



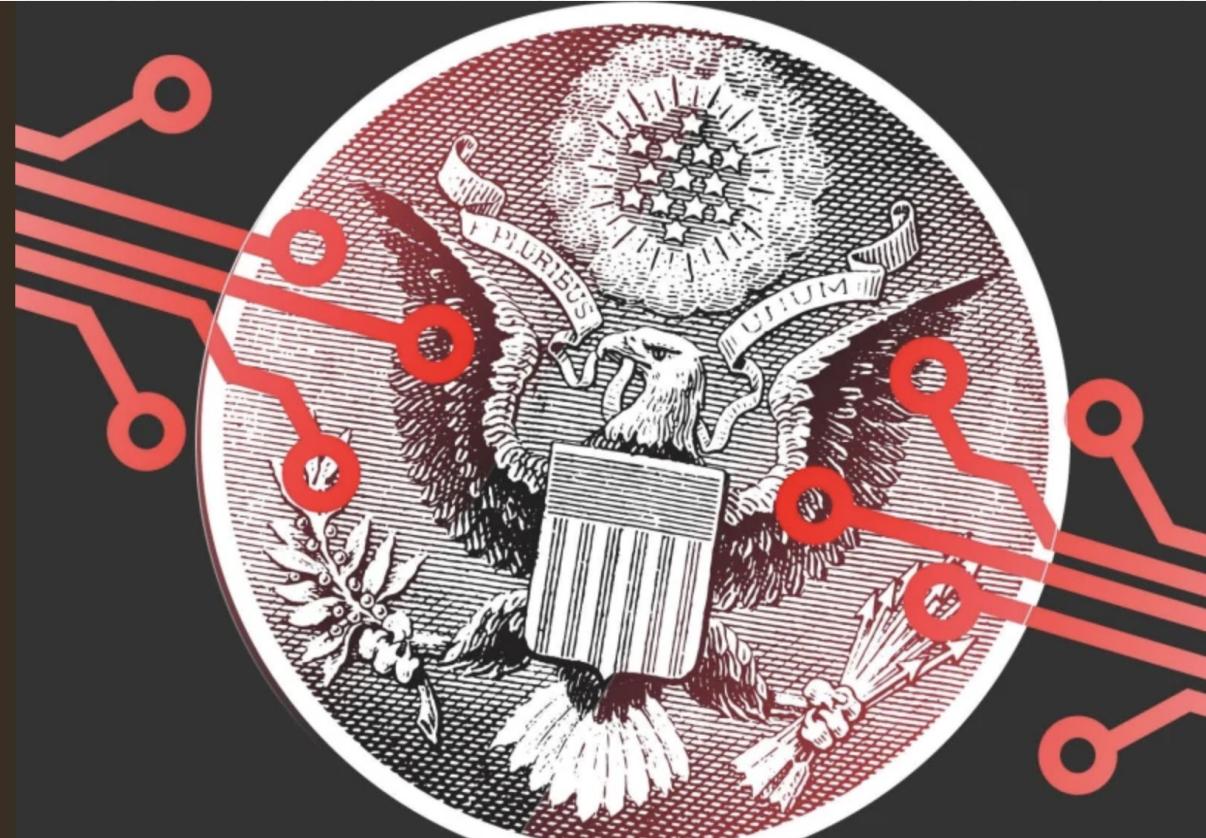
# ANATOMY OF THE SOLARWINDS ATTACK

Andy Thompson, Research Evangelist, CyberArk Labs

The Big Read Cyber Security

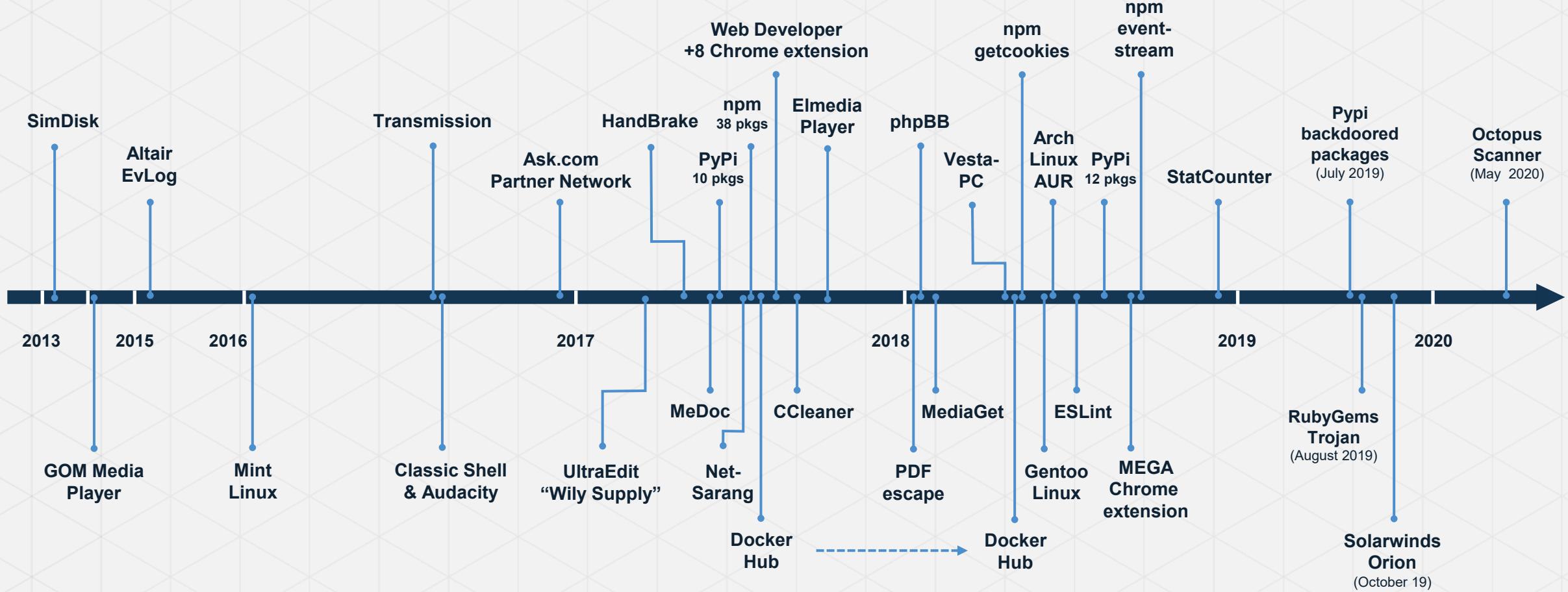
+ Add to myFT

# 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 compromised

# THE RISE OF THE DIGITAL SUPPLY CHAIN ATTACK



# SOLARWINDS ATTACK CHAIN

Orion Software Pipeline Infection



Target SolarWinds Customers

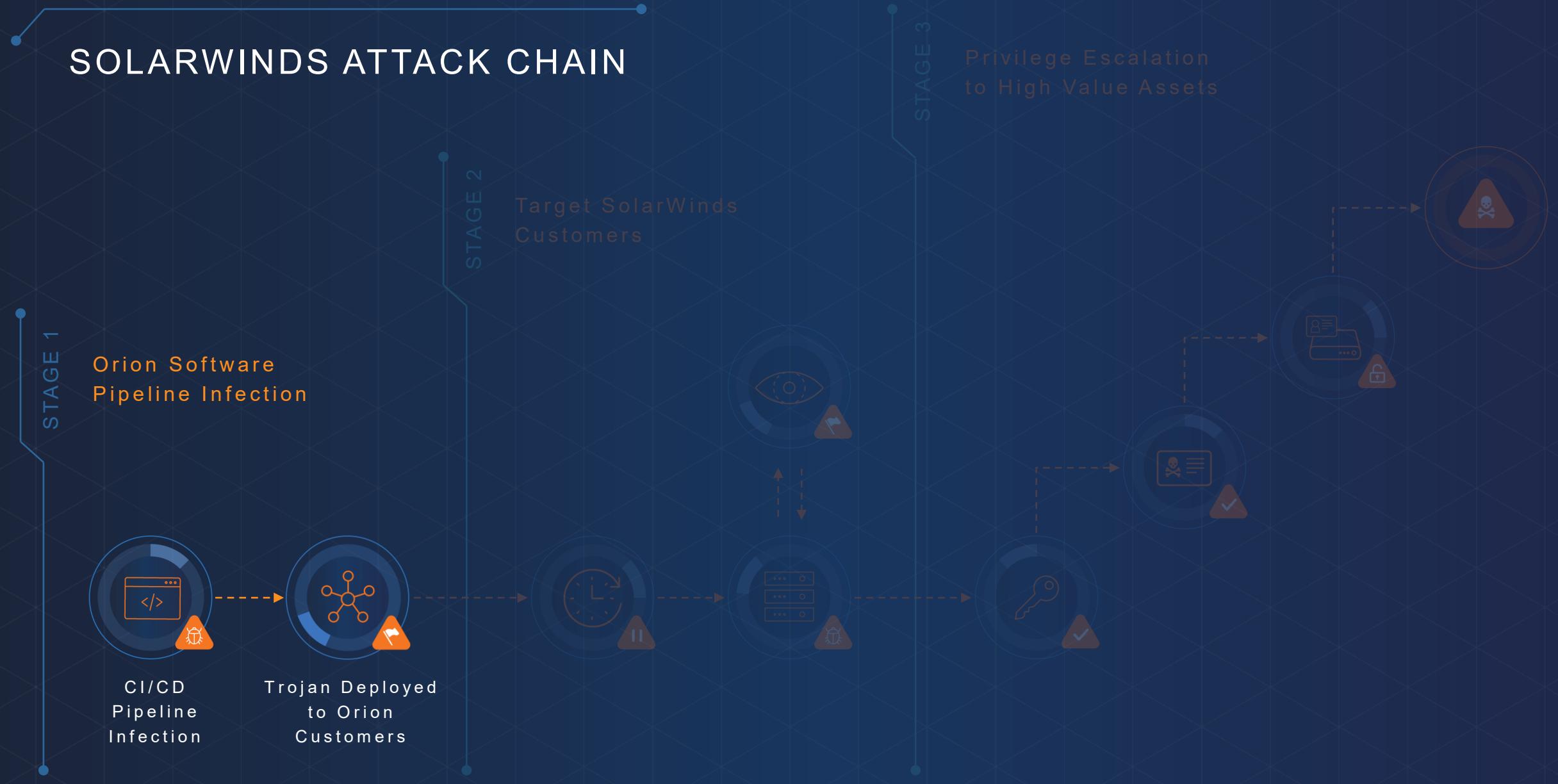


STAGE 3

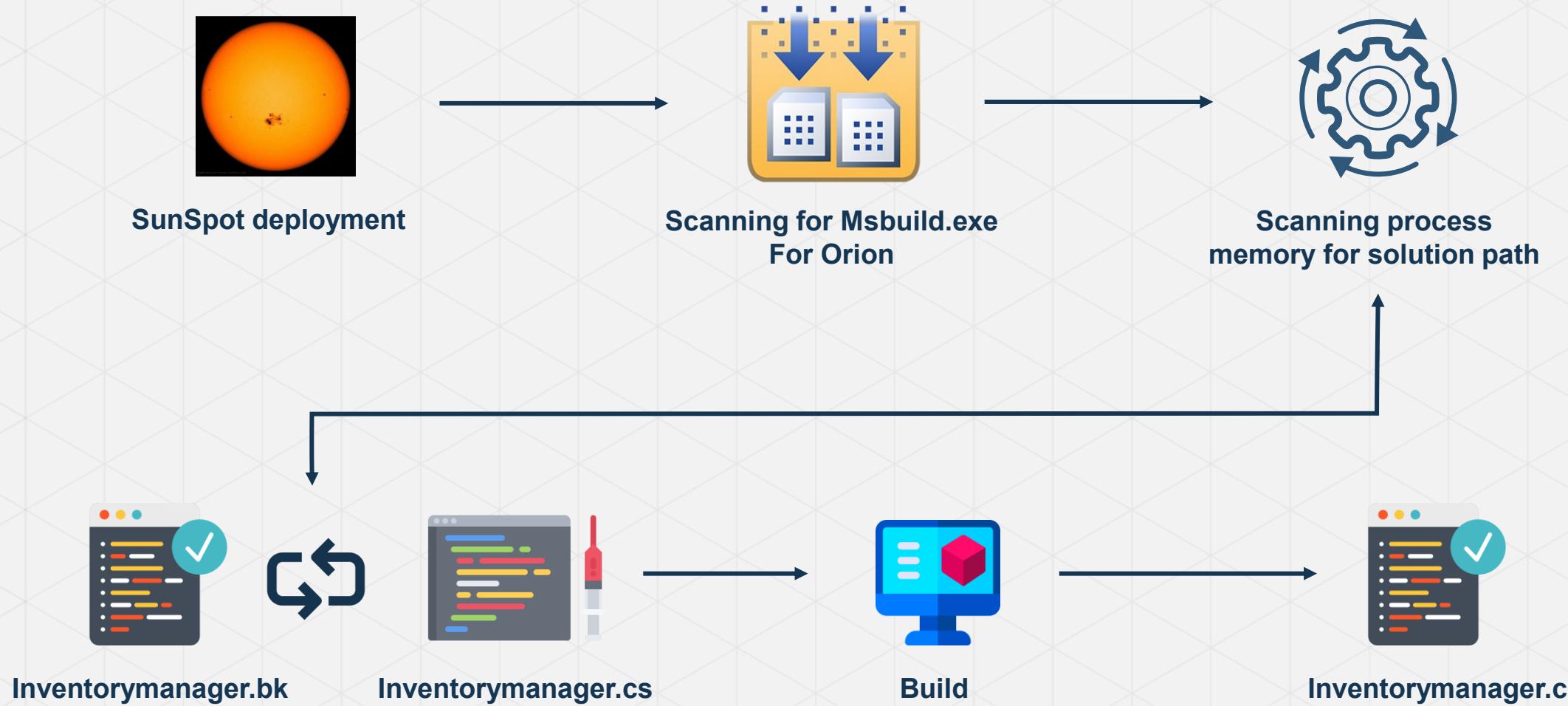
Privilege Escalation to High Value Assets



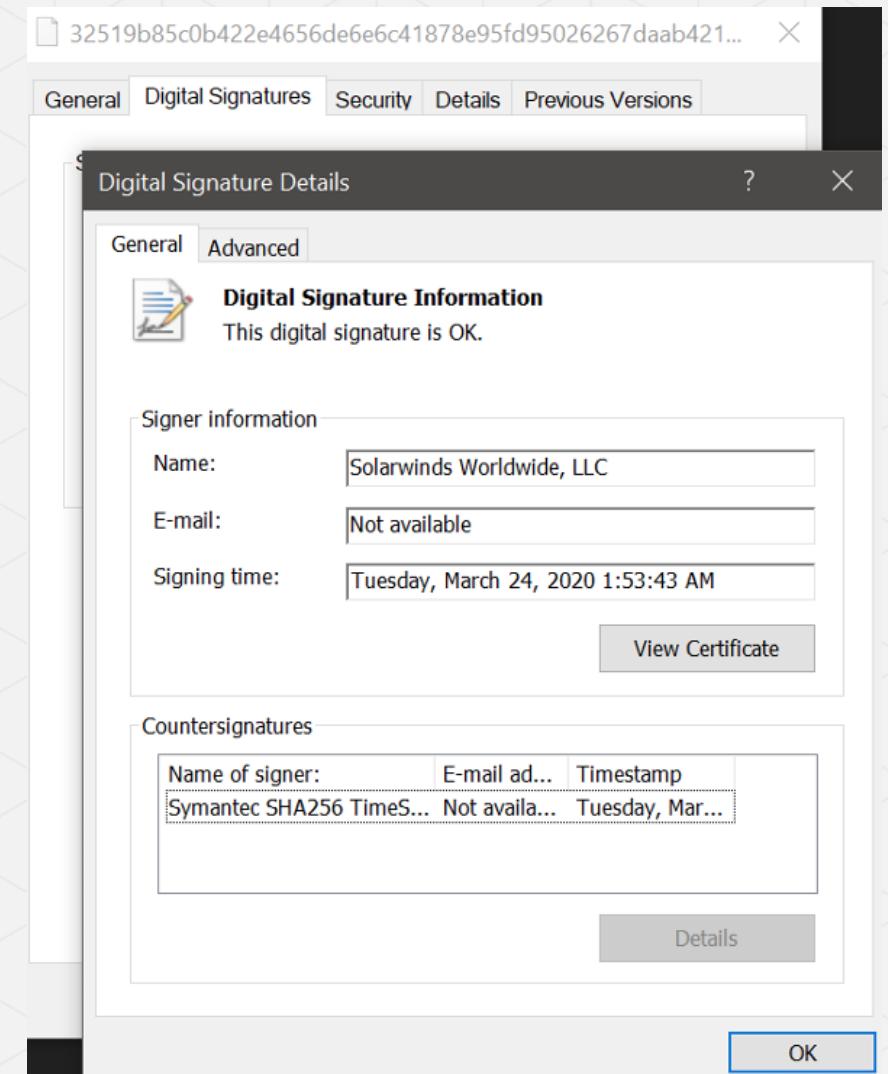
# SOLARWINDS ATTACK CHAIN



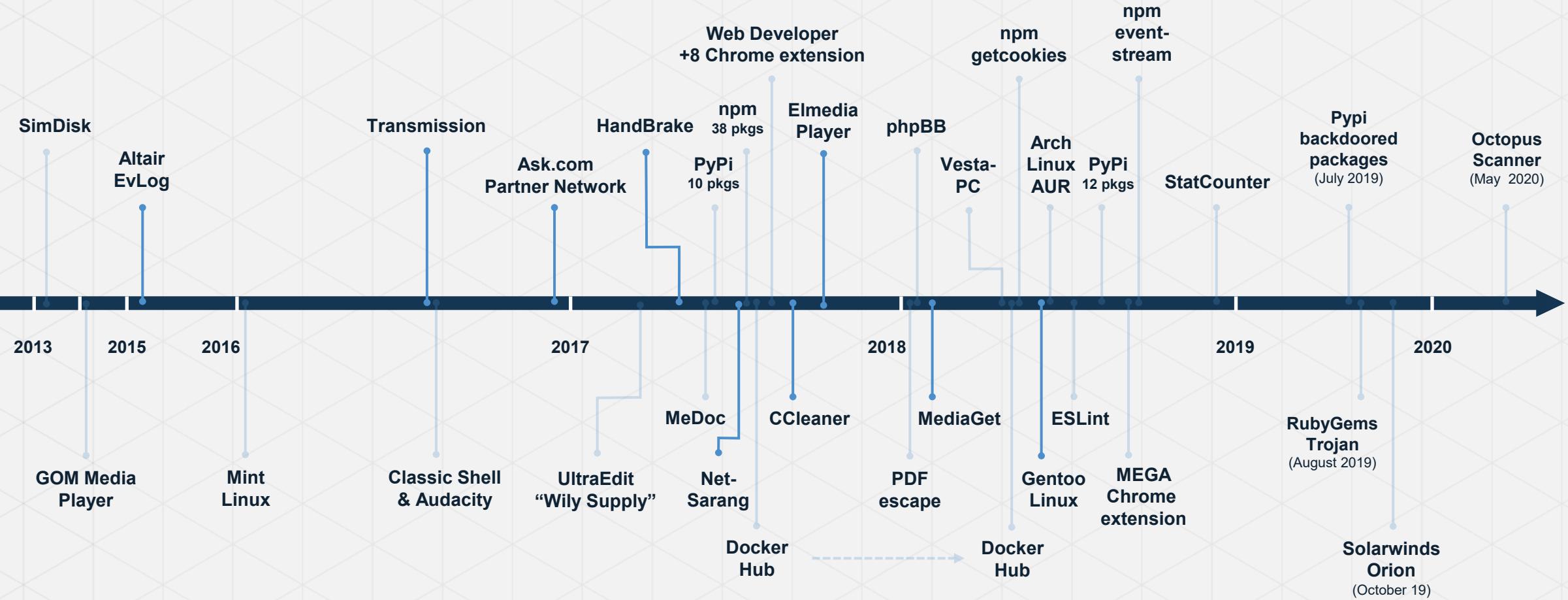
# TROJANIZING OPERATION



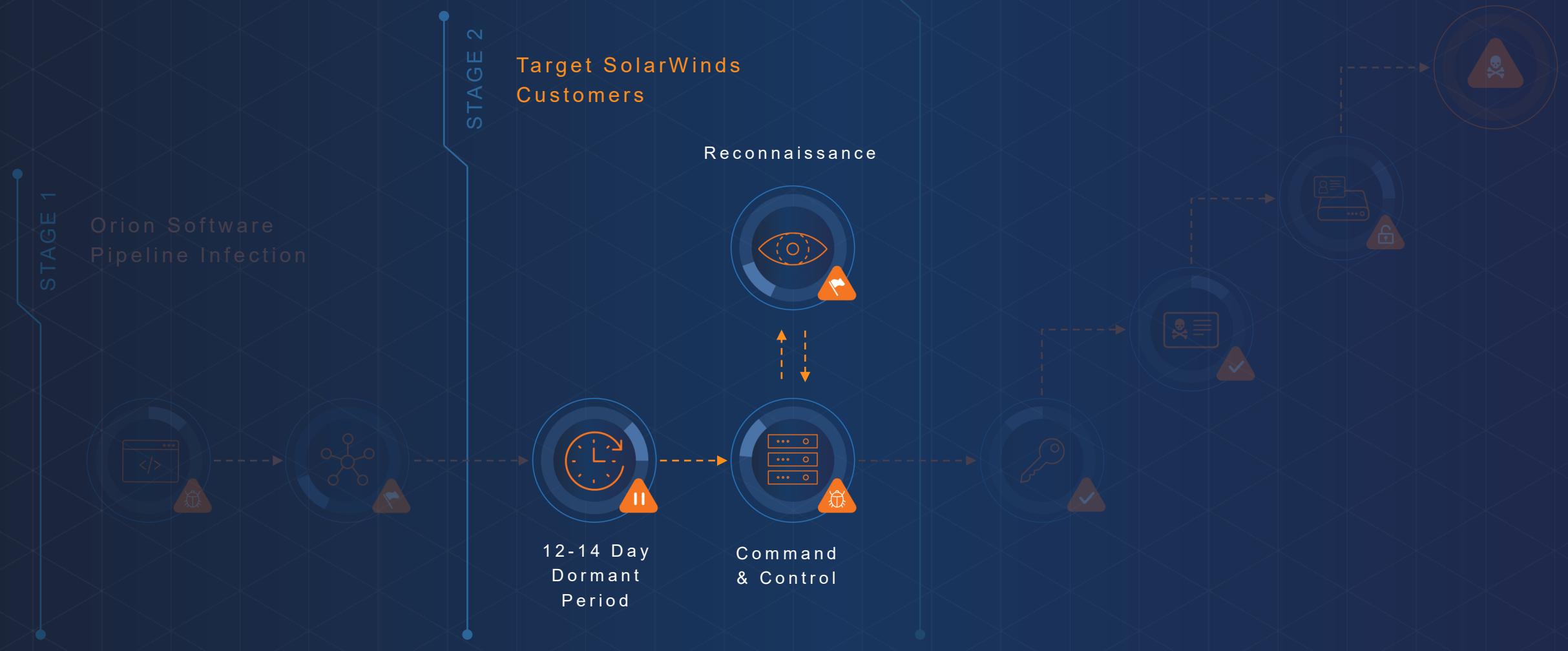
# SIGNED MALWARE



# SIGNED CODE



# SOLARWINDS ATTACK CHAIN



# 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.

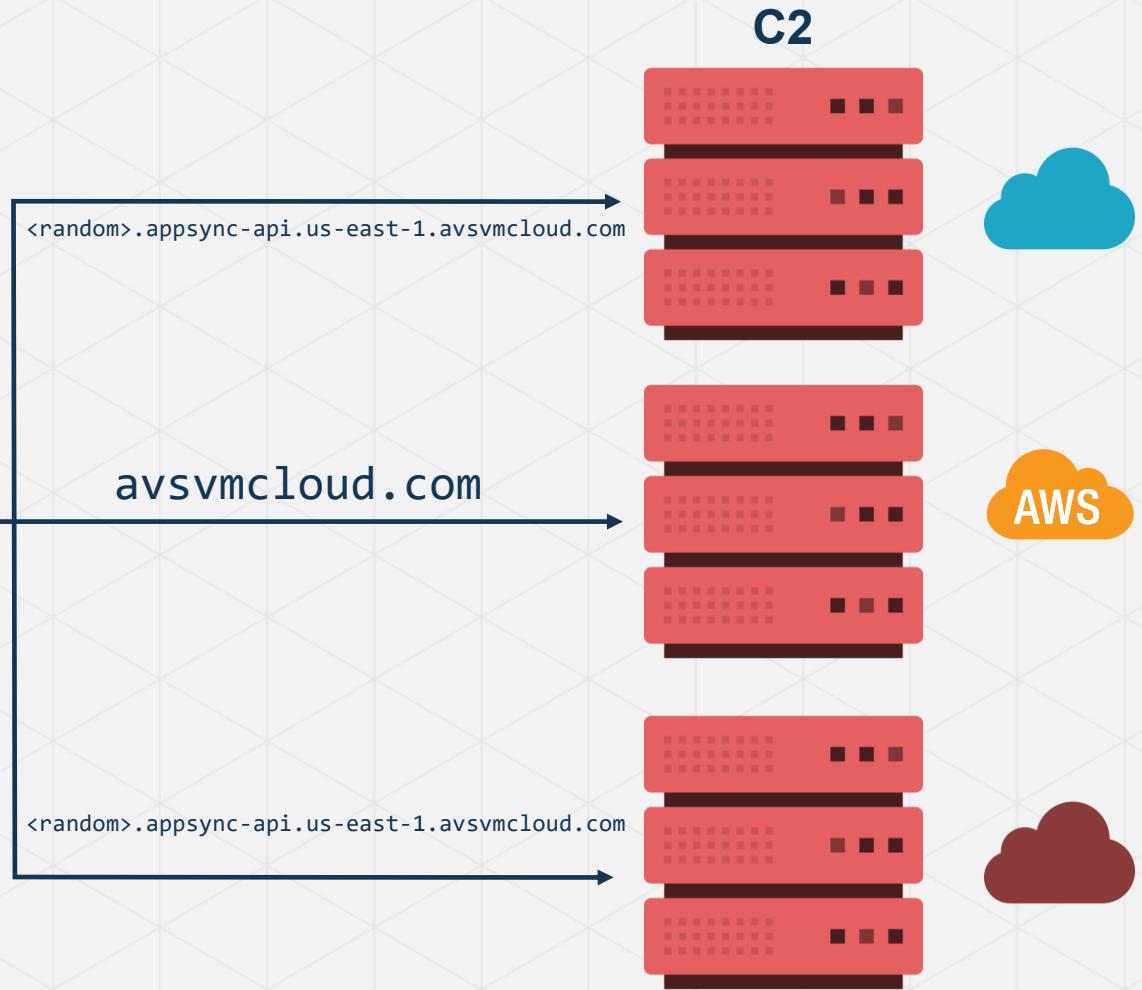
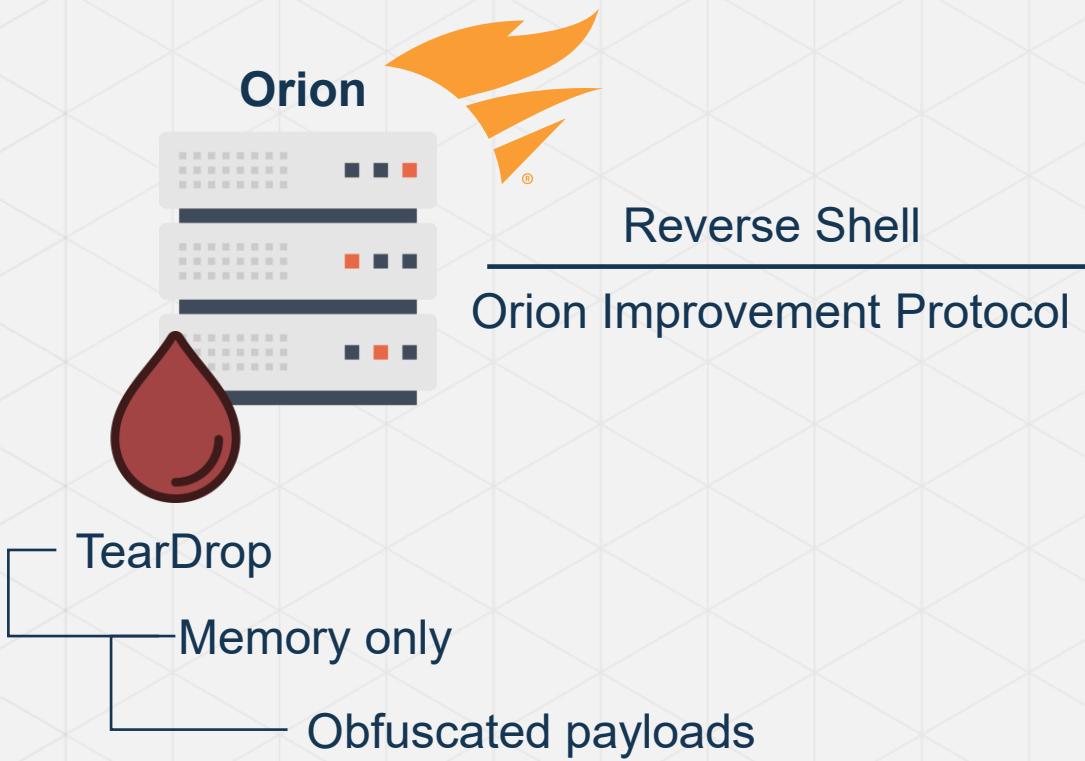
sysmon64 3538022140597504361  
carbonblack 11385275378891906608  
f-secure filter 13783346438774742614



**cybkerneltracker.sys 17097380490166623672**



ollydbg 4501656691368064027  
tanium 7175363135479931834  
x64dbg 14193859431895170587  
diskmon 7810436520414958497



# SOLARWINDS ATTACK CHAIN

Orion Software Pipeline Infection

Target SolarWinds Customers

Privilege Escalation to High Value Assets

STAGE 1

STAGE 2

STAGE 3



Target Reached



Bypass MFA



Fortify Access



Privilege Escalation

# 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.SntpCredentialsV3
| 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/eme
|     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: hEypn9WaIfzm<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!



## DARKReading

SIGN UP FOR OUR NEWSLETTERS

Authors Slideshows Video Tech Library University Security Now Calendar Black Hat News

THE EDGE ANALYTICS ATTACKS / BREACHES APP SEC CLOUD ENDPOINT IoT OPERATIONS PERI

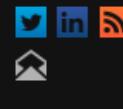
### ATTACKS/BREACHES

12/22/2020  
06:35 PM



Jai Vijayan  
News

Connect Directly



### SolarWinds Campaign Focuses Attention on 'Golden SAML' Attack Vector

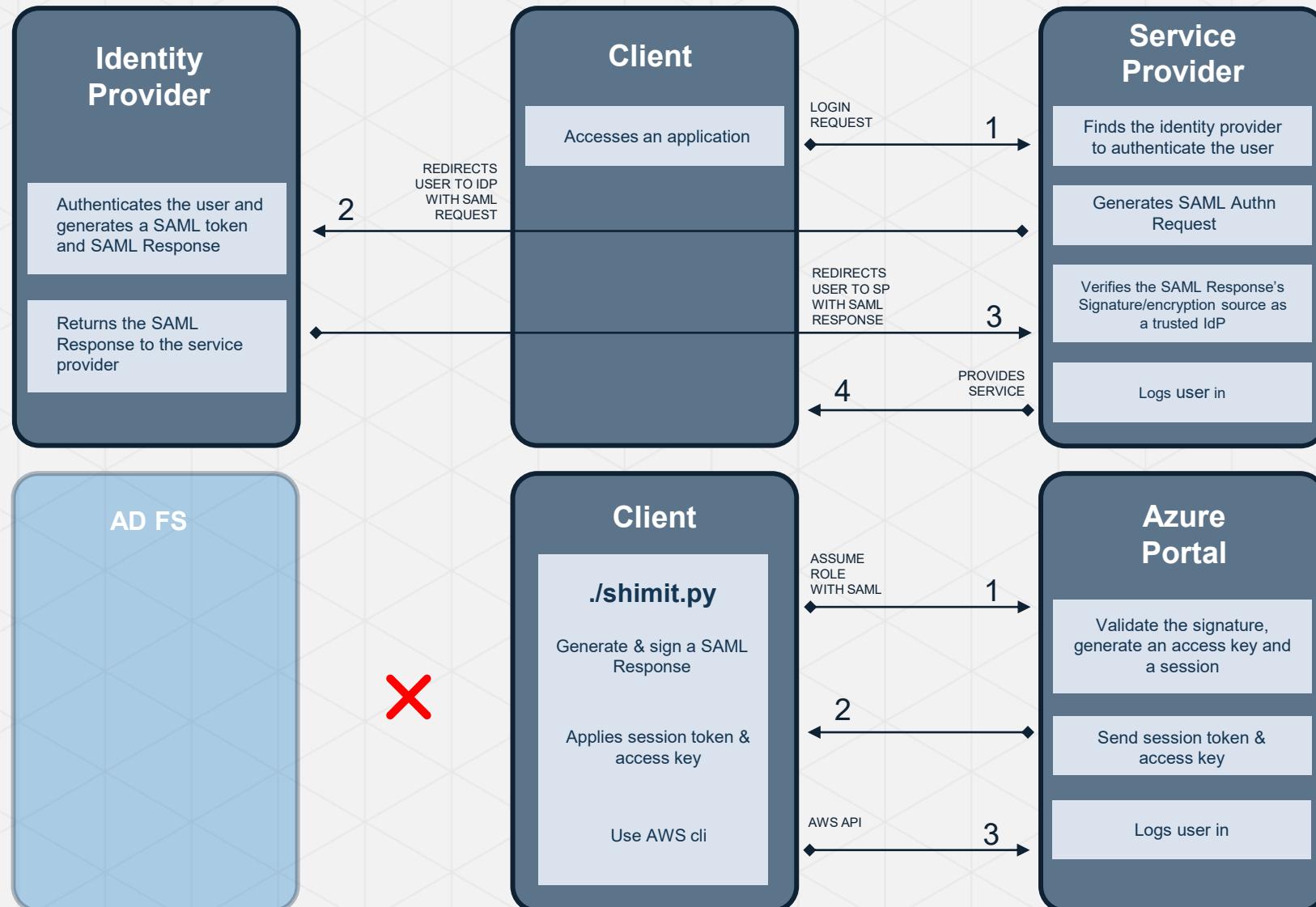
Adversaries that successfully execute attack can achieve persistent anytime, anywhere access to a victim network, security researchers say.

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

## Golden SAML



# 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.



# 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

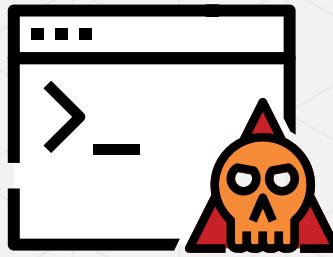
U.S. Senate Testimony – February 23, 2021



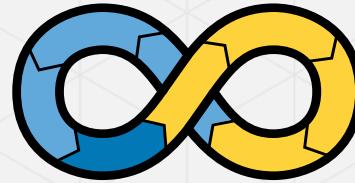
# SUPPLY CHAIN DEFENSE



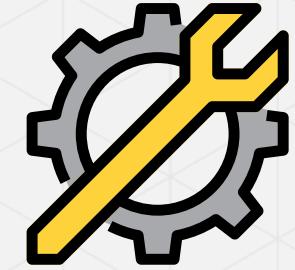
**SolarWinds  
Breach**



**Trojanized  
Code**

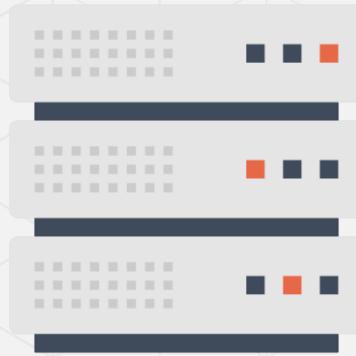


**CI/CD Pipeline  
Access**



**CI/CD  
Orchestrators**

# INITIAL FOOTHOLD CONTAINMENT



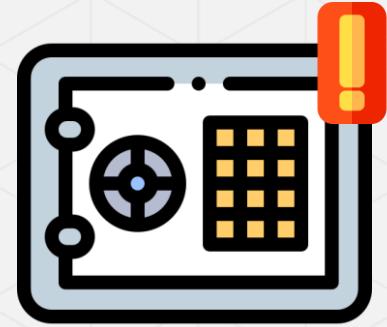
Orion  
Server



SunBurst  
Malware



End-Point Agents  
Termination



Access to local  
Credentials storage

# FORTRESSING TIER 0 ASSETS



Azure AD  
Portal

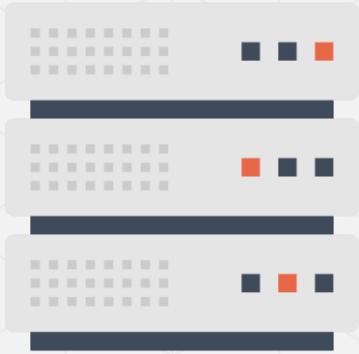


Malicious  
Configurations



Backdoor  
Tenant

# FORTRESSING TIER 0 EXTENSIONS



IAM / MFA  
Server



Compromised  
Secret

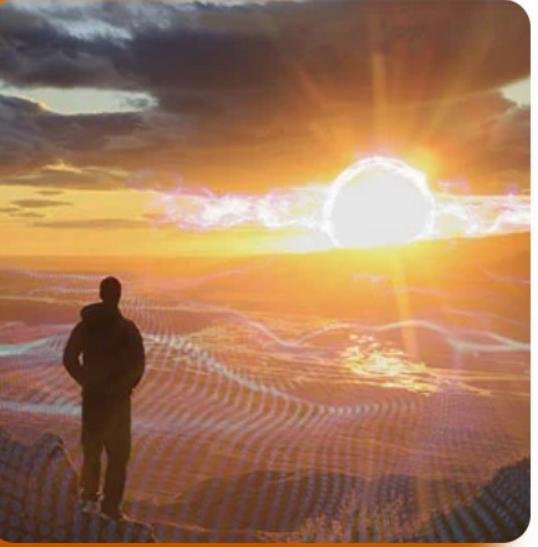


Golden SAML

## 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.

**Assess Your Risk**

- 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



# CYBERARK®

Andy Thompson, Research Evangelist, CyberArk Labs

[Andy.Thompson@CyberArk.com](mailto:Andy.Thompson@CyberArk.com)

@R41nM4kr