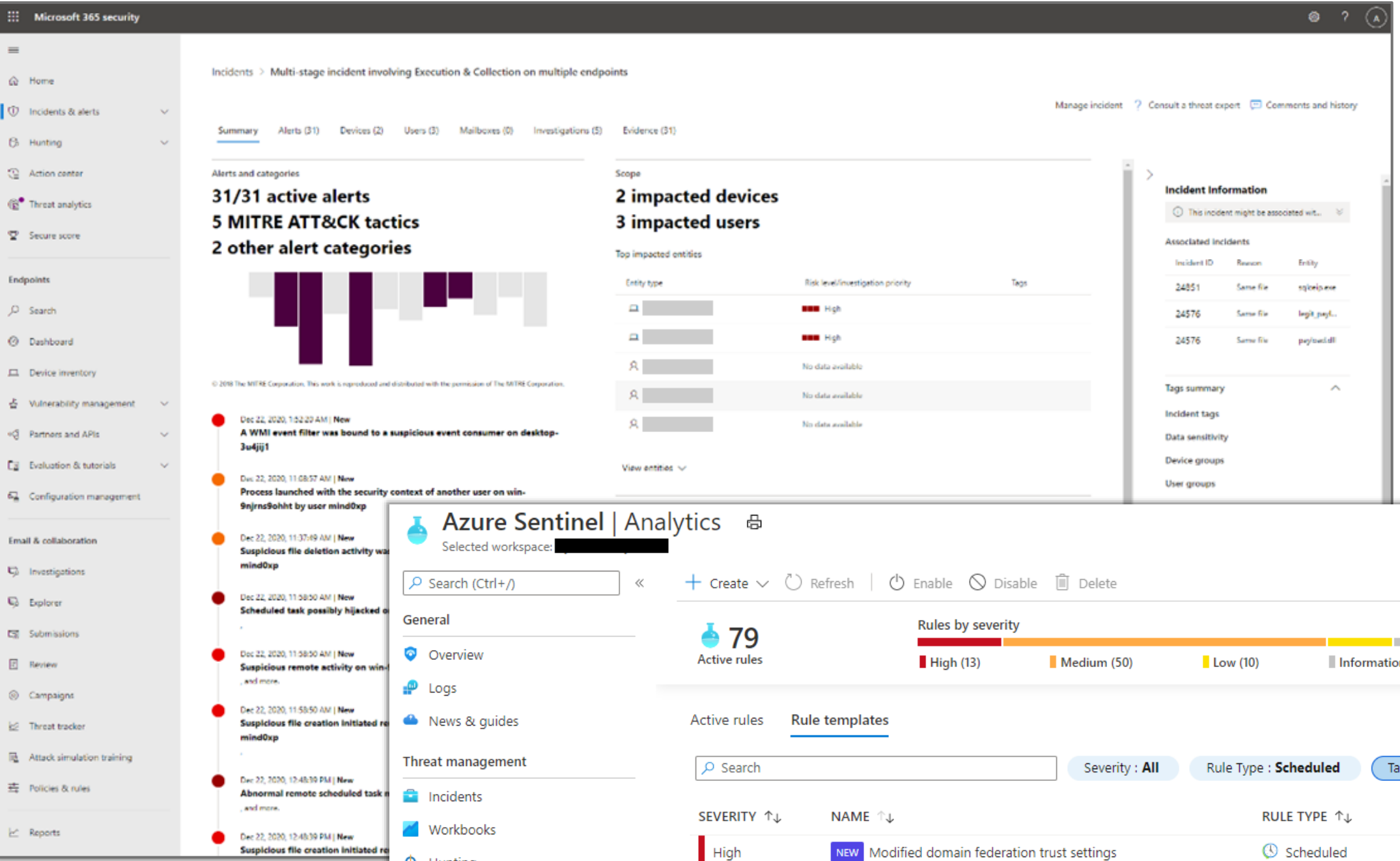
1. SAML 署名キーを盗む
2. 管理者特権を獲得する

クラウドでのハンズオン キーボード攻撃

攻撃者は盗んだ署名キーまたは管理者特権を使って SAML トークンを作成し、これでクラウド リソースにアクセスし、関心のあるアカウントを探し、メールを盗み出します。






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 ビデオ シリーズ

次のステップ

01 この場所にある Solorigate ビデオ シリーズを見る

02 Microsoft Security にアクセスして最新情報を入手する: www.microsoft.com/ja-jp/security/business

03 ブログを読む: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security