Cybersecurity Case Studies Report

Case #1: SolarWinds Hack (2020)

What is the name of the cyber incident?
SolarWinds Hack (2020 supply chain attack).

Who was the target or victim?
SolarWinds, U.S. government agencies, and major corporations.

How did the attackers first gain access?
By compromising the SolarWinds software build system and injecting malicious code into Orion updates.

What did the attackers do after gaining access?
They installed a backdoor (SUNBURST), established persistence, and selectively targeted high-value systems.

Post-connection activities:
Privilege escalation, lateral movement, credential theft, data exfiltration, and defense evasion.

Why was the attack dangerous?
It spread through trusted updates and enabled widespread espionage.

Why was it difficult to detect or stop?
It appeared as legitimate traffic and used stealth techniques.

What was the impact?
Sensitive data breaches, national security risks, and long-term compromise.

What security measures could help?
Zero Trust architecture, monitoring, and secure software supply chain practices.

Most important lesson:
Do not blindly trust software updates.

Most damaging post-connection action:
Lateral movement and credential theft enabled deep system access.

Case #2: Target Data Breach (2013)

What is the name of the cyber incident?
Target Data Breach (2013).

Who was the target or victim?
Target Corporation and millions of customers.

How did the attackers first gain access?
Through stolen credentials from a third-party HVAC vendor.

What did the attackers do after gaining access?
They explored the network, accessed POS systems, and installed malware.

Post-connection activities:
Lateral movement, privilege escalation, malware installation, data collection, and exfiltration.

Why was the attack dangerous?
It led to massive financial data theft.

Why was it difficult to detect or stop?
Attackers used valid credentials and alerts were ignored.

What was the impact?
Millions of stolen credit cards, financial losses, and reputational damage.

What security measures could help?
Network segmentation, MFA, and better alert response.

Most important lesson:
Third-party access is a major security risk.

Most damaging post-connection action:
POS malware installation and data exfiltration.