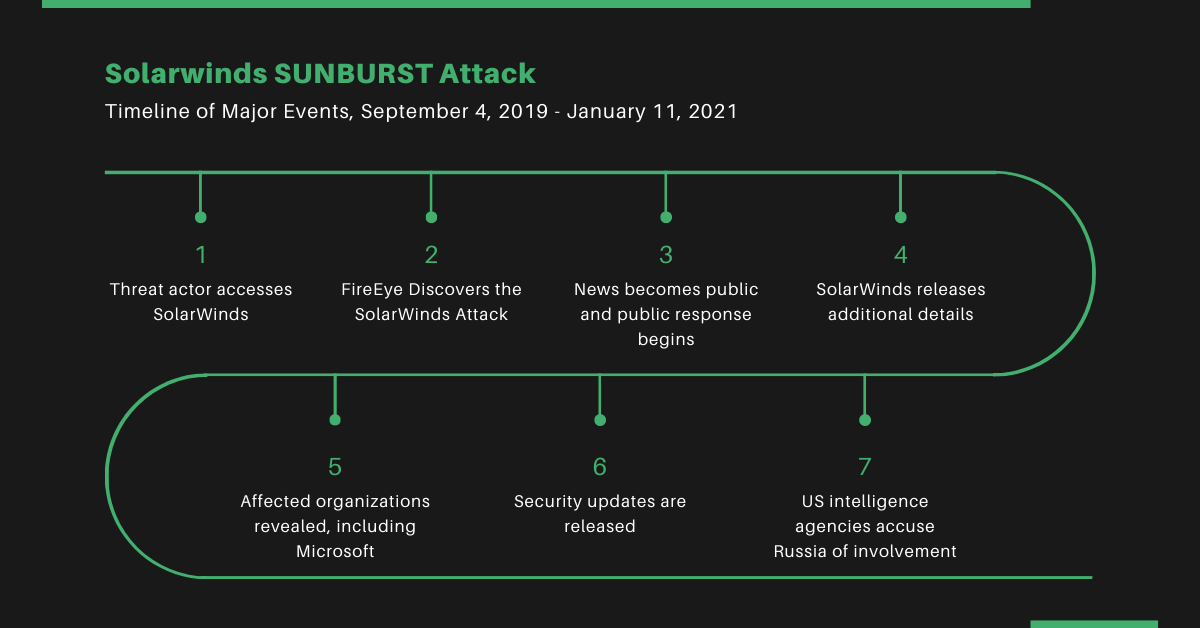


**Case study: SolarWinds Supply Chain Attack**

**By: Noor Saba Basit**

**SolarWinds Supply Chain Attack**

The **SolarWinds attack,** also known as the **Sunburst attack,** was a major supply chain attack that was discovered in **December 2020**. Hackers inserted malicious code into an update of the SolarWinds Orion platform. This update was downloaded by over **18,000 organizations**, including **U.S. government agencies, tech companies, and Fortune 500 firms**. This attack gave the attackers long-term access to sensitive systems, which remained undetected for months and severely impacted the **Confidentiality** and **Integrity** of the victims’ data and operations.

## **Attack Timeline**

* **September 4, 2019**: Attackers gained initial, unauthorized access to SolarWinds' internal network.
* **September 12, 2019**: Conducted dry-run code injection into the Orion platform; injected test versions of the SUNBURST backdoor and mimicked legitimate network traffic.
* **October 2019**: Continued with testing of code injection during Orion builds.
* **February 20, 2020**: Malicious SUNBURST backdoor is compiled into Orion software updates.
* **March 26, 2020**: Compromised Orion updates begin distribution to customers.
* **June 4, 2020**: Attackers remove the SUNBURST code from SolarWinds production systems.

**Attack Analysis Using the Cyber Attack Equation**

**Attack = Motive + Method + Vulnerability**

* **Motive (Why was the attack done?)**
* **Cyber-espionage**: The attackers wanted to spy on U.S. government agencies and large private companies secretly. The affected private companies include **Microsoft**, **Cisco**, **Intel**, **VMware, FireEye** (they discovered the breach), **NVIDIA, and Belkin.**
* **Stealing sensitive data**: The goal was long-term access to emails, confidential files, and internal communications.
* **Method (How was the attack carried out?)**
* **Supply chain attack**: Hackers secretly added malicious code (called *SUNBURST*) to a legitimate software update of the SolarWinds Orion platform.
* **Trusted disguise**: Because Orion was widely trusted, the malware spread to thousands of high-profile targets undetected.
* **Remote access**: The malware allowed the hackers to have backdoor access to victim systems, allowing data theft and spying.
* **Vulnerability (What weakness did the attackers exploit?)**
* **Weak security in the software update process**: The attackers were able to insert malware into Orion updates without being noticed.
* **Over-trusting third-party software**: Organizations automatically trusted and installed updates without checking them.
* **Lack of early detection**: The malware remained hidden for months, showing how detection systems failed.

## **Tactics, Techniques, and Purpose (TTPs) of the SolarWinds Attack**

SolarWinds cyberattack involved a well-planned strategy where attackers compromised the software update mechanism of **SolarWinds Orion**. The goal was to infiltrate major government and private sector networks without being detected for a long time.

**MITRE ATT&CK Framework** groups attacker behavior into three key parts: **Tactics** (what the attacker wanted to do), **Techniques** (how they did it), and **Purpose** (why they did it).

### Tactics (What the attacker wanted to do)

Tactics are the **high-level goals** or objectives that the attacker has during each phase of the attack. In the SolarWinds incident, the following tactics were used:

* **Initial Access**: Gain entry into the targeted networks.
* **Persistence**: Remain in the network over time without detection.
* **Defense Evasion**: Avoid being caught by antivirus or monitoring tools.
* **Credential Access**: Steal usernames and passwords.
* **Lateral Movement**: Move from one system to another inside the network.
* **Collection**: Gather sensitive or confidential information.
* **Exfiltration**: Send the stolen data out of the victim’s network.

### Techniques (How the attack was carried out)

Techniques refer to the **specific** **methods** an attacker uses to achieve their goals. Each technique is assigned a number by MITRE. Here are the main ones used in the SolarWinds attack:

|  |  |  |
| --- | --- | --- |
| Technique | Description | MITRE ID |
| **Supply Chain Compromise** | Attackers inserted malicious code into SolarWinds’ software update (Orion platform). This was the initial infection vector. | T1195.002 |
| **Code Signing** | The malware was signed with a valid digital certificate, making it look like a trusted update. | T1553.002 |
| **Use of Backdoor (SUNBURST)** | The malicious update created a hidden backdoor in the victim’s systems, allowing the attacker to control the network. | T1059 |
| **Time-based Evasion** | The malware waited weeks before executing, reducing the chance of early detection. | T1497.003 |
| **Command and Control via HTTP** | The malware communicated with the attackers using normal-looking internet traffic (HTTP), blending in with regular activity. | T1071.001 |
| **Credential Dumping** | Attackers stole login credentials from memory, especially from tools like LSASS in Windows. | T1003.001 |
| **Forging SAML Tokens** | Attackers forged authentication tokens to impersonate high-level users and access systems undetected. | T1606.002 |
| **Disabling Security Tools** | Some actions were taken to turn off or bypass security software. | T1562 |

These techniques were combined in a way that allowed the attackers to remain inside networks for months without being noticed.

### Purpose (Why the attack was launched)

The main **purpose** of the SolarWinds attack was **cyber espionage**. The attackers, who are believed to be a nation-state actor (linked to Russia’s APT29 or “Cozy Bear”), wanted to:

* **Spy on sensitive government communications**
* **Steal intellectual property from private companies**
* **Collect classified or confidential data**
* **Stay undetected for as long as possible**
* **Build long-term access** for future attacks or intelligence gathering

This attack was **not focused on financial theft** or destruction of data. Instead, it was a **silent operation** to gather intelligence across several sectors.

## **Damage to the CIA Triad**

### 1. ****Confidentiality****

* **What\_happened:**   
  The attackers gained unauthorized access to **emails, confidential communications, and internal documents** of many U.S. federal agencies and private companies.
* **How it affected confidentiality:**
  + Sensitive information such as internal communications, security policies, software source code, and privileged credentials was exposed.
  + The attackers had prolonged access to secret data as the breach remained undetected for months.
* **Real-world impact:**
  + Data exfiltration from agencies like the U.S. Treasury, Homeland Security, and tech companies (e.g., Microsoft).
  + Some stolen data may still be in the hands of foreign intelligence, posing long-term national security threats.

### 2. ****Integrity****

* **What\_happened:**  
  The attackers inserted a **malicious backdoor (Sunburst malware)** into legitimate software updates of the SolarWinds Orion platform.
* **How it affected integrity:**
  + It undermined the trust in software supply chains by **compromising the integrity of SolarWinds’ update mechanism**.
  + Once the update was installed, the malware allowed attackers to **inject malicious code** and commands into the victim’s environment.
* **Real-world impact:**
  + Organizations could no longer trust the integrity of their system logs, software updates, or even user credentials.
  + Potential for undetected manipulation of internal systems and data.

### 3. ****Availability****

* **What\_happened:**  
  The attack was **designed in a way to make it remain undetected**, so it did not directly cause outages or take systems offline.
* **How it affected availability:**
  + Although the attack itself didn’t make systems unavailable, **investigation and remediation efforts required temporary shutdowns** of affected systems.
  + Agencies and companies had to isolate or rebuild entire parts of their infrastructure, causing **delays and disruptions**.
* **Real-world impact:**
  + It indirectly affected the availability due to incident response measures and system audits that required the temporary shutdown of systems.

## **Conclusion**

The SolarWinds attack remains a powerful reminder of how even the most secure organizations can be threatened by advanced, sneaky cyber threats. By exploiting the trust placed in third-party software, the attackers successfully infiltrated high-value targets, including U.S. government agencies and leading corporations, through a compromised software update.

The attack caused **significant damage to the CIA triad**, with **confidentiality** being breached through stolen sensitive data, **integrity** being compromised via tampered software updates, and **availability** being indirectly affected during the long recovery process. Advanced Tactics, Techniques, and Procedures (TTPs), like supply chain compromise, credential dumping, and evasion methods, allowed the attackers to remain undetected for a long period of time.

This case highlights the importance of stronger **supply chain security**, **zero-trust models**, and **advanced threat detection**. It also reinforces how **nation-state actors** are capable of launching highly coordinated and damaging cyber-espionage campaigns against critical infrastructure across the globe.