Vidyavardhini's College of Engineering & Technology

Department of Computer Engineering

Academic Year : 2023-24

Experiment No. 10: Case Study on Session Hijacking and Trojan Horses.

Introduction:

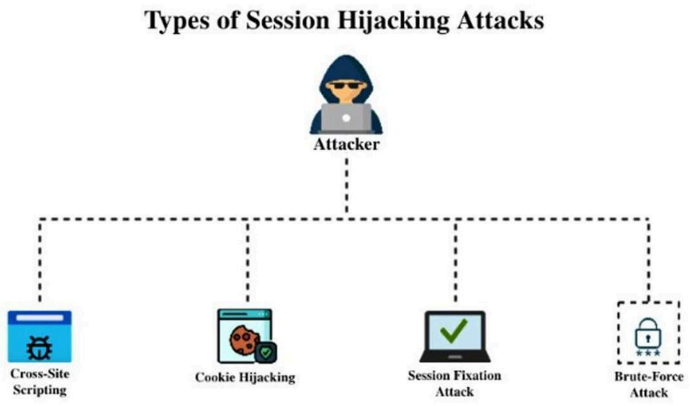
Session hijacking and Trojan horses are two prevalent cyber threats that can severely compromise the security of computer systems and networks. In this case study, we will explore a hypothetical scenario involving these two threats and examine their impact on an organization.

Background:

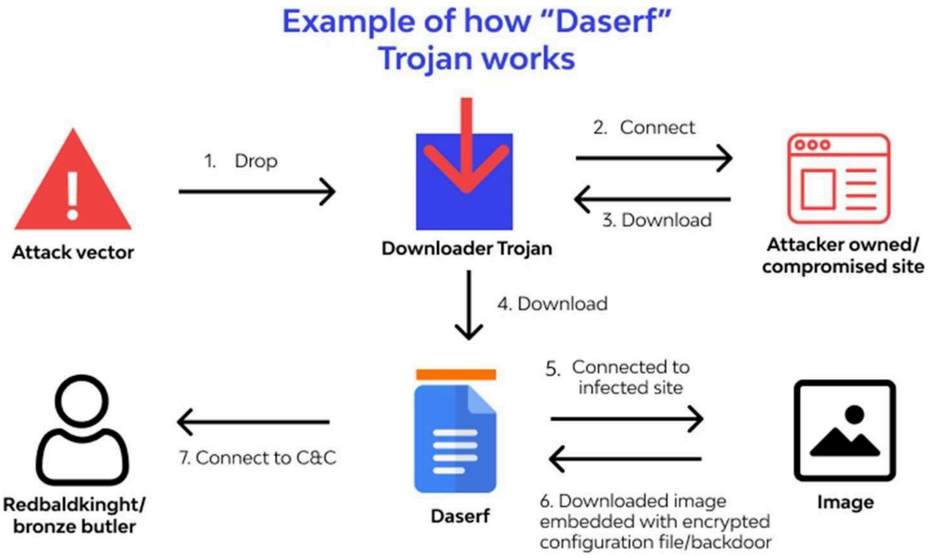
Scenario: XYZ Corporation is a large multinational company with operations spanning across various countries. The company relies heavily on its internal network for communication, data storage, and day-to-day operations. Recently, the IT department at XYZ Corporation noticed some unusual activity on their network.

Incident Description:

1. Session Hijacking: One afternoon, employees at XYZ Corporation began reporting strange behavior with their accounts. Some employees found themselves logged out of their accounts unexpectedly, while others noticed unauthorized access to their emails and sensitive documents. Upon investigation, the IT team discovered evidence of session hijacking. Attackers had intercepted and taken control of active sessions, allowing them to masquerade as legitimate users and access sensitive information.



2. Trojan Horse: Simultaneously, several employees received an email seemingly from a trusted source within the organization. The email contained an attachment labeled as an important document regarding upcoming company policies. Unsuspecting employees downloaded and opened the attachment, unknowingly installing a Trojan horse onto their computers. The Trojan horse silently installed itself and established a backdoor connection to the attacker's command- and-control server, allowing the attackers to remotely access and control the infected machines.


Example of how "Daserf" Trojan works
Attack vector
1. Drop
Downloader Trojan
2. Connect
3. Download
Attacker owned/ compromised site
4. Download
Redbaldkinght/ bronze butler
7. Connect to C&C
Daserf
5. Connected to infected site
6. Downloaded image embedded with encrypted configuration file/backdoor
Image

Investigation and Response:

Upon detecting the security breaches, XYZ Corporation's IT security team immediately launched an investigation to contain the damage and mitigate further risks. They analyzed network logs, endpoint security logs, and conducted forensic examinations of affected systems to identify the extent of the compromise.

1. Session Hijacking Mitigation: To mitigate the impact of session hijacking, the IT team implemented stricter session management policies, including the use of session tokens, encryption, and multi-factor authentication. They also conducted employee training sessions to raise awareness about the risks of session hijacking and the importance of safeguarding account credentials.

2. Trojan Horse Removal: To address the Trojan horse infection, the IT team deployed updated antivirus software across all endpoints and initiated a company-wide malware scan to detect and remove any traces of the Trojan horse. Additionally, they disabled any suspicious network connections and patched known vulnerabilities to prevent future infections.

Preventive Measures:

1. Regular Security Awareness Training: Employees play a crucial role in maintaining cybersecurity. Regular training sessions should educate employees about the latest threats, phishing techniques, and best practices for securing their accounts and devices.

2. Multi-layered Defense Mechanisms: Implementing a multi-layered approach to cybersecurity, including firewalls, intrusion detection systems, antivirus software, and encryption, can help organizations better defend against sophisticated cyber-attacks like session hijacking and Trojan horses.

3. Continuous Monitoring and Incident Response: Proactive monitoring of network activities and prompt incident response are essential for detecting and mitigating security breaches before they escalate

into major incidents.

Conclusion: Session hijacking and Trojan horses pose significant threats to organizations' cybersecurity posture. By implementing robust security measures, conducting regular employee training, and maintaining vigilant monitoring and incident response capabilities, organizations can effectively defend against these threats and safeguard their sensitive information and assets.