CyberSentinel Threat Analysis Report

Case ID: f415171b
Timestamp: 2026-01-14 18:17:14
Threat Type: Malware
Severity: High
Token Usage: 382

Scenario

Multiple workstations show unusual CPU spikes and outbound connections to unknown IPs.

Analysis

The unusual CPU spikes and outbound connections to unknown IPs indicate a potential malware infection. The sudden increase in CPU usage could be a result of the malware's malicious activities, such as data encryption or file scanning. The outbound connections to unknown IPs suggest that the malware is communicating with its command and control (C2) server, which could be used to receive further instructions or transmit stolen data. This behavior is consistent with a ransomware attack, where the malware demands payment in exchange for restoring access to encrypted files.

Recommendations

1. Immediately disconnect all infected workstations from the network to prevent further spread of the malware.
2. Run a full scan on all affected systems using an antivirus solution to detect and remove any malicious software.
3. Monitor network traffic and system logs to identify any suspicious activity and track the malware's communication with its C2 server. This will help in understanding the extent of the infection and taking targeted remediation steps.

Context Sources

No specific sources cited