Microsoft

Présentation de Solorigate

Tim Burrell

Responsable partenaires en ingénierie

Microsoft Threat Intelligence Center

18 février 2021

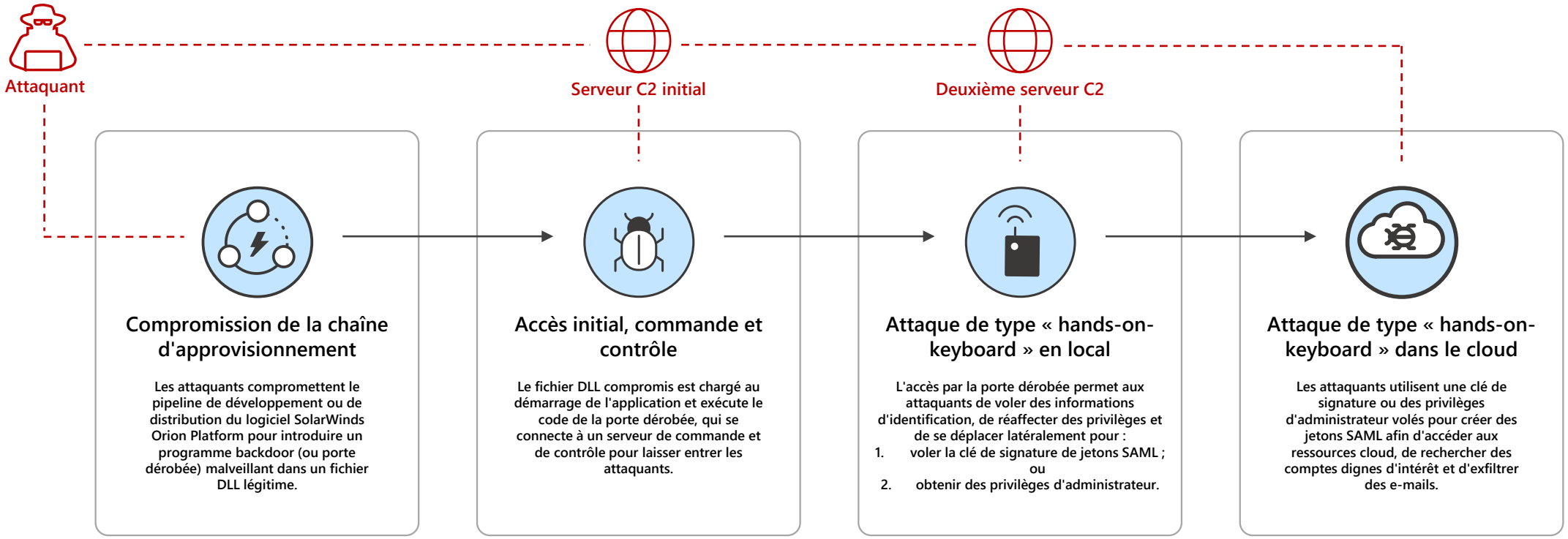
Série de vidéos consacrées à Solorigate

Comment protéger votre organisation des attaques de type Solorigate ?

Microsoft Security

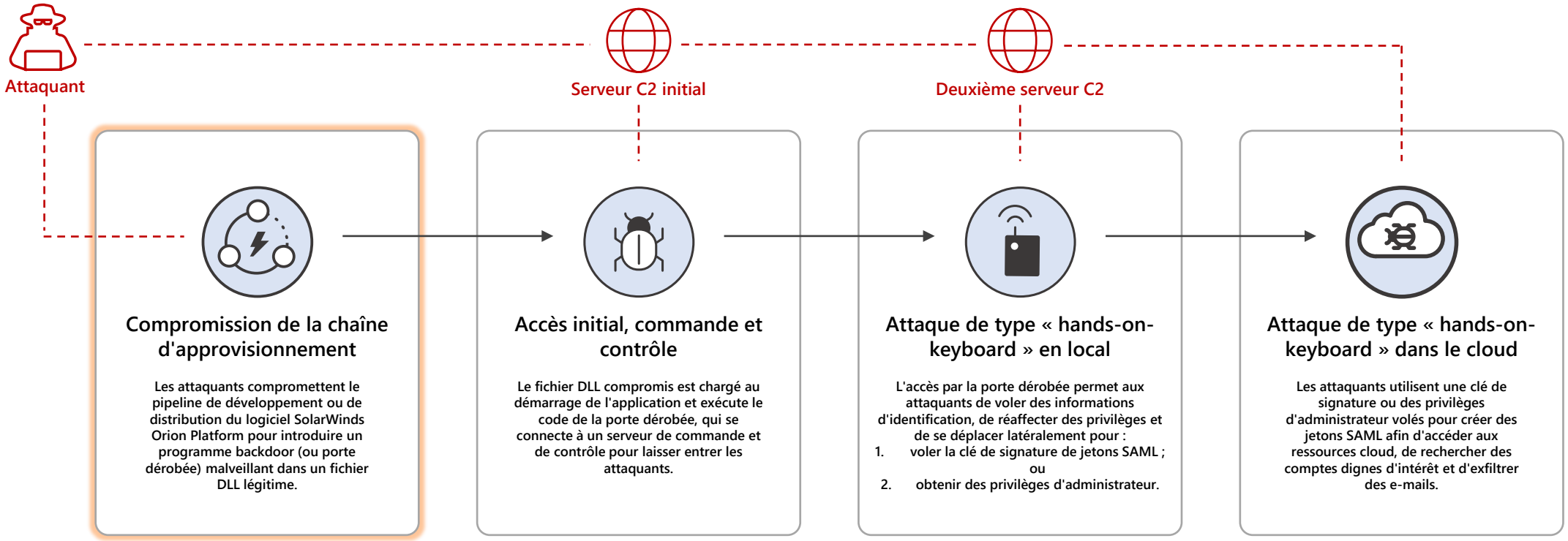
Attaque Solorigate

Chaîne d'attaque de bout en bout de haut niveau



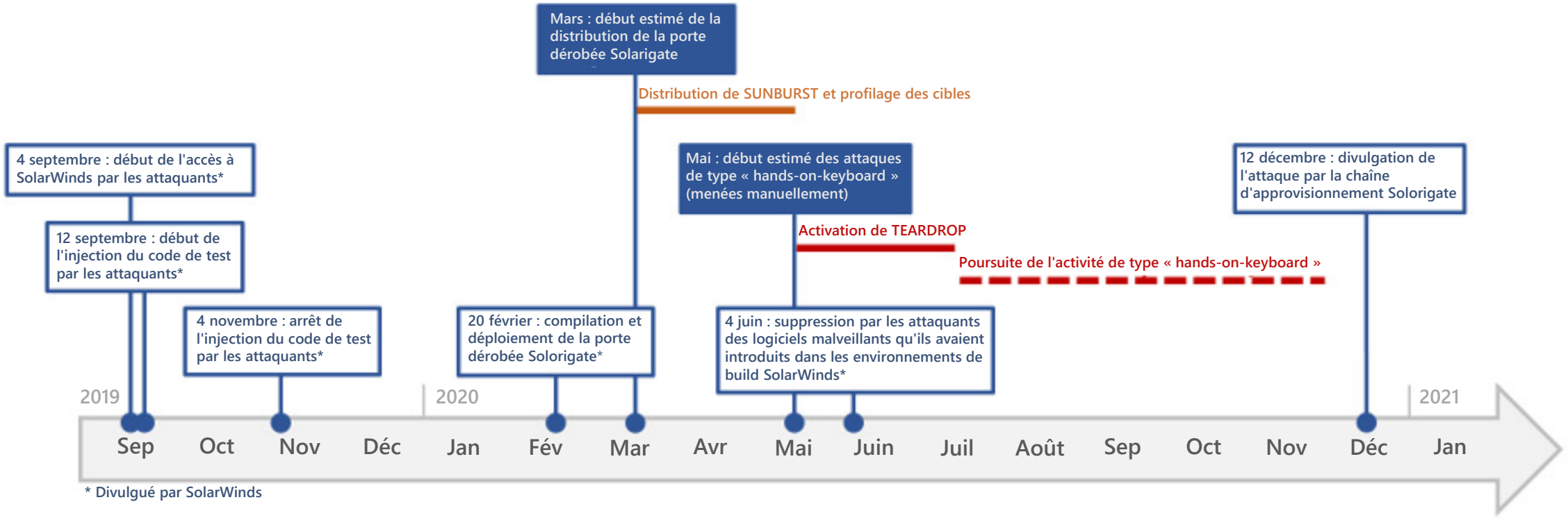
Attaque Solorigate

Chaîne d'attaque de bout en bout de haut niveau



Attaque Solorigate

Chronologie

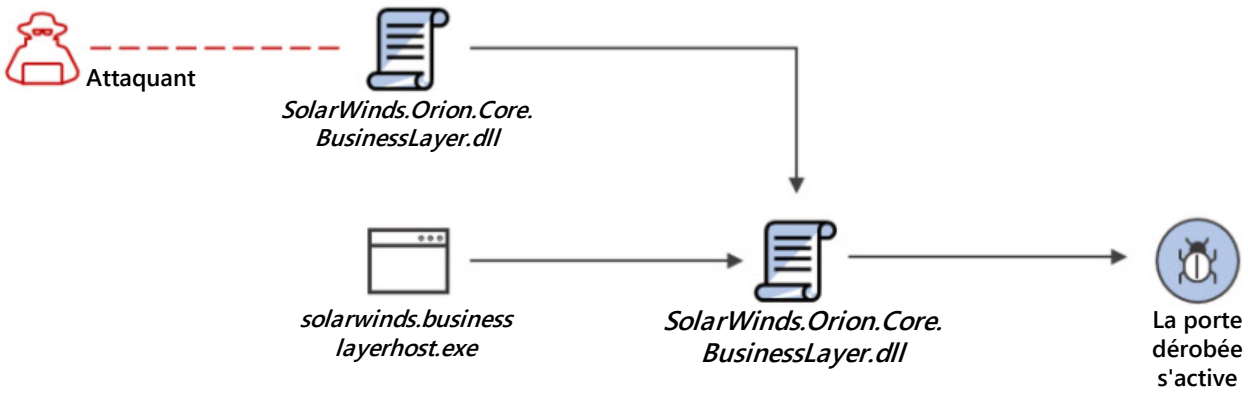


* Divulgué par SolarWinds

Les informations étaient correctes en date du 1er janvier 2021. Veuillez consulter le site aka.ms/solorigate pour accéder aux mises à jour les plus récentes.

ATTAQUE PAR LA CHAÎNE D'APPROVISIONNEMENT
Les attaquants introduisent du code malveillant dans un composant DLL d'un logiciel légitime. Le fichier DLL compromis est distribué aux organisations qui utilisent le logiciel correspondant.

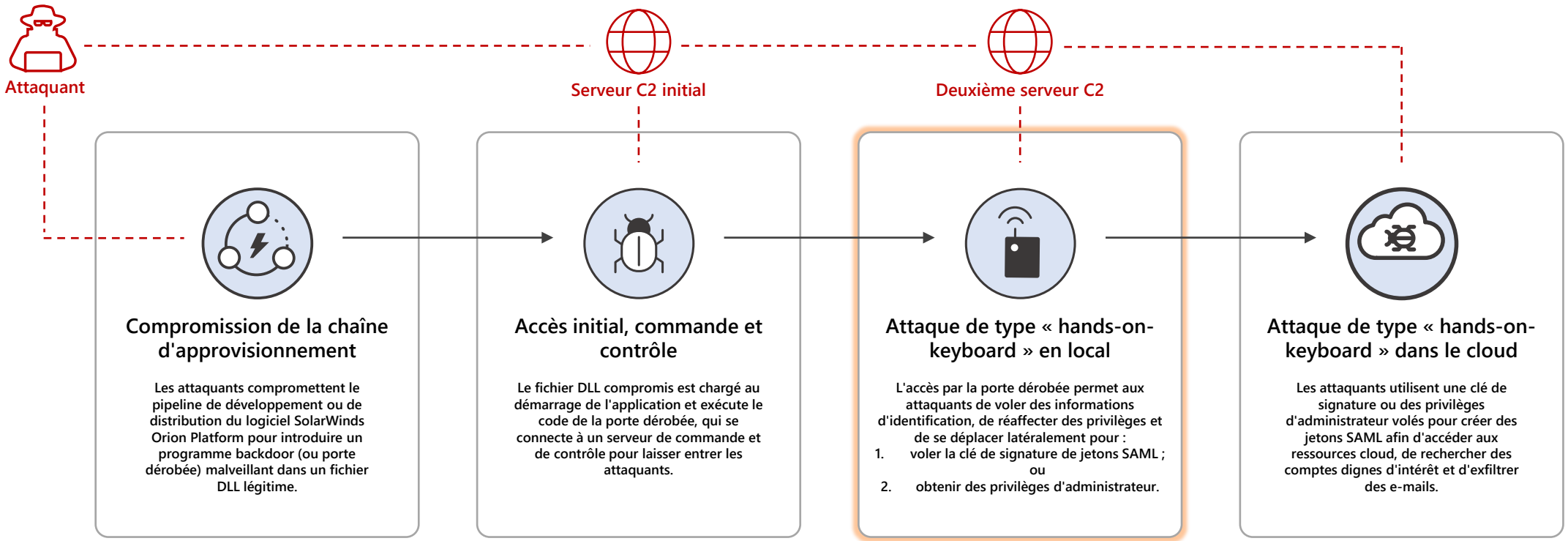
EXÉCUTION, PERSISTANCE
Au démarrage du logiciel, le fichier DLL compromis se charge et le code malveillant inséré appelle la fonction qui contient les fonctionnalités de la porte dérobée.




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

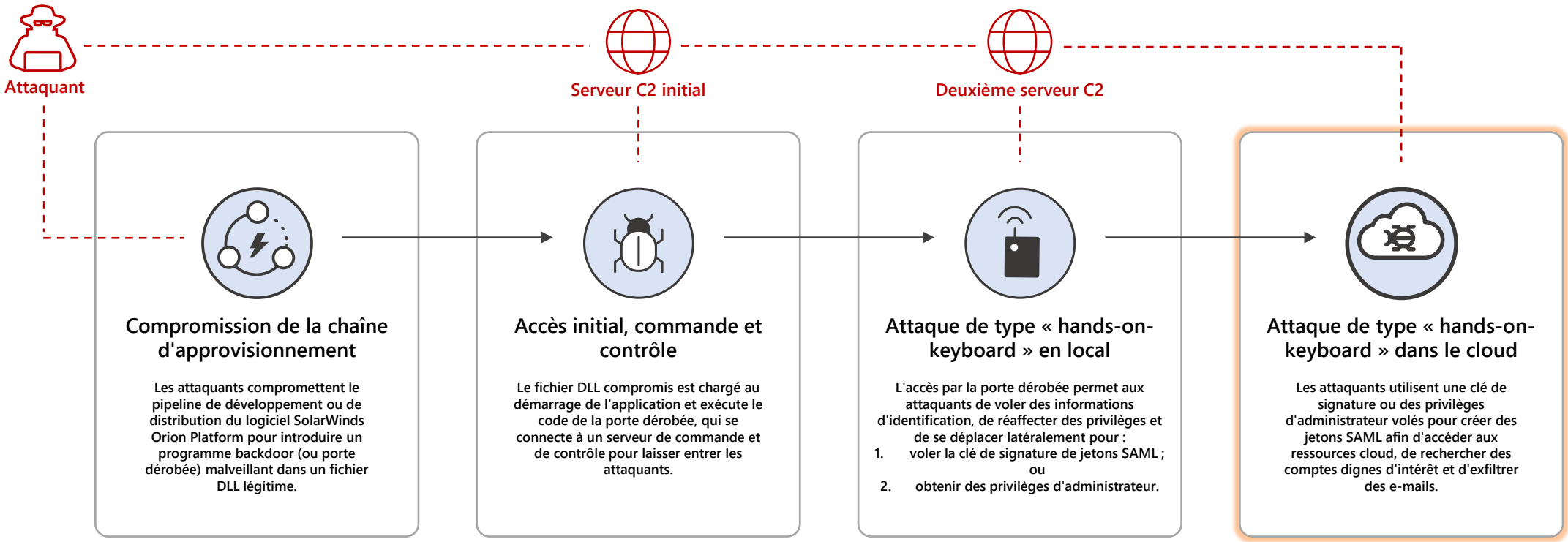
Attaque Solorigate

Chaîne d'attaque de bout en bout de haut niveau



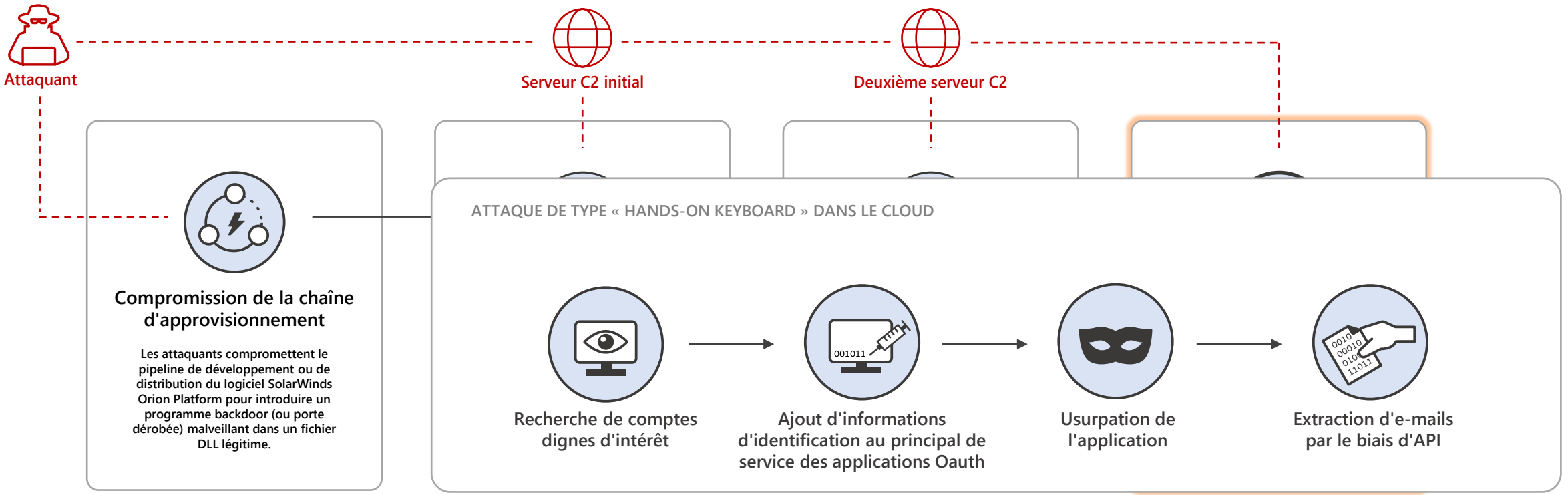
Attaque Solorigate

Chaîne d'attaque de bout en bout de haut niveau



Attaque Solorigate

Chaîne d'attaque de bout en bout de haut niveau



Moyens de défense recommandés

Sept étapes à suivre pour vous protéger des techniques vues dans Solorigate

1. Utilisez des produits antivirus et PEPT à jour.

2. Bloquez les points de terminaison C2 connus qui utilisent votre infrastructure réseau.

3. Sécurisez vos clés de signature de jetons SAML et envisagez d'adopter une sécurité matérielle pour vos certificats de signature de jetons SAML. Pour les services ADFS (Active Directory Federation Services), consultez les recommandations de Microsoft en matière de bonnes pratiques : https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs

4. Suivez les meilleures pratiques en matière de droits d'utilisateurs administrateurs et réduisez le nombre d'utilisateurs membres de rôles d'annuaire à niveau de privilège élevé.

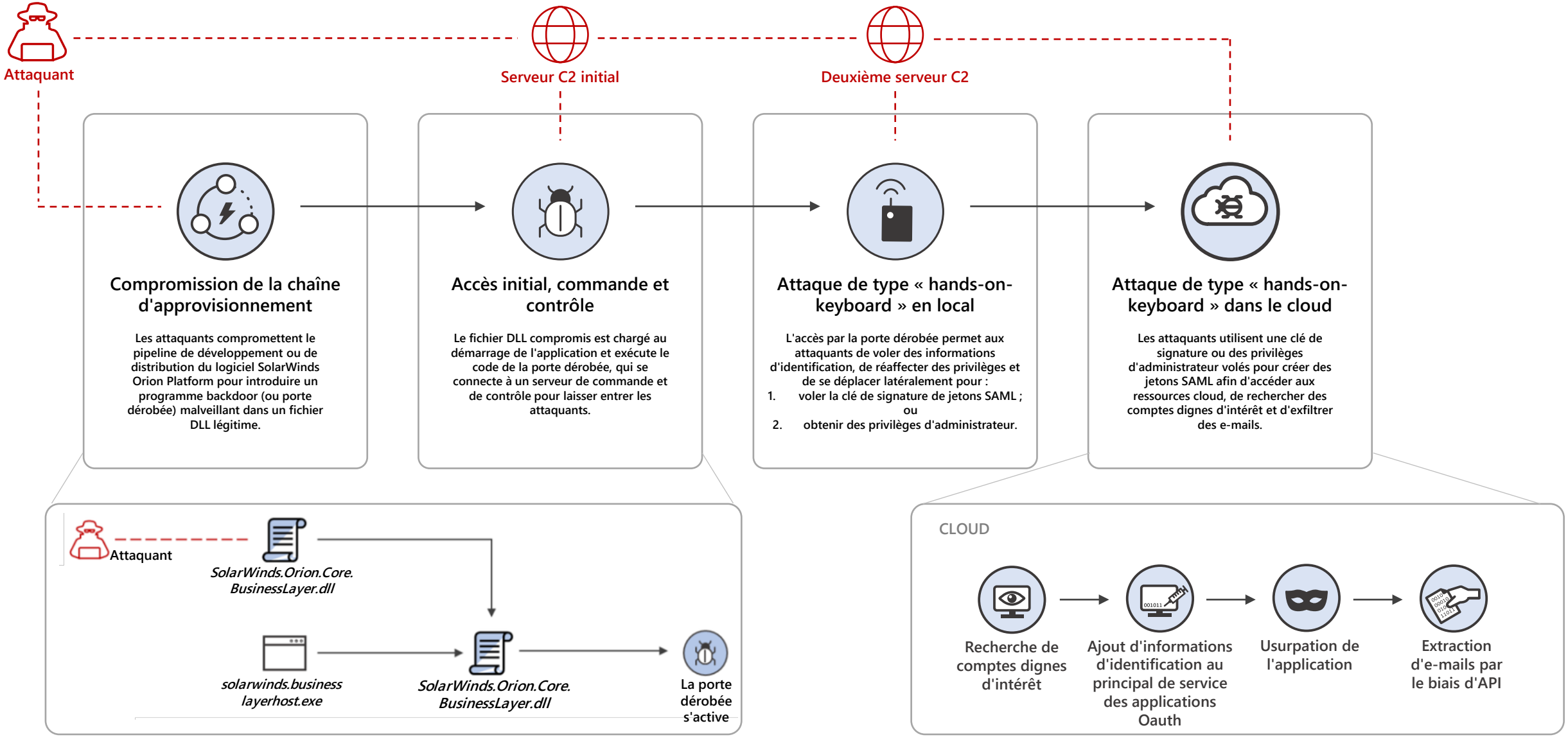
5. Veillez à ce que les comptes de service disposant de droits d'administration utilisent des secrets à haute entropie (c'est-à-dire des certificats) stockés de manière sécurisée. Surveillez les éventuelles modifications, ainsi que les connexions et les utilisations de comptes de service anormales.

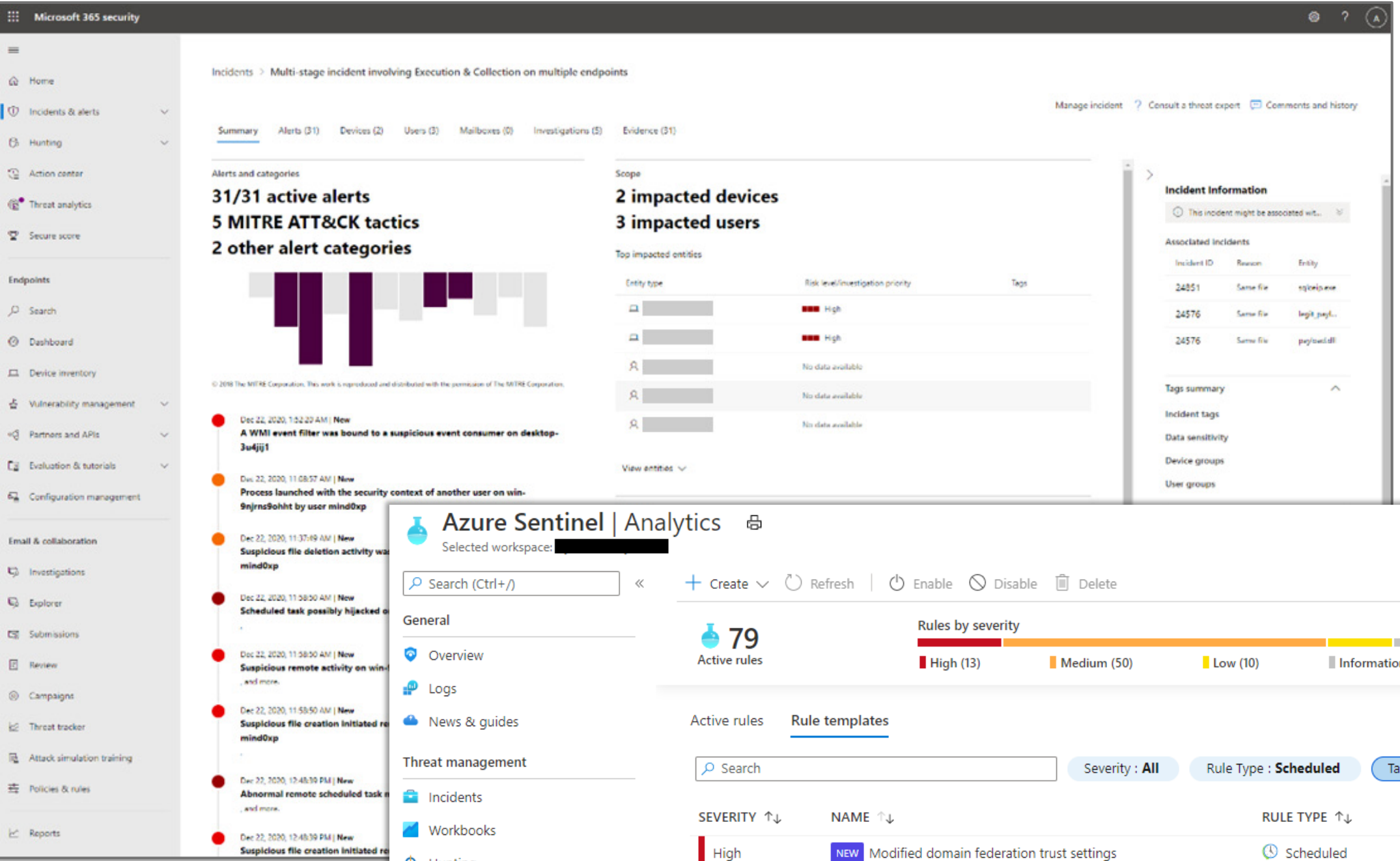
6. Supprimez ou désactivez les applications et les principaux de service inutilisés ou superflus. Réduisez les autorisations sur ceux dont vous disposez encore.

7. Consultez les recommandations supplémentaires suivantes pour sécuriser votre infrastructure d'identité Azure AD : https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

Attaque Solorigate

Chaîne d'attaque de bout en bout de haut niveau




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
Suspicious file deletion activity
Scheduled task possibly hijacked
Suspicious remote activity on win-
Suspicious file creation initiated
Abnormal remote scheduled task

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

Série de vidéos consacrées à Solorigate

Étapes suivantes

01 Regardez la série de vidéos consacrées à Solorigate à cet emplacement

02 Visitez le site de Sécurité Microsoft pour plus de mises à jour : www.microsoft.com/en-us/security/business

03 Lisez les billets de blog sur : www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security