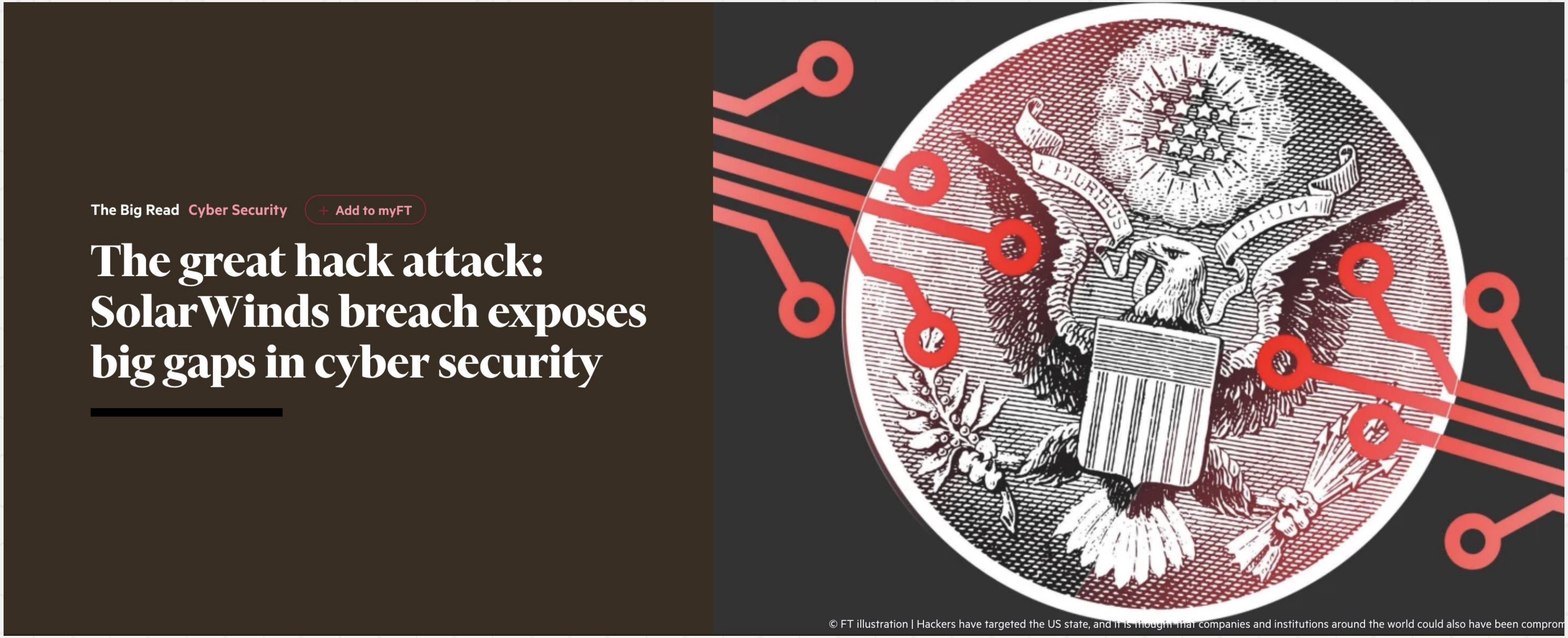
CYBERARK®

ANATOMY OF THE SOLARWINDS ATTACK

Andy Thompson, Research Evangelist, CyberArk Labs



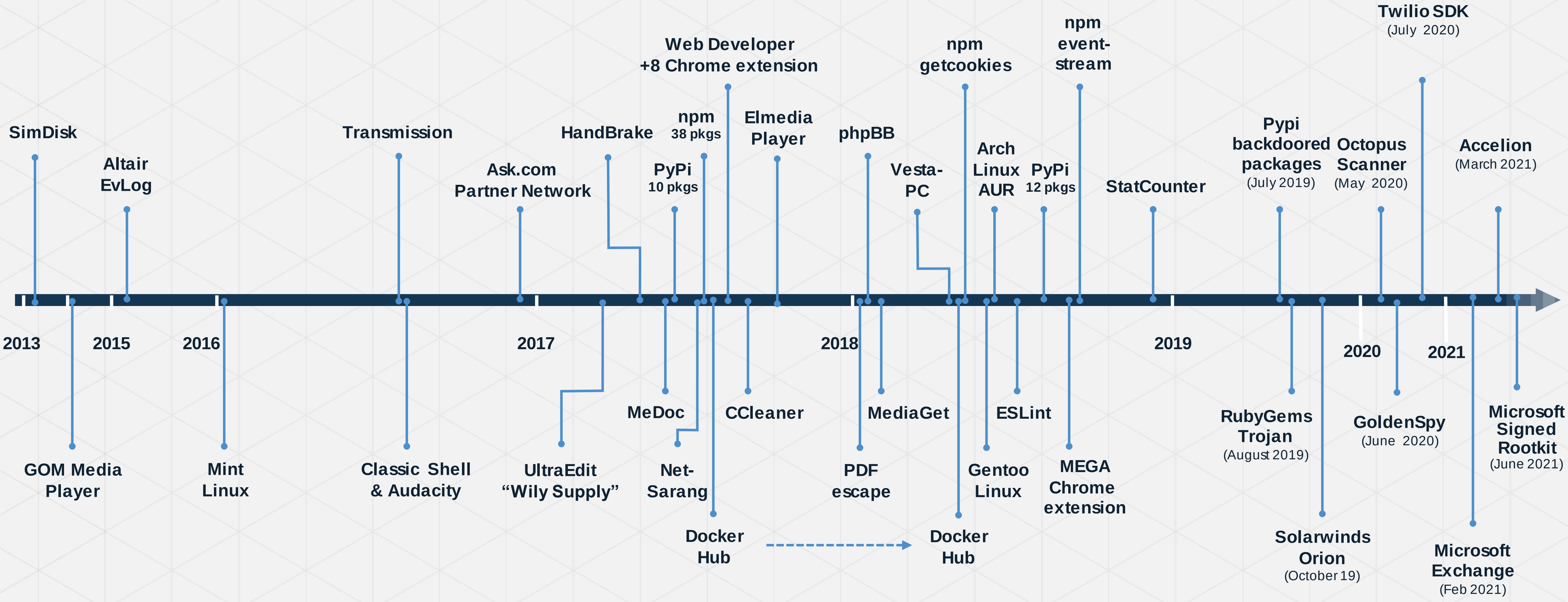
The Big Read Cyber Security

The great hack attack: SolarWinds breach exposes big gaps in cyber security

© FT illustration | Hackers have targeted the US state, and it is thought that companies and institutions around the world could also have been comprom

https://www.ft.com/content/c13dbb51-907b-4db7-8347-30921ef931c2

THE RISE OF THE DIGITAL SUPPLY CHAIN ATTACK



SimDisk

2013

GOM Media Player

2015

Altair EvLog

2016

Mint Linux

Transmission

Classic Shell & Audacity

Ask.com Partner Network

2017

UltraEdit “Wily Supply”

HandBrake

MeDoc

PyPi 10 pkgs

Net-Sarang

npm 38 pkgs

Docker Hub

Web Developer +8 Chrome extension

CCleaner

Elmedia Player

2018

PDF escape

phpBB

MediaGet

Vesta-PC

Docker Hub

npm getcookies

Gentoo Linux

Arch Linux AUR

ESLint

PyPi 12 pkgs

MEGA Chrome extension

npm event-stream

StatCounter

2019

Pypi backdoored packages (July 2019)

RubyGems Trojan (August 2019)

Solarwinds Orion (October 19)

2020

Octopus Scanner (May 2020)

GoldenSpy (June 2020)

Twilio SDK (July 2020)

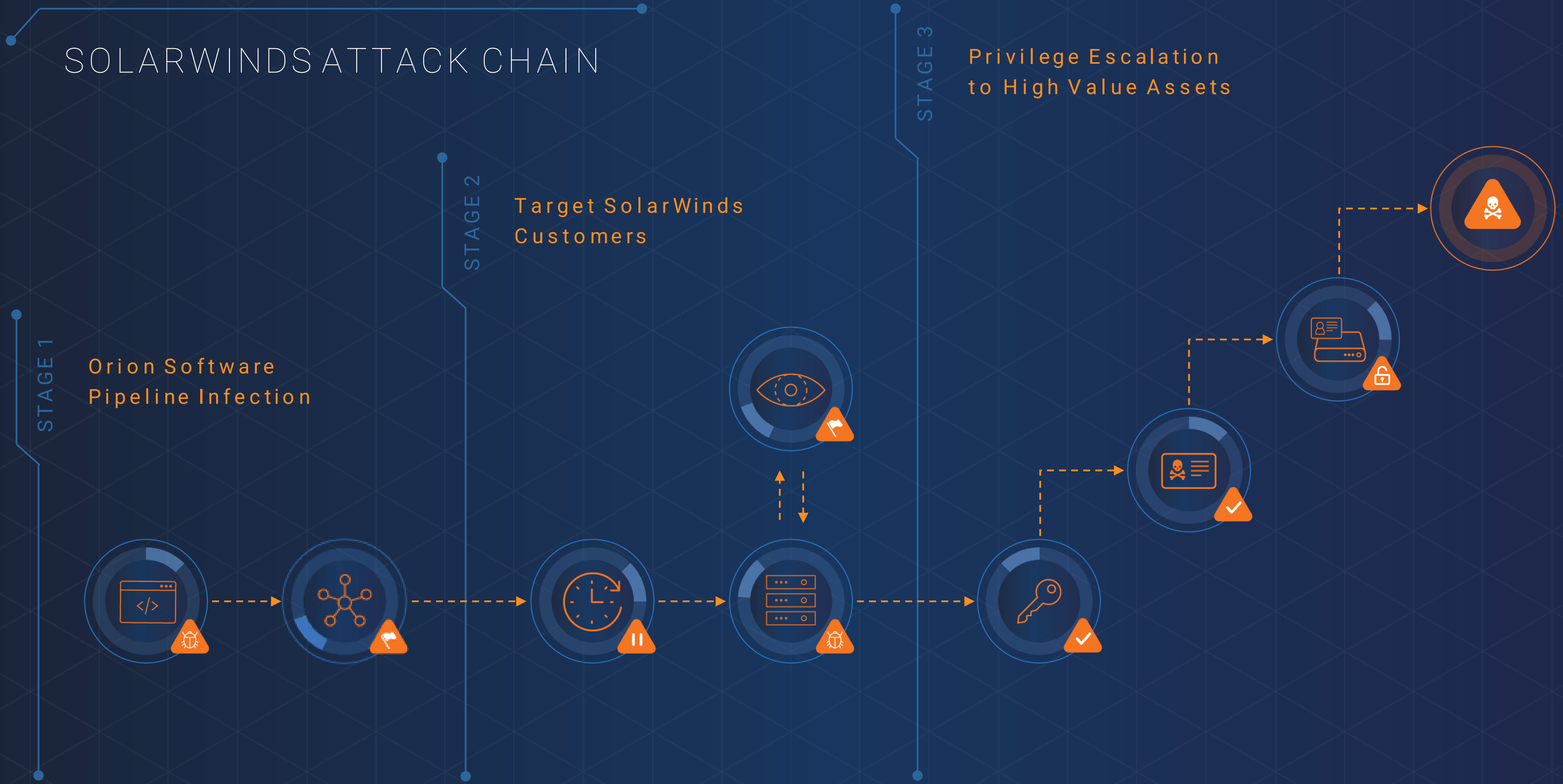
2021

Microsoft Exchange (Feb 2021)

Accelion (March 2021)

Microsoft Signed Rootkit (June 2021)

SOLARWINDS ATTACK CHAIN



STAGE 1

Orion Software Pipeline Infection

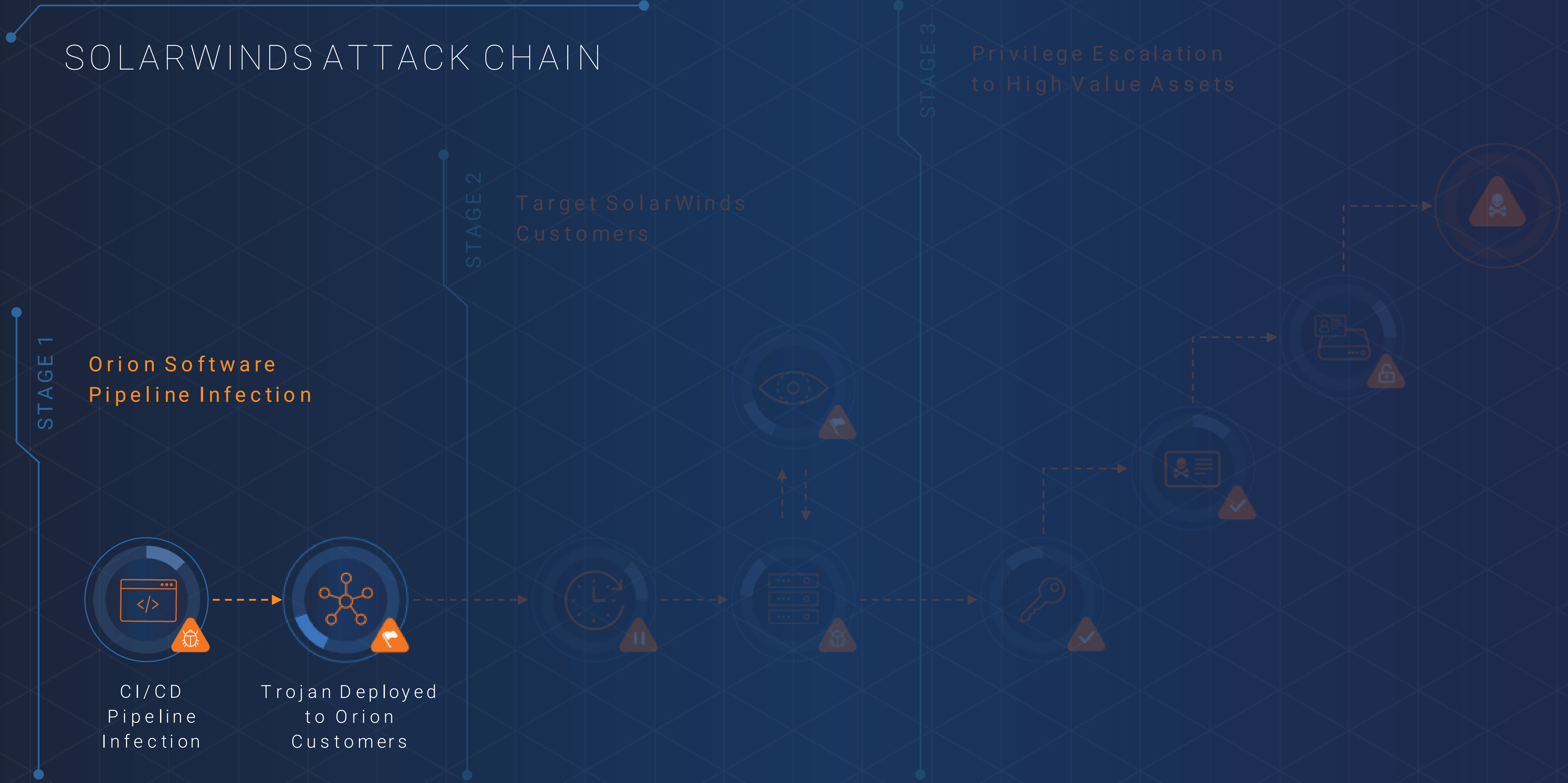
STAGE 2

Target SolarWinds Customers

STAGE 3

Privilege Escalation to High Value Assets

SOLARWINDS ATTACK CHAIN



STAGE 1

Orion Software Pipeline Infection

CI/CD Pipeline Infection

Trojan Deployed to Orion Customers

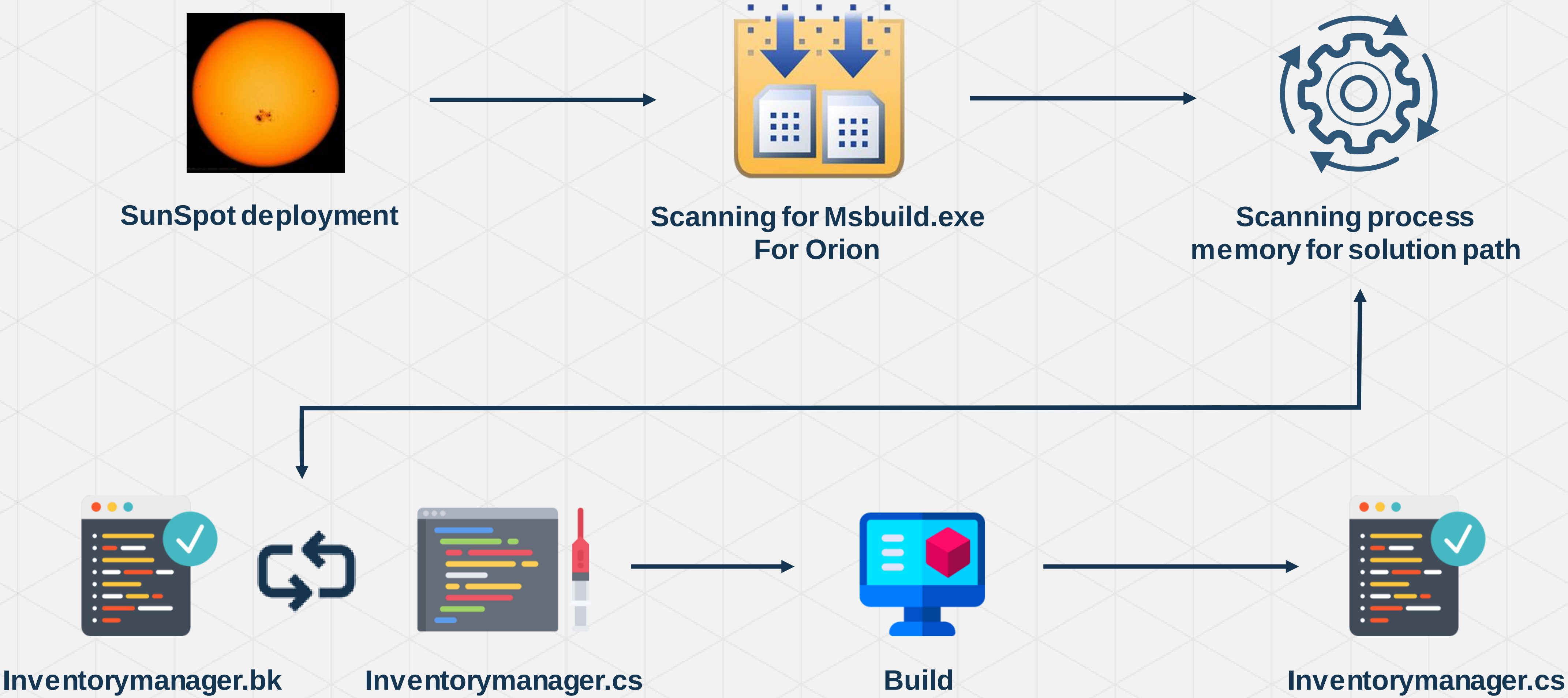
STAGE 2

Target SolarWinds Customers

STAGE 3

Privilege Escalation to High Value Assets

TROJANIZING OPERATION



SunSpot deployment

Scanning for Msbuild.exe
For Orion

Scanning process
memory for solution path

Inventorymanager.bk

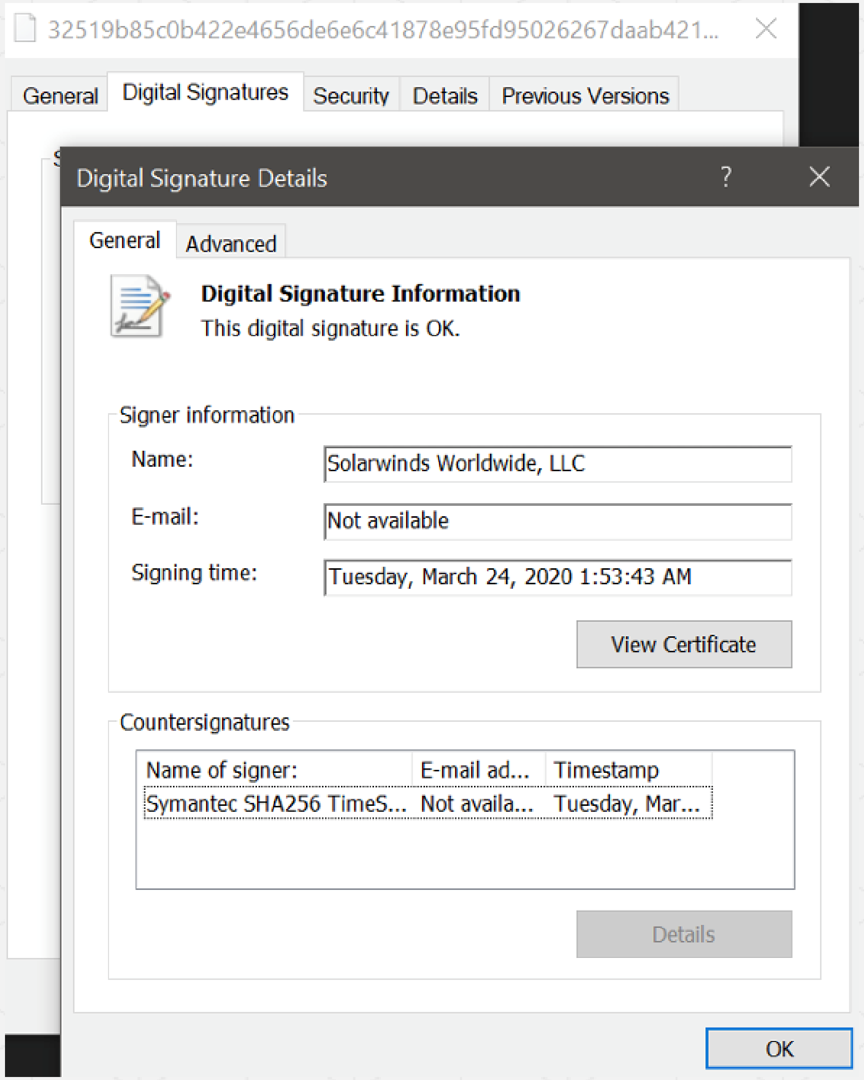
Inventorymanager.cs

Build

Inventorymanager.cs

https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

SIGNED MALWARE



Digital Signature Information

This digital signature is OK.

Signer information

Name: Solarwinds Worldwide, LLC

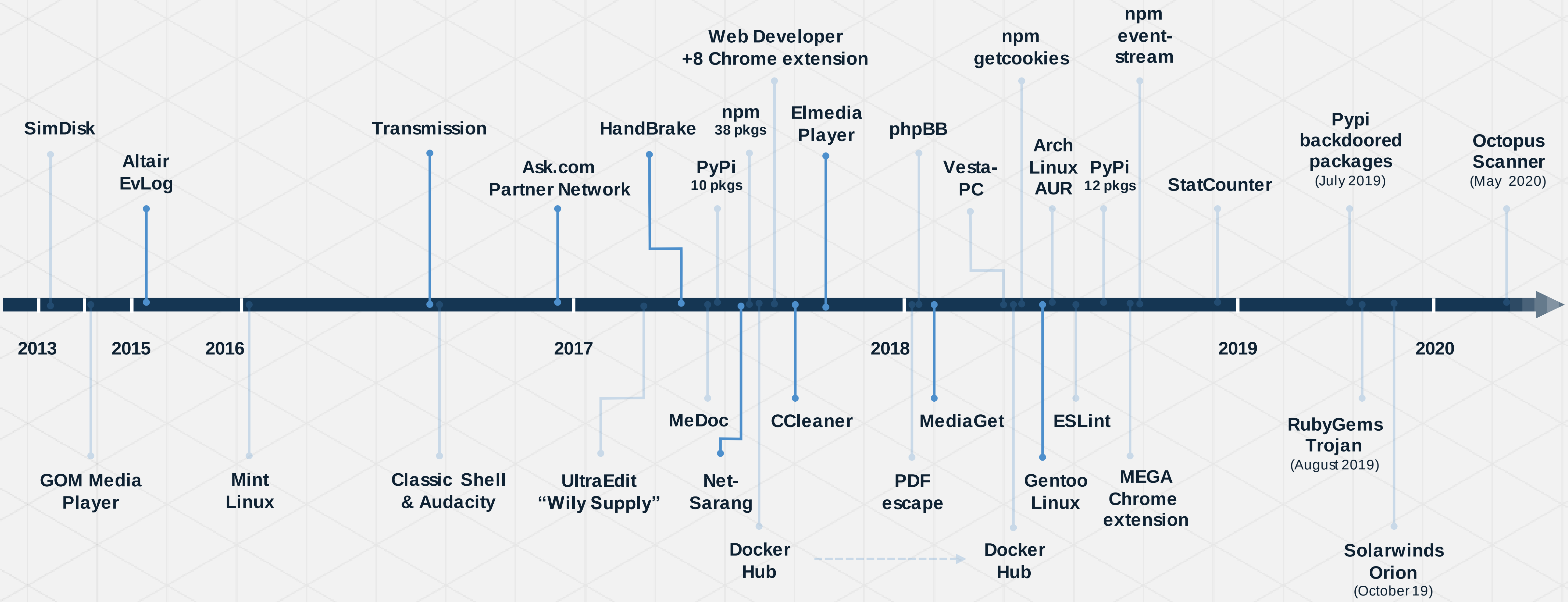
E-mail: Not available

Signing time: Tuesday, March 24, 2020 1:53:43 AM

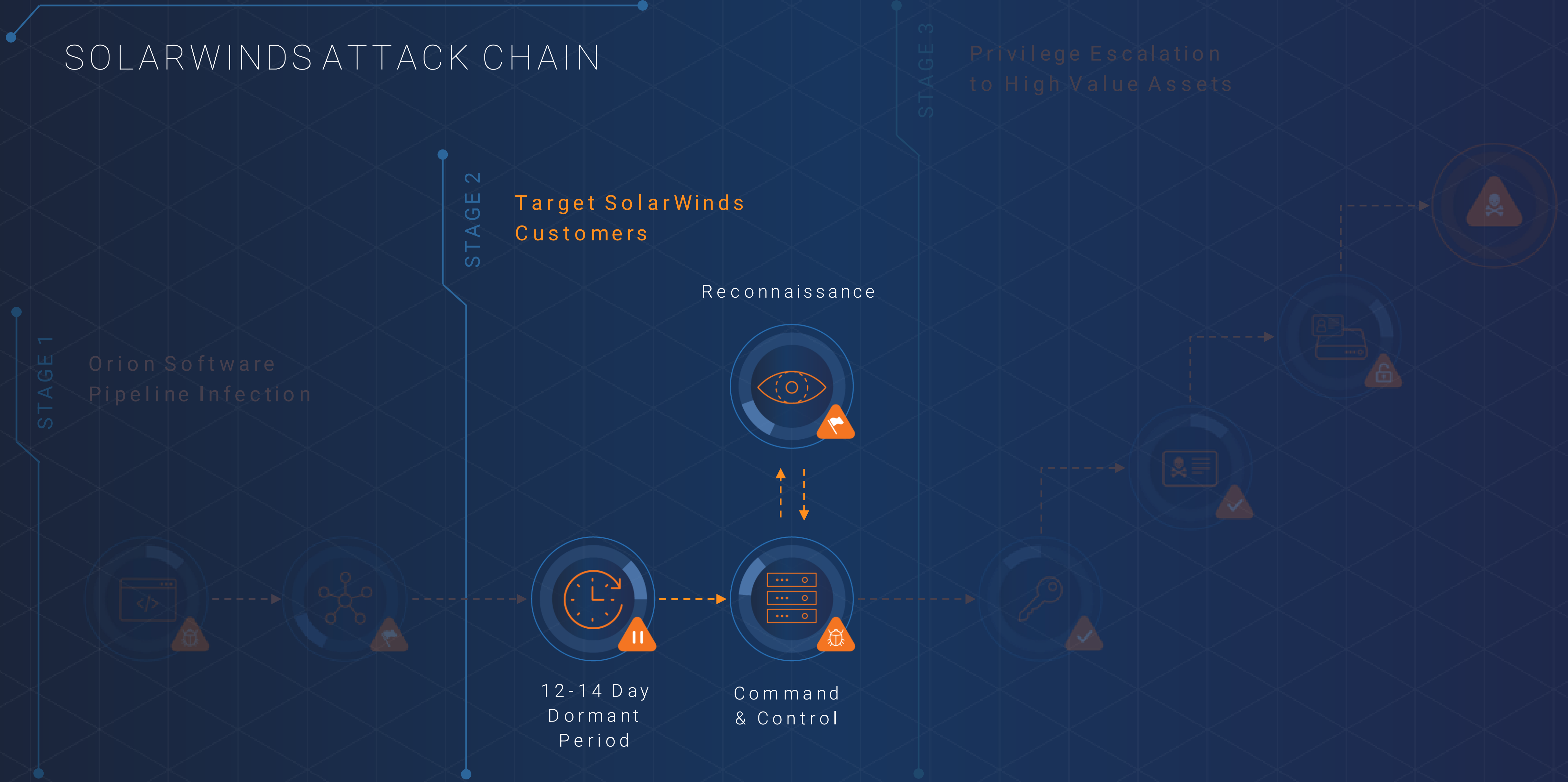
Countersignatures

Name of signer:	E-mail ad...	Timestamp
Symantec SHA256 TimeS...	Not availa...	Tuesday, Mar...

SIGNED CODE


SimDisk
Altair EvLog
GOM Media Player
Mint Linux
Transmission
Classic Shell & Audacity
Ask.com Partner Network
UltraEdit “Wily Supply”
HandBrake
MeDoc
PyPi 10 pkgs
npm 38 pkgs
Net-Sarang
Docker Hub
Web Developer +8 Chrome extension
CCleaner
Elmedia Player
phpBB
PDF escape
MediaGet
Vesta-PC
Docker Hub
npm getcookies
Gentoo Linux
Arch Linux AUR
ESLint
PyPi 12 pkgs
MEGA Chrome extension
npm event-stream
StatCounter
Pypi backdoored packages (July 2019)
RubyGems Trojan (August 2019)
Solarwinds Orion (October 19)
Octopus Scanner (May 2020)
2013
2015
2016
2017
2018
2019
2020

SOLARWINDS ATTACK CHAIN



STAGE 1

Orion Software Pipeline Infection

STAGE 2

Target SolarWinds Customers

Reconnaissance

12-14 Day Dormant Period

Command & Control

STAGE 3

Privilege Escalation to High Value Assets

RECONNAISSANCE & OPSSEC

Avoiding early detection
and analysis

# The following hashes are checked against processes, services, and drivers by SUNBURST.

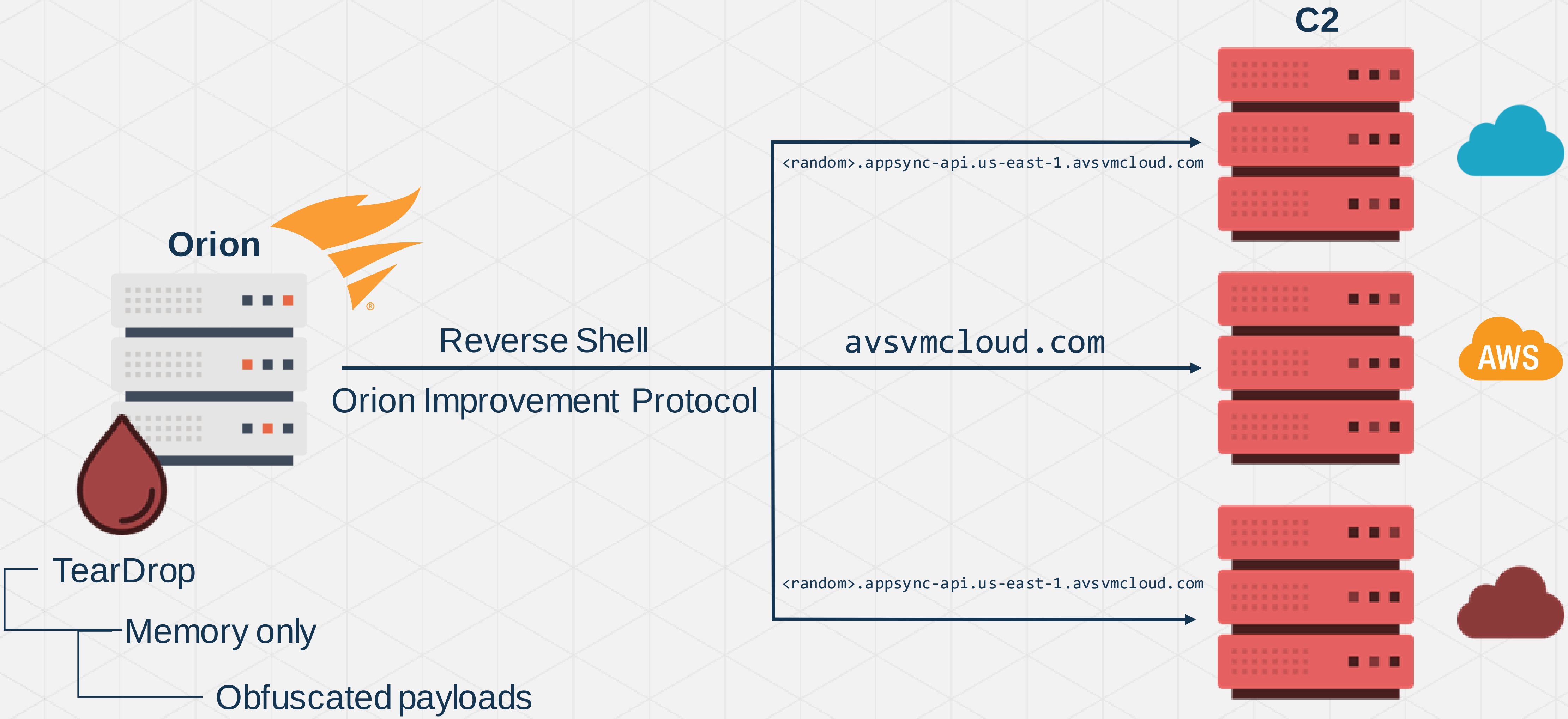
# The hash is calculated by performing a FNV-1a 64bit hash of the lowercase string then XOR by 6605813339339102567.

sysmon64 3538022140597504361
carbonblack 11385275378891906608
f-secure filter 13783346438774742614

cybkerneltracker.sys 17097380490166623672

ollydbg 4501656691368064027
tanium 7175363135479931834
x64dbg 14193859431895170587
diskmon 7810436520414958497

https://github.com/fireeye/sunburst_countermeasures/blob/main/fnv1a_xor_hashes.txt



C2

Orion

Reverse Shell

Orion Improvement Protocol

<random>.appsync-api.us-east-1.avsvmcloud.com

avsvmcloud.com

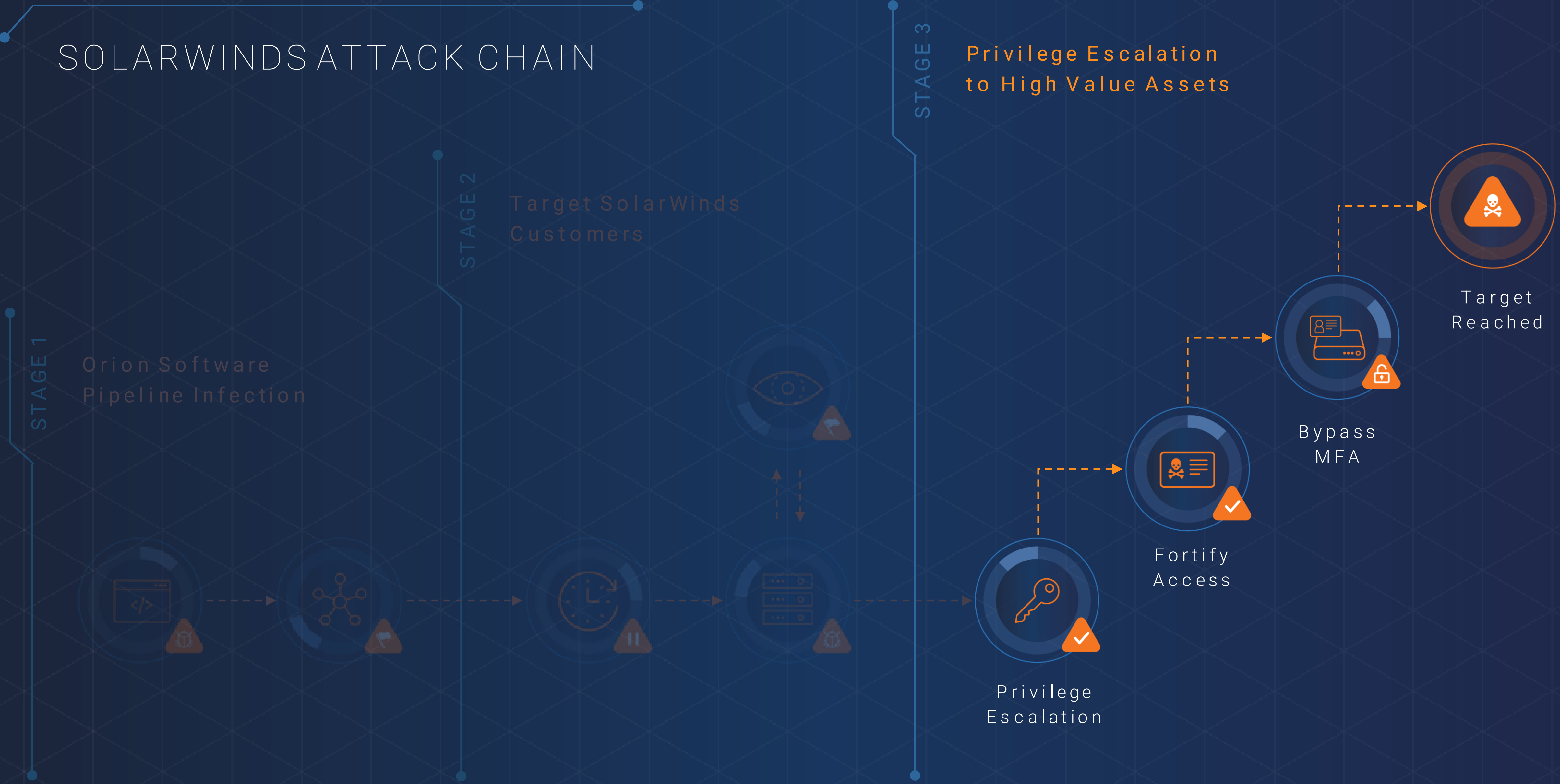
<random>.appsync-api.us-east-1.avsvmcloud.com

TearDrop

Memory only

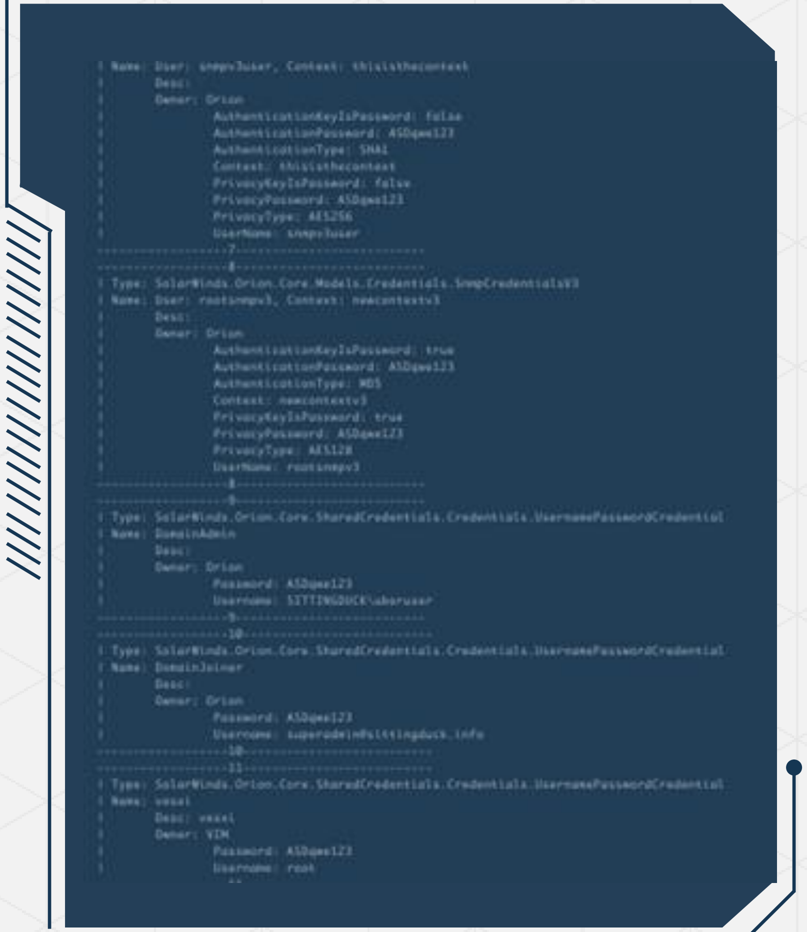
Obfuscated payloads

SOLARWINDS ATTACK CHAIN

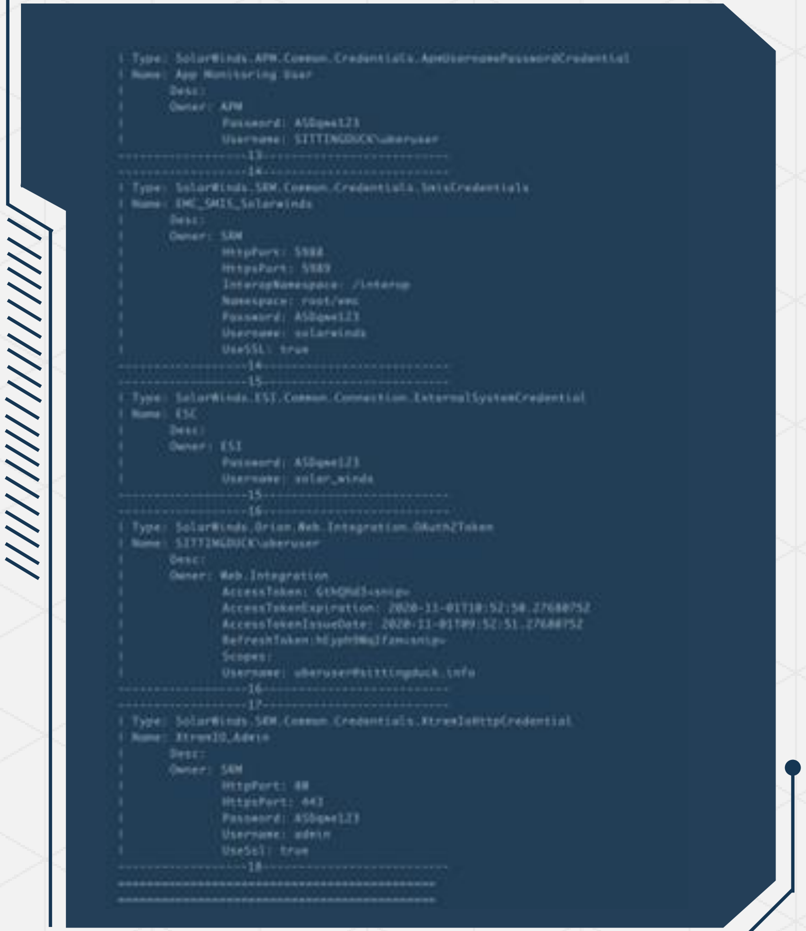


STAGE 1
Orion Software Pipeline Infection
STAGE 2
Target SolarWinds Customers
STAGE 3
Privilege Escalation to High Value Assets
Privilege Escalation
Fortify Access
Bypass MFA
Target Reached

ESCALATION OF PRIVILEGES…

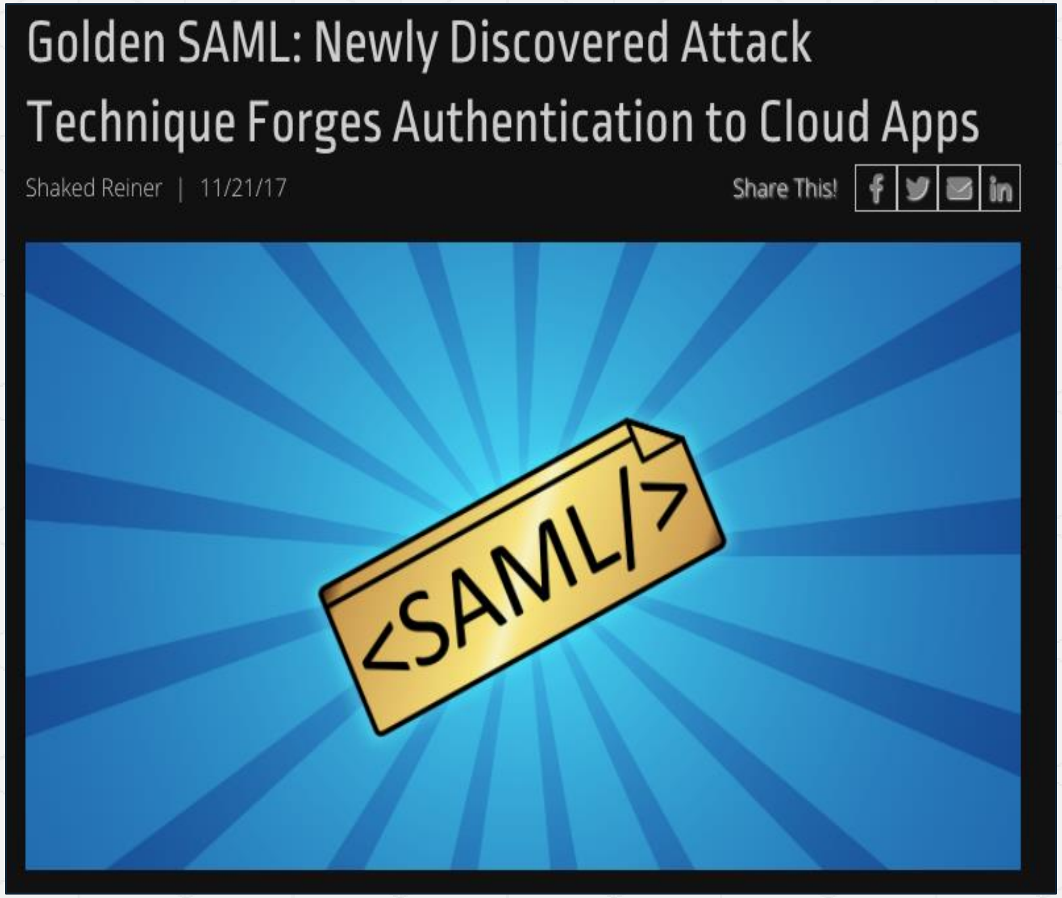


```
| Name: User: snmpv3user, Context: thisisthecontext
|       Desc:
|       Owner: Orion
|               AuthenticationKeyIsPassword: false
|               AuthenticationPassword: ASDqwe123
|               AuthenticationType: SHA1
|               Context: thisisthecontext
|               PrivacyKeyIsPassword: false
|               PrivacyPassword: ASDqwe123
|               PrivacyType: AES256
|               UserName: snmpv3user
--------------------7--------------------------
--------------------8--------------------------
| Type: SolarWinds.Orion.Core.Models.Credentials.SnmpCredentialsV3
| Name: User: rootsnmpv3, Context: newcontextv3
|       Desc:
|       Owner: Orion
|               AuthenticationKeyIsPassword: true
|               AuthenticationPassword: ASDqwe123
|               AuthenticationType: MD5
|               Context: newcontextv3
|               PrivacyKeyIsPassword: true
|               PrivacyPassword: ASDqwe123
|               PrivacyType: AES128
|               UserName: rootsnmpv3
--------------------8--------------------------
--------------------9--------------------------
| Type: SolarWinds.Orion.Core.SharedCredentials.Credentials.UsernamePasswordCredential
| Name: DomainAdmin
|       Desc:
|       Owner: Orion
|               Password: ASDqwe123
|               Username: SITTINGDUCK\uberuser
--------------------9--------------------------
--------------------10-------------------------
| Type: SolarWinds.Orion.Core.SharedCredentials.Credentials.UsernamePasswordCredential
| Name: DomainJoiner
|       Desc:
|       Owner: Orion
|               Password: ASDqwe123
|               Username: superadmin@sittingduck.info
--------------------10-------------------------
--------------------11-------------------------
| Type: SolarWinds.Orion.Core.SharedCredentials.Credentials.UsernamePasswordCredential
| Name: vesxi
|       Desc: vesxi
|       Owner: VIM
|               Password: ASDqwe123
|               Username: root
```



```
| Type: SolarWinds.APM.Common.Credentials.ApmUsernamePasswordCredential
| Name: App Monitoring User
|       Desc:
|       Owner: APM
|               Password: ASDqwe123
|               Username: SITTINGDUCK\uberuser
--------------------13-------------------------
--------------------14-------------------------
| Type: SolarWinds.SRM.Common.Credentials.SmisCredentials
| Name: EMC_SMIS_Solarwinds
|       Desc:
|       Owner: SRM
|               HttpPort: 5988
|               HttpsPort: 5989
|               InteropNamespace: /interop
|               Namespace: root/emc
|               Password: ASDqwe123
|               Username: solarwinds
|               UseSSL: true
--------------------14-------------------------
--------------------15-------------------------
| Type: SolarWinds.ESI.Common.Connection.ExternalSystemCredential
| Name: ESC
|       Desc:
|       Owner: ESI
|               Password: ASDqwe123
|               Username: solar_winds
--------------------15-------------------------
--------------------16-------------------------
| Type: SolarWinds.Orion.Web.Integration.OAuth2Token
| Name: SITTINGDUCK\uberuser
|       Desc:
|       Owner: Web.Integration
|               AccessToken: GthQHd3<snip>
|               AccessTokenExpiration: 2020-11-01T10:52:50.2768075Z
|               AccessTokenIssueDate: 2020-11-01T09:52:51.2768075Z
|               RefreshToken:hEjyhN0WqlfZmx<snip>
|               Scopes:
|               Username: uberuser@sittingduck.info
--------------------16-------------------------
--------------------17-------------------------
| Type: SolarWinds.SRM.Common.Credentials.XtremIoHttpCredential
| Name: XtremIO_Admin
|       Desc:
|       Owner: SRM
|               HttpPort: 80
|               HttpsPort: 443
|               Password: ASDqwe123
|               Username: admin
|               UseSsl: true
--------------------18-------------------------
===============================================
===============================================
```

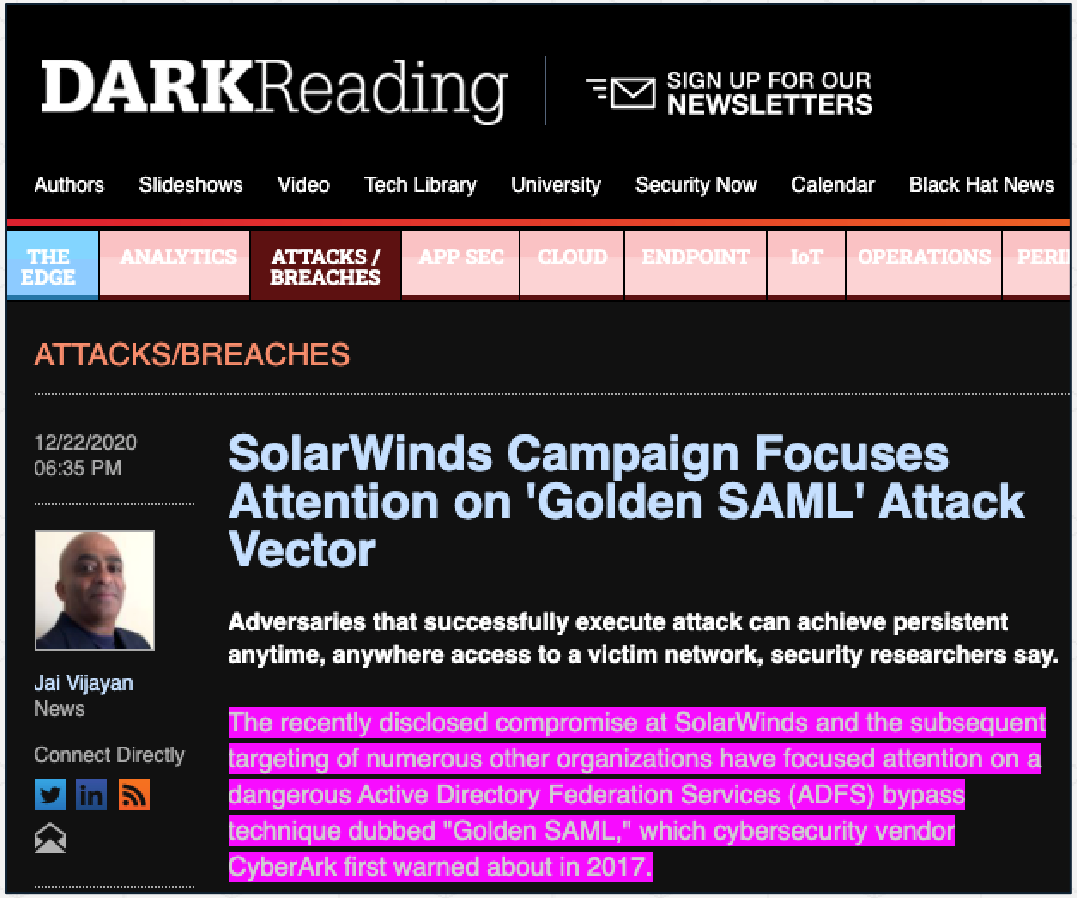
GOLDEN SAML BY CYBERARK LABS @ 2017



Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps

Shaked Reiner | 11/21/17

Share This!



ATTACKS/BREACHES

12/22/2020
06:35 PM

Jai Vijayan
News

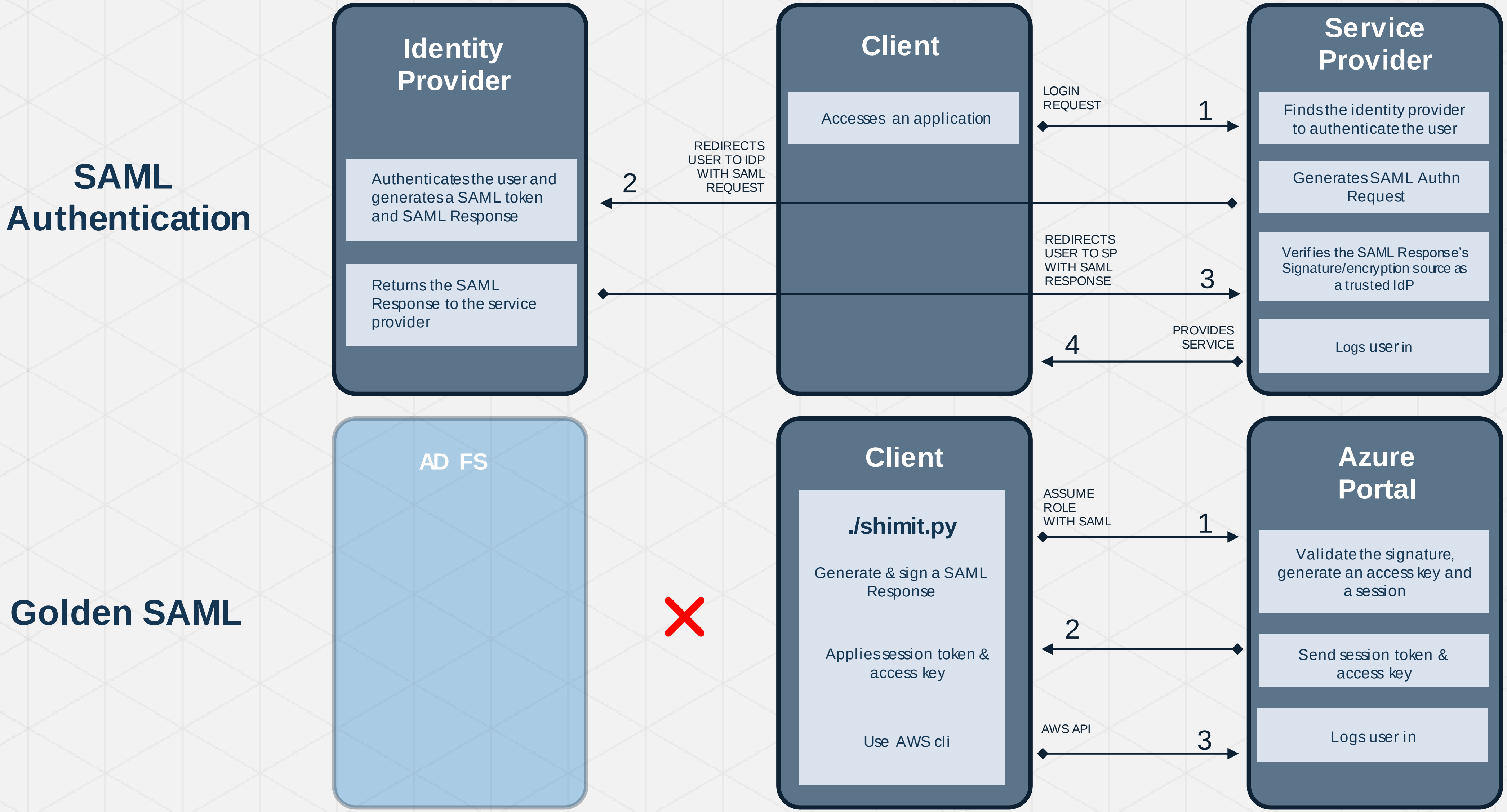
Connect Directly

SolarWinds Campaign Focuses Attention on 'Golden SAML' Attack Vector

Adversaries that successfully execute attack can achieve persistent anytime, anywhere access to a victim network, security researchers say.

The recently disclosed compromise at SolarWinds and the subsequent targeting of numerous other organizations have focused attention on a dangerous Active Directory Federation Services (ADFS) bypass technique dubbed "Golden SAML," which cybersecurity vendor CyberArk first warned about in 2017.

GOLDEN SAML



SAML Authentication

Identity Provider

- Authenticates the user and generates a SAML token and SAML Response
- Returns the SAML Response to the service provider

Client

- Accesses an application

Service Provider

- Finds the identity provider to authenticate the user
- Generates SAML Authn Request
- Verifies the SAML Response's Signature/encryption source as a trusted IdP
- Logs user in

1 LOGIN REQUEST

2 REDIRECTS USER TO IDP WITH SAML REQUEST

3 REDIRECTS USER TO SP WITH SAML RESPONSE

4 PROVIDES SERVICE

Golden SAML

AD FS

Client

./shimit.py

- Generate & sign a SAML Response
- Applies session token & access key
- Use AWS cli

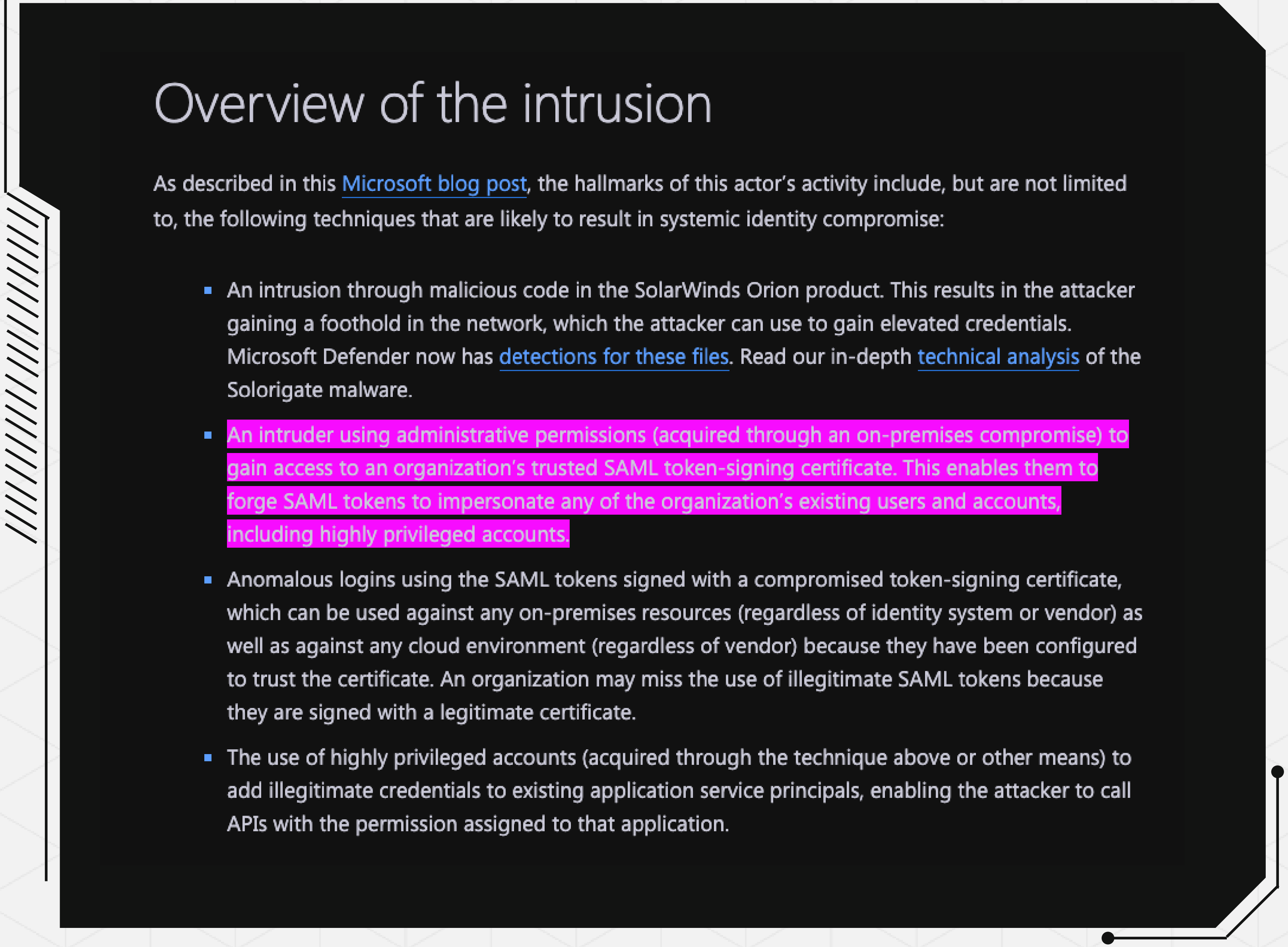
Azure Portal

- Validate the signature, generate an access key and a session
- Send session token & access key
- Logs user in

1 ASSUME ROLE WITH SAML

2

3 AWS API



Overview of the intrusion

As described in this Microsoft blog post, the hallmarks of this actor's activity include, but are not limited to, the following techniques that are likely to result in systemic identity compromise:

- An intrusion through malicious code in the SolarWinds Orion product. This results in the attacker gaining a foothold in the network, which the attacker can use to gain elevated credentials. Microsoft Defender now has detections for these files. Read our in-depth technical analysis of the Solorigate malware.
- An intruder using administrative permissions (acquired through an on-premises compromise) to gain access to an organization's trusted SAML token-signing certificate. This enables them to forge SAML tokens to impersonate any of the organization's existing users and accounts, including highly privileged accounts.
- Anomalous logins using the SAML tokens signed with a compromised token-signing certificate, which can be used against any on-premises resources (regardless of identity system or vendor) as well as against any cloud environment (regardless of vendor) because they have been configured to trust the certificate. An organization may miss the use of illegitimate SAML tokens because they are signed with a legitimate certificate.
- The use of highly privileged accounts (acquired through the technique above or other means) to add illegitimate credentials to existing application service principals, enabling the attacker to call APIs with the permission assigned to that application.

https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

MITIGATION STRATEGIES

SOLARWINDS BREACH: ZEROING IN

“We believe for any solution to be effective; prescriptions must apply a **“zero trust” presumption**, **access provided on a least privileged basis**…”

SolarWinds CEO Sudhakar Ramakrishna

U.S. Senate Testimony – February 23, 2021

SUPPLY CHAIN DEFENSE

SolarWinds Breach

Trojanized Code

CI/CD Pipeline Access

CI/CD Orchestrators

INITIAL FOOTHOLD CONTAINMENT

Orion
Server

SunBurst
Malware

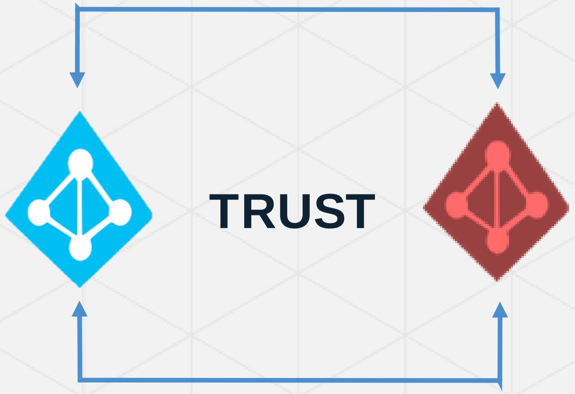
End-Point Agents
Termination

Access to local
Credentials storage

FORTRESSING TIER 0 ASSETS

Azure AD Portal

Malicious Configurations

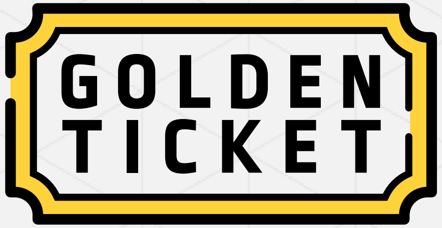


Backdoor Tenant

FORTRESSING TIER 0 EXTENSIONS

IAM / MFA Server

Compromised Secret

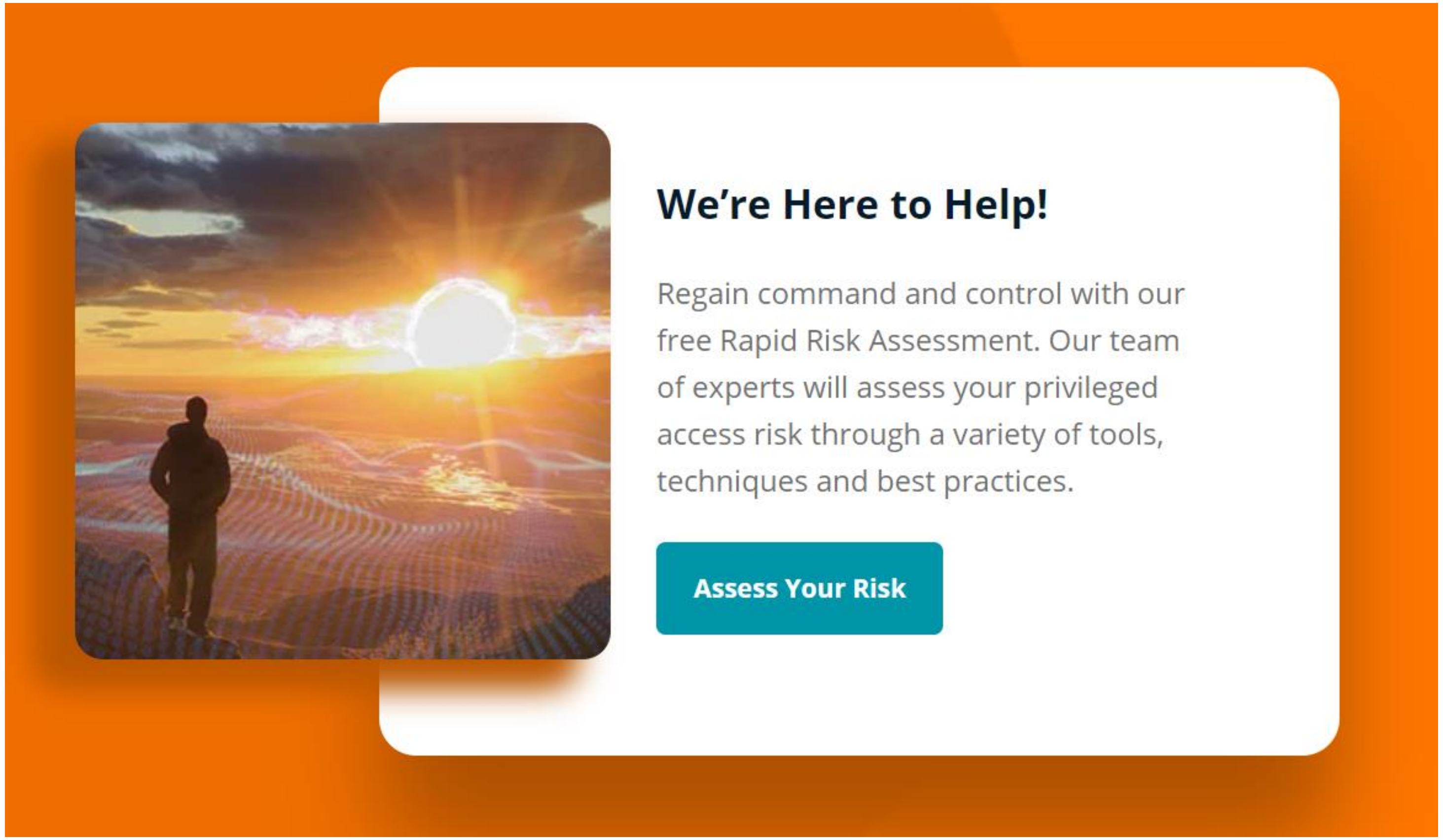


Golden SAML

IMMEDIATE TAKEAWAYS

- How will your org respond to a privileged breach?
- Evaluate your Tier 0 assets
  - Review your CI/CD pipelines
- Security controls are ineffective without Identity Security

NEXT STEPS



We're Here to Help!

Regain command and control with our free Rapid Risk Assessment. Our team of experts will assess your privileged access risk through a variety of tools, techniques and best practices.

- Register for a PAM Rapid Risk Assessment: https://www.cyberark.com/try-buy/rapid-risk-assessment/
- If interested in learning more, visit the CyberArk Engagement Zone and request a meeting

Andy Thompson, Research Evangelist, CyberArk Labs

Andy.Thompson@CyberArk.com

@R41nM4kr