Devoir III – CEG 4399

CEG 4399 - Design of Secure Computer Sys.

Université d'Ottawa

Professeur : Amir H. Razavi

Noms et numéros des étudiants :
Gbegbe Decaho Jacques 300094197

Date de soumission: 28 November 2024

Assignment 3

Introduction

UNIVERSITY OF Ottawa

Faculty of Engineering and Computer Science

CSI 4139 - CEG 4399 - SEC 5100 – Fall 2024

Assignment 3

Part 1 - Research

Question 1 (30%)

Research an attack on any system that has occurred in the last 5 years that relates to mobile security or operating system security being compromised. Write a 1-2 page report on this attack that includes the following information:

- Description of the affected systems
- Description of the attack itself
- Description of the results of this attack (Was it successful? Who was harmed, and in what way?)
- Description of the attackers, if known. (Who are they?)
- Description of mechanisms that would have prevented this attack, or other mitigation strategies that could have been used.

Attack : SolarWinds Supply Chain Attack (2020)

1. Description of the affected systems :

   The SolarWinds attack targeted the widely used IT management software, SolarWinds Orion, compromising its update mechanism to infiltrate major organizations and government agencies. Victims included U.S. federal agencies such as the Treasury and Homeland Security, private companies like Microsoft, and critical infrastructure operators. This supply chain attack created a backdoor in affected systems, allowing attackers to steal data and compromise networks globally.

2. Description of the attack itself

   The SolarWinds attack was a sophisticated supply chain attack targeting the Orion software's update mechanism. Hackers, believed to be the Russian state-sponsored group Cozy Bear (APT29), injected malicious code called SUNBURST into a legitimate software update. Once installed, the update created a backdoor, allowing attackers to steal credentials, escalate privileges, move laterally across networks, and exfiltrate sensitive data. This breach went undetected for months,

affecting thousands of organizations worldwide, including government agencies and major corporations.

3. Description of the results of this attack (Was it successful? Who was harmed, and in what way?)

The SolarWinds attack was highly successful, remaining undetected for months and compromising thousands of systems globally. Sensitive data from U.S. federal agencies and Fortune 500 companies was exfiltrated, causing widespread security breaches. The financial impact was substantial, with damages estimated to exceed $100 million. Additionally, the attack resulted in long-term reputational harm for SolarWinds, highlighting the severe risks of supply chain vulnerabilities.

4. Description of the attackers, if known. (Who are they?)

The SolarWinds attack is attributed to **Cozy Bear**, a hacking group linked to Russia's Foreign Intelligence Service (SVR). Known for its advanced cyber-espionage capabilities, Cozy Bear has a history of targeting high-profile organizations and government entities. In this attack, they leveraged a supply chain vulnerability to infiltrate thousands of systems worldwide, exfiltrating sensitive data while remaining undetected for months. Their actions highlight the sophistication of state-sponsored cyber-espionage campaigns.

5. Description of mechanisms that would have prevented this attack, or other mitigation strategies that could have been used.

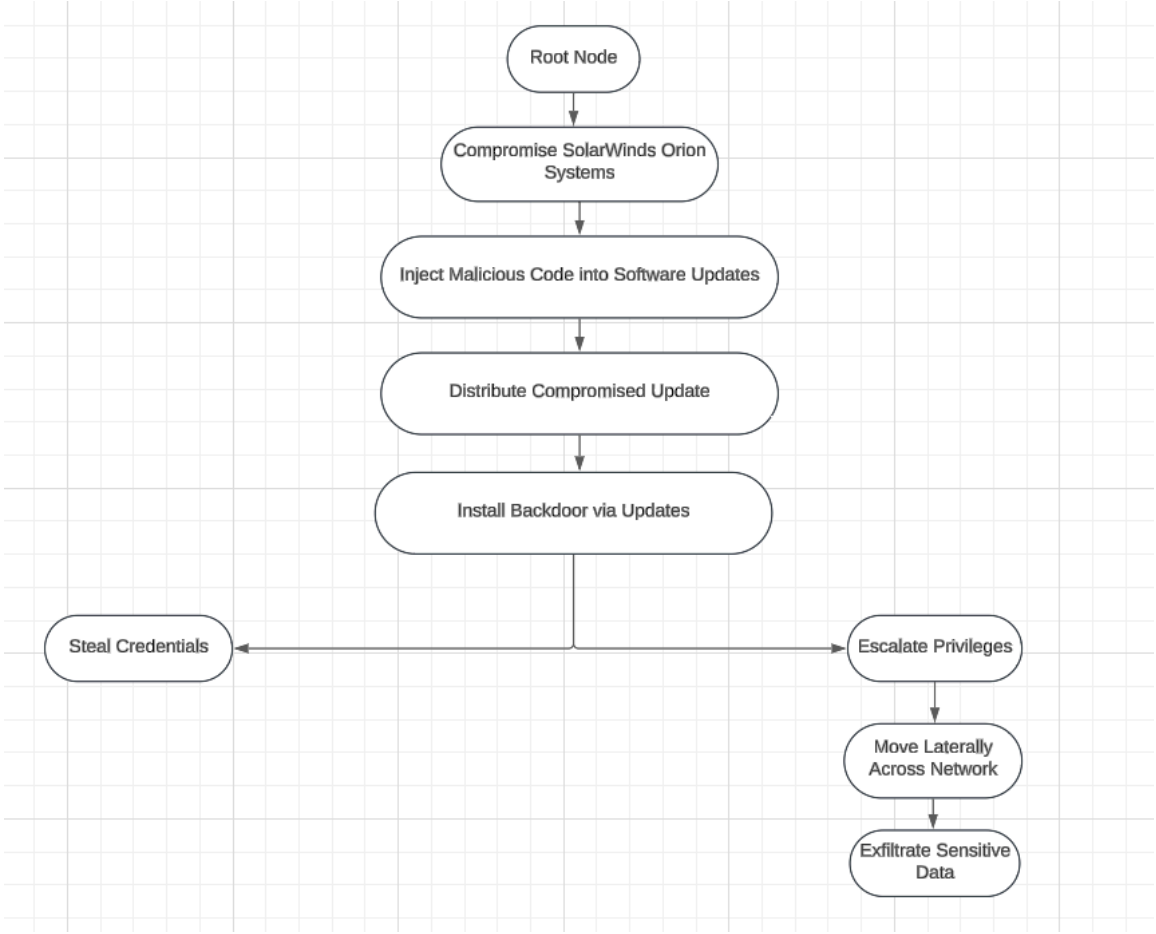
SolarWinds could have mitigated the attack by implementing strict code auditing processes and enhanced digital code signing to ensure the integrity of software updates. Adopting a Zero Trust Architecture would enforce rigorous identity verification, assuming all systems and users are potentially compromised. Network segmentation could isolate critical systems, limiting lateral movement by attackers. Additionally, sharing threat intelligence among organizations would improve early detection and prevention of supply chain attacks.

Question 2 (20%)

Create a visualization of the attack that was researched in question 1. Imagine you are an IT professional that was working at an affected company during this attack, and you are preparing a visualization as part of a presentation to your team that will brief them on the security incident. One visualization is sufficient for this question. Some examples of visualizations are listed, but if another type of visual is better suited to your attack, you can use that type.

- Network diagrams
- Attack tree diagrams (illustrating a hierarchy of attack goals, such as what was compromised first to achieve later goals)
- Timeline diagram
- Pseudocode
- Data exfiltration diagrams (show which computers data flowed through to reach the external internet)

Attack Tree Diagram : SolarWinds Supply Chain Attack



Part 2 - Knowledge

Question 3 (10%)

List and explain two common vulnerabilities found in UNIX systems and two in Windows systems. How can they be mitigated?

Two Common Vulnerabilities in UNIX Systems:

- **Default File Permissions :** UNIX systems often have overly permissive default file permissions, allowing unintended users to access sensitive files or directories. This can result in unauthorized modifications or data exposure. To mitigate this, strict file permission policies should be enforced, applying the principle of least privilege, and leveraging tools like SELinux or AppArmor to enhance access control.

- **Shell Injection Attacks :** Shell injection occurs when poorly sanitized inputs in scripts or applications allow attackers to execute malicious commands in the shell. This can lead to unauthorized access or execution of harmful code. Mitigation involves validating and sanitizing all user inputs, avoiding direct execution of user-provided commands, and using safer alternatives such as parameterized queries.

Two Common Vulnerabilities in Windows Systems:

- **Weak Password Policies :** Windows systems are vulnerable to brute force or dictionary attacks due to weak or guessable user passwords. This can lead to unauthorized access to systems and data breaches. To mitigate this risk, organizations should enforce strong password policies that require complex, lengthy, and regularly updated passwords, along with multi-factor authentication (MFA) for added security.

- **DLL Injection :** DLL injection involves the insertion of malicious code into legitimate processes via compromised Dynamic Link Libraries (DLLs). This can grant attackers control over the affected processes and allow them to escalate privileges. Mitigation strategies include using application whitelisting, implementing code signing to verify legitimate DLLs, and deploying tools like Windows Defender Application Control to block unauthorized DLL loading.

Question 4 (10%)

Explain what "geo-tagging" is and discuss one potential security risk associated with this feature on mobile devices.

Geo-tagging allows location metadata, such as GPS coordinates, to be embedded in photos, videos, or social media posts.
A potential risk could be that sharing a geotagged photo while on vacation could reveal that you are away from home, which could lead to a burglary.
To avoid this scenario, users should turn off geotagging in their mobile device settings, use privacy-focused apps to remove location data before sharing, and avoid posting real-time location updates on social media platforms.

Question 5 (10%)

Define "containment" in the context of incident response. Provide examples of two containment strategies.

Containment in incident response involves measures to limit the spread and impact of a security incident while preserving evidence for investigation.
Examples include :

- Network segmentation, which isolates infected systems to prevent the spread of malware (like taking a compromised server offline during a ransomware attack)
- Account suspension, which temporarily disables compromised user accounts to prevent unauthorized access (like locking an account after suspicious login activity is detected).

Question 6 (10%)

List and describe three common indicators of compromise (IOCs) that may signal a security incident.

Common indicators of compromise (IOCs) include:

- Unusual network activity: such as sudden spikes in outbound traffic or communication with suspicious IP addresses.
- Unauthorized access logs, such as login attempts from unknown locations or at unusual times.

- The presence of malware or suspicious files, such as unknown executables in critical directories

Question 7 (10%)

Explain the importance of post-incident activity. What are two activities conducted during this phase to improve future incident response efforts?

Post-incident activities are essential for identifying the attack's cause, addressing vulnerabilities, and strengthening future responses.
Key actions include :

- Root cause analysis : which identifies exploited vulnerabilities and preventive measures.
- Updating security policies and procedures, such as revising response plans, implementing stricter access controls, and mandating employee training based on lessons learned.