Task 5

Recent Malware Incidents

Introduction

In this report, I describe three recent malware or cyberattack incidents (2025), explain their attack methods, and outline how each was mitigated or resolved. The goal is to show both variety in methods and the countermeasures used.

➢ Incident 1: Lumma Stealer Takedown (May 2025)

Lumma Stealer (also called LummaC2) was a widely used information-stealer malware targeting Windows devices. Between March and May 2025, it infected hundreds of thousands of machines. In May 2025, an international coalition of law enforcement agencies and technology firms carried out a takedown operation, seizing domains and disrupting the command-and-control (C2) infrastructure of Lumma.

Attack Method

- Infostealer functionality: Designed to harvest sensitive user data such as browser credentials and wallets.
- Distribution vectors: Spread via phishing and malicious downloads.
- C2 infrastructure: Used numerous domains to control infected clients.

Mitigation / Resolution

- Domain seizure and sinkholing.
- Disruption of C2 systems.
- Coordination with law enforcement and tech firms.
- Notifications and cleanup for affected users.

➢ Incident 2: XCSSET macOS Malware Variant (2025)

Microsoft flagged a new variant of the macOS malware XCSSET, targeting developers using Xcode. This new version added clipboard hijacking for cryptocurrency wallets and new persistence mechanisms.

Arsha Karma
AJCE

Attack Method

- Targeted developer tools by infecting Xcode projects.
- Stole cookies, credentials, and local data.
- Clipboard hijacking of cryptocurrency addresses.
- Persistence enhancements to evade detection.

Mitigation / Response

- Alerts and collaboration with Apple and GitHub.
- Removal of malicious repositories.
- Developer vigilance: auditing dependencies.
- Security tool updates to detect new variant.

➢ Incident 3: Endgame Gear Supply-Chain Malware (mid-2025)

Endgame Gear, a gaming hardware company, disclosed that its mouse configuration tool was replaced by a malware-infected version on its website during 26 June – 9 July 2025. The malicious file acted as an infostealer and was available only on the product page.

Attack Method

- Supply-chain compromise: attackers replaced the tool with a trojanized version.
- Infostealer payload stolen user data.
- Limited distribution vector via the website only.

Mitigation / Response

- Removal of infected file from the website.
- Centralized and secured downloads.
- Enhanced anti-malware scanning and protections.
- User guidance for cleanup and reinstallation.

Conclusion

These three incidents highlight different attack vectors: an information-stealer botnet, a targeted developer malware, and a supply-chain compromise. Mitigation required a mix of technical takedowns, vendor collaboration, and user vigilance.

Arsha Karma
AJCE