MACRO PRAXIS | Research Institute

Turn Back Time (TBT) – Breach Analysis

SOLARWINDS ATTACK – US EAST COAST UTILITY BREACH

ANALYSIS AUTHOR: Bobby Boughton, MacroPraxis Research Institute Fellow
PUBLICATION DATE: March 1st, 2025

BREACH: SOLARWINDS SUPPLY CHAIN ATTACK – US EAST COAST ELECTRIC POWER PROVIDER – 2020

MITRE ATT&CK FRAMEWORK													
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
			Potential Deception Discovery										Actual Breach Discovery

Breach Information:	
Breach Date:	**2020 (attacker access from March 2020 – December 2020)**
Breach Name:	**SolarWinds Supply Chain Attack**
Target Name:	US East Coast Electric Power Provider (undisclosed to public for security reasons)
Attacker Name:	APT29 (Cozy Bear – Russian Intelligence)
Type of Attack:	Supply Chain Compromise & Advanced Persistent Threat (APT)
Attack Dwell Time:	Undetected for 10 months
Impact of Attack:	1. **Long-Term Cyber Espionage Risks:** o Attackers maintained persistent access for months, most likely collecting sensitive infrastructure data, grid security details, and internal operational blueprints. o Potential exposure of ICS/SCADA system configurations, have been determined by the company to increase their risk of future cyber threats. 2. **Regulatory & Compliance Fallout:** o The breach triggered NERC-CIP regulatory audits, leading to mandatory security enhancements and compliance-driven security upgrades. o The company is now subject to additional government oversight and increased cybersecurity mandates to try to prevent future incidents. 3. **Reputation & Customer Trust:** o Though they did not disclose the attack publicly, the company feels it now receives Increased scrutiny from "concerned" customers, regulators, and stakeholders, which has lead to erosion of trust and credibility in the utility's security posture.

		○ The company believes there remains some risk of legal action or fines if customers or investors determine that the breach was not properly disclosed. 4. **Incident Response & Security Overhaul Costs:** ○ According to the internal memo, the utility spent approximately **$450 million** on forensic investigations, cybersecurity upgrades, network segmentation, and security monitoring improvements. ○ System-wide patching and security revamps impacted internal IT operations, requiring enhanced security monitoring and long-term cyber resilience strategies.		
Total Impact:		The anonymous East Coast Electric Power Provider, in a confidential memo, calculated an estimated total financial impact of **$535 million** for the **two fiscal years following the attack due to the SolarWinds supply chain attack.** While no immediate operational disruptions occurred, the cyber espionage risks, compliance fallout, reputational damage, and extensive security overhaul costs contributed to significant financial consequences. This breach highlights the critical need for improved supply chain security, threat intelligence, and proactive cybersecurity measures to mitigate risks in critical infrastructure sectors.		
#	**Tactics for MITRE ATT&CK:**	**Attack Tactics Description:**	**Security FAILURE:**	**Deception TECH:**
1	Reconnaissance	• **Reconnaissance on SolarWinds:** Attackers identified SolarWinds as a high-value target due to its extensive client base, including government agencies and Fortune 500 companies. • **Supply Chain Compromise:** By infiltrating SolarWinds' development environment, the attackers inserted malicious code into the Orion software updates. This approach allowed them to potentially access any organization that installed these compromised updates. • **Post-Deployment Reconnaissance:** Once the compromised Orion software was deployed, the malware remained dormant for about two weeks. After this period, it initiated reconnaissance within the infected networks to identify security tools and ensure it could operate undetected.	Trusted Supply Chain. EDR / SIEM did not detect scans.	**Baits, Breadcrumbs & Decoys -** Deploying decoy systems and services could have diverted attackers away from real assets and triggered alerts upon interaction.
2	Resource Development	• **Establishing Command-and-Control (C2) Infrastructure:** The attackers set up a sophisticated C2 infrastructure to manage compromised systems. They registered multiple domains and configured servers to handle communications with the SUNBURST malware, ensuring stealth and resilience.	No direct failure - Occurred outside the Utility's environment.	

		• **Developing the SUNSPOT Malware:** To facilitate the injection of SUNBURST into the Orion software, the attackers created SUNSPOT, a custom malware designed to monitor SolarWinds' build environment and inject malicious code during the software compilation process.		
3	Initial Access	• **Compromising SolarWinds' Development Environment:** The attackers infiltrated SolarWinds' systems, potentially using methods such as exploiting zero-day vulnerabilities, conducting brute-force attacks, or employing social engineering tactics like targeted phishing. This access allowed them to insert malicious code into the SolarWinds Orion software updates. • **Embedding the SUNBURST Backdoor:** Within SolarWinds' compromised development environment, the attackers injected the SUNBURST backdoor into the Orion platform's legitimate software updates. This backdoor was designed to blend seamlessly with normal network traffic, making detection challenging. • **Distribution to SolarWinds Customers:** The tainted Orion updates, containing the SUNBURST malware, were digitally signed and distributed to approximately 18,000 SolarWinds customers between March and June 2020. Organizations that applied these updates inadvertently installed the backdoor, granting attackers potential access to their networks. • **Activation and Initial Network Access:** After installation, the SUNBURST malware remained dormant for about two weeks to evade immediate detection. Post dormancy, it initiated communication with attacker-controlled command-and-control (C2) servers, enabling the adversaries to perform reconnaissance and further exploit the compromised networks.	SolarWinds exposure to zero days. Utility's exposure to trusted supply chain digitally signed software updates.	
4	Execution	• **Delayed Initiation:** Upon installation, the SUNBURST malware remained dormant for approximately 12 to 14 days. This deliberate delay	EDR / SIEM – Not detected – Traffic blended with normal Orion operations.	**Baits –** Deceptive files and services that trigger alerts upon contact and profiling could have detected activities early.

		helped evade immediate detection by security systems. • **Environment Verification:** Before initiating malicious activities, SUNBURST performed checks to identify specific security processes and forensic tools on the host system. If any were detected, the malware would terminate its execution to avoid exposure. • **Command and Control (C2) Communication Setup:** After the dormancy period and environment checks, SUNBURST established communication with its C2 servers. It masqueraded this traffic as the Orion Improvement Program (OIP) protocol, blending with legitimate network activity. • **Execution of Malicious Commands:** Once communication was established, the malware could execute a range of commands, including file transfer, system reboot, and system profiling. These capabilities allowed attackers to control and navigate the compromised environment effectively.		
5	Persistence	• **Insertion of SUNBURST Backdoor:** Attackers embedded the SUNBURST malware into legitimate SolarWinds Orion software updates. When organizations installed these updates, the malware was introduced into their systems, establishing an initial foothold. • **Creation of Scheduled Tasks:** SUNBURST created scheduled tasks on infected systems to ensure its execution upon system startup or at specified intervals. This method allowed the malware to persist through reboots and remain active without manual intervention. • **Credential Theft and Lateral Movement:** After establishing persistence, the attackers employed credential theft techniques to harvest administrative credentials. This enabled them to move laterally within the network, accessing additional systems and maintaining persistence across multiple devices. • **Use of Legitimate Tools for Persistence:** The threat actors utilized legitimate administrative tools and protocols within the compromised environment	IAM / PAM / SIEM	**Honeytoken accounts** (decoy accounts) could have alerted security teams upon unauthorized use. **Baits –** Deceptive files and services that trigger alerts upon contact and profiling could have detected activities early.

		to blend in with normal operations. This tactic reduced the likelihood of detection and allowed them to maintain persistent access over extended periods.		
6	Privilege Escalation	• **Exploitation of Orion's Elevated Privileges:** The SolarWinds Orion platform operated with high-level privileges within enterprise environments. Attackers leveraged these inherent privileges to facilitate lateral movement and access sensitive systems without the need for additional privilege escalation tactics. • **Harvesting Credentials from Orion's Database:** Attackers extracted credentials stored within the Orion database, which often included those for critical assets like Active Directory, firewalls, and network management tools. Possessing these credentials enabled rapid escalation of privileges across the network. • **Utilization of SAML Token Forging:** By compromising the Security Assertion Markup Language (SAML) token-signing certificates, attackers could forge authentication tokens. This allowed them to impersonate legitimate users, including those with administrative privileges, granting them expansive access to both on-premises and cloud resources. • **Deployment of Additional Malware Tools:** In certain instances, the attackers introduced supplementary malware, such as the RAINDROP loader, to facilitate the deployment of tools capable of extracting credentials from Active Directory databases. This further solidified their elevated access within the compromised environment.	IAM / PAM	**Honeytoken accounts** (decoy accounts) could have alerted security teams upon unauthorized use. **Baits –** Deceptive files and services that trigger alerts upon contact and profiling could have detected activities early. **Decoys -** Decoy Active Directories could have altered on SAML compromise.
7	Defense Evasion	• **Code Signing with Valid Certificates:** The attackers ensured that the malicious SUNBURST malware was digitally signed using legitimate SolarWinds certificates. This tactic made the malware appear as authentic software, allowing it to bypass security mechanisms that trust signed code. • **Masquerading as Legitimate Network Traffic:** SUNBURST's communication with its command-and-control (C2) servers was designed to blend seamlessly with legitimate SolarWinds Orion	EDR / SIEM	

		Improvement Program (OIP) traffic. By mimicking standard network protocols and patterns, the malware's malicious activities remained concealed within normal operations. • **Obfuscation and Removal of Indicators:** The malware employed obfuscation techniques to hide its code and functionality, making analysis and detection more challenging. Additionally, the attackers removed indicators of their presence, such as logs and other forensic evidence, to erase traces of their activities. • **Time-Stomping to Alter File Metadata:** To further evade detection, the attackers modified the timestamps of their malicious files to match those of legitimate Windows files. This technique, known as time-stomping, made it difficult for security teams to identify unauthorized files based on their metadata. • **Avoidance of Sandboxes and Virtualized Environments:** SUNBURST included checks to detect if it was running in a sandbox or virtualized environment commonly used for malware analysis. If such environments were detected, the malware would alter its behavior or terminate execution to avoid scrutiny.		
8	Credential Access	• **Extraction of Credentials from Orion Database:** Attackers exploited the elevated privileges of the SolarWinds Orion platform to access its database, which contained credentials for various network devices and systems. By extracting these credentials, they gained access to critical infrastructure components. • **Replication of Directory Services via DCSync:** Utilizing privileged accounts, the adversaries performed DCSync attacks, allowing them to replicate directory services data, including password hashes, from domain controllers. This enabled them to impersonate users and escalate privileges within the network. • **Manipulation of Federated Authentication:** The attackers manipulated federated authentication environments by forging Security Assertion Markup Language (SAML) tokens. By compromising token-	IAM / PAM / EDR / SIEM	**Honeytoken accounts** (decoy accounts) could have alerted security teams upon unauthorized use. **Baits –** Deceptive files and services that trigger alerts upon contact and profiling could have detected activities early. **Decoys -** Decoy Active Directories could have altered on SAML compromise.

		signing certificates, they generated valid tokens to impersonate legitimate users, granting them unauthorized access to both on-premises and cloud resources. • **Abuse of API Permissions:** By leveraging compromised credentials, the threat actors abused application programming interfaces (APIs) to escalate privileges and maintain persistent access. This tactic facilitated the manipulation of cloud services and further exploitation of the victim's environment.		
9	Discovery	• **Network Enumeration:** Attackers conducted comprehensive scans to map out the network topology, identifying active hosts, open ports, and services running within the environment. This allowed them to pinpoint critical systems and potential pathways for lateral movement. • **Active Directory Reconnaissance:** Leveraging their access, the adversaries queried Active Directory to gather information about domain structures, organizational units, user accounts, group memberships, and trust relationships. This reconnaissance was crucial for planning privilege escalation and lateral movement strategies. • **Identification of Security Mechanisms:** The attackers sought out details regarding deployed security solutions, such as antivirus software, intrusion detection systems, and endpoint protection platforms. Understanding these defenses enabled them to tailor their tactics to avoid detection. • **Cloud Environment Exploration:** Recognizing the integration of on-premises networks with cloud services, the threat actors investigated configurations and permissions within platforms like Microsoft 365 and Azure Active Directory. This exploration aimed to identify opportunities for expanding their access into cloud resources.	EDR / SIEM	**Baits, Breadcrumbs & Decoys -** Deploying decoy systems and services could have diverted attackers away from real assets and triggered alerts upon interaction. (Programmable Automation Controllers), RTAC, Ethernet Gateways, Relays, fake power station engineering workstations).
10	Lateral Movement	• **Utilization of Compromised Credentials:** By harvesting credentials stored within the SolarWinds Orion platform, attackers obtained legitimate access	PAM / IDS / SIEM / Segmentation	**Honeytoken accounts** (decoy accounts) could have alerted security teams

		to various network segments. This allowed them to move laterally without raising immediate suspicion. • **Exploitation of Remote Administration Tools:** The adversaries leveraged existing remote administration protocols, such as Remote Desktop Protocol (RDP), to navigate the network. Utilizing these standard tools enabled them to blend their activities with normal administrative operations, thereby evading detection. • **Deployment of Post-Exploitation Frameworks:** Attackers deployed sophisticated frameworks like Cobalt Strike to facilitate lateral movement. These tools provided capabilities for reconnaissance, credential dumping, and execution of arbitrary code across the network. • **Abuse of Active Directory Trust Relationships:** By compromising privileged accounts, the threat actors exploited trust relationships within Active Directory environments. This enabled them to access additional domains and systems, effectively broadening their reach within the targeted infrastructure.		upon unauthorized use.
11	Collection	• **Identifying and Accessing Sensitive Data:** After establishing a foothold within the network, attackers conducted thorough reconnaissance to locate sensitive information, including emails, documents, and intellectual property. They utilized the elevated privileges obtained during earlier phases to access these data repositories. • **Utilizing Standard Protocols for Data Gathering:** To avoid detection, the adversaries employed legitimate protocols and tools native to the compromised environment. By mimicking normal user behavior and leveraging existing system functionalities, they reduced the likelihood of triggering security alerts. • **Encrypting Data Prior to Exfiltration:** Before transmitting collected data, attackers encrypted the information to prevent interception and analysis by security tools. This encryption ensured that even if	IAM / MDR / SIEM	**Baits, Breadcrumbs & Decoy Databases** and Fake High Value Utility infrastructure and power station engineering Data

		the data transfer were detected, the contents would remain inaccessible without the decryption key. • **Staging Data for Exfiltration:** The collected data was often moved to intermediate systems within the network, a process known as staging, to prepare for exfiltration. This tactic allowed attackers to consolidate information and schedule transfers during periods of low network activity to minimize the risk of detection.		
12	Command & Control	• **Delayed Activation:** After the compromised SolarWinds Orion software was installed, the embedded SUNBURST malware remained dormant for approximately 12 to 14 days. This delay helped evade immediate detection by security systems. • **Domain Generation Algorithm (DGA):** Post dormancy, SUNBURST utilized a Domain Generation Algorithm to create and attempt connections to subdomains of a primary command and control domain (e.g., `avsvmcloud[.]com`). This method allowed the malware to establish initial contact with the attackers' infrastructure. • **Masquerading as Legitimate Traffic:** The malware's network communications were designed to blend with legitimate SolarWinds traffic by mimicking the Orion Improvement Program (OIP) protocol. This tactic reduced the likelihood of detection by network monitoring tools. • **Command Execution and Data Exfiltration:** Upon successful connection to the C2 servers, the attackers could issue commands to the compromised systems, including executing arbitrary code, transferring files, and exfiltrating sensitive data. • **Use of Trusted Cloud Services:** The attackers hosted their C2 infrastructure on reputable cloud service providers, such as Amazon Web Services (AWS) and Microsoft Azure. Leveraging these trusted platforms helped the malicious traffic blend in with legitimate network activity, further evading detection.	IDS / MDR / SIEM	

13	Exfiltration	• **Targeting Critical Infrastructure Data:** Once inside the utility's network, the attackers identified and accessed sensitive operational data, including grid operations, power distribution models, SCADA (Supervisory Control and Data Acquisition) configurations, and compliance-related reports. This data provided valuable intelligence on the utility's infrastructure, potentially exposing vulnerabilities that could be exploited in future cyber or physical attacks. • **Use of Encrypted and Stealthy Channels:** The attackers exfiltrated data over encrypted channels to prevent interception by security monitoring tools. By masquerading data transfers as normal network traffic, they avoided triggering alerts from intrusion detection systems (IDS) or SIEM platforms. • **Exploiting Cloud and Remote Access Services:** To avoid detection, the attackers routed stolen data through trusted cloud services such as Microsoft Azure and Amazon Web Services (AWS). These cloud services were already used by the utility for remote access and operations, making it difficult for security teams to distinguish malicious exfiltration from legitimate data traffic. • **Timing Transfers to Avoid Detection:** Exfiltration was strategically executed during off-peak operational hours, ensuring minimal network activity that could otherwise raise suspicion. This method allowed large volumes of sensitive infrastructure data to be extracted over time without immediate discovery.	IDS / SIEM / IR	Fake High-Value **Baits and Decoy database servers** could have detected, slowed down, or altered MDR/ SIEM to attempt to stop the data theft.
14	Impact	• **Financial Losses:** The utility incurred substantial costs related to incident response, system remediation, and cybersecurity enhancements. On average, organizations affected by the SolarWinds attack faced financial impacts amounting to approximately 11% of their annual revenue. • **Operational Disruptions:** Although the attack primarily served espionage purposes, the utility faced operational challenges during the investigation and remediation processes. These activities necessitated temporary shutdowns of certain systems to ensure	**Detected when federal authorities alerted impacted organizations.**	**Decoys, Honeytoken Accounts, Baits & Breadcrumbs** - could have helped detect and contain the attack sooner.

		thorough cleansing and security, leading to potential service delivery delays. • **Regulatory and Compliance Challenges:** The breach prompted scrutiny from regulatory bodies, including the North American Electric Reliability Corporation (NERC). Approximately 25% of power utilities were exposed to the SolarWinds hack, highlighting growing vulnerabilities in industrial control systems. The utility had to demonstrate compliance with cybersecurity standards and implement additional measures to prevent future incidents. • **Strategic Reassessment of Cybersecurity Posture:** The attack served as a catalyst for the utility to reevaluate its cybersecurity strategies, emphasizing the importance of securing supply chains and third-party software integrations. This reassessment aimed to bolster defenses against sophisticated threats targeting critical infrastructure.		

Key Takeaways:

1. **The Utility Detected the Attack Too Late (Stage 14 – Impact).**
   - By the time the attack was identified, the attackers had already compromised critical infrastructure data, extracted sensitive grid operations details, and established long-term footholds within the network.
   - Detection only occurred after federal authorities issued alerts to impacted organizations, rather than through the utility's own cybersecurity defenses.
2. **Deception Technology Could Have Provided Early Detection (Stage 4 – Execution).**
   - If the utility had deployed deception technology, such as baits and decoy credentials, it could have detected malicious activity when the attackers first began executing commands via the SUNBURST malware.
   - Identifying the breach during Stage 4 rather than Stage 14 would have allowed security teams to attempt to halt the intrusion before the attackers gained extensive access to internal systems and sensitive data.
3. **Earlier Detection Could Have Mitigated the $535 Million Financial Impact.**
   - Had the breach been caught earlier, the utility could have avoided the extensive regulatory fines, security overhaul costs, and reputational damage.
   - Faster containment could have prevented attackers from accessing critical grid control data, reducing long-term espionage risks and minimizing the risk of future targeted attacks.
4. **Deception Technology Should Be a Core Component of Critical Infrastructure Security.**
   - Supply chain attacks like SolarWinds demonstrate the need for advanced detection capabilities beyond traditional identity & access control, endpoint security, SIEM monitoring, and network segmentation strategies.
   - Integrating deception tools, such as honeytoken accounts, decoy systems, and fake SCADA data, would have created an early-warning system to identify unauthorized access before real assets were compromised.

Disclaimer:

The **Turn Back Time (TBT) Analysis** is a hypothetical evaluation based on publicly available breach information and industry best practices. It illustrates how deception technology could have **improved early detection and response capabilities**. However, **no cybersecurity solution can guarantee complete prevention of cyber threats**.

Deception technology is **one component of a multi-layered security strategy**, and its effectiveness depends on **deployment scope, integration with existing security tools, and evolving attack techniques**. This analysis is **for informational purposes only** and should not be interpreted as a **guarantee of breach prevention**.

The MACROPRAXIS Research Institute is **not liable for any cybersecurity incidents, financial losses, or damages** resulting from the use or implementation of deception technology. Customers are advised to conduct **independent security assessments** and integrate deception tools as part of a **comprehensive cybersecurity strategy**.