Supply Chain Attacks

Justin Schermerhorn and Ryan Becker

What is a Supply Chain Attack?

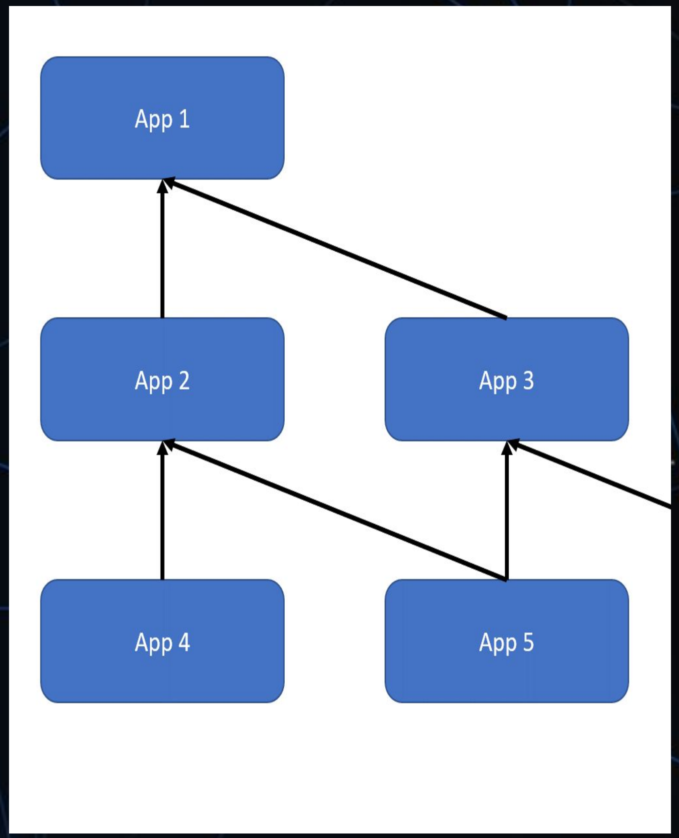
An attack that is launched by targeting vulnerable third party vendors or services that are vital to the supply chain

Example: Targeting updates provided by third party vendor that the target application uses

Importance

203 Average third party dependencies per application	**84%** Believe it is one of the biggest cyber threats	**59%** Companies do not have a recovery plan
45% Of Respondents' Organizations experienced supply chain threats	**36%** vetted the third party dependencies beforehand	**430%** The amount supply chain attacks have risen

Why are third parties vulnerable?



Dependency Complexity

Lack of visibility into vendor practices

Weak Security Practices

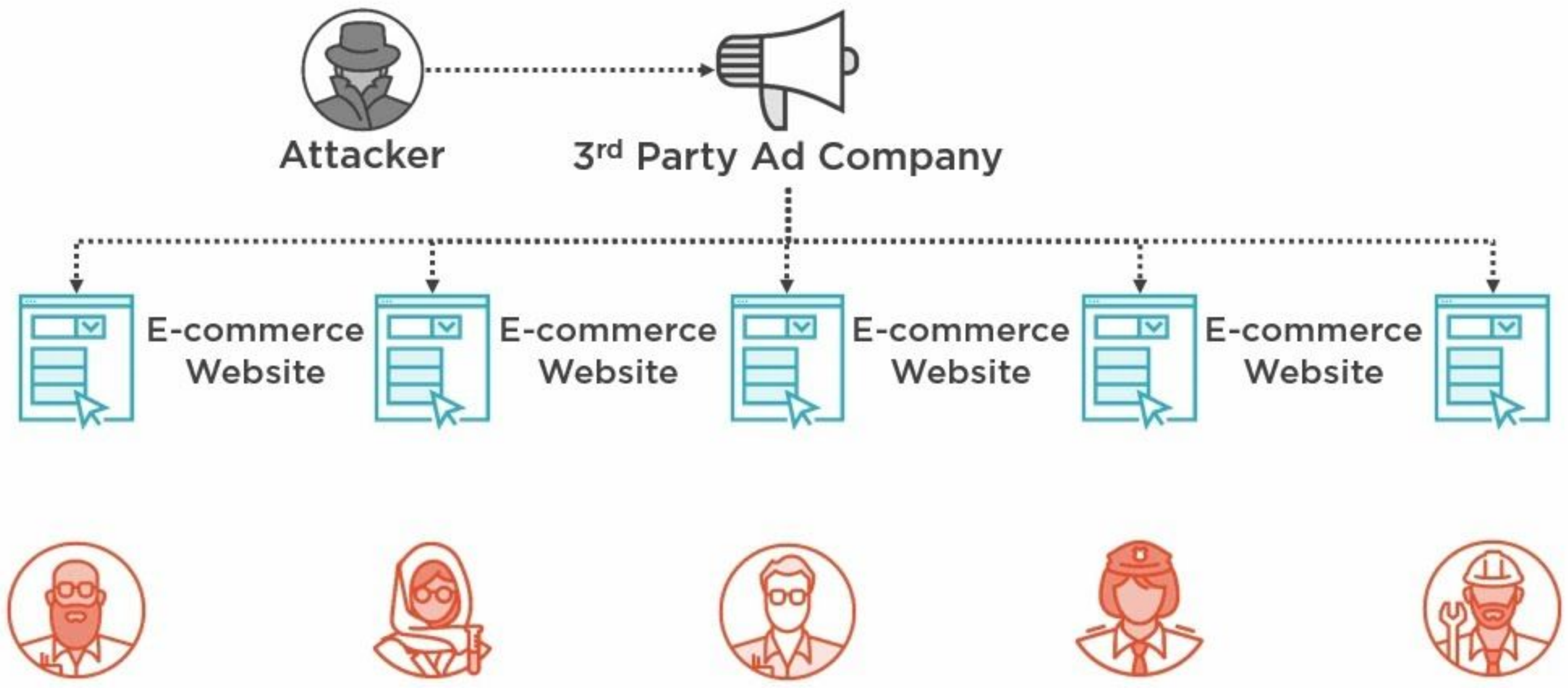
Over-reliance on trust rather than verification

Known Assets
Unknown Assets
Impersonating Assets
3rd Party Assets

Wide Impact Potential

A single compromise affects multiple clients

Supply Chain Attack Example



Attacker

3rd Party Ad Company

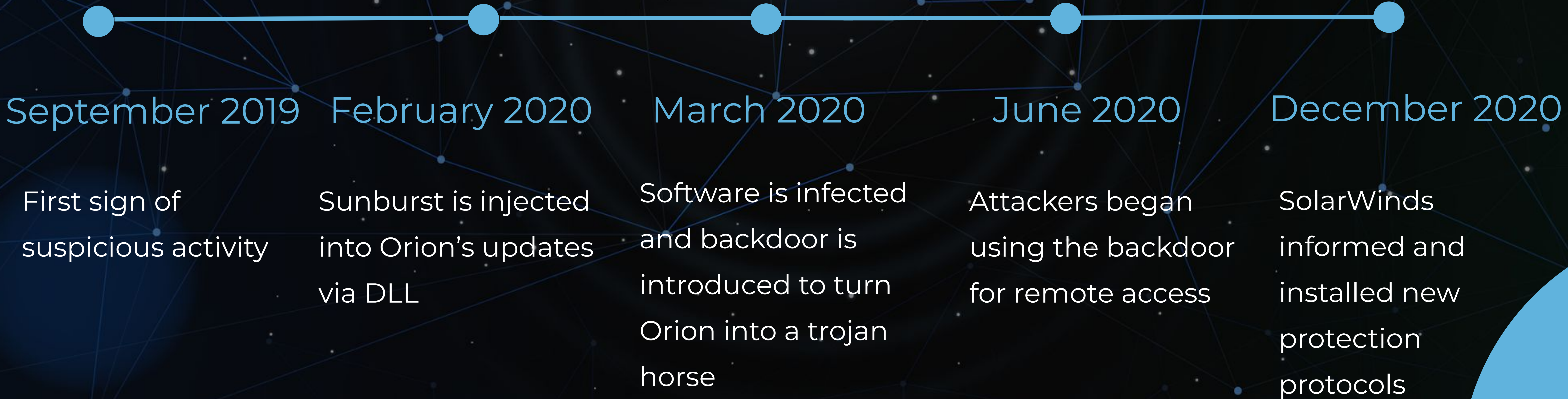
E-commerce Website

E-commerce Website

E-commerce Website

E-commerce Website

Solarwind Attack



September 2019

First sign of suspicious activity

February 2020

Sunburst is injected into Orion’s updates via DLL

March 2020

Software is infected and backdoor is introduced to turn Orion into a trojan horse

June 2020

Attackers began using the backdoor for remote access

December 2020

SolarWinds informed and installed new protection protocols

How did it occur?

Malware Delivered

Delivered via Windows Dynamic Linked Library

Replace DLL file

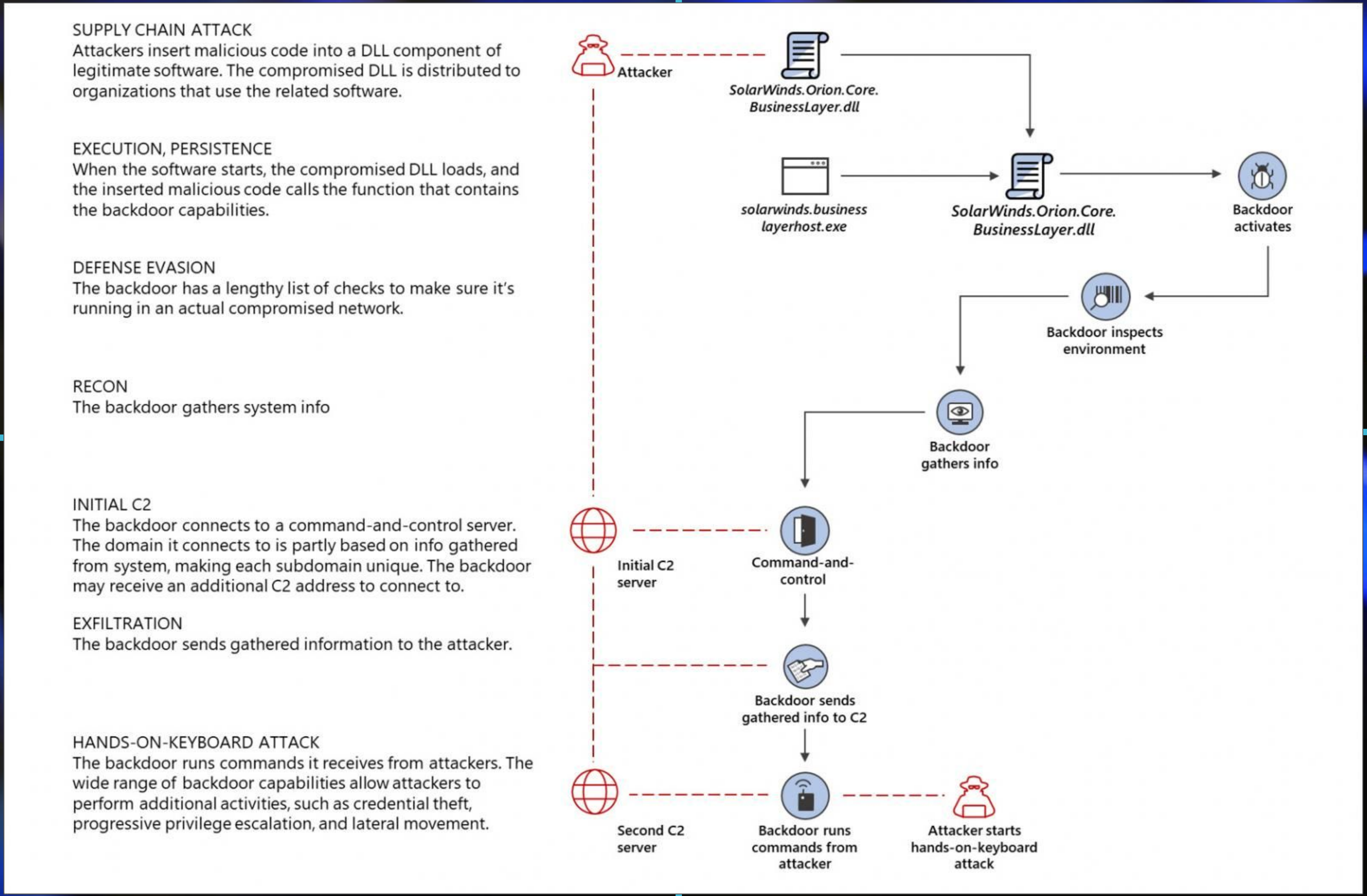
New DLL file replaced the old trusted file solarwinds.orion.core.businesslayer.dll

Execution

Executing the solarwinds.orion.core.businesslayer.dll will execute a command and control server

Gather Information

Information will be gathered and sent back to the attacker



SUPPLY CHAIN ATTACK
Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE
When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

DEFENSE EVASION
The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

RECON
The backdoor gathers system info

INITIAL C2
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

EXFILTRATION
The backdoor sends gathered information to the attacker.

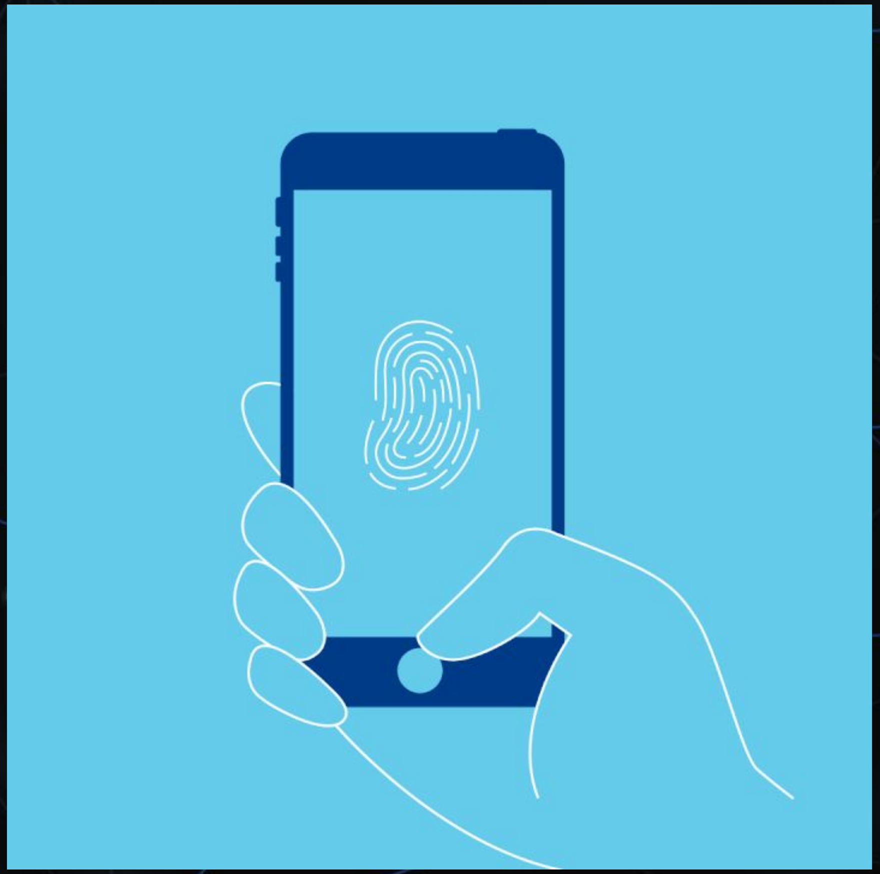
HANDS-ON-KEYBOARD ATTACK
The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.

Attacker
SolarWinds.Orion.Core.BusinessLayer.dll
solarwinds.business layerhost.exe
SolarWinds.Orion.Core.BusinessLayer.dll
Backdoor activates
Backdoor inspects environment
Backdoor gathers info
Initial C2 server
Command-and-control
Backdoor sends gathered info to C2
Second C2 server
Backdoor runs commands from attacker
Attacker starts hands-on-keyboard attack

How to prevent?

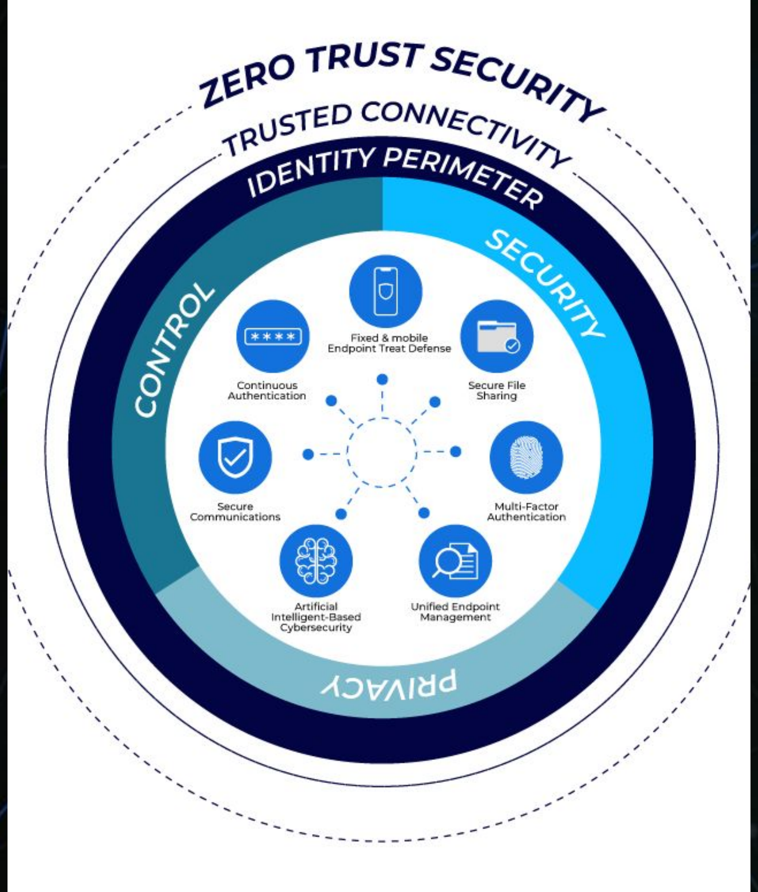
Vendor Management

Thorough review of vendor’s security practices



Authenticating

Incorporate MFA or IAM


ZERO TRUST SECURITY
TRUSTED CONNECTIVITY
IDENTITY PERIMETER
CONTROL
SECURITY
PRIVACY
Fixed & mobile Endpoint Treat Defense
Continuous Authentication
Secure File Sharing
Secure Communications
Multi-Factor Authentication
Artificial Intelligent-Based Cybersecurity
Unified Endpoint Management

Zero Trust Model

Always authenticate and verify appropriate data is being transmitted

THANK YOU!

CREDITS

- https://panorays.com/blog/how-to-prevent-supply-chain-attacks/#:~:text=Key%20Elements%20in%20Preventing%20Supply%20Chain%20Attacks,-Given%20that%20supply&text=These%20include%20key%20supply%20chain,into%20your%20entire%20supply%20chain.
- https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/supply-chain-attack/
- https://venafi.com/blog/solarwinds-sunburst-attack-explained-what-really-happened/
- https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/
- SlidesCarnival and Pexel for the presentation template