Benchmark – Cyber Operations Case Studies

Ryan Coon

CYB-610

Professor Ian Standefer

May 7, 2025

Introduction:

The SolarWinds supply chain attack, which took place between 2019 and 2020, is recognized as one of the most significant cyberattacks in recent history. This sophisticated operation involved the insertion of malicious code into updates of the SolarWinds Orion software, a widely used network management tool. The attackers, believed to be affiliated with the Russian foreign intelligence service (SVR), compromised the software updates, which were then installed by over 18,000 SolarWinds customers, including numerous U.S. government agencies and major corporations(Fortinet, n.d.). Once inside the networks, the attackers established persistent access, allowing them to conduct extensive surveillance and exfiltrate sensitive data. The attack highlighted critical vulnerabilities in supply chain security and prompted a reevaluation of cybersecurity practices across both public and private sectors.

Potential Motivations:

The potential motivations behind this attack likely involved espionage, intellectual property theft, and the establishment of persistent access for future operations. The attackers, widely believed to be affiliated with the Russian government, likely sought to compromise sensitive information from various US government agencies and private sector organizations including Microsoft, Cisco, Intel, Deloitte, and even some parts of the Pentagon (Team, 2022). This attack highlights the devastating consequences of supply chain vulnerabilities.

Phases of the Cyber Operation:

The attack unfolded in phases, beginning with the compromise of SolarWinds' Orion software update mechanism. This is the initial access phase, where malicious code was introduced into legitimate software updates. The attackers leveraged this to deploy the SUNBURST backdoor to numerous SolarWinds customers. This represents the persistence phase; the attackers established a foothold within numerous networks, with the use of custom malware and legitimate system tools allowing for long-term access and surveillance(Aqua, 2023). This was followed by the exploitation phase, where attackers accessed compromised systems and exfiltrated sensitive data. The data exfiltration phase involved stealing specific information based on the attackers' goals. Finally, the attackers likely maintained persistent access for extended periods, indicating a long-term campaign of intelligence gathering and potentially disruptive activities(Williams, 2020). Network traffic analysis during this attack revealed an unusually high volume of communication from compromised systems to command-and-control servers, a clear indicator of malicious activity. This traffic was often encrypted and obfuscated, making detection and analysis difficult.

Penetration Testing and Network Security:

The targeted organizations could have used penetration testing to identify the flaws within their systems. By simulating attacks, they could have discovered vulnerabilities in their update mechanisms and network configurations. This proactive approach would have allowed for the implementation of security controls, reducing the likelihood of a successful attack. A penetration test could have helped secure the network by identifying and remediating vulnerabilities before attackers could exploit them. This would have included identifying weaknesses in the software update process and implementing stronger access controls to prevent unauthorized access to systems.

Penetration Testing and the CIA Triad:

A penetration test supports the CIA triad (Confidentiality, Integrity, Availability) by proactively identifying vulnerabilities that could compromise these principles. By finding weaknesses in access controls, the test helps ensure confidentiality, preventing unauthorized access to sensitive data. It also identifies vulnerabilities that could lead to data modification or deletion, thus supporting data integrity(Imperva, 2019). Finally, by identifying potential points of failure, a penetration test helps ensure the availability of systems and data, minimizing downtime in the event of an attack.

US Laws Governing Cyber Operations:

Several laws provide US entities with authority to perform cyber operations. The Computer Fraud and Abuse Act (CFAA) criminalizes unauthorized access to computer systems and data, while the National Defense Authorization Act (NDAA) grants the Department of Defense certain authorities for cyber operations in defense of national security(ICLG, 2024). These laws define acceptable boundaries for cyber activities, aiming to balance national security interests with individual rights and international law.

Legal Authority to "Hack Back":

US law does not generally grant organizations the legal authority to "hack back" in response to cyberattacks. Retaliatory actions can lead to legal repercussions, including criminal charges under the CFAA(US Department of Justice, 2015). Organizations should focus on defensive measures, incident response, and law enforcement cooperation to address cyber threats.

Business Strategies for Network Sustainability, Availability, and Reliability:

To ensure the sustainability, availability, and reliability of a network, organizations should implement a multi-layered security strategy. This includes robust access controls, regular security assessments, incident response planning, and employee security awareness training. These strategies are relevant to all stakeholders, from executives to IT staff and end-users, as everyone plays a role in maintaining the security of the network. Regular communication and collaboration among stakeholders are essential to ensure that security strategies are effectively implemented and maintained. Stakeholders need to understand their roles and responsibilities in maintaining the organization’s security posture.

Qualitative and Quantitative Analytic Methodologies:

To effectively apply qualitative and quantitative analytic methodologies for predicting trends and communicating security strategies that align with business objectives, a comprehensive approach is essential. Qualitative analysis involves gathering insights through expert judgment, interviews, and focus groups, which helps identify potential risks and challenges based on experience and contextual understanding. This method is particularly useful for understanding the nuances of security threats and organizational culture, allowing businesses to prioritize risks and allocate resources effectively (Geveye, 2023). On the other hand, quantitative analysis employs statistical methods and data modeling to analyze numerical data, enabling organizations to identify patterns and trends over time. By leveraging historical data, businesses can forecast future security incidents and measure the effectiveness of existing strategies (Couchbase, 2024).

Combining these methodologies enhances the overall strategic planning process. For instance, while qualitative insights can inform the context behind data trends, quantitative metrics provide the hard evidence needed to support decision-making. This dual approach not only improves process efficiency but also ensures that security strategies are data-driven and aligned with business objectives (Evrin, 2021).

Penetration Testing and the CIA Triad:

Penetration testing tools, technologies, and concepts can significantly support the CIA triad. Tools like vulnerability scanners, network mappers, and exploitation frameworks can be used to identify vulnerabilities and assess the impact of potential attacks. The concepts of risk assessment, security controls, and incident response planning are crucial for ensuring confidentiality, integrity, and availability. By proactively identifying and mitigating vulnerabilities, organizations can significantly reduce the risk of data breaches, data modification, and service disruptions. The results of penetration tests should be used to inform and improve security controls, thereby ensuring the long-term security and resilience of the organization's systems.

References:

Aqua. (2023, February 12). *SolarWinds Attack: Play by Play and Lessons Learned - Aqua*. Aqua. https://www.aquasec.com/cloud-native-academy/supply-chain-security/solarwinds-attack/

Couchbase. (2024, February 14). *Data Analysis Methods: Qualitative vs. Quantitative*. The Couchbase Blog. https://www.couchbase.com/blog/data-analysis-methods/

Evrin, V. (2021, April 28). *Risk Assessment and Analysis Methods: Qualitative and Quantitative*. ISACA; ISACA. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods

Fortinet. (n.d.). *SolarWinds Supply Chain Attack*. Fortinet. https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack

Geveye, M. O. (2023, March 20). *Qualitative and Quantitative Risk Analysis*. Centraleyes. https://www.centraleyes.com/qualitative-and-quantitative-risk-analysis/

ICLG. (2024). Cybersecurity Laws and Regulations USA . *Gambling 2019 | Laws and Regulations | Singapore | ICLG*, *1*(1). https://iclg.com/practice-areas/gambling-laws-and-regulations/singapore

Imperva. (2019). *What is Penetration Testing | Step-By-Step Process & Methods | Imperva*. Imperva. https://www.imperva.com/learn/application-security/penetration-testing/

Team, R. (2022, August 2). *SolarWinds supply chain attack risks and prevention*. Reflectiz. https://www.reflectiz.com/blog/solarwinds-supply-chain-attack/

U.S. Department of Justice. (2015, February 19). *Computer Fraud and Abuse Act*. U.S. Department of Justice. https://www.justice.gov/jm/jm-9-48000-computer-fraud

Williams, J. (2020, December 15). *What You Need To Know About the SolarWinds Supply-Chain Attack | SANS Institute*. Www.sans.org. https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/