APPLICATION SECURITY CASE STUDY REPORT

CASE STUDY OF 5 MALWARE ATTACKS(2016-PRESENT)

Swanand Garge

202201589

WHAT IS A MALWARE ATTACK?

Malware attacks involve malicious software designed to harm computer systems, networks, or devices. They come in various forms such as viruses, worms, Trojans, ransomware, and spyware. Malware spreads through email attachments, infected websites, or software downloads. Once installed, it can steal data, encrypt files, disrupt operations, or control devices remotely. Effective cybersecurity measures like antivirus software, firewalls, and user education are crucial for prevention.

INDEX

SAMSAM RANSOMWARE ATTACK (2018)

When happened: The SamSam ransomware attack occurred primarily in 2018.

Where happened: Although the attack primarily targeted organizations in the United States, its impact extended globally, affecting entities in Europe, the Middle East, and beyond.

What happened: The SamSam ransomware attack stood out for its highly targeted approach, focusing on specific organizations rather than spreading indiscriminately. Attackers gained access to networks through various means, including exploiting vulnerabilities in remote desktop protocols (RDP) or using stolen credentials obtained through phishing or other means. Once inside the network, they manually deployed the SamSam ransomware, encrypting files on infected systems and demanding ransom payments, typically in Bitcoin, for decryption keys.

How it happened: The attackers often conducted extensive reconnaissance on target networks, identifying vulnerable systems and high-value targets before launching the attack. This meticulous approach allowed them to maximize the impact of the ransomware. Exploiting vulnerabilities in remote desktop protocols (RDP) or using stolen credentials obtained through phishing attacks provided the initial access to networks. Once inside, the attackers manually deployed the ransomware, utilizing robust encryption algorithms that made decryption without the proper keys virtually impossible.

What was done to control that malware: To control the spread of SamSam ransomware, organizations implemented robust cybersecurity measures such as strengthening access controls, applying security patches promptly to mitigate vulnerabilities, enhancing employee awareness through cybersecurity training, and deploying advanced endpoint security solutions capable of detecting and blocking ransomware activity.

TRICKBOT BANKING TROJAN (2016-PRESENT)

When happened: TrickBot infections have been ongoing since 2016.

Where happened: TrickBot has been reported worldwide, with significant impacts observed in the United States, Europe, Australia, Asia, and India.

What happened: TrickBot is a sophisticated banking Trojan that primarily spreads through phishing emails containing malicious attachments or links. Once a user interacts with the malicious payload, TrickBot establishes persistence on the infected system, communicates with command-and-control servers operated by threat actors, and downloads additional payloads, including ransomware like Ryuk. The Trojan targets financial institutions and their customers, stealing sensitive information such as login credentials and banking details for financial gain.

How it happened: The primary propagation method of TrickBot is through phishing emails, which trick users into downloading and executing malicious attachments or clicking on links to fake websites impersonating legitimate entities. Once executed, TrickBot establishes a foothold on the infected system, enabling threat actors to conduct further malicious activities, such as stealing banking information or deploying additional malware payloads.

What was done to control that malware: To control TrickBot infections, organizations implemented multi-layered cybersecurity defenses, including email filtering and anti-phishing solutions to block malicious emails containing TrickBot payloads, regular security updates to mitigate vulnerabilities exploited by the Trojan, network segmentation to limit the spread of infections, and employee training to recognize and report phishing attempts.

GANDCRAB RANSOMWARE CAMPAIGN (2018-2019)

When happened: The GandCrab ransomware campaign was active from 2018 to 2019.

Where happened: The campaign impacted organizations globally, with victims reported across North America, Europe, Asia, the Middle East, and India.

What happened: GandCrab was a prolific ransomware-as-a-service (RaaS) operation responsible for infecting thousands of victims worldwide. It utilized various distribution methods, including exploit kits, phishing emails, and compromised websites, to infect systems and encrypt files for ransom. The ransomware demanded payments in cryptocurrencies, typically Bitcoin, to unlock encrypted files, often providing customer support to facilitate payments and decryption.

How it happened: GandCrab ransomware was distributed through various means, including exploit kits that targeted vulnerabilities in software or operating systems, phishing emails containing malicious attachments or links to compromised websites hosting exploit payloads. Once executed, GandCrab encrypted files on infected systems, displaying ransom notes demanding payments in cryptocurrency for decryption keys.

What was done to control that malware: To control the spread of GandCrab ransomware, law enforcement agencies collaborated with cybersecurity firms to disrupt the infrastructure used by the ransomware operators, leading to the takedown of command-and-control servers and decryption tools to assist victims. Additionally, organizations strengthened their cybersecurity defenses by implementing web filtering and intrusion prevention systems, regularly backing up critical data, deploying endpoint security solutions capable of detecting and blocking ransomware activity, and educating users about the dangers of downloading attachments or clicking on links from unknown sources.

LAZARUS GROUP'S WANNACRY 2.0 (2018)

When happened: WannaCry 2.0, attributed to the Lazarus Group, targeted organizations globally in 2018.

Where happened: The attack had significant impacts in Europe, Asia, North America, and India.

What happened: WannaCry 2.0 exploited the EternalBlue vulnerability in Microsoft's Server Message Block (SMB) protocol to propagate ransomware, encrypting files on infected systems and demanding Bitcoin payments for decryption. The attack targeted critical infrastructure sectors, including healthcare and government, causing widespread disruption and financial losses.

How it happened: The attack propagated through unpatched systems vulnerable to the EternalBlue exploit, allowing it to spread rapidly across networks. Once inside the network, WannaCry encrypted files and displayed ransom notes demanding payments in Bitcoin for decryption keys.

What was done to control that malware: To control the spread of WannaCry 2.0, organizations implemented security patches promptly to mitigate vulnerabilities exploited by the ransomware, disabled outdated and unnecessary protocols and services, such as SMBv1, to reduce the attack surface, implemented network segmentation to contain the spread of infections, monitored network traffic for signs of EternalBlue exploitation, and developed incident response plans to mitigate the impact of ransomware attacks.

DNSPIONAGE CYBER ESPIONAGE CAMPAIGN (2018-PRESENT)

When happened: The DNSpionage cyber espionage campaign has been ongoing since 2018.

Where happened: The campaign targeted organizations worldwide, including North America, Europe, the Middle East, Asia, and India.

What happened: DNSpionage attackers gained initial access through spear-phishing emails containing malicious attachments or links to spoofed websites. Once inside the network, they manipulated DNS records to redirect legitimate traffic to malicious servers controlled by them, enabling data exfiltration and further compromise. The campaign utilized various malware variants, including DNSChanger and Karkoff, to maintain persistence on infected systems and evade detection by security solutions.

How it happened: DNSpionage attackers used sophisticated spear-phishing tactics to trick users into opening malicious attachments or clicking on links to fake websites. Once inside the network, they exploited vulnerabilities in DNS infrastructure to redirect traffic to malicious servers under their control, allowing them to intercept sensitive information and conduct further malicious activities.

What was done to control that malware: To control DNSpionage attacks, organizations implemented email security controls to block phishing emails and prevent users from accessing malicious attachments or links, monitored DNS traffic for signs of unauthorized changes, encrypted DNS traffic using protocols like DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT) to prevent interception and manipulation, hardened DNS servers and implemented least privilege access controls, and collaborated with ISPs and cybersecurity organizations to identify and mitigate DNSpionage infrastructure.

CONCLUSION

In conclusion, the detailed analysis of significant malware attacks after 2016 underscores the evolving and pervasive nature of cyber threats worldwide. From targeted ransomware campaigns like SamSam to sophisticated banking Trojans such as TrickBot, cybercriminals continue to exploit vulnerabilities in network defenses and human vulnerabilities to infiltrate systems and inflict damage. The global impact of these attacks highlights the urgent need for organizations to bolster their cybersecurity posture through robust defense mechanisms, proactive threat detection, regular software updates, and comprehensive employee training. By understanding the tactics, techniques, and procedures employed by threat actors and implementing effective control measures, organizations can better protect themselves against the ever-present threat of malware attacks and safeguard their sensitive data and operations. Collaboration between stakeholders, including government agencies, law enforcement, cybersecurity firms, and businesses, is essential in mitigating the impact of malware attacks and ensuring a secure digital environment for all.