

Visão geral sobre o Solorigate

Tim Burrell

Gerente parceiro de Engenharia

Centro de Inteligência Contra Ameaças da Microsoft

18 de fevereiro de 2021

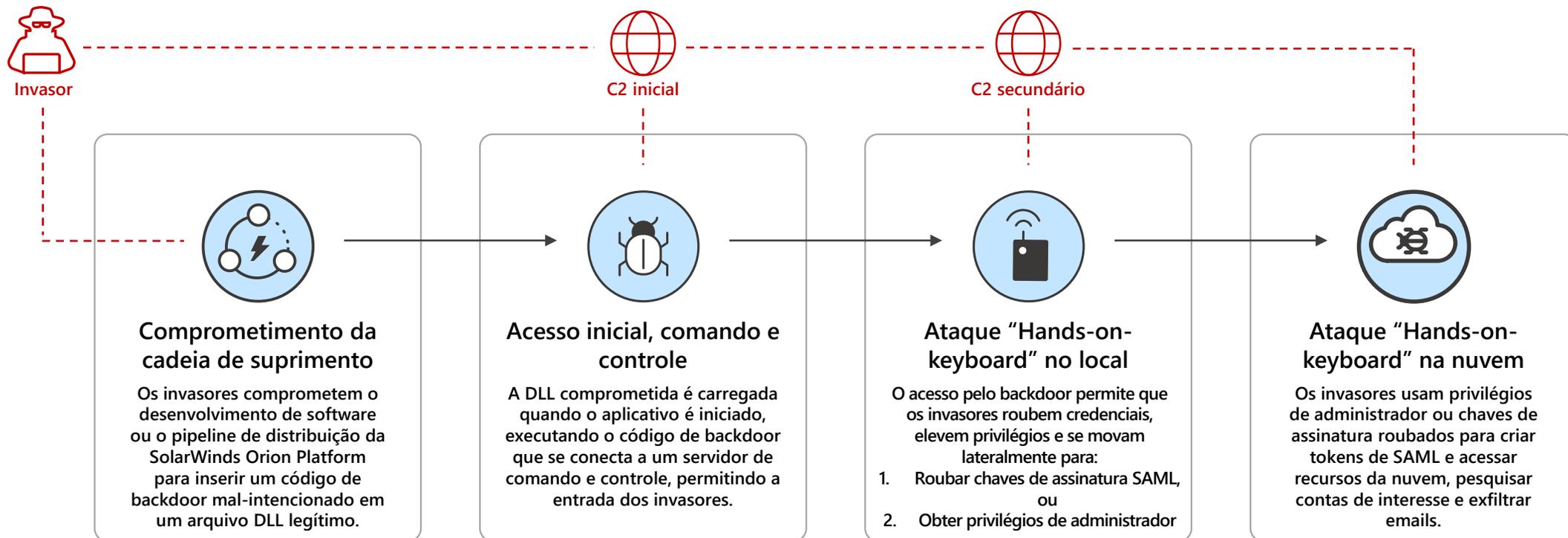
Série de vídeos sobre o Solorigate

Como ajudar a proteger sua organização de ataques como o Solorigate.

- 01** Visão geral do Solorigate
- 02** Como ocorreu o Solorigate
- 03** Como o invasor consegue acessar contas
- 04** Sete etapas para ajudar a proteger sua organização
- 05** É hora de investir na modernização de seu SOC

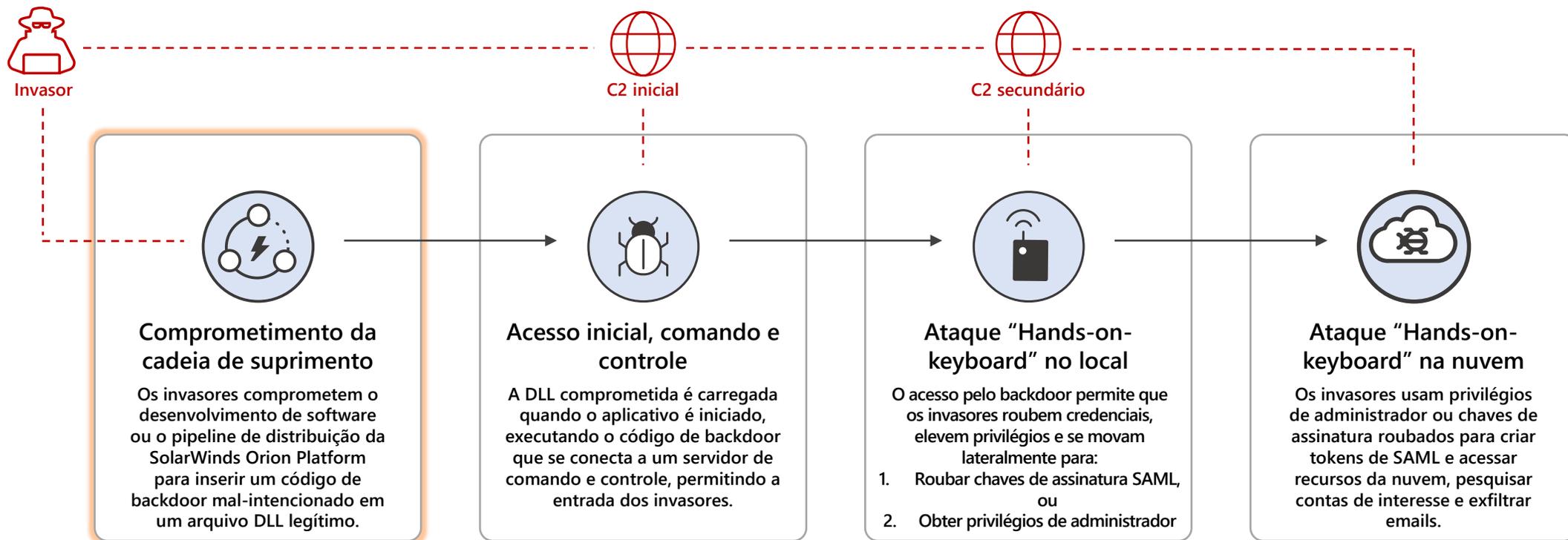
Ataque Solorigate

Cadeia de ataque de ponta a ponta de alto nível



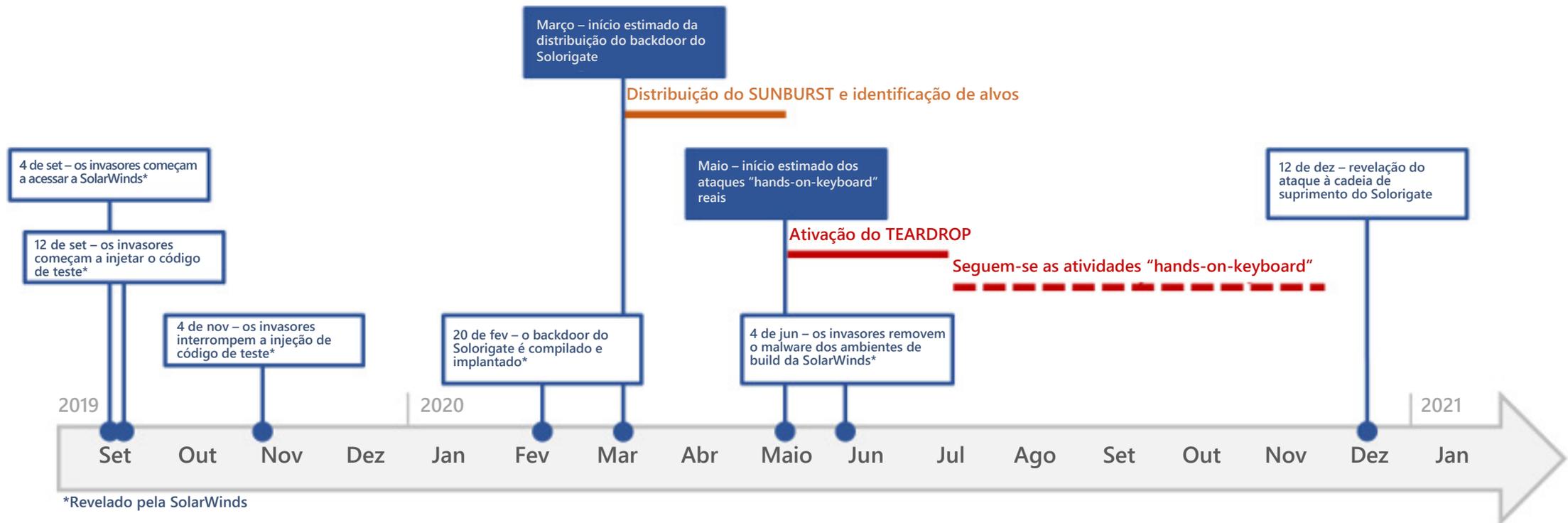
Ataque Solorigate

Cadeia de ataque de ponta a ponta de alto nível



Ataque Solorigate

Linha do tempo



*Revelado pela SolarWinds

Microsoft

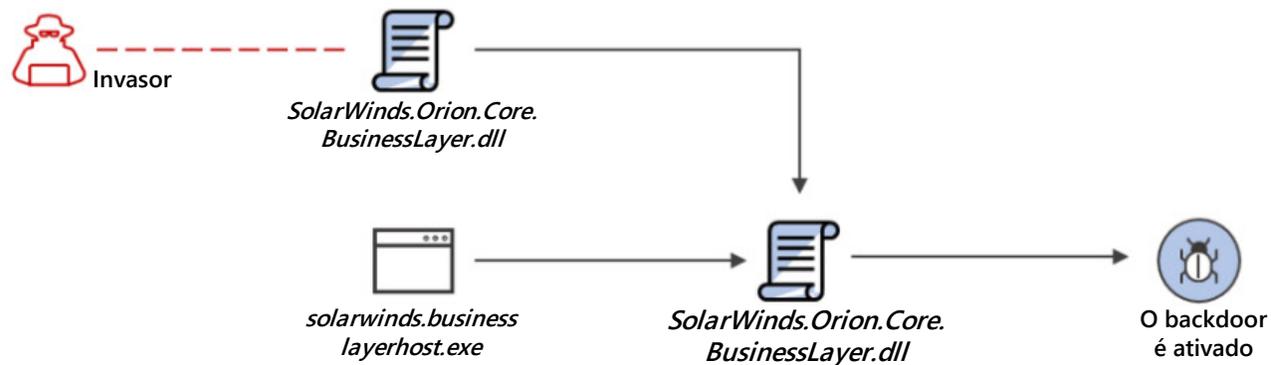
Informação verificada em 21/01/2021. Confira as últimas atualizações em aka.ms/solorigate

ATAQUE À CADEIA DE SUPRIMENTO

Os invasores inserem código mal-intencionado em um componente DLL de um software legítimo. A DLL comprometida é distribuída às organizações que usam esse software.

EXECUÇÃO, PERSISTÊNCIA

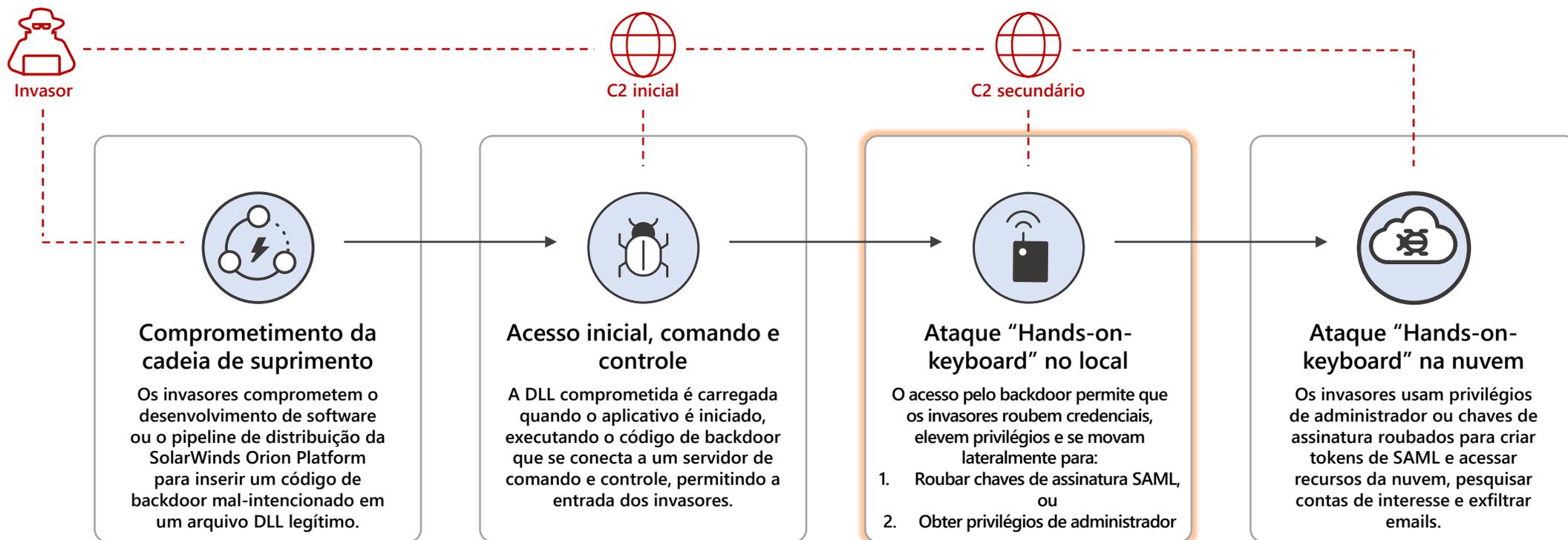
Quando o software é iniciado, a DLL comprometida é carregada, e o código mal-intencionado inserido chama a função que contém as funcionalidades de backdoor.



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

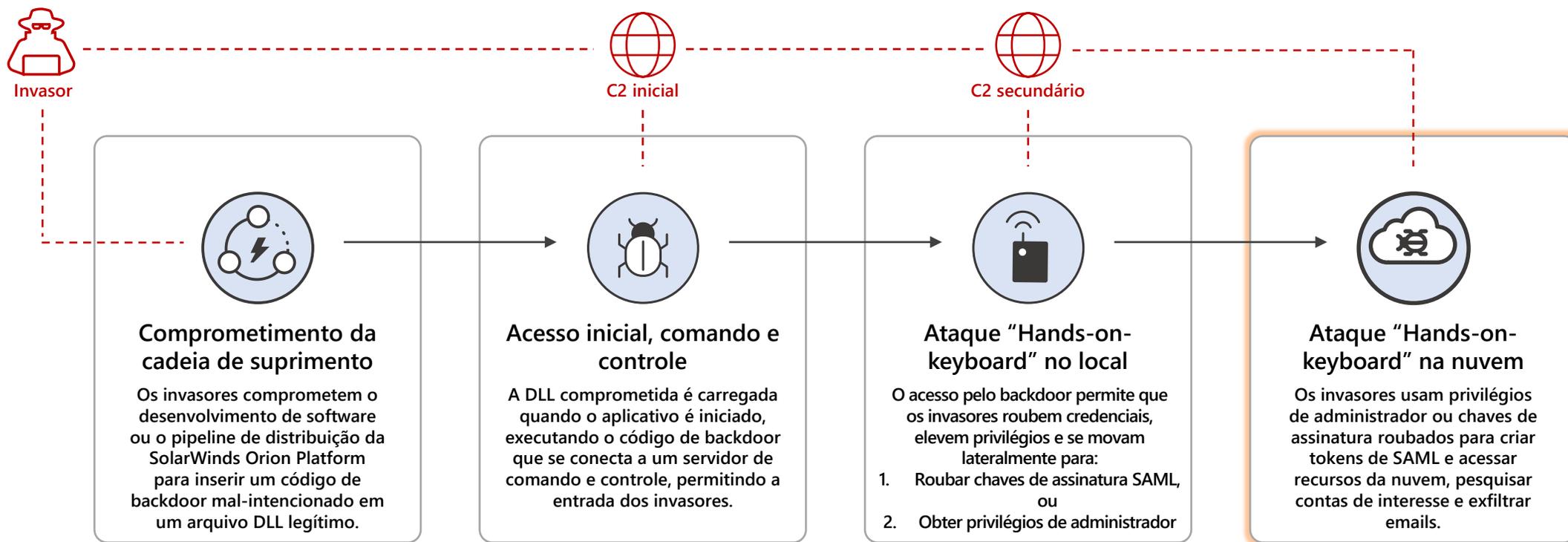
Ataque Solorigate

Cadeia de ataque de ponta a ponta de alto nível



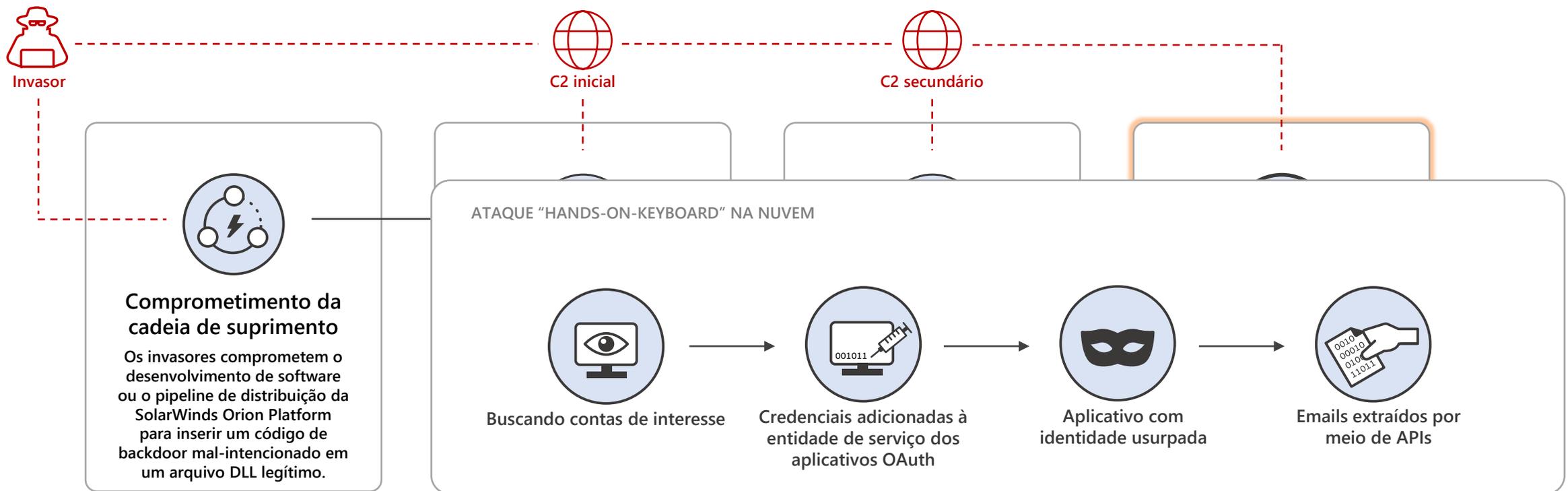
Ataque Solorigate

Cadeia de ataque de ponta a ponta de alto nível



Ataque Solorigate

Cadeia de ataque de ponta a ponta de alto nível



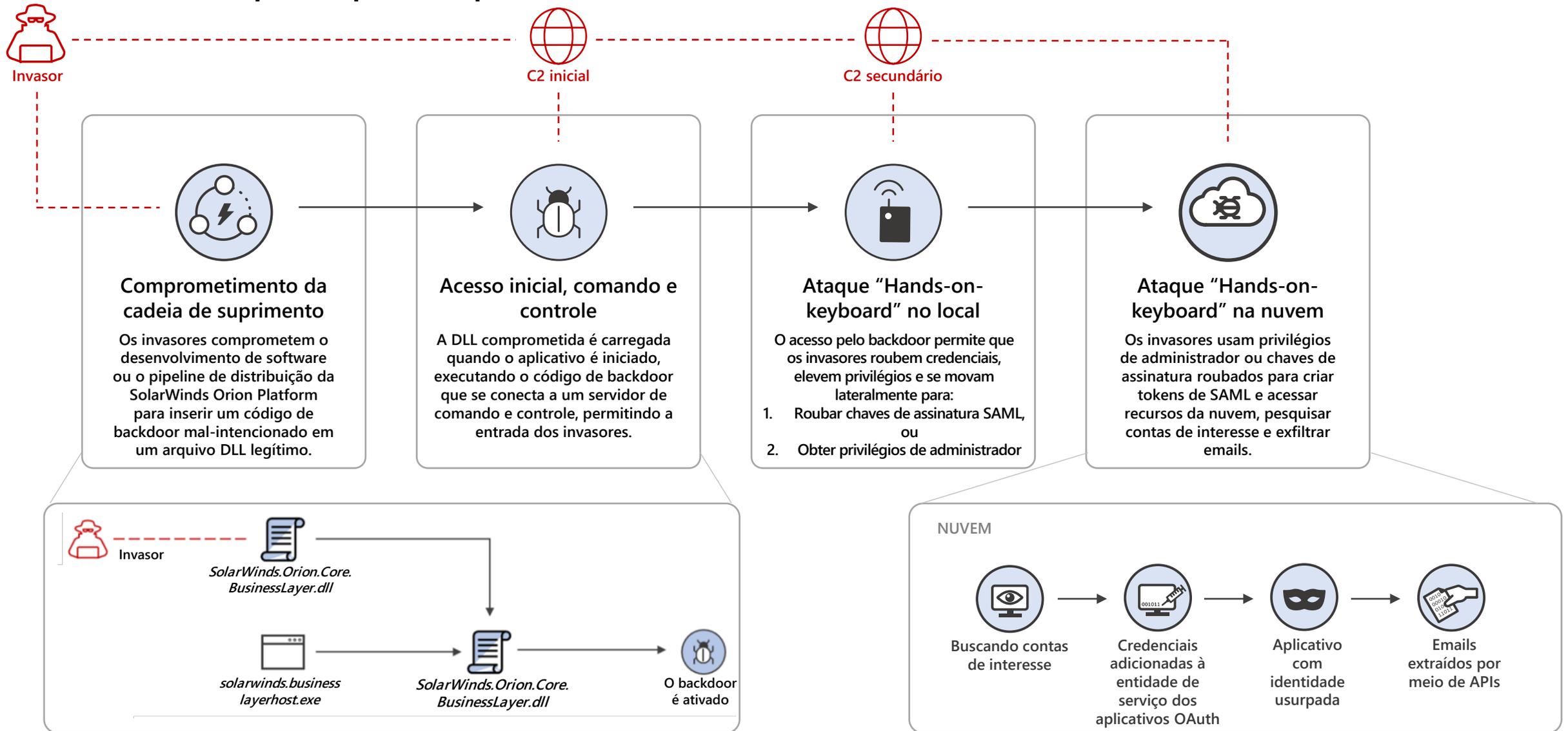
Defesas recomendadas

Sete etapas para ajudar a se proteger das técnicas vistas no Solorigate

1. Executar antivírus atualizados e produtos EDR.
2. Bloquear pontos de extremidade C2 conhecidos que usam a infraestrutura da sua rede.
3. Proteger as chaves de assinatura do seu token SAML e avaliar o uso de segurança de hardware para seus certificados de assinatura de token SAML. Para os Serviços de Federação do Active Directory (AD FS), analise as recomendações de melhores práticas da Microsoft: <https://docs.microsoft.com/pt-br/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs>
4. Siga as melhores práticas de direitos de usuário administrador e reduza a quantidade de usuários que são membros de funções de diretório de alto privilégio.
5. Verificar se as contas de serviço com direitos administrativos usam segredos de alta entropia (ou seja, certificados) armazenados de forma segura. Monitore alterações, entradas e uso de contas de serviço anômalas.
6. Remover ou desabilitar entidades de serviço e aplicativos não usados ou desnecessários. Reduza as permissões daqueles que continuarem ativos.
7. Conferir estas recomendações adicionais para proteger sua infraestrutura de identidade do Azure AD: <https://docs.microsoft.com/pt-br/azure/security/fundamentals/steps-secure-identity>

Ataque Solorigate

Cadeia de ataque de ponta a ponta de alto nível



- 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



© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

- Dec 22, 2020, 1:02:29 AM | New
A WMI event filter was bound to a suspicious event consumer on desktop-3u4jij1
- Dec 22, 2020, 11:08:57 AM | New
Process launched with the security context of another user on win-9njrns9ohht by user mind0xp
- Dec 22, 2020, 11:37:49 AM | New
Suspicious file deletion activity was mind0xp
- Dec 22, 2020, 11:58:50 AM | New
Scheduled task possibly hijacked o
- Dec 22, 2020, 11:58:50 AM | New
Suspicious remote activity on win... and more.
- Dec 22, 2020, 11:58:50 AM | New
Suspicious file creation initiated re mind0xp
- Dec 22, 2020, 12:48:39 PM | New
Abnormal remote scheduled task n... and more.
- Dec 22, 2020, 12:48:39 PM | New
Suspicious file creation initiated re

Scope

2 impacted devices
3 impacted users

Top impacted entities

Entity type	Risk level/investigation priority	Tags
[Device Icon]	High	
[Device Icon]	High	
[User Icon]	No data available	
[User Icon]	No data available	
[User Icon]	No data available	

View entities

Incident information

This incident might be associated with...

Associated incidents

Incident ID	Reason	Entity
24851	Same file	sqkwpjwe
24576	Same file	legit payl...
24576	Same file	pay/waldf

Tags summary

- Incident tags
- Data sensitivity
- Device groups
- User groups

Azure Sentinel | Analytics

Selected workspace: [Redacted]

Search (Ctrl+) Create Refresh Enable Disable Delete

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks (Preview)
- Entity behavior

79 Active rules

Rules by severity



Active rules Rule templates

Search

Severity: All

Rule Type: Scheduled

Tactics: 2 selected

Data Sources: 3 selected

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 vídeos sobre o Solorigate

Próximas Etapas

- 01** Assista à série de vídeos sobre o Solorigate neste local
- 02** Confira mais atualizações na Segurança da Microsoft:
www.microsoft.com/pt-br/security/business
- 03** Leia as postagens no blog em:
www.microsoft.com/security/blog

<https://aka.ms/solorigate>

