2020 SolarWinds Breach

The supply chain attack on SolarWinds exposed several vulnerabilities

Overview

A trojan virus in a routine patch compromised the cyber security of thousands

In March, 2020 threat actors gained access to SolarWinds' development resources

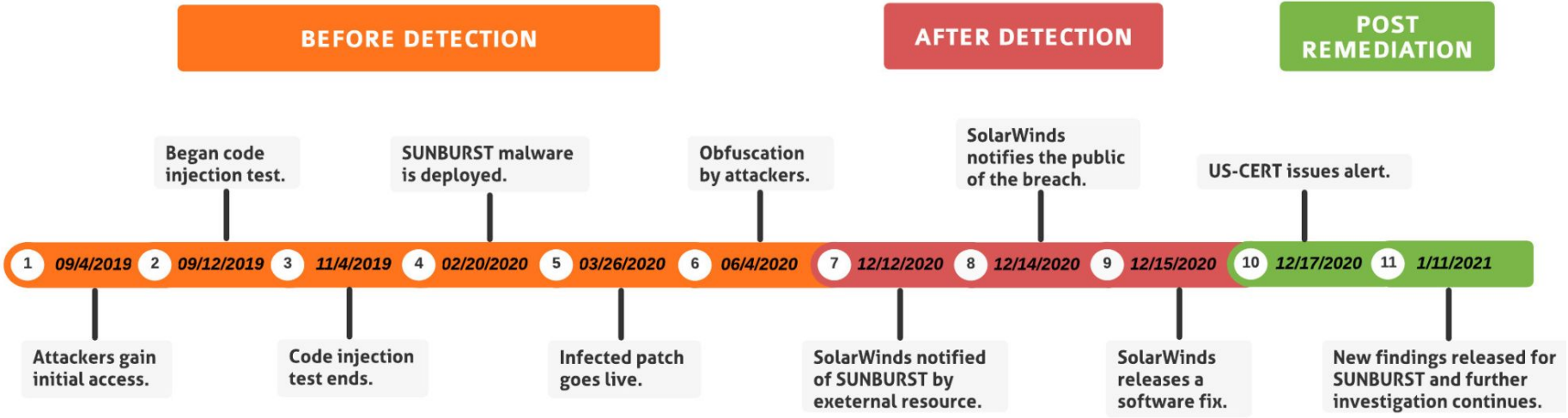
They used back door access to put malicious software into an update

Update was released to customers

About half of its customers downloaded the update and were exposed for about a year

It was a learning experience about supply chain vulnerabilities which led to new tools and techniques to better mitigate against such threats

Timeline In Detail



Affected Devices: Orion Platform

- Network Performance Monitoring
- Network Traffic Analyzer
- Network Configuration Manager
- IP Address Manager
- VOIP
- User Device Tracking
- Server and Application Monitor
- Storage Monitor
- Virtualization Manager
- Web Performance Monitor
- Log Analyzer

Once the update was downloaded and the device connected to the internet the attackers were able to gain access remotely via a backdoor.

Damages

- Email Accounts
- Network Monitoring Tools
- Compromised Networks
- Proprietary information
- Internal Documents

Highlighted detection problems in both the private and public sector

DHS admitted they failed to catch the attack due to it being in an update not being scanned

Method could be used on future updates

Could allow potential jumps from corporate networks to system controls

Victims

- US Government
- US Military Branches
- Government Contractors
- Fortune 500 Companies
- Educational Institutions
- Information Technology Companies

Less than 18,000 of its 33,000 customers had downloaded the malicious code

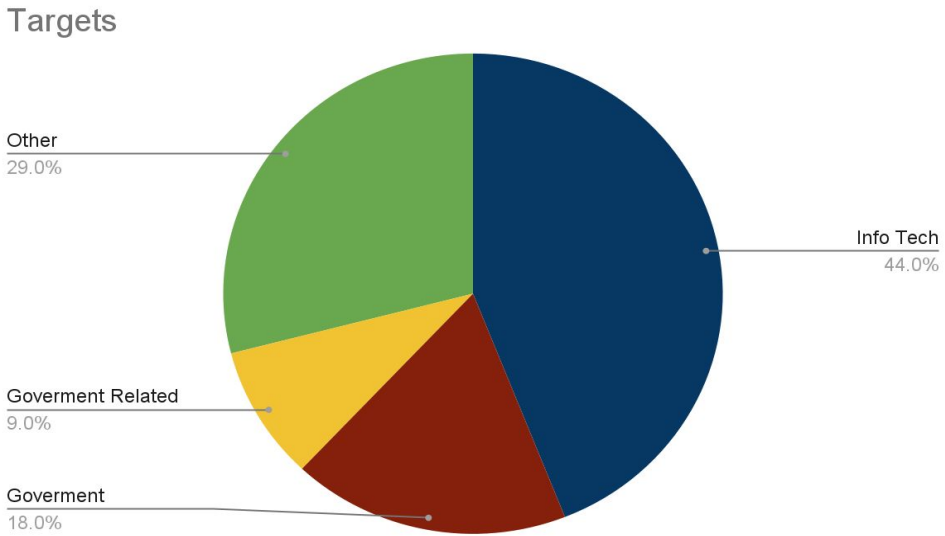
The attack compromised the confidentiality and integrity of data

The attack revealed that it could happen again in future updates either from SolarWinds or other third party vendors

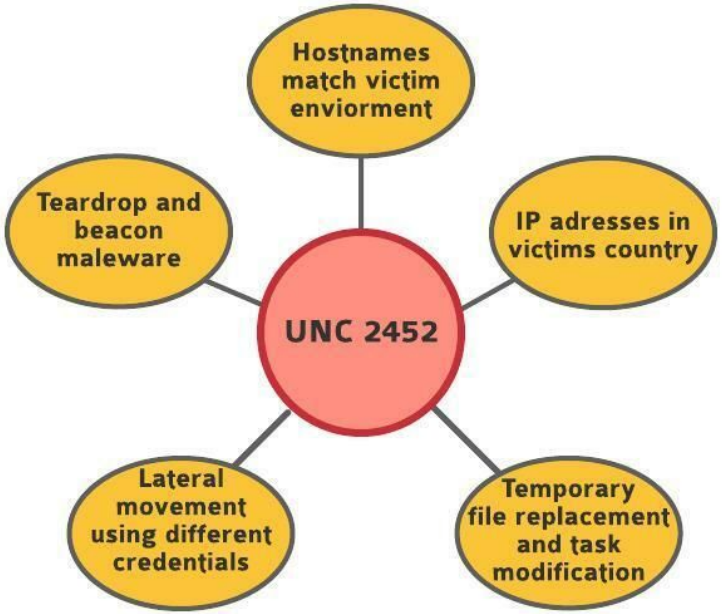
Threat Actors

UNC2452

- Believed to be associated with Russian Foreign Intelligence Service
- Targets
  - Internal Documents
  - Email
  - Intellectual Property
  - Security documents
- Unlikely Actions
  - Data Destruction
  - Denial of Service
  - Acquisition of PII
  - Acquisition of Financial Information



Attacker At A Glance

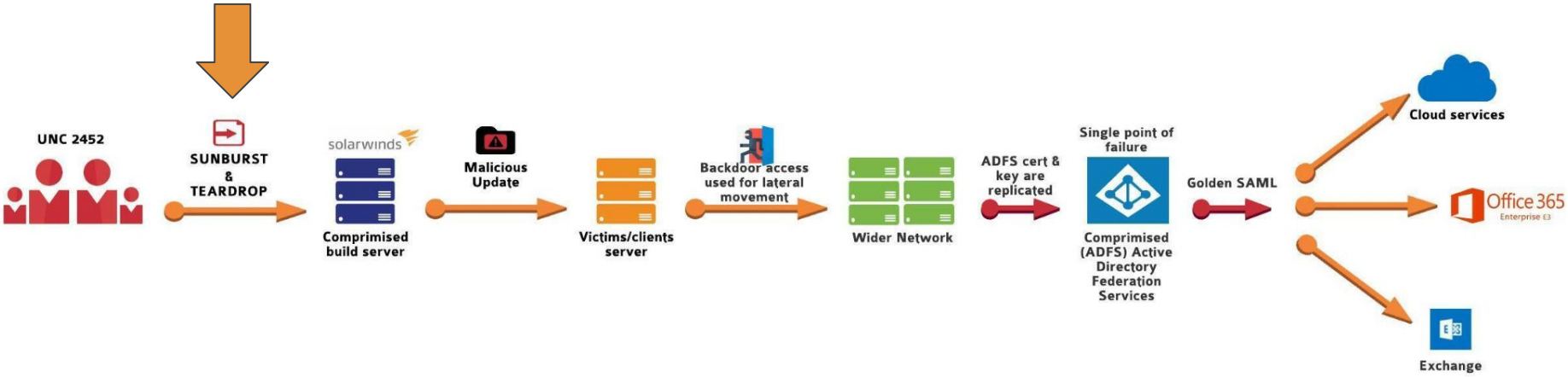


Attack In Detail

Exploit

- Base Score: 9.8 Critical
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Attack Vector: Network
- Attack Complexity: Low
- No user interaction or privileges required
- Loss of CIA

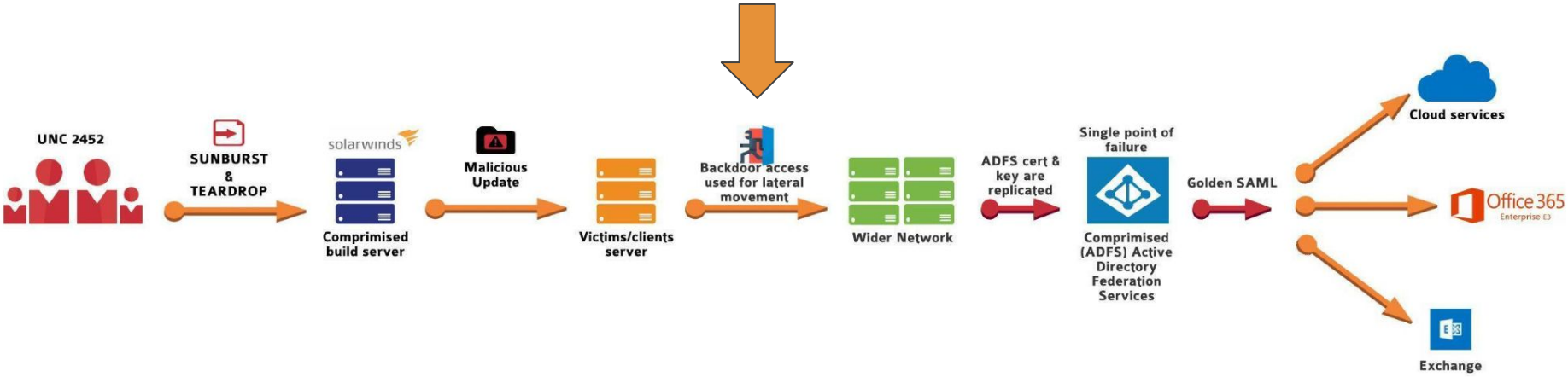
Attack Flow


UNC 2452
SUNBURST
&
TEARDROP
solarwinds
Comprimised
build server
Malicious
Update
Victims/clients
server
Backdoor access
used for lateral
movement
Wider Network
ADFS cert &
key are
replicated
Single point of
failure
Comprimised
(ADFS) Active
Directory
Federation
Services
Golden SAML
Cloud services
Office 365
Enterprise E3
Exchange

Attack Against SolarWinds

- Started with simple proof of concept test code to check processor type and return binary data to the attackers
- Malicious code to check when digital repository was used
- Created a temporary update file to house malicious code
- Temporary file was swapped with update code during compiling process
- Infected update pushed out to victims

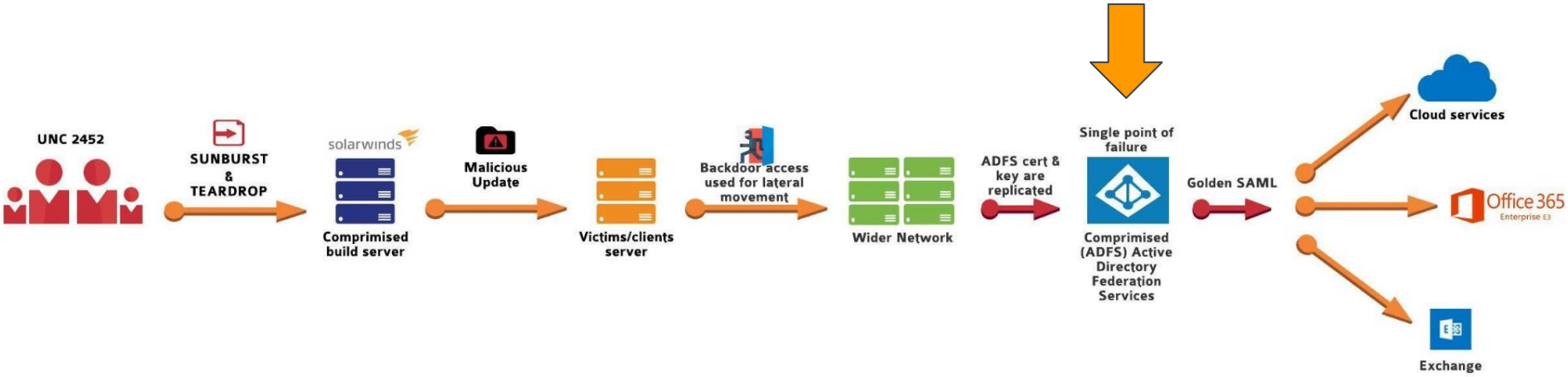
Attack Flow


UNC 2452
SUNBURST & TEARDROP
solarwinds
Comprimised build server
Malicious Update
Victims/clients server
Backdoor access used for lateral movement
Wider Network
ADFS cert & key are replicated
Single point of failure
Comprimised (ADFS) Active Directory Federation Services
Golden SAML
Cloud services
Office 365
Enterprise E3
Exchange

Attacker Malware

- SUNBURST - backdoor
- TEARDROP - payload embedder
- Cobalt Strike Beacon Implant v4 - remote operation, C2 capabilities, data exfiltration, keylogger
- MimiKatz - credential harvesting
- Additional malware with similar purposes

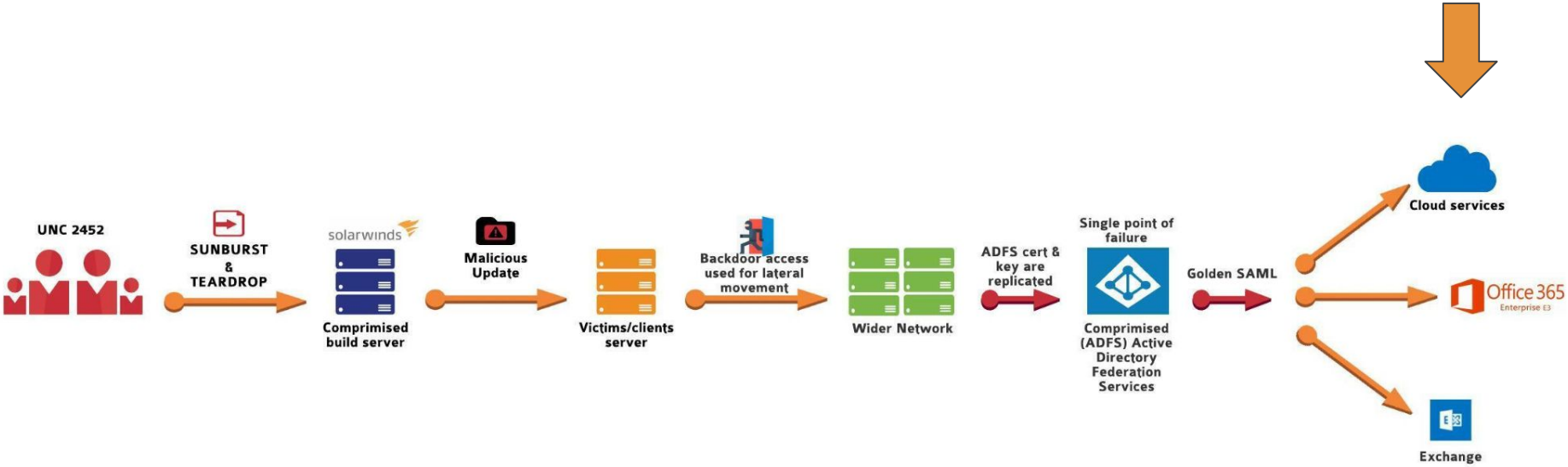
Attack Flow


UNC 2452
SUNBURST & TEARDROP
solarwinds
Comprimised build server
Malicious Update
Victims/clients server
Backdoor access used for lateral movement
Wider Network
ADFS cert & key are replicated
Single point of failure
Comprimised (ADFS) Active Directory Federation Services
Golden SAML
Cloud services
Office 365
Enterprise E3
Exchange

GoldenSAML Lateral Movement

- Attacker gains access to Microsoft Active Directory servers
- AD access allowed for reconnaissance to identify privileged accounts
- Steal Token Certificates
- Steal database files
- Altered AD DKM to obtain secret keys
- Bypasses Multi Factor Authentication

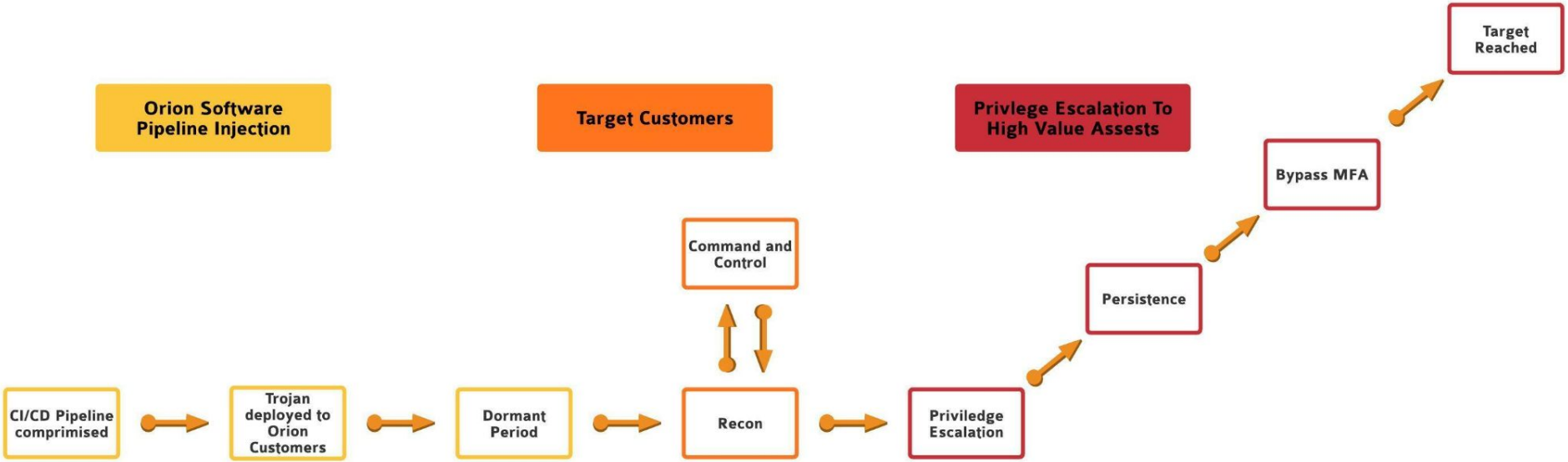
Attack Flow


UNC 2452
SUNBURST & TEARDROP
solarwinds
Comprimised build server
Malicious Update
Victims/clients server
Backdoor access used for lateral movement
Wider Network
ADFS cert & key are replicated
Single point of failure
Comprimised (ADFS) Active Directory Federation Services
Golden SAML
Cloud services
Office 365
Enterprise E3
Exchange

Attacker Methods and Exfiltration

- Attacker created multiple access points to hijacked networks
  - Service Accounts
  - Application Accounts
- Data exfiltration using passive DNS servers
  - Servers rented from US companies AWS and GoDaddy to avoid suspicion
- Anti-Forensic scrubbing to hide traceable details from code

Method


Orion Software Pipeline Injection
Target Customers
Privlege Escalation To High Value Assests
Target Reached
Bypass MFA
Persistence
Command and Control
CI/CD Pipeline comprimised
Trojan deployed to Orion Customers
Dormant Period
Recon
Priviledge Escalation

Mitigation and Prevention

Detection

- The actual attack was well-publicized and systems should be searched for tell-tale evidence.
- The update in question is CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp
  - 02af7cec58b9a5da1c542b5a32151ba1
- The malware is contained in the file SolarWinds.Orion.Core.BusinessLayer.dll
  - b91ce2fa41029f6955bff20079468448
- Search for Malicious IP addresses and Remote Access Credentials
  - Look for a single system access multiple systems
- SMB sessions
  - Look for pattern of deletion and creation for backdoor removal

Mitigation

- Update older software and utilize current security patches
- Isolate/contain SolarWinds servers by blocking the internet
- Restrict connectivity to endpoints from SolarWinds Servers
- Restrict admin accounts on SolarWinds Servers
- Block internet access from endpoints with SolarWinds software
- Change account passwords
- Review network device configurations for modifications
- Update Firewall rules using information released by security experts

Knowledge for the future

Critical Lessons Learned

- Be protective of on-premises Microsoft Active Directory. This was the primary way that the attackers were able to get from SolarWinds products to other internal resources.
- Require increased code validation. Knowing where code is coming from and protecting it from tampering is of the utmost importance.
- Impose limited trust especially with suppliers. This is a good mitigation strategy to protect against further supply chain attacks.
- Test components used in products.

Additional Lessons Learned

- Examine all traffic leaving the network. It is not enough just to filter traffic entering the network but also the traffic leaving to prevent data exfiltration.
- Understand the location of sensitive data and protect it.
- Research potential attackers' tools, techniques and procedures.
- Increase network segmentation.
- Improve security architecture.
- Increase security in the development process for updates and other software.
- Implement defense in depth.

Summary

- Beware supply chain vulnerabilities. This is a large relatively unsecured vector for future malware infections.
- Credential and key management needs to be a top security priority
- Careful examination of code where applicable is essential to the development process.
- Routine threat hunting and cybersecurity management is a viable prevention method.
- Regularly checking on current cybersecurity events is useful.
- Always follow best security practices.

MITRE ATT&CK Techniques

- T1012 - Query Registry
- T1027 - Obfuscated Files or Info
- T1057 - Process Discovery
- T1070.004 - File Deletion
- T1071.001 - Web Protocols
- T1071.004 - Application Layer Protocol DNS
- T1083 - File and Directory Discovery
- T1105 - Ingress Tool Transfer
- T1132.001 - Standard Encoding
- T1195.002 - Compromise Software Supply Chain
- T1518 - Software Discovery
- T1518.001 - Security Software Discovery
- T1543.003 - Windows Service
- T1553.002 - Code Signing
- T1568.002 - Domain Generation Algorithms
- T1569.002 - Service Execution
- T1584 - Compromise Infrastructure

Resources

Resources 1

Full Report: *https://github.com/t-wic/Fullstack_2107-csu-rm-cyb-pt/blob/main/Solar%20Winds%20Report%20Paper.pdf*

- https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12
- https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know
- https://www.gizmodo.com.au/2021/05/solarwinds-hackers-cyber-attacks-timeline/
- https://www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html
- https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/
- https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor
- https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12
- https://www.solarwinds.com/orion-platform
- https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/
- https://nvd.nist.gov/vuln/detail/CVE-2020-10148

Resources 2

- https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
- https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wbnr-unc2452-presentation-slides.pdf
- https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wbnr-unc2452-presentation-slides.pdf
- https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
- https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-039b
- https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-148a
- https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/
- https://krebsonsecurity.com/2020/12/u-s-treasury-commerce-depts-hacked-through-solarwinds-compromise/
- https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor
- https://github.com/mandiant/sunburst_countermeasures
- https://www.solarwinds.com/sa-overview/securityadvisory
- https://www.crn.com.au/news/12-lessons-learned-from-solarwinds-breach-rsa-conference-564841

Thank You

BLAKE WESTBROOK & TIMOTHY WICKEY

2107-csu-rm-cyb-pt

Fullstack Academy

Professor Bryan Durrance

1/9/2022