SolarWinds 2020 Investigation

Case Study

Introduction

SolarWinds is an American IT company that specialises in IT management and monitoring through their flagship product Orion. In March 2020 the Orion platform was compromised, leading to private companies and government agencies being breached. This case study explores the specifics of the SolarWinds breach, focusing on how it was executed, the threat actors involved, and the tactics, techniques, and procedures (TTPs) used. The study aims to provide insights into the challenges posed by advanced persistent threats and supply chain vulnerabilities in modern cybersecurity.

Overview of the Attack

The SolarWinds attack, discovered in December 2020 (Congress, 2021), targeted the Orion software platform used by thousands of organizations worldwide for IT management. The attack was highly sophisticated, exploiting a vulnerability in SolarWinds' software supply chain. The attackers covertly breached the SolarWinds' network in 2019, testing their code injection in October before finally injecting the malicious SUNBURST backdoor into the Orion platform 4 months later (Fortinet, n.d.).
SolarWinds started releasing updates containing the malicious SUNBURST to their customers in March 2020 (Fortinent, n.d.) as part of regular maintenance. This led to the attackers gaining remote access to the affected systems without detection. The attackers used the initial access gained through the SUNBURST backdoor to conduct lateral movement within affected networks, often escalating privileges to gain deeper access to sensitive systems and data.Once inside, the attackers carried out surveillance and exfiltrated information from their targets (Center for Cybersikkerhed, 2021).
The attack was successful because it targeted the software supply chain, making SolarWinds a popular target because their software is so widely used by a range of different organisations from private businesses to government agencies (Aquasec 2023).
SolarWinds estimated that out of their 300,000 customers, around 18,000 of them were vulnerable to the attack (Congress, 2021). This shows how effective supply chain attacks can be because the attackers breached thousands of organisations by just compromising one software update.

Threat Actors Involved

By January 2021 the USA formally accused Russia of the SolarWinds attack, attributing it to the Russian intelligence service (SVR) (Center for Cybersikkerhed, 2021). The SVR conducted the attack through an affiliated group called “Nobelium” (CybersecurityDive,

2021). Nobelium has been active since 2004 (Sekoia, 2024) and is known for their highly sophisticated attacks on major government and privately owned organisations, targeting them strategically in partnership with the Russian government. They typically gain access to a target's network through spearfish fishing campaigns, where they then exfiltrate the data that they were after. They're specifically infamous because of their ability to move laterally throughout a target's network covertly, often staying dormant and using backdoors to stay undetected for extended periods of time (Sekoia, 2024). Nobelium's operations align with broader Russian geopolitical objectives, showcasing how cyberattacks have become increasingly more common amongst nation states. The group's ability to target sensitive governmental and private-sector organisations reflects Russia's growing reliance on cyber espionage to gain intelligence and influence global events. Such operations are often conducted covertly, without the need for traditional military intervention, making them a preferred tool for advancing national interests in the digital age. This form of cyber warfare enables Russia to conduct strategic intelligence-gathering, which can directly influence diplomatic relations and military strategies (The Record, 2023).

Tactics, Techniques and Procedures

The Tactics, Techniques, and Procedures (TTPs) in the SolarWinds attack were highly sophisticated, involving a supply chain compromise via the SUNBURST backdoor [T1195.002 - Supply Chain Compromise]. Nobelium used SUNSPOT, a custom malware developed by the group StellarParticle, to insert the SUNBURST backdoor into the Orion software builds [T1587.001 - Malware Development] (CrowdStrike, 2021). SUNSPOT monitored the compilation process and replaced a source file with the SUNBURST code without alerting developers [T1584.002 - Build System Compromise]. To maintain operational security, SUNSPOT ensured the build process did not fail, preventing detection by SolarWinds developers (CrowdStrike, 2021).
Once the SUNBURST backdoor was inserted into the software, it imitated Orion network traffic in order to make the malicious update appear legitimate [T1071.004 - Application Layer Protocol] (Center for Cybersikkerhed, 2021). After installation, the backdoor remained dormant for up to two weeks, checking for security tools like anti-virus and forensic software before activating [T1562.001 - Disable or Modify Tools]. It then used a unique domain generation algorithm (DGA) [T1568.002 - Domain Generation Algorithms] to establish command-and-control (C2) communications, allowing attackers to identify and target specific assets (Center for Cybersikkerhed, 2021). The malware's stealth features and careful design ensured prolonged access to compromised systems, enabling the attackers to gather intelligence without detection. These tactics reflect the high level of operational security employed by Nobelium to maintain undetected access for espionage purposes.

Conclusion

Overall, the 2020 SolarWinds attack shows the increasing threat and sophistication of nation state sponsored cyber attacks. Nobelium relied on exploiting the trust between SolarWinds as a software supplier and their customers, this led to thousands of unsuspecting organisations downloading what they thought were legitimate updates but were really the

SUNBURST malware. This attack underscores the need for heightened vigilance in monitoring third-party software and the growing risks posed by cyber threats that exploit established trust relationships.

Bibliography

(2021) *Solarwinds attack—no easy fix - CRS reports - congress.gov*. Available at: https://crsreports.congress.gov/product/pdf/IN/IN11559 (Accessed: 12 January 2025).

(No date) *Solarwinds Supply Chain attack* (no date) *Fortinet*. Available at: https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack (Accessed: 12 January 2025).

(2021) *CFCs*. Available at: T (Accessed: 12 January 2025).

(2023) *Solarwinds attack: Play by play and lessons learned* (2023) *Aqua*. Available at: https://www.aquasec.com/cloud-native-academy/supply-chain-security/solarwinds-attack/?.com (Accessed: 12 January 2025).

Schwartz, S. (2021) *Solarwinds threat actor targeted it service providers in thousands of attacks, Microsoft says*, *Cybersecurity Dive*. Available at: https://www.cybersecuritydive.com/news/microsoft-nobelium-breach-russia/608803/?.com (Accessed: 12 January 2025).

Apt29 aka nobelium, Cozy Bear (2024) *Sekoia.io*. Available at: https://www.sekoia.io/en/glossary/apt29-aka-nobelium-cozy-bear/ (Accessed: 12 January 2025).

Kremlin-backed hacking group puts fresh emphasis on stealing credentials (2023) *Cyber Security News | The Record*. Available at: https://therecord.media/nobelium-hacking-group-stealing-credentials?.com (Accessed: 12 January 2025).

Sunspot malware: A technical analysis (2021) *CrowdStrike*. Available at: https://www.crowdstrike.com/en-us/blog/sunspot-malware-technical-analysis/ (Accessed: 12 January 2025).

(No date) *Mitre ATT&CK®*. Available at: https://attack.mitre.org/techniques/ (Accessed: 22 January 2025).

Risk Assessment

Asset Identification and Valuation

Assets are valued in terms of the consequences that loss of confidentiality, integrity and availability (CIA) would lead to.

Asset Value	**Consequences of Loss of CIA**
High	Loss of CIA would have an immediate and considerable impact on cash flow, operations and contractual obligations.
Medium	Loss of CIA would have a lower impact but loss will still lead to additional costs.
Low	Loss of CIA would have no effect on cash flow, operations and obligations.

Inherent Risk

Each asset and vulnerability will have a determined probability of a specific risk materialising.

Impact x Likelihood = RISK

Probability	**Guidance**
Certain	- History of regular occurrences. - No special skills required.
Likely	- The event will occur in most circumstances
Possible	- Has occurred - No special skills required
Unlikely	- The event could occur at some time

Rare	- No history of occurrence - High level of technical or social engineering skill and determination required

Impact and Likelihood

The magnitude of harm that an adverse event can cause and how probable the event is

Impact	**Score**	**Disruption to business / system**
Insignificant	1	Little to no impact on the business
Minor	2	Minor reduction in normal service
Moderate	3	Short system outages with lengthy disruption to services
Major	4	Longer outages and lengthy service disruptions
Catastrophic	5	Complete system disruption no exact time known for when the system will be back online

.

Likelihood	**Score**	**How likely is this going to happen?**
Rare	1	Highly improbable this will happen
Unlikely	2	Unlikely that this will happen
Possible	3	A distinct possibility that this will occur
Likely	4	It is likely that this will occur
Highly Likely	5	It is highly likely or a certain possibility that this will occur

Risk Assessment

Serial	**Asset**	**Value**	**Vulnerability**	**Adversity**	**Operational? Reputational? Financial?**	**Severity?**	**Likelihood?**	**Risk**
1	Orion	High	Missing patches,	Malicious State	Operational	5	5	25

	Software		poor coding practices, lack of secure updates & Poor developer training or code review	sponsored actor exploiting CI/CD pipelines & Non malicious Insider threat With poor code validation or secure practises	Reputational Financial			
2	Distribution Server	High	Server located in a poorly secured environment & Misconfigured server settings & Weak network filtering or lack of encrypted protocols	Malicious State sponsored actor using stolen credentials or exploiting weak access controls & Power outage disrupting operations	Operational Reputational Financial	5	4	20
3	Build Environment	High	Outdated CI/CD tools, insecure pipeline configurations & Poor procedure for handling build artifacts	Malicious State sponsored attackers targeting vulnerable pipelines & Non malicious Insider threat misconfiguring or causing error because of poor training	Operational Reputational Financial	4	4	16
4	Source Code Repository	High	Unchecked dependencies or libraries, improper input validation & Insider threat or uninformed developer introducing vulnerabilities	Malicious Insider threat inserting malware intentionally & Non malicious Insider threat developer unknowingly introducing vulnerabilities accidentally	Operational Reputational Financial	4	4	16
5	Monitoring and Testing Processes	High	Ineffective or outdated monitoring tools & Unencrypted logging & Failure to act on alerts or misinterpretation of anomalies	Malicious State sponsored threat bypassing detection mechanisms & Non malicious Insider threat misconfiguring monitoring tools or missing alerts	Operational Reputational	3	3	9
6	Authentication and Access	High	Shared or weak credentials stored on	Malicious Insider threat or external attackers exploiting	Operational Reputational	5	3	15

	Controls		insecure devices & Stolen credentials, poor access control policies.	poor IAM practices or bruteforcing & Non malicious Insider threat employee credential sharing or being negligent				
7	Internal Communication Systems	Medium	Unencrypted messages, open email protocols & Lack of employee awareness training	Malicious hackers targeting internal email or messaging platforms & Non malicious Insider threat employees unknowingly clicking malicious links	Operational Reputational	3	4	12
8	Digital Signing Systems	High	Weak key management or outdated key protocols & Mismanaged signing keys or improper procedures	Malicious attackers exploiting weak key management	Operational Reputational Financial	5	4	20
9	Customer Communication Systems	Low	Lack of email security protocols (e.g. DKIM) & Impersonation due to weak authentication	Malicious threat actors using compromised systems to spread misinformation	Operational Reputational	3	3	9
10	Database	High	Lack of physical security for database servers & SQL injection vulnerabilities, weak encryption & Improper database permissions, poor query practices	Malicious Hackers exploiting insecure form fields & Non malicious Insider threat employee incorrectly sanitising form fields	Operational Financial	4	4	16

Risk Assessment (with counter measures)

Serial	Asset	Controls	Type	Severity?	Likelihood?	Residual Risk
1	Orion Software	Implement secure development lifecycle practices & Perform forensic analysis on software tampering and have incident response playbooks for compromised updates	Deterrent & Response	3	3	9
2	Distribution Server	Restrict physical access to servers via secure areas, locks, and keycard systems & Harden server configurations & Regularly audit server configurations and maintain backup/restore mechanisms	Vulnerability & Deterrent & Response	3	2	6
3	Build Environment	Use MFA for CI/CD pipeline access & Restrict access to build environment to essential personnel only	Vulnerability	3	3	9
4	Source Code Repository	Use signed commits and code provenance tracking	Response	3	2	6
5	Monitoring and Testing Processes	Establish baselines for anomaly detection	Response	3	3	6
6	Authentication and Access Controls	Regularly rotate passwords and credentials	Vulnerability	4	3	12
7	Internal Communication Systems	Segment internal networks to isolate	Avoidance	2	3	6

		critical communication channels				
8	Digital Signing Systems	Enforce secure key management policies	Vulnerability	3	3	9
9	Customer Communication Systems	Encrypt all sensitive customer communications	Vulnerability	2	2	4
10	Database	Perform database integrity audits and vulnerability scans	Deterrent	3	3	9

Threat Modelling of the Solar Winds attack using the Cyber Kill Chain

1. Reconnaissance

Nobelium would have actively and passively conducted research to gather information about SolarWinds and their software development process. They likely examined SolarWinds' public facing infrastructure identifying potential vulnerabilities. They may also have collected data on Orion's build environment, developer practices and software dependencies. They would have aggregated a list of SolarWinds customers to ensure the specific organisations they were targeting were vulnerable to the supply chain attack.

Key Steps:

- Identifying SolarWinds as a valuable target due to its extensive customer base.
- Mapping the Orion development and distribution ecosystem.
- Utilising open-source intelligence (OSINT) and tools to locate entry points.

2. Weaponisation

Nobelium prepared the SUNBURST backdoor and the SUNSPOT malware to help with its insertion. They would have done this by testing the malware against the Orion platforms source code during the time that they were covertly monitoring SolarWinds developer environments.

Key Steps:

- Developing SUNBURST to mimic legitimate Orion network traffic.
- Crafting SUNSPOT to replace source code during compilation without detection.
- Ensuring the malware's compatibility with Orion updates.

3. Delivery

The attackers successfully delivered the malicious payload by compromising the SolarWinds supply chain. This was achieved by embedding SUNSPOT into legitimate Orion software

updates. Once SolarWinds distributed these updates to its customers, the malicious code was deployed across thousands of organisations worldwide.

Key Steps:

- Embedding SUNSPOT into Orion updates.
- Leveraging the trust SolarWinds' customers placed in its software updates.
- Distributing the compromised updates through the usual update mechanisms.

4. Exploitation

After delivery, the SUNSPOT malware had safeguards programmed, ensuring that Orion builds did not fail, ensuring the developers did not detect it. SUNSPOT monitored running processes for those involved in compilation of the Orion product and replaced one of the source files to include the SUNBURST backdoor code.

Key Steps:

- Safeguards added to SUNSPOT to ensure Orion builds didn't fail, alerting developers.
- Monitoring running processes with SUNSPOT
- Exploiting access privileges granted to the Orion software.

5. Installation

Once active, SUNBURST established a persistent presence in the compromised systems.It laid dormant for two weeks and imitated legitimate Orion traffic in order to stay concealed, creating a foothold that allowed Nobelium to maintain access for multiple sessions.

Key Steps:

- Deploying the SUNBURST backdoor within victim environments.
- Creating persistence mechanisms to maintain access despite system reboots or security measures.
- Monitoring and avoiding detection by laying dormant for two weeks.

6. Command and Control (C2)

In the C2 phase, SUNBURST connected to remote servers controlled by the attackers. It used a domain generation algorithm (DGA) to communicate with these servers, ensuring anonymity and resilience against takedowns. The attackers then identified high-value targets among the affected organisations.

Key Steps:

- Establishing encrypted communication channels with compromised systems.
- Filtering targets by analysing network traffic and system characteristics.

7. Actions on Objectives

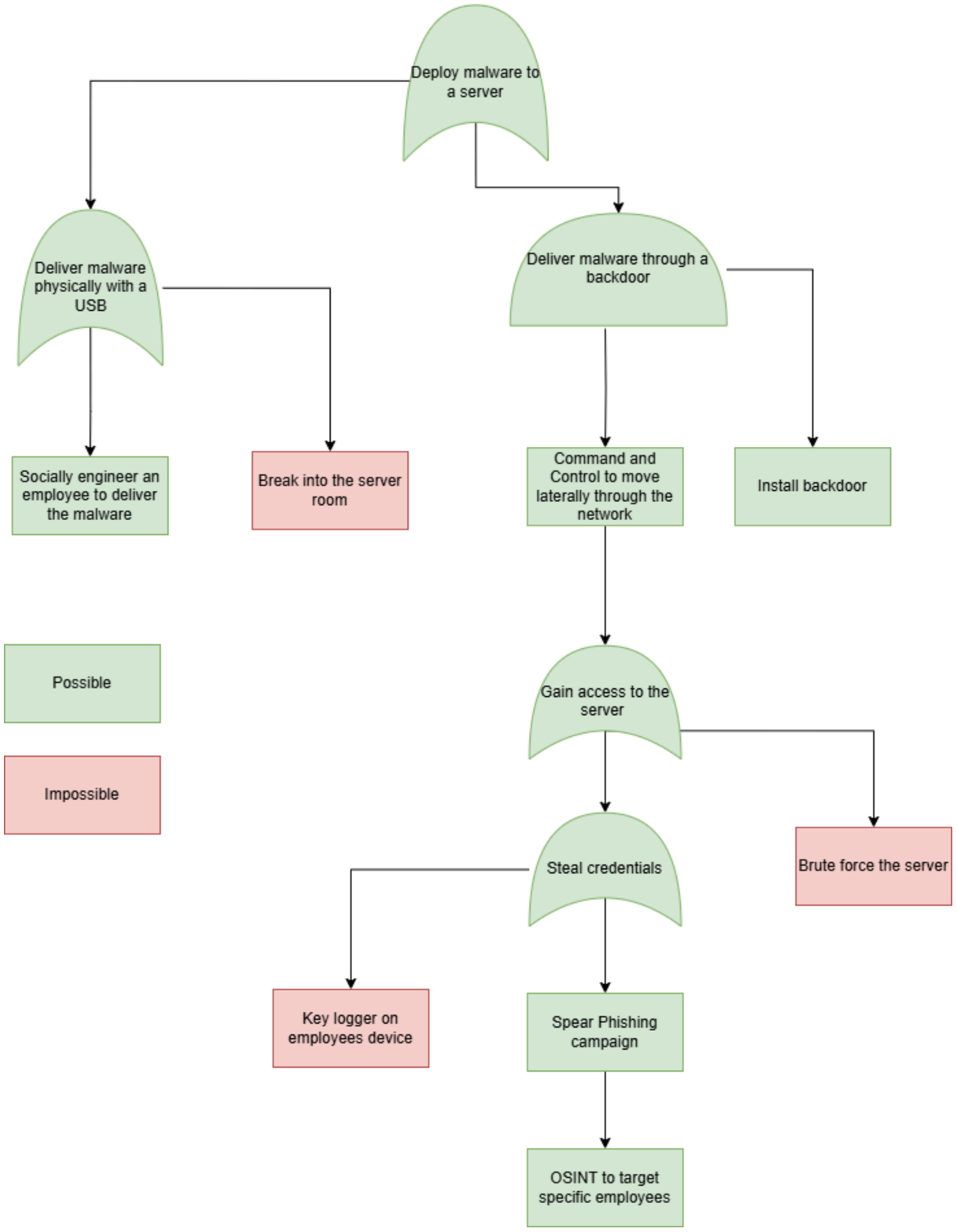
With C2 established, Nobelium can now move laterally throughout the victims network conducting data exfiltration, surveillance, and espionage. The group focused on high-profile government agencies and private-sector organisations, extracting sensitive information.

Key Steps:

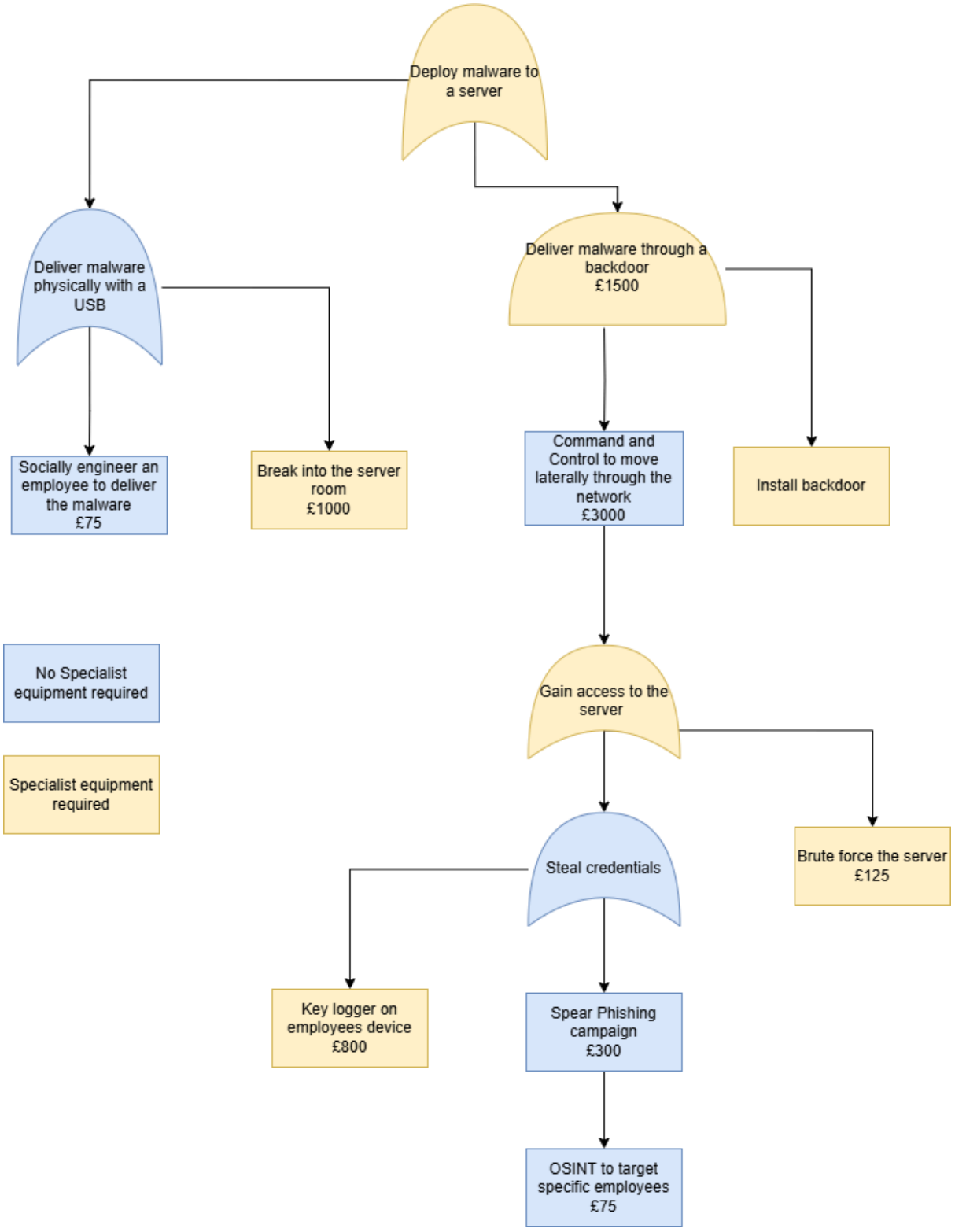
- Conducting lateral movement within networks to access sensitive data.
- Exfiltrating valuable information, such as intellectual property and government secrets.

Attack Tree

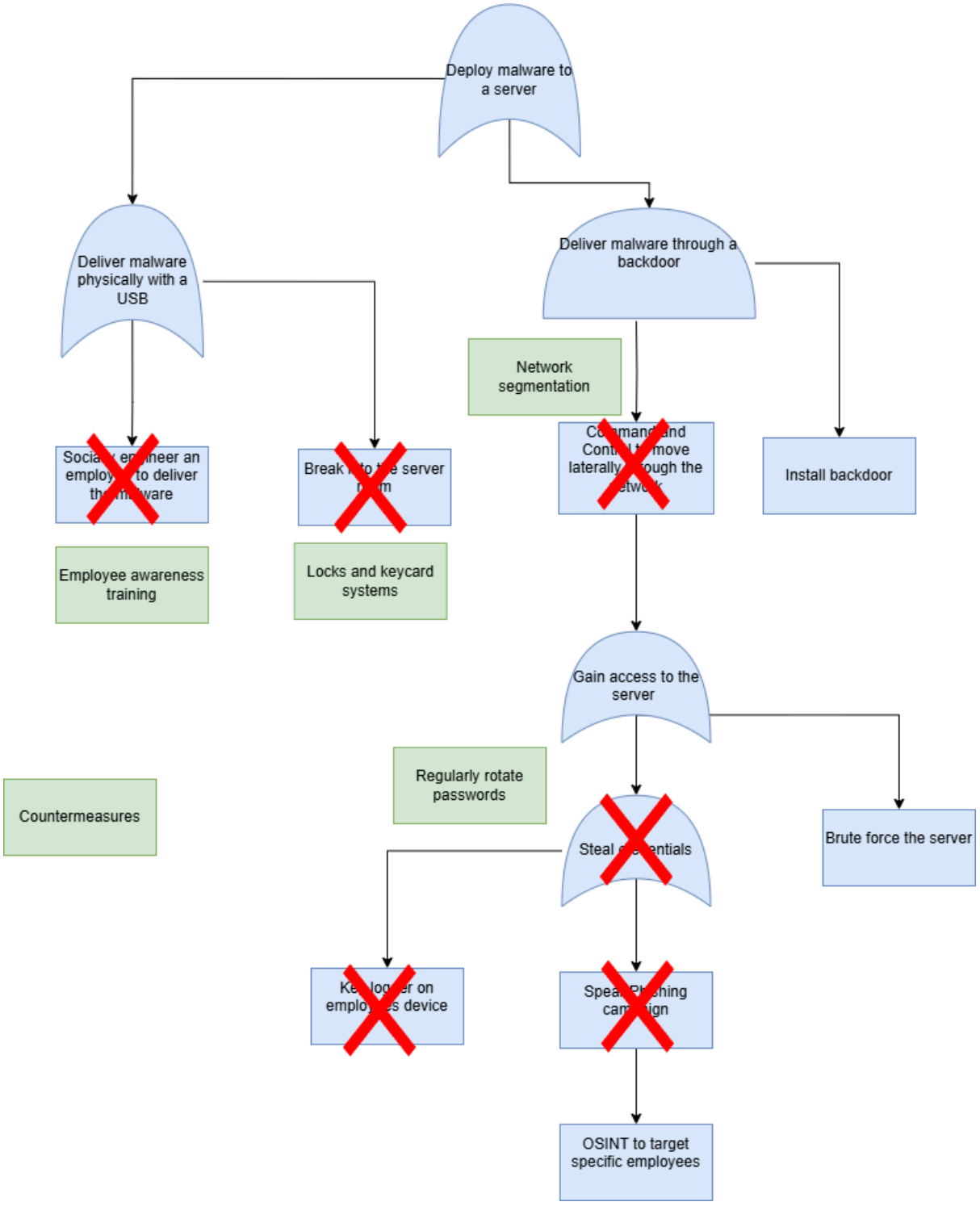
Possible/Impossible Nodes



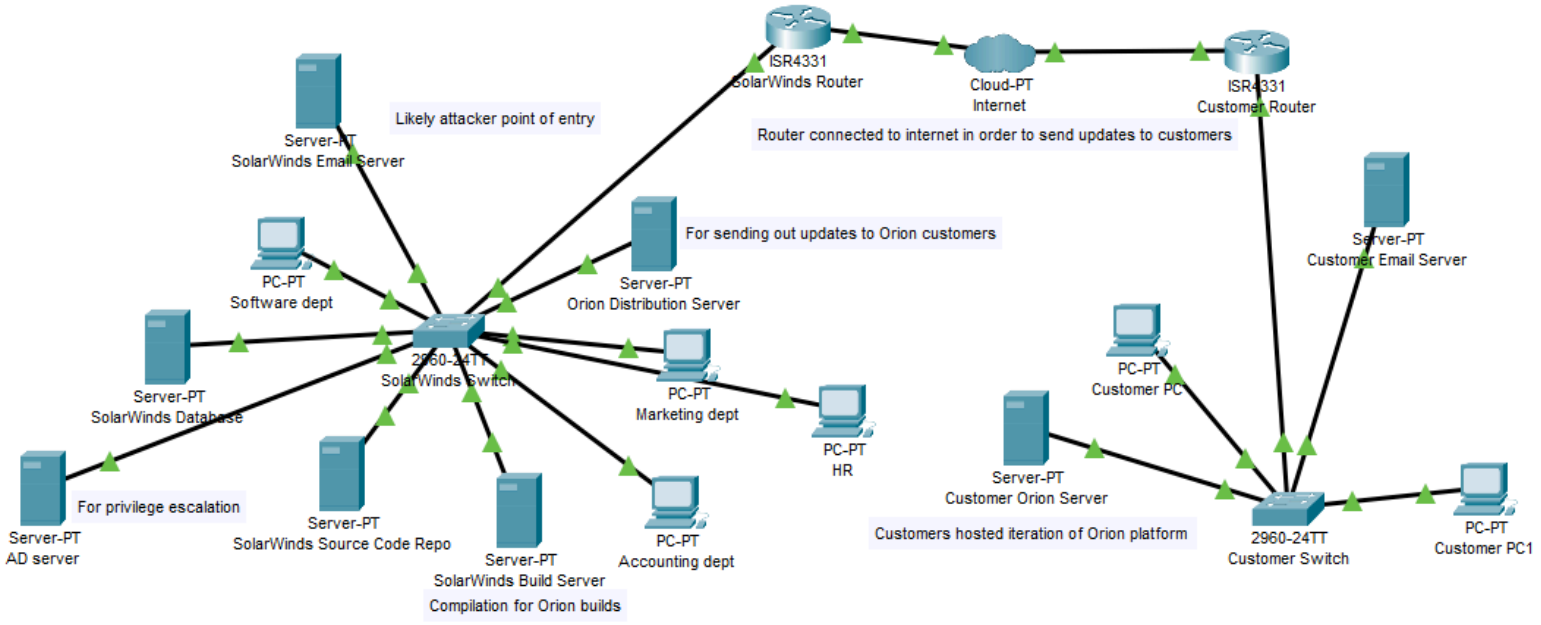
Specialist Equipment Required



Countermeasures



Infrastructure diagram of Solar Winds pre-breach



This CPT infrastructure of SolarWinds pre-breach shows the core assets used by SolarWinds and the connection to the customers' environments.

The SolarWinds environment consists of several critical components:

1. **Orion Server**: This was the central piece of SolarWinds' monitoring software and the primary vector exploited during the attack. The Orion Server was responsible for distributing updates to customers making it a crown jewel asset for an attacker targeting the software supply chain of SolarWinds customers.
2. **Active Directory (AD) Server**: Responsible for managing user authentication and access control, which would be a key target for lateral movement once the attacker gains a foothold through persistence.
3. **SolarWinds Email Server**: Handles internal and external email communication, highlighting a potential point of initial compromise through phishing campaigns allowing attackers to gain access to the internal network.
4. **Database Server**: Contains critical data related to monitoring and system logs, which could be valuable for attackers attempting to hide their tracks.
5. **Source Code Repository**: Stores the source code of the Orion platform ready for the data to be fetched by the build server. An attacker could exploit this and reverse engineer the source code for malicious purposes if they have unrestricted access to it.
6. **Build Server**: Responsible for compiling Orion builds, would be a high value target for any attacker attempting to code inject malware into the Orion platform before it is distributed as an update for customers.
7. **Computers**: Employee personal workstations, could be targeted for data exfiltration.

The customer's environment consists of several critical components:

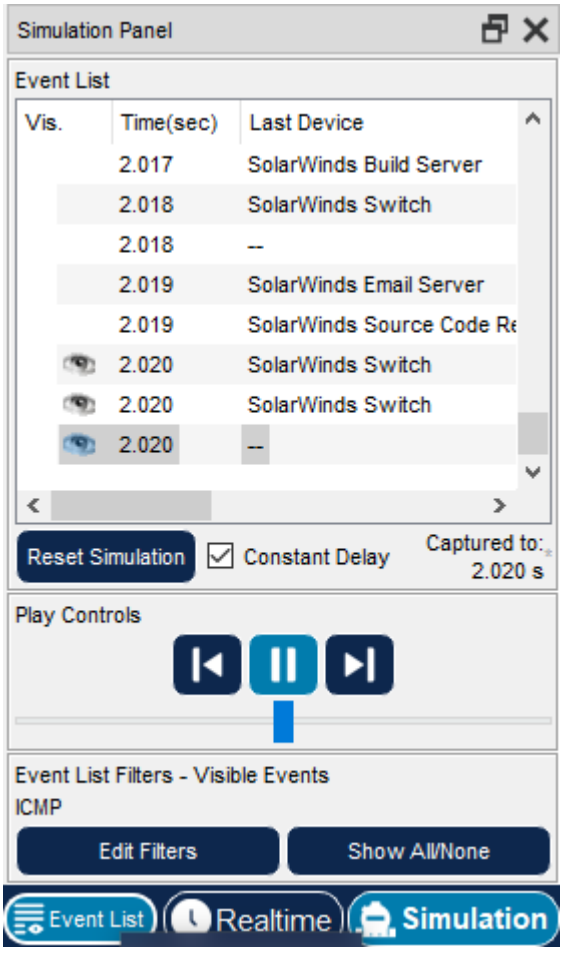
1. **Customer Devices**: Various endpoints (e.g., PCs and email servers) are shown, representing systems at risk of data exfiltration when the attackers use command and control to move through the network.

2. **Orion Server**: Self hosted iteration of the Orion platform in the customer's environment. It would have heightened privileges because it needs access to monitor the entire network. Key for attackers trying to get into a target's network with no privilege escalation.

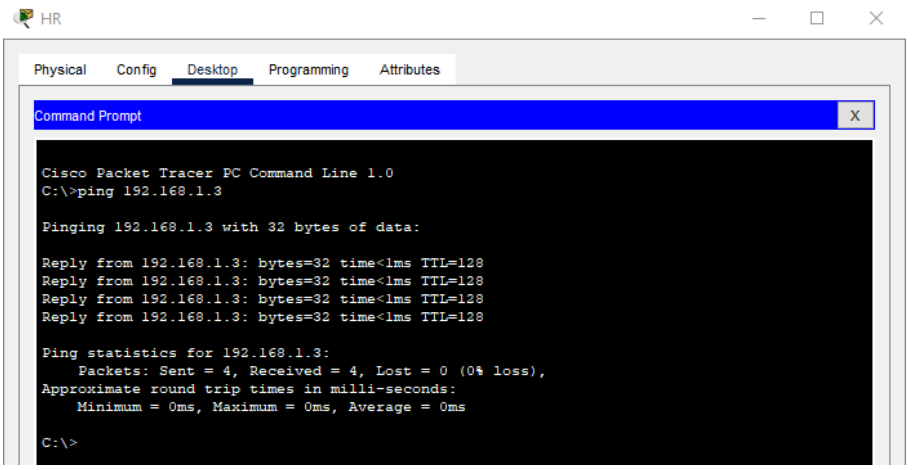
Connectivity and Functionality

The Orion Distribution Server acts as the bridge between SolarWinds and its customers, propagating updates through the SolarWinds Router to the cloud and then to customer environments. Within the customer network, the Orion Server monitors all connected devices, which would have allowed attackers to move laterally and access sensitive systems.

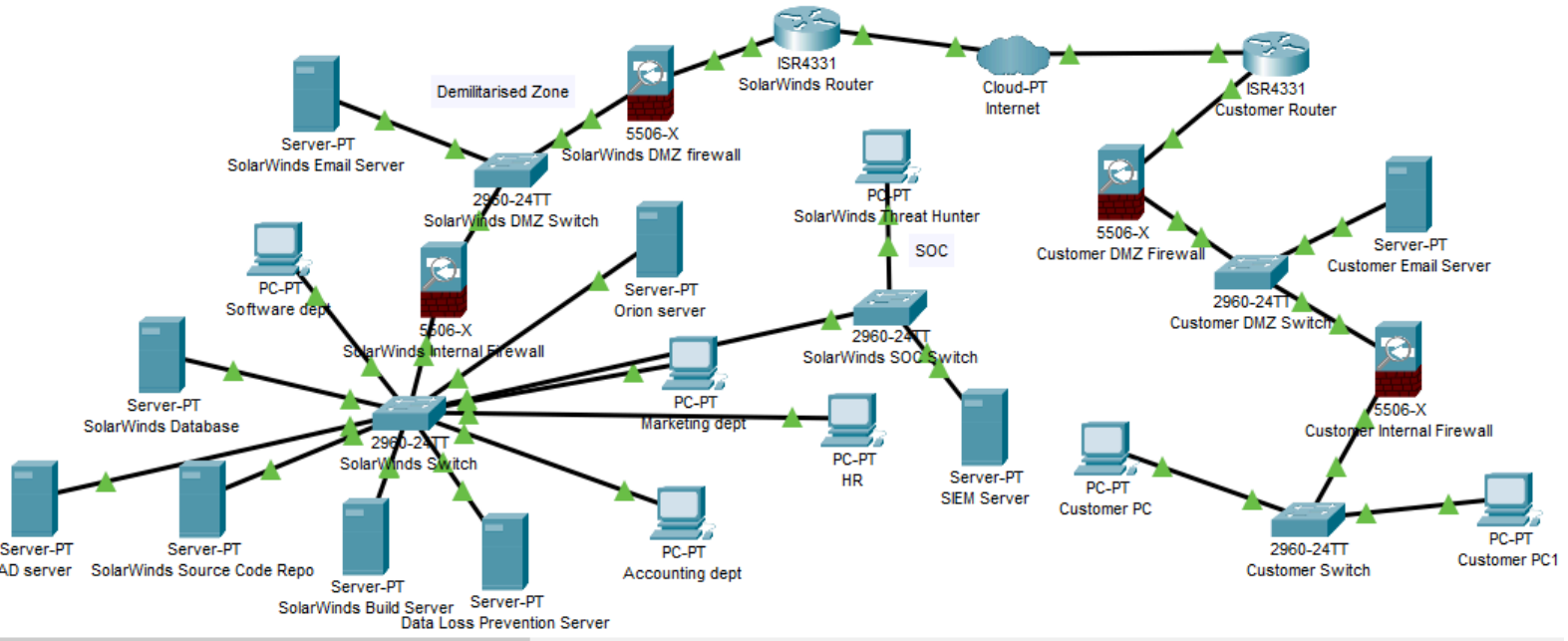
All components in this network are linked logically to ensure communication is possible. End-to-end connectivity can be verified by testing ping functionality between critical nodes, such as the SolarWinds Orion server and the build server. This is essential for demonstrating the operational validity of the diagram.



Simulation and terminal screenshots showing ICMP (ping) requests and replies between devices on both networks.



Infrastructure diagram of Solar Winds post-breach



This CPT infrastructure of SolarWinds post-breach shows the new mitigation techniques used to prevent another attack.

Security Operations Centre (SOC): Post-breach, the SOC centralises monitoring to detect and respond to threats within the SolarWinds network. Logs from the Orion server, firewalls, DMZ, and other critical infrastructure are aggregated into a SIEM server for analysis. An IDS/IPS is deployed to monitor for malicious traffic patterns, such as the lateral movement seen in the SolarWinds breach. SOC analysts operate from dedicated VLANs to prevent exposure to compromised resources. Alerts from DLP systems and network monitoring tools are sent to the SOC in real time, for incident response. This setup ensures proactive defense, reducing the risk of a repeat attack.

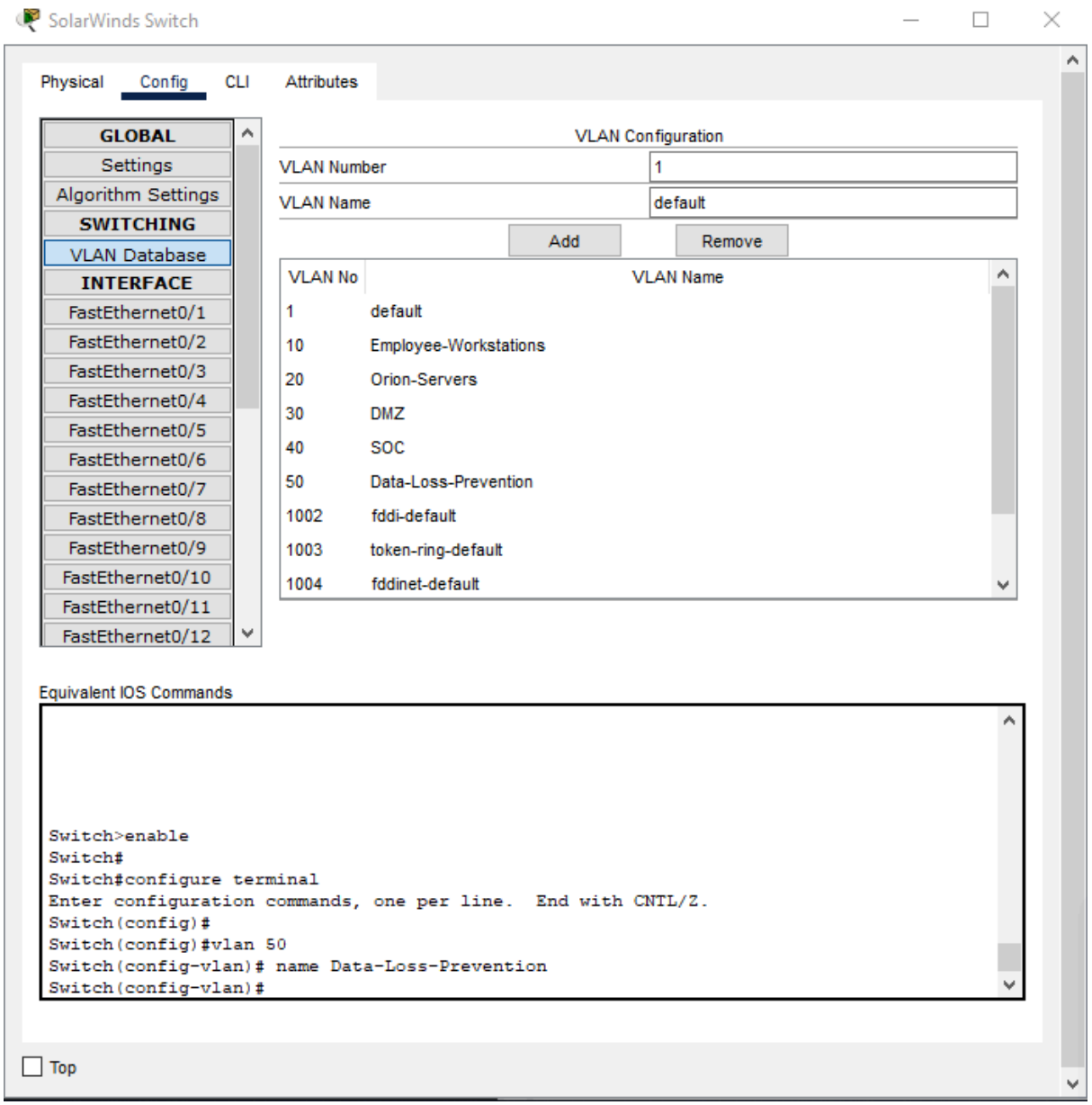
Demilitarised zone (DMZ):The SolarWinds network has a DMZ configured to secure external-facing services such as the email server. A dedicated DMZ VLAN isolates these resources, preventing direct access to the internal network. Granular rules on the DMZ firewall restrict traffic to necessary ports and protocols, while an IDS/IPS monitors for unusual activity, such as unauthorised file uploads. This configuration ensures attackers cannot leverage DMZ resources to gain internal access. For example, the email server's communication with the internal network is limited to specific services, mitigating vulnerabilities that enabled the original breach. Regular audits and updates enhance overall security.

VLAN segmentation within SolarWinds prevents attackers from spreading across the network. Key assets like the Orion server, Data Loss Backup Server, and SOC tools are placed in isolated VLANs. Inter-VLAN communication is tightly controlled using ACLs. For example, the Orion server VLAN is configured to communicate only with specific internal servers and the SOC VLAN. Workstations for departments like Marketing and HR are

separated, reducing potential attack paths. If an endpoint is compromised, VLAN isolation minimises the attacker's ability to move laterally. This segmentation strategy protects critical SolarWinds infrastructure while allowing necessary communication for operations.

A DLP server is deployed to monitor sensitive SolarWinds data, such as customer credentials and source code. Positioned on a secure VLAN, the server scans outbound traffic from key assets like the Orion server and email systems for signs of data exfiltration. During the original breach, attackers exfiltrated data undetected—this mitigation ensures such activity is flagged and blocked. Alerts are sent to the SOC, triggering immediate investigation and response. Policies are enforced to quarantine unauthorised transfers. The DLP system's integration with the SOC strengthens SolarWinds' ability to prevent data theft in future attacks.

Screenshot of newly added VLANS



Security Assurance Architecture of Solar Winds

Possible security policies:

Email Policy- A strong email security policy mitigates the risk of a phishing attack, along with accidental malware downloads and credential theft. Phishing campaigns are used by threat actors to gain initial access into a network, email filtering, attachment scanning and employee training are countermeasures related to this policy that could reduce this risk.

Incident Recovery Policy- This policy ensures a structured response to incidents, minimising impact and restoring availability of critical assets. Lack of immediate detection and containment can allow attackers to maintain persistence in a victims environment for an extended period of time. Backup restoration, forensic analysis and incident reviews would help recovery.

Digital Signature Acceptance Policy- This policy ensures that all software updates and third party code be digitally signed and verified before it is deployed to customers. Customers are at risk of supply chain attacks in which attackers insert trojanised code into updates if the proper precautions are not taken. By enforcing strict signature validation and certificate checks unauthorised code being injected into software updates can be prevented.

Server Malware Protection Policy- This policy mandates that all servers have satisfactory malware detection, prevention and response mechanisms. Attackers use servers to spread malware covertly, by implementing behaviour monitoring and file quarantining, malicious activity can be mitigated earlier.

Software Build Integrity Policy- This policy enforces secure compilation practices to prevent unauthorised modifications during the software build process. Attackers can tamper with source code before compilation, therefore implementing strong access controls, cryptographic signing and build environment monitoring could prevent software compromises.

Software Build Integrity Policy

1. Overview

Insecure software build environments opens the organisation up to possibly distributing malicious software to users. Attackers can manipulate source code during compilation to introduce malicious payloads to software that was otherwise safe with developers completely oblivious. This policy ensures build environments free from unauthorised changes and resistant to compromise by attackers. Strict access controls, integrity verification and monitoring will harden the security of software builds from malicious code injections.

2. Purpose

The purpose of this policy is to protect the processes associated with software development and deployment from unauthorised inspection, modification and malicious code injections. It defines requirements for code integrity, build process monitoring, developer access controls and software provenance tracking.

3. Scope

This policy applies to all <Company Name> developers, engineers and third-party vendors involved in the software development lifecycle. This policy covers all build servers, CI/CD pipelines, software compilation environments and components operating within <Company Name> premises or on their cloud.

4. Policy

4.1 Code Integrity Controls

- All source code must be digitally signed and verified before inclusion in the build process.
- Build artifacts must be hashed and integrity-checked to detect unauthorised modifications.
- Only authorised and reviewed code commits shall be merged into production repositories.
- Any modification to source code during the build process must be logged and reviewed by an independent security team.
- Software composition analysis (SCA) tools must be used to detect vulnerabilities in third-party dependencies.

4.2 Build Environment Security

- Access to build environments must follow Zero Trust principles.
- Build servers must be segmented from general development environments to prevent unauthorised access.
- Continuous monitoring of build processes is required to detect unexpected file changes or process injections.
- Build logs must be saved and reviewed previously to track modifications and detect anomalies.
- Logging mechanisms must be implemented to ensure build logs cannot be modified or erased.

4.3 Developer Access

- Multi-Factor Authentication (MFA) is mandatory for all developers accessing build systems.
- Any third-party integration (e.g., libraries, dependencies) must undergo security assessment before use.
- Background checks and security training are required for personnel involved in secure software development.
- Access to the build environment should be restricted to authorised personnel only, with activity logs maintained.
- All code commits must undergo peer review and automated security testing before approval.

4.4 Automated Security Measures

- Real-time anomaly detection tools must be deployed to identify unauthorised process injections.
- Any unexpected modifications in build configurations must trigger an immediate security review.
- Code dependencies must be monitored for vulnerabilities, and outdated or untrusted libraries should be flagged.
- Memory integrity protections should be enabled to prevent malware from modifying compiled binaries before deployment.

4.5 Build Process Auditing and Change Management

- All changes to the build process must be documented and reviewed.
- Code provenance tracking must be enforced to verify the authenticity of every software component.
- Security incidents related to the build process must be logged, analysed, and remediated promptly.

5. Policy Compliance

5.1 Compliance Measurement

- Regular security audits and penetration tests will be conducted on the build environment.
- Automated integrity verification tools will run after every build to detect tampering.
- All code modifications must be logged and cryptographically signed for traceability.

5.2 Exceptions

- Any deviations from this policy require written approval from the Security Team and CISO.
- Temporary exceptions should be logged, monitored, and reviewed periodically.

5.3 Non-Compliance

- Failure to comply with this policy may result in access revocation, disciplinary actions, or contract termination.
- Regular compliance reviews must be conducted, with violations reported to senior leadership.

6. Related Standards, Policies and Processes

- NIST 800-161 https://csrc.nist.gov/pubs/sp/800/161/r1/final

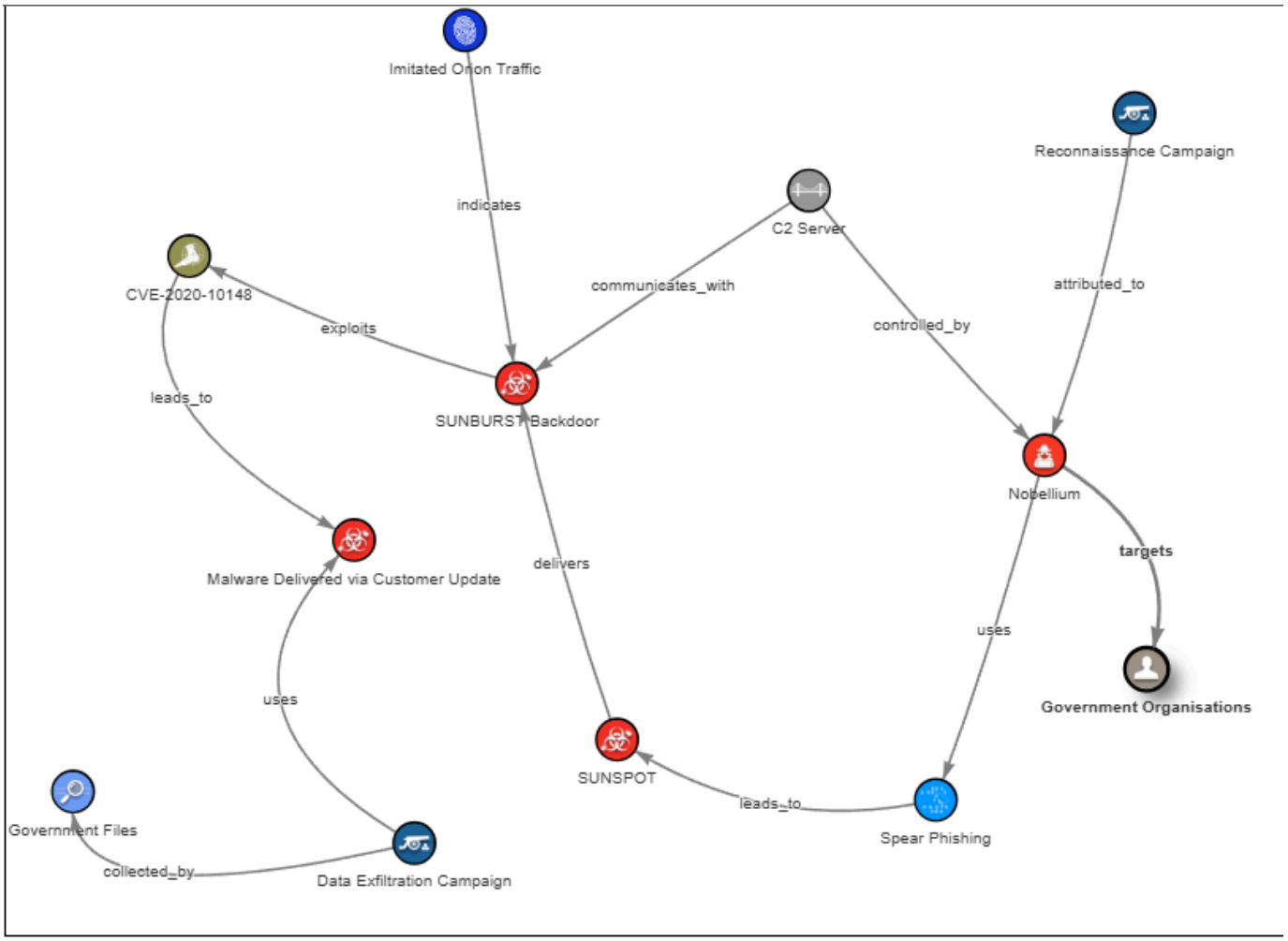
7. Definitions and Terms

None.

8. Revision History

None.

STIX JSON SDO & Descriptions



Threat Actor: Nobellium (APT29)

- **SDO**: threat-actor--Nobellium
- **Description**: Nobellium is a Russian cyber espionage group known for its creation of the SUNBURST malware. The group's goals are primarily espionage and data exfiltration. Nobellium's tactics often involve sophisticated and targeted attacks on government organisations and large private companies.

- **External Reference**: MITRE ATT&CK categorises them as G0016

Intrusion Set: SUNSPOT

- **SDO**: intrusion-set--sunspot
- **Description**: SUNSPOT refers to the specific malware delivered by Nobellium that leveraged the SolarWinds Orion platform for espionage. This malware monitored running processes and replaced a source file to include the SUNBURST backdoor. The malware had several safeguards in place ensuring that the builds did not fail so developers were not alerted to the breach.

Malware: SUNBURST Backdoor

- **SDO**: malware--sunburst
- **Description**: The SUNBURST backdoor was a remote-access trojan (RAT) deployed via compromised updates in the SolarWinds Orion platform. This malware allowed the attackers to gain persistent access to affected systems, facilitating further exploitation and data exfiltration.The attackers used this RAT as a delivery mechanism for more sophisticated cyber espionage.

Attack Pattern: Spear Phishing

- **SDO**: attack-pattern--spear-phishing
- **Description**: Spear-phishing was the likely initial entry point for the attack. Nobellium probably used targeted phishing emails to trick SolarWinds employees into executing malicious attachments, which then led to the compromise of the company's internal network.
- **External Reference**: MITRE ATT&CK references the technique T1566, which is associated with the spear-phishing tactic, detailing how attackers manipulate victims into taking actions that will compromise their systems.

Vulnerability: CVE-2020-10148

- **SDO**: vulnerability--orion-build-server
- **Description**: The vulnerability CVE-2020-10148 highlights a weakness in the SolarWinds Orion build server's. Nobellium exploited this vulnerability after gaining initial access via spear-phishing to run commands and deploy the SUNBURST malware, which affected both the internal SolarWinds network and customers who installed the compromised updates.
- **External Reference**: NIST national vulnerability database (NVD) references the CVE

Indicators: Imitated Orion Traffic

- **SDO**: indicator--malicious-ip
- **Description**: The SUNBURST malware imitated legitimate Orion traffic to avoid detection by security systems.

Malware Delivered via Customer Update

- **SDO**: malware--sunburst-customer-update
- **Description**: Infected SolarWinds Orion updates served as the delivery vector for the SUNBURST malware, affecting organisations that deployed the updates. This was a highly effective method of delivering a backdoor, as it leveraged trusted software updates.

Command and Control (C2) Server

- **SDO**: malware--c2-server
- **Description**: The C2 server was used by Nobellium to control and communicate with the infected systems. This infrastructure element is critical for maintaining persistence and exfiltrating data from the compromised networks.

Campaigns: Data Exfiltration and Reconnaissance

- **SDOs**: campaign--data-exfiltration, campaign--reconnaissance
- **Data Exfiltration Campaign**: The Data Exfiltration Campaign was one of the key objectives of Nobellium's attack. The goal was to exfiltrate sensitive documents and data from targeted organisations, particularly government entities.
- **Reconnaissance Campaign**: Nobellium would've also conducted a reconnaissance campaign to map out the target environment.

Relationships Between SDOs

The relationships between various SDOs show the flow of the attack and give a structured timeline on the events during and before the attack:

- **SUNSPOT** → **SUNBURST**: The SUNSPOT malware delivers the SUNBURST backdoor, marking the key point of malware deployment.
- **Spear Phishing** → **SUNSPOT**: The spear-phishing attack led to the attackers gaining initial access to the network leading to SUNSPOT being deployed in the build server.
- **SUNBURST** → **Orion Build Server Vulnerability**: The SUNBURST malware exploits the CVE-2020-10148 vulnerability in the Orion build server to gain deeper access to the compromised systems.
- **Data Exfiltration Campaign** → Government Files: The data exfiltration campaign collected sensitive government files, which were exfiltrated as part of the espionage efforts.

Appendix

{

"type": "bundle",

"id": "bundle--12345678-1234-5678-1234-567812345678",

```
"spec_version": "2.1",
"objects": [
 {
   "type": "threat-actor",
   "id": "threat-actor--Nobellium",
   "created": "2020-12-01T00:00:00.000Z",
   "modified": "2020-12-01T00:00:00.000Z",
   "name": "Nobellium",
   "description": "Russian cyber espionage group associated with the SolarWinds attack.",
   "threat_actor_types": ["nation-state"],
   "aliases": ["APT29"],
   "goals": ["Espionage", "Data Exfiltration"],
   "external_references": [
     { "source_name": "mitre-attack", "url": "https://attack.mitre.org/groups/G0016/" }
   ]
 },
 {
   "type": "malware",
   "id": "intrusion-set--sunspot",
   "created": "2020-12-01T00:00:00.000Z",
   "modified": "2020-12-01T00:00:00.000Z",
   "name": "SUNSPOT",
   "description": "Malware leveraging the SolarWinds Orion platform for espionage.",
   "attributed_to": ["threat-actor--Nobellium"],
   "external_references": [
     { "source_name": "cisa", "url": "https://us-cert.cisa.gov/ncas/alerts/aa20-352a" }
```

```
    ]
  },
  {
    "type": "malware",
    "id": "malware--sunburst",
    "created": "2020-12-01T00:00:00.000Z",
    "modified": "2020-12-01T00:00:00.000Z",
    "name": "SUNBURST Backdoor",
    "description": "Remote access trojan (RAT) implanted in SolarWinds Orion updates after the attackers gained access via spear-phishing.",
    "malware_types": ["remote-access-trojan"],
    "is_family": false
  },
  {
    "type": "relationship",
    "id": "relationship--intrusion-malware",
    "relationship_type": "delivers",
    "source_ref": "intrusion-set--sunspot",
    "target_ref": "malware--sunburst"
  },
  {
    "type": "relationship",
    "id": "relationship--intrusion-malware2",
    "relationship_type": "uses",
    "source_ref": "intrusion-set--sunspot",
    "target_ref": "malware--teardrop"
  },
```

```
{
  "type": "attack-pattern",
  "id": "attack-pattern--spear-phishing",
  "created": "2020-12-01T00:00:00.000Z",
  "modified": "2020-12-01T00:00:00.000Z",
  "name": "Spear Phishing",
  "description": "Nobellium used spear-phishing to target SolarWinds employees, tricking them into executing a malicious attachment that granted them initial access to the network.",
  "external_references": [
    { "source_name": "mitre-attack", "url": "https://attack.mitre.org/techniques/T1566/" }
  ]
},
{
  "type": "relationship",
  "id": "relationship--spearphishing-threatactor",
  "relationship_type": "uses",
  "source_ref": "threat-actor--Nobellium",
  "target_ref": "attack-pattern--spear-phishing"
},
{
  "type": "relationship",
  "id": "relationship--spearphishing-gainaccess",
  "relationship_type": "leads_to",
  "source_ref": "attack-pattern--spear-phishing",
  "target_ref": "intrusion-set--sunspot"
},
{
```

```
    "type": "vulnerability",
    "id": "vulnerability--orion-build-server",
    "created": "2020-12-01T00:00:00.000Z",
    "modified": "2020-12-01T00:00:00.000Z",
    "name": "CVE-2020-10148",
    "description": "Weakness in SolarWinds Orion build server's update process exploited by SUNBURST malware after the initial access via spear-phishing.",
    "external_references": [
      { "source_name": "cve", "url": "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10148" }
    ]
  },
  {
    "type": "relationship",
    "id": "relationship--malware-vulnerability",
    "relationship_type": "exploits",
    "source_ref": "malware--sunburst",
    "target_ref": "vulnerability--orion-build-server"
  },
  {
    "type": "indicator",
    "id": "indicator--malicious-ip",
    "created": "2020-12-01T00:00:00.000Z",
    "modified": "2020-12-01T00:00:00.000Z",
    "name": "Imitated Orion Traffic",
    "description": "SUNBURST imitates genuine Orion traffic.",
    "indicator_types": ["malicious-activity"]
```

```
},
{
  "type": "relationship",
  "id": "relationship--indicator-malware",
  "relationship_type": "indicates",
  "source_ref": "indicator--malicious-ip",
  "target_ref": "malware--sunburst"
},
{
  "type": "identity",
  "id": "government",
  "name": "Government Organisations",
  "description": "Governments targeted by Nobellium"
},
{
  "type": "relationship",
  "id": "relationship--nobellium-targets-gov-orgs",
  "relationship_type": "targets",
  "source_ref": "threat-actor--Nobellium",
  "target_ref": "government"
},
{
  "type": "malware",
  "id": "malware--sunburst-customer-update",
  "created": "2020-12-01T00:00:00.000Z",
  "modified": "2020-12-01T00:00:00.000Z",
```

```
    "name": "Malware Delivered via Customer Update",
    "description": "Malware delivered through the SolarWinds Orion update process, affecting customers who installed the compromised updates.",
    "malware_types": ["remote-access-trojan"],
    "is_family": false
  },
  {
    "type": "relationship",
    "id": "relationship--build-server-leads-to-customer-malware",
    "relationship_type": "leads_to",
    "source_ref": "vulnerability--orion-build-server",
    "target_ref": "malware--sunburst-customer-update"
  },
  {
    "type": "infrastructure",
    "id": "malware--c2-server",
    "name": "C2 Server",
    "description": "Command-and-control (C2) server",
    "is_family": false
  },
  {
    "type": "relationship",
    "id": "relationship--c2-communicates-with-sunburst",
    "relationship_type": "communicates_with",
    "source_ref": "malware--c2-server",
    "target_ref": "malware--sunburst"
  },
```

```
  {
    "type": "relationship",
    "id": "relationship--c2-controlled-by-nobellium",
    "relationship_type": "controlled_by",
    "source_ref": "malware--c2-server",
    "target_ref": "threat-actor--Nobellium"
  },
  {
    "type": "campaign",
    "id": "campaign--data-exfiltration",
    "created": "2020-12-01T00:00:00.000Z",
    "modified": "2020-12-01T00:00:00.000Z",
    "name": "Data Exfiltration Campaign",
    "description": "Campaign focused on exfiltrating sensitive data from targeted organizations using SUNBURST malware.",
    "external_references": [
      { "source_name": "cisa", "url": "https://us-cert.cisa.gov/ncas/alerts/aa20-352a" }
    ]
  },
  {
    "type": "relationship",
    "id": "relationship--data-exfiltration-malware-update",
    "relationship_type": "uses",
    "source_ref": "campaign--data-exfiltration",
    "target_ref": "malware--sunburst-customer-update"
  },
  {
```

```
    "type": "observed-data",
    "id": "data--government-files",
    "created": "2020-12-01T00:00:00.000Z",
    "modified": "2020-12-01T00:00:00.000Z",
    "name": "Government Files",
    "description": "Sensitive government documents and data exfiltrated during the Data Exfiltration Campaign.",
    "external_references": [
      { "source_name": "cisa", "url": "https://us-cert.cisa.gov/ncas/alerts/aa20-352a" }
    ]
  },
  {
    "type": "relationship",
    "id": "relationship--data-exfiltration-collected-data",
    "relationship_type": "collected_by",
    "source_ref": "campaign--data-exfiltration",
    "target_ref": "data--government-files"
  },
  {
    "type": "campaign",
    "id": "campaign--reconnaissance",
    "name": "Reconnaissance Campaign",
    "description": "Reconnaissance campaign attributed to Nobelium, focused on identifying and mapping out the target environment for future exploitation and attack."
  },
  {
    "type": "relationship",
```

```
      "id": "relationship--nobelium-reconnaissance",
      "relationship_type": "attributed_to",
      "source_ref": "campaign--reconnaissance",
      "target_ref": "threat-actor--Nobellium"
    }
  ]
}
```