Task 5

Recent Malware Incidents: Attack Methods and Mitigation Strategies

I have researched and compiled a comprehensive report on three significant recent malware incidents, analyzing their attack methods and the mitigation strategies used to resolve them. The report examines:

Three Major Incidents Analyzed:

1. Change Healthcare Ransomware Attack (2024)

- The largest healthcare data breach in U.S. history
- Affected 190 million Americans (1 in 3 Americans)
- Cost $2.457 billion in response efforts
- Caused by ALPHV/BlackCat ransomware group exploiting a server without MFA

2. MOVEit Zero-Day Ransomware Campaign (2023)

- Supply chain attack by Cl0p ransomware group
- Exploited CVE-2023-34362 vulnerability in file transfer software
- Affected over 2,700 organizations and 93.3 million individuals
- Used SQL injection to deploy LEMURLOOT web shell

3. Snowflake Data Breach (2024)

- Credential-based attack by UNC5537/Scattered Spider
- Compromised over 160 organizations including AT&T, Ticketmaster, and Santander
- Exploited accounts lacking multi-factor authentication
- Resulted in theft of billions of customer records

Key Attack Methods Identified:

Common Attack Vectors:

- Compromised credentials and lack of multi-factor authentication
- Zero-day vulnerabilities in widely-used software
- Supply chain attacks targeting shared platforms
- Double and triple extortion tactics

Mitigation and Resolution Strategies:

Immediate Response Measures:

- System isolation and network disconnection
- Incident response team activation and forensic investigation
- Law enforcement and regulatory agency notification

Long-term Security Improvements:

- Mandatory multi-factor authentication implementation
- Enhanced network segmentation and monitoring
- Regular vulnerability patching and security updates
- Comprehensive backup and recovery procedures

The report provides detailed analysis of each incident, including attack timelines, impact assessments, and specific remediation steps taken. It concludes with actionable recommendations for organizations to improve their cybersecurity posture based on lessons learned from these high-profile breaches.

https://spin.ai/resources/ransomware-tracker/

https://www.pentestpeople.com/blog-posts/the-top-5-most-dangerous-cyber-attacks-of-all-time

https://www.cobalt.io/blog/11-biggest-ransomware-attacks-in-history

https://www.cm-alliance.com/cybersecurity-blog/major-cyber-attacks-ransomware-attacks-and-data breaches-of-june-2025

https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/ https://ccoe.dsci.in/blog/7-biggest-ransomware-attacks-in-india

By ashfin prem