CyberSentinel Threat Analysis Report

Case ID:	d7a0d68d
Timestamp:	2025-12-18 19:09:40
Threat Type:	Malware
Severity:	**High**
Token Usage:	357

Scenario

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

Analysis

The unusual CPU spikes on multiple workstations suggest an active malware presence, potentially exploiting system resources to evade detection. The outbound connections to unknown IPs further indicate that the malware is attempting to communicate with a command and control (C2) server or other malicious actors. This behavior is characteristic of advanced persistent threats (APTs), where malware is designed to remain hidden for extended periods, gathering sensitive information and maintaining persistence on infected systems.

Recommendations

1. Conduct an immediate network scan to identify the source IP addresses associated with the outbound connections

2. Run a full system scan using up-to-date antivirus software to detect and remove any detected malware

3. Isolate affected workstations and perform a thorough forensic analysis of the system logs, registry, and memory dumps to understand the extent of the malware's presence

Context Sources

No specific sources cited