SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering

K. J. Somaiya College of Engineering, Mumbai - 400 077
(A Constituent College of Somaiya Vidyavihar University)
Dept. of INFORMATION TECHNOLOGY
T.Y. B. Tech. Semester - V (2024 - 25)
INS IA - I

Somaiya TRUST

The SolarWinds Cyberattack

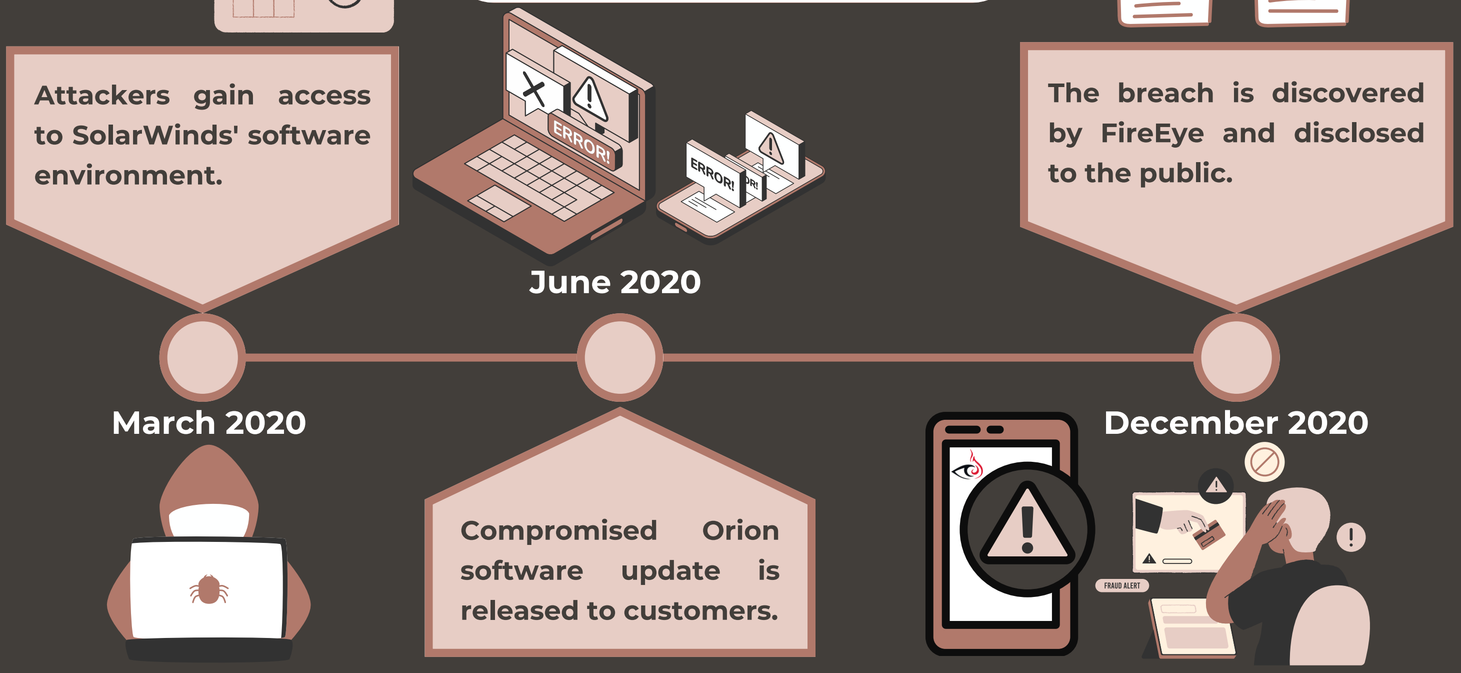
A Case Study on Supply Chain Vulnerabilities in Network Security

Poster Prepared By :
16010422233 - Prachi Gandhi
16010422234 - Chandana Galgali
16010422235 - Mahek Thakkar

Introduction

In December 2020, one of the most sophisticated cyberattacks in history was discovered. This attack, known as the SolarWinds cyberattack, revealed critical vulnerabilities in global supply chains, as attackers compromised trusted third-party vendors to infiltrate government agencies and corporations worldwide. This case study focuses on understanding how such supply chain attacks happen and what lessons can be learned to strengthen cybersecurity.

Incident Timeline



Attackers gain access to SolarWinds' software environment.

March 2020

June 2020

Compromised Orion software update is released to customers.

The breach is discovered by FireEye and disclosed to the public.

December 2020

Security Vulnerabilities and Solutions

Security Area	Key Vulnerabilities	Proposed Solutions and Recommendations
Cryptography	Weak certificate handling allowed attackers to sign malicious updates.	• HMAC for integrity checking. • Certificate transparency logs to detect fraud. • Key rotation to avoid long-term abuse.
Access Control	Weak RBAC policies enabled lateral movement.	• Stricter RBAC to limit user access. • Enforce MFA for high-privilege accounts. • Regular audits of access permissions.
Network Security	Exploited TCP/IP vulnerabilities (IP spoofing, session hijacking).	• Implement Zero Trust Architecture. • Use IDS to detect suspicious behavior. • Network segmentation to limit movement.
Web and API Security	Insecure API endpoints exposed systems.	• Conduct regular security audits. • Follow secure coding practices.
General Security	Lack of proactive detection and response.	• Use SIEM systems for centralized monitoring. • Deploy behavioral analytics. • Encrypt sensitive data with AES-256.

Background of the Incident

In March 2020, attackers infiltrated the software development environment of SolarWinds, a leading IT management company. They inserted malicious code into a routine software update of SolarWinds' Orion platform. This update, distributed to over 18,000 customers, included government agencies, critical infrastructure, and private sector companies. For nearly nine months, the attackers had undetected access to sensitive systems, allowing them to spy on and potentially steal classified information from U.S. federal agencies and Fortune 500 companies.

Impact of the Attack

Category	Impact
Affected Customers	• Over 18,000 organizations installed the compromised software • Included U.S. federal agencies and Fortune 500 companies
Government Breach	• At least 9 U.S. federal agencies were breached • Agencies affected: DHS, Treasury, Commerce
Private Sector	• Companies like Microsoft and FireEye were targeted • Microsoft's source code was viewed by attackers
Data Exfiltration	• Exposure of sensitive government communications • Intellectual property from private companies was stolen
Financial Impact	• SolarWinds incurred $18 million in remediation costs (Q1 2021) • Industry-wide damages estimated in the billions
Undetected Duration	• Attackers had undetected access for approximately 9 months

References

1. FireEye, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor," FireEye Threat Research, Dec. 2020.
2. Microsoft, "Solorigate: Analyzing the Compromised DLL File That Started a Sophisticated Cyberattack," Microsoft Security Blog, Feb. 2021.
3. A. Karami, R. Hill, and M. Freemantle, "Analyzing the SolarWinds Hack: An Investigation of Supply Chain Security Vulnerabilities," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4895–4907, Nov. 2021. doi: 10.1109/TIFS.2021.3114599.
4. Danish Center for Cyber Security (CFCS), "CFCS SolarWinds Report," CFCS, 2021.
5. OWASP Foundation, "OWASP Top Ten Web Application Security Risks," OWASP, 2020.

Conclusion

The SolarWinds cyberattack revealed significant vulnerabilities in the global supply chain, impacting government agencies and private corporations alike. To prevent future supply chain attacks, organizations must implement stronger cryptographic practices, enforce strict access control policies, and adopt advanced network security protocols. These measures can help reduce the risk of similar cyber incidents.