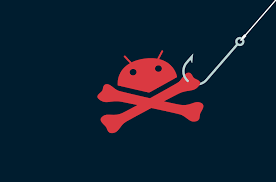
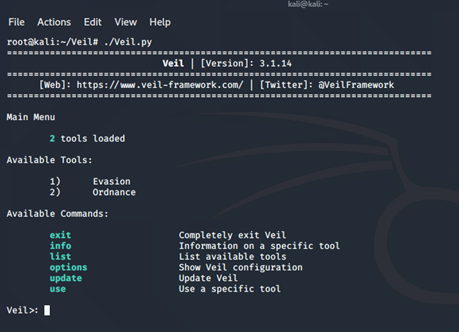
Task 2 Intern Intelligence

Incident Response Simulation

**1)Virus Creation**

An employee receives a phishing email and opens the malicious attachment. Once executed, the file creates a backdoor in the system, allowing the attacker remote access. The attacker then deploys malware across the network.

The attacker uses **Veil** to generate an undetectable payload. Veil is a tool designed to bypass antivirus detection by obfuscating the payload.



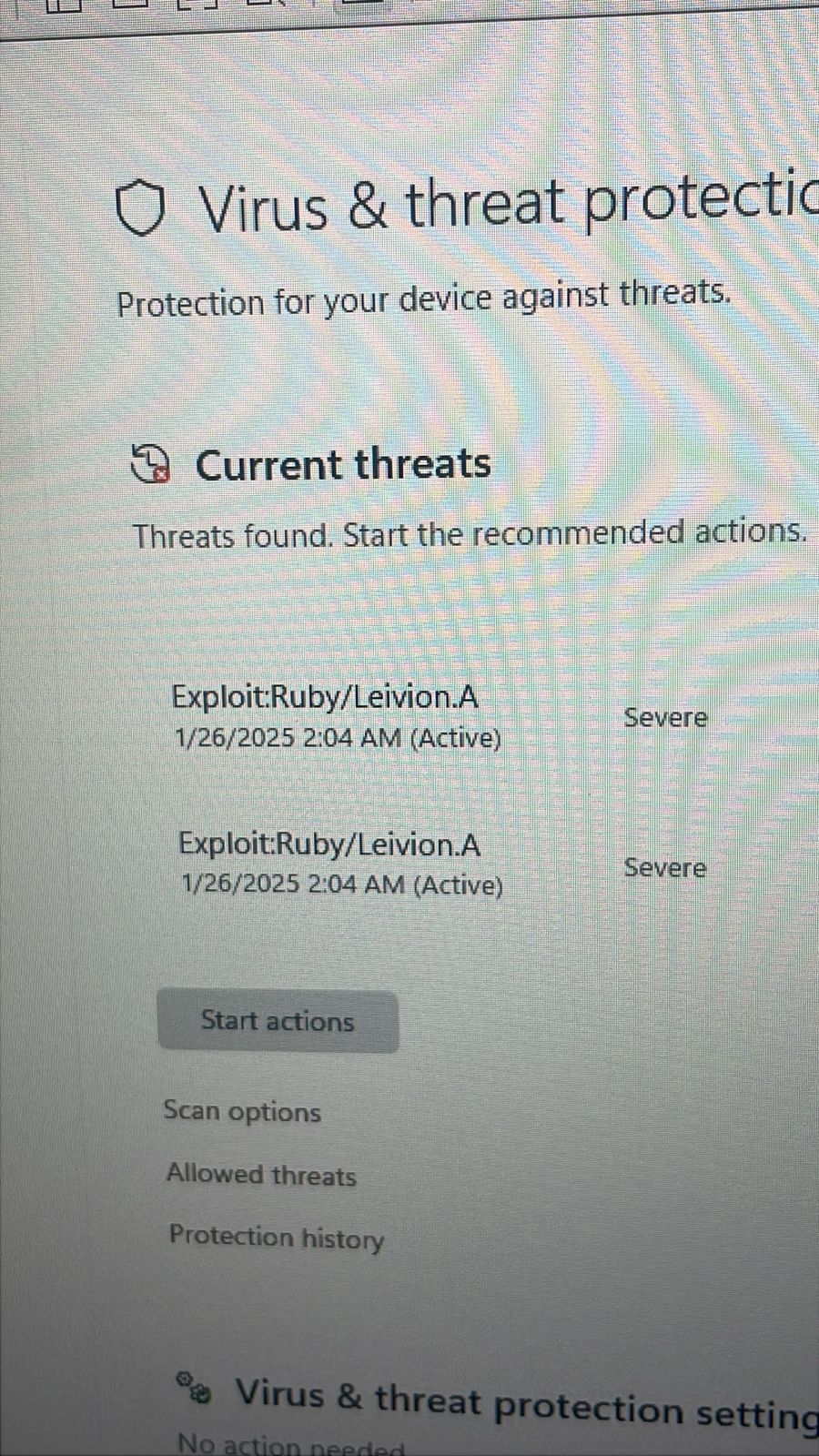


**Virus Propagation**

The malware begins spreading across the network, infecting multiple computers. It automatically encrypts files and disables certain system services. Meanwhile, Data Loss Prevention (DLP) systems detect unusual data exfiltration activities.

**Virus Detection & Incident Response**

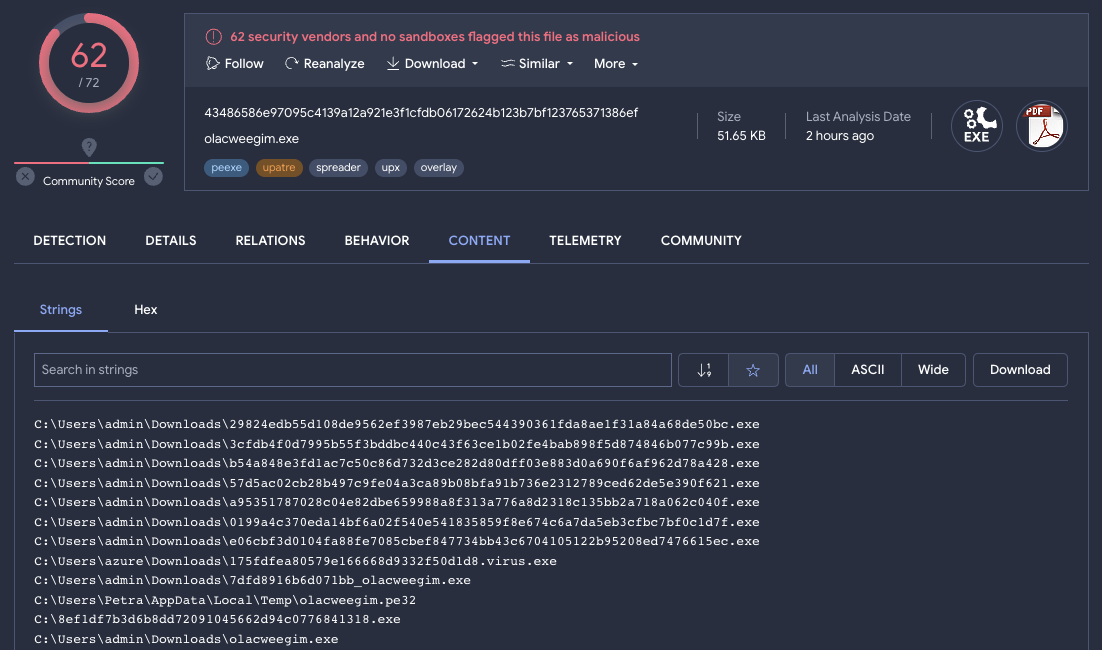
The security team analyzes system logs using SIEM and IDS tools to identify suspicious activities. Antivirus and EDR solutions detect infected systems, which are then quarantined.



**Virus Removal & Recovery**

Once the virus is detected, infected systems are isolated and cleaned. Meanwhile, the SOC (Security Operations Center) team performs a Root Cause Analysis (RCA) and updates security policies to prevent future attacks.

**Malware Analysis Using VirusTotal**

****As part of the incident response process, the suspicious file was uploaded to VirusTotal for further analysis. The goal was to identify potential malware signatures, detection rates, and behavioral indicators.