Task 5: Recent Malware Incidents

1. PromptLock – AI-Powered Ransomware

Attack Method:
PromptLock is a new kind of ransomware that uses a locally hosted AI model to create unique malicious scripts during the attack. It targets Windows, macOS, and Linux systems. Because it doesn't connect to external servers, it avoids detection by traditional antivirus tools.

Resolution:
So far, PromptLock has only been found in research settings. No real-world attacks have occurred yet. However, security experts are monitoring it and advising organizations to improve threat detection and prepare for AI-based threats.

2. Gayfemboy – IoT Botnet Malware

Attack Method:
Gayfemboy is a modern version of the Mirai botnet that infects routers and smart devices. It scans for devices with known vulnerabilities, especially those running outdated firmware. Once inside, it can launch large-scale DDoS attacks and hide from detection.

Resolution:
Security company Fortinet released updates that detect and block this malware using web filtering and intrusion prevention systems (IPS). Administrators are advised to update their devices and apply these security rules.

3. WinRAR Zero-Day (CVE-2025-8088)

Attack Method:
This vulnerability in older versions of WinRAR allowed attackers to place malware into the Windows startup folder using a malicious RAR file. The malware would then run automatically when the computer restarted. Hackers used this in real phishing campaigns.

Resolution:
WinRAR released a patch in version 7.13. However, since WinRAR doesn't update automatically, users must manually download and install the new version to stay protected.