Microsoft

Общ преглед на Solorigate

Тим Бърел

Технически ръководител партньор

Център на Microsoft Threat Intelligence

18 февруари 2021 г.

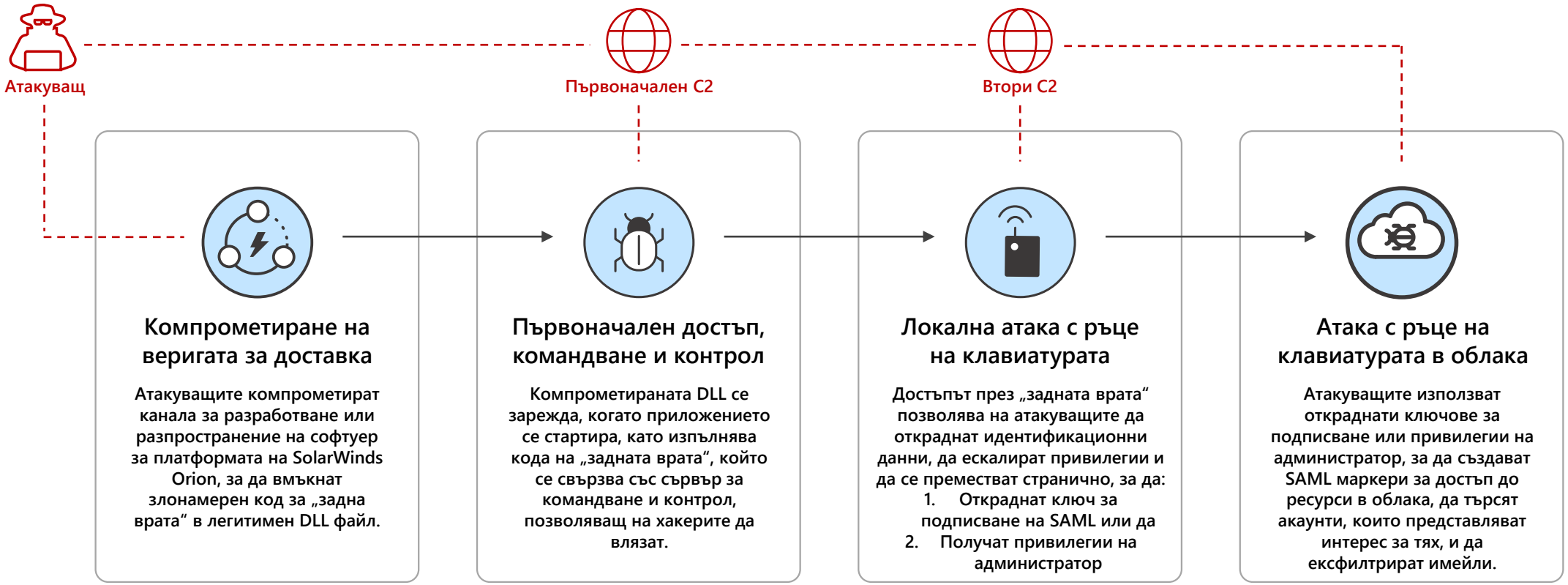
Поредица от видеоклипове за Solorigate

Как да защитите вашата организация от атаки в стил Solorigate.

Microsoft Security

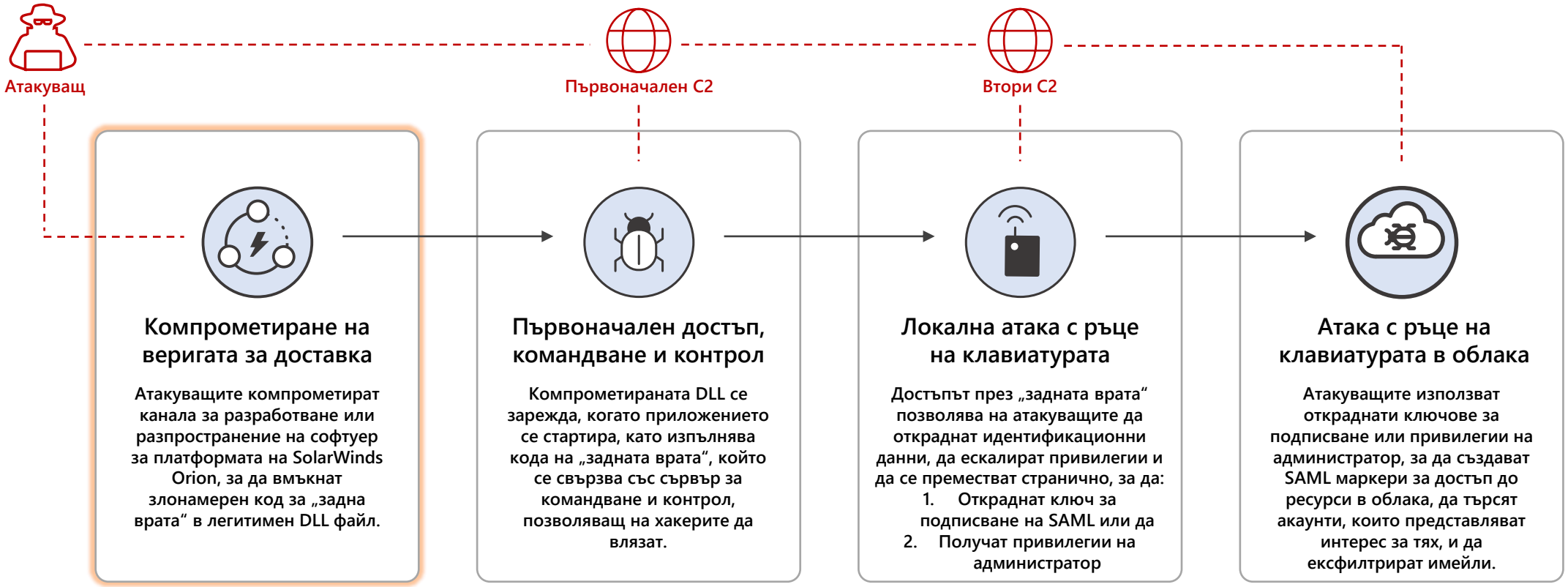
Атака Solorigate

Верига на цялостна атака от най-високо ниво



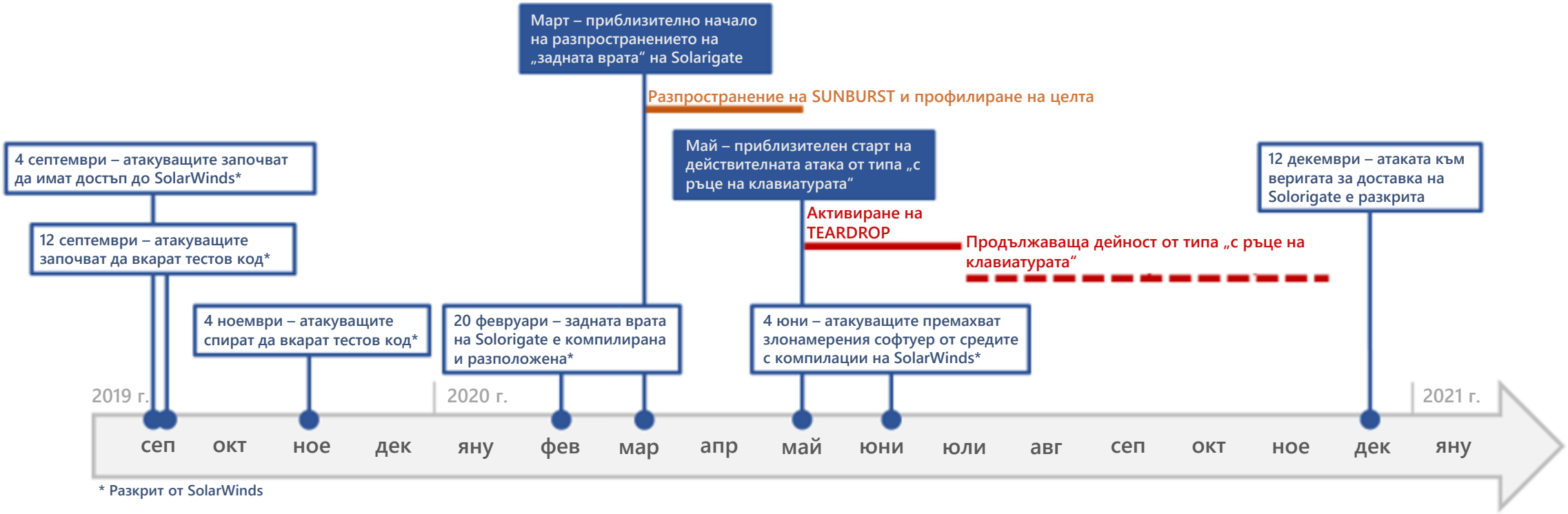
Атака Solorigate

Верига на цялостна атака от най-високо ниво



Атака Solorigate

Времева линия



* Разкрит от SolarWinds

Microsoft

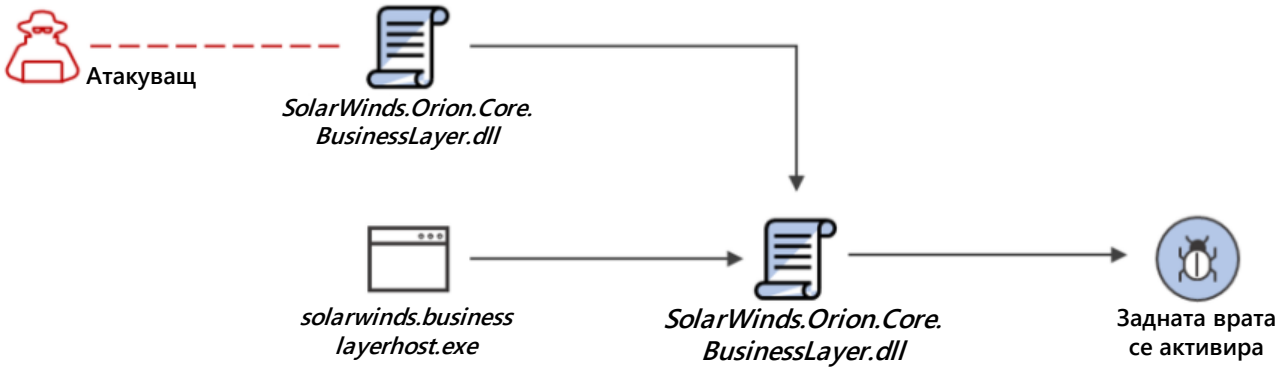
Информацията е правилна към 21.1.2021 г., вижте aka.ms/solorigate за най-новите актуализации

АТАКА КЪМ ВЕРИГА ЗА ДОСТАВКА

Атакуващите вмъкват злонамерен код в DLL компонент на легитимен софтуер. Компрометираната DLL се разпространява до организации, които използват свързания софтуер.

ИЗПЪЛНЕНИЕ, УСТОЙЧИВОСТ

Когато софтуерът се стартира, компрометираната DLL се зарежда и вмъкнатият злонамерен код извиква функцията, която съдържа възможностите за задна врата.



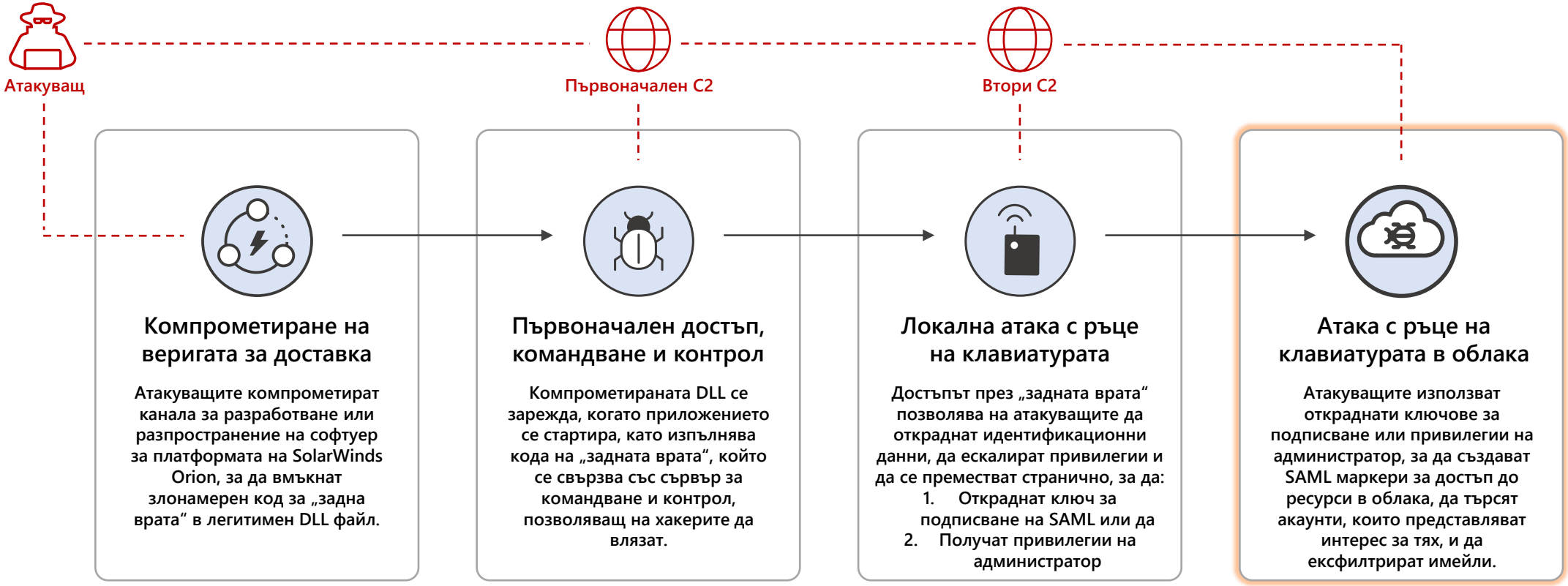

```
"Signer": "Solarwinds Worldwide, LLC",
"SignerHash": "47d92d49e6f7f296260da1af355f941eb25360c4",
```

Атака Solorigate

Верига на цялостна атака от най-високо ниво

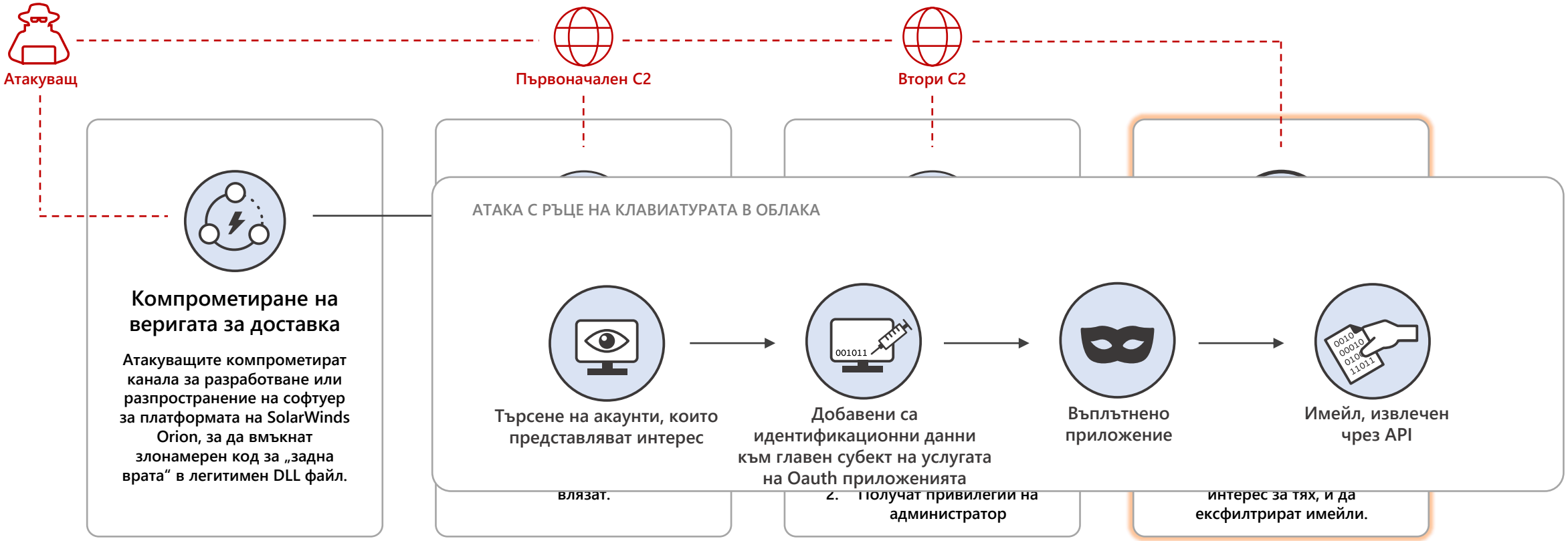
Атака Solorigate

Верига на цялостна атака от най-високо ниво



Атака Solorigate

Верига на цялостна атака от най-високо ниво



Препоръчителни защити

7 стъпки, които ще ви помогнат да се защитите от техниките, видени в Solorigate

1. Изпълнявайте актуални антивирусни и EDR продукти.

2. Блокирайте известни крайни точки на C2 с помощта на мрежовата си инфраструктура.

3. Защитавайте своите ключове за подписване на SAML маркери и помислете за хардуерна защита на вашите сертификати за подписване на SAML маркери. За услугите на Active Directory за улесняване на достъпа прегледайте препоръките за най-добри практики на Microsoft: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs

4. Следвайте най-добрите практики за потребителски права на администраторите и намалете броя на потребителите, които са членове на роли в указателя с високи привилегии.

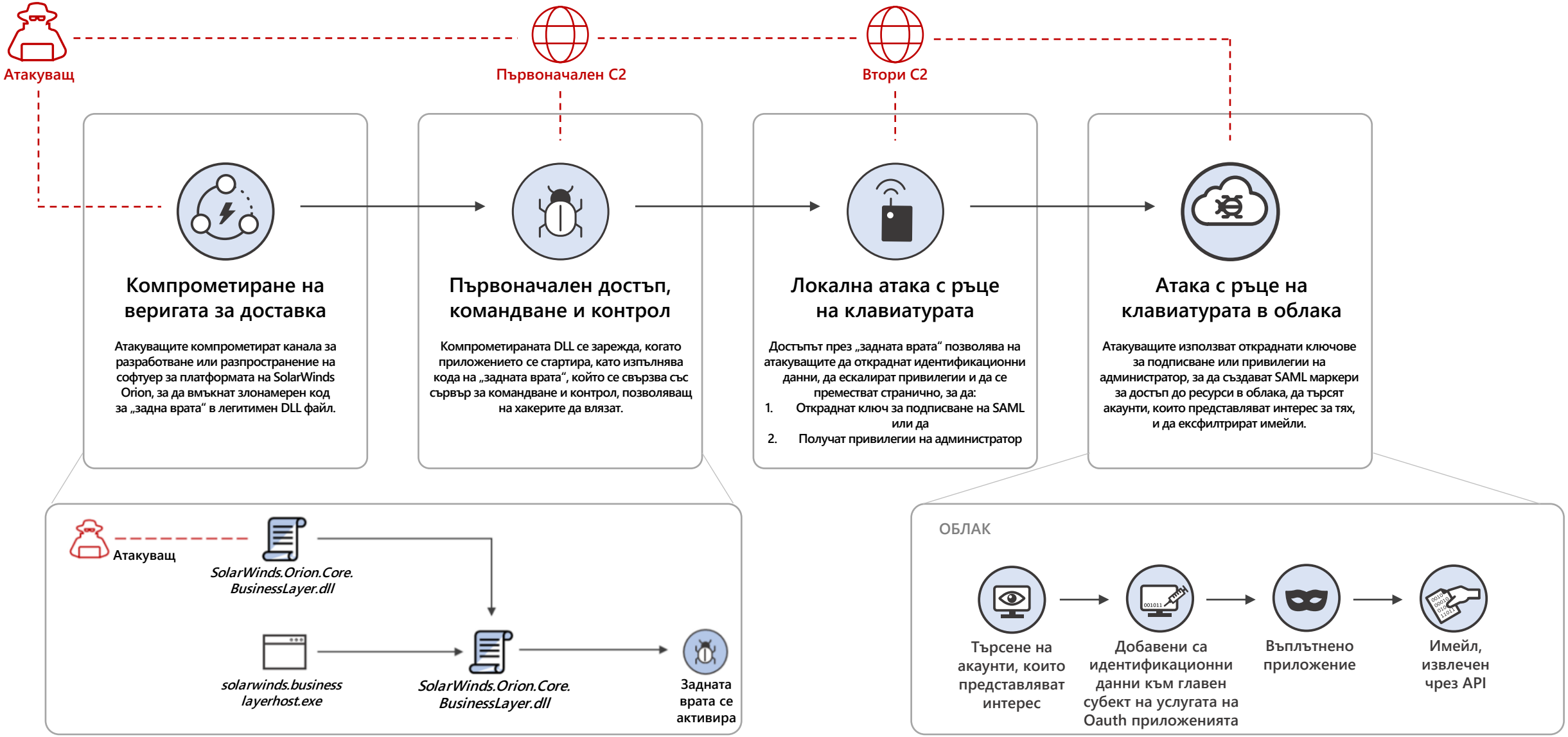
5. Уверете се, че акаунтите за услуги с администраторски права използват тайни с висока ентропия (т.е. сертификати), които се съхраняват защитено. Следете за промени, влизания и използване на анормални акаунти за услуги.

6. Премахнете или забранете неизползваните или ненужните главни субекти на приложения и услуги. Намалете разрешенията за тези, които все още имате.

7. Вижте тези допълнителни препоръки за защита на вашата инфраструктура за самоличности на Azure AD: https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

Атака Solorigate

Верига на цялостна атака от най-високо ниво



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

Dec 22, 2020, 1:52:20 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 wa
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, 12:48:19 PM | New
Abnormal remote scheduled task r
, and more.

Dec 22, 2020, 12:48:19 PM | New
Suspicious file creation initiated re

Scope

2 impacted devices
3 impacted users

Top impacted entities

Entity type	Risk level/investigation priority	Tags
	High	
	High	
	No data available	
	No data available	
	No data available	

View entities

Incident Information

This incident might be associated wit...

Associated incidents

Incident ID	Reason	Entity
24851	Same file	sqlceip.exe
24576	Same file	legit_payl...
24576	Same file	payload.dll

Tags summary
Incident tags
Data sensitivity
Device groups
User groups

Azure Sentinel | Analytics

Selected workspace: [redacted]

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

Поредица от видеоклипове за Solorigate

Следващи стъпки

01 Гледайте поредицата видеоклипове за Solorigate на това място

02 Посетете Microsoft Security за още актуализации: www.microsoft.com/en-us/security/business

03 Прочетете публикациите в блога на адрес: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft