Incident Response Report

Internship Task 2 – Future Interns Cybersecurity SOC Internship

By: Tshiamo Mantswe

Date: June 30, 2025

Executive Summary

On July 3, 2025, multiple malware alerts including ransomware, rootkit, and trojan infections were detected on user systems within the organization, originating from an initial compromise likely caused by phishing or malicious downloads. The attack progressed across hosts due to inadequate endpoint protection and network segmentation, resulting in significant security risks. Immediate containment steps such as isolating affected devices and credential resets are recommended. To prevent recurrence, it is advised to strengthen user training, deploy advanced endpoint detection tools, enforce multi-factor authentication, and enhance SIEM monitoring and incident response processes.

Incident Overview

Incident ID	Timestamp	User	IP Address	Action	Threat Type	Severity
001	2025-07-03 09:10 AM	bob	172.16.0.3	Malware detected	Ransomware Behavior	High
002	2025-07-03 07:51 AM	eve	10.0.0.5	Malware detected	Rootkit Signature	High
003	2025-07-03 07:45 AM	charlie	172.16.0.3	Malware detected	Trojan Signature	Medium

Incident Timeline

Timestamp	Event Description
2025-07-03 07:45 AM	Malware (Trojan) detected on device used by charlie (172.16.0.3)
2025-07-03 07:51 AM	Malware (Rootkit) detected on eve’s system (10.0.0.5)
2025-07-03 09:10 AM	Malware (Ransomware behavior) detected on bob’s system (172.16.0.3)

Impact

The ransomware infection on user bob’s device poses a high risk of data encryption, potentially leading to operational disruption and financial losses. The rootkit detection on eve’s system indicates the attacker’s persistent presence, increasing the likelihood of unauthorized data access or further compromise. The Trojan infection suggests initial breach capability that allowed lateral movement within the network. Overall, these threats represent a critical risk to organizational security and data integrity.

Detection & Analysis

The incident involved three malware detections within a short time frame across two systems. All detections were identified through the SIEM logs provided.

- At 07:45 AM, a Trojan was detected on user charlie's device (IP: 172.16.0.3). Trojans often serve as an initial access vector, which can open a backdoor for further exploitation.
- At 07:51 AM, a Rootkit Signature was detected on user eve's system (IP: 10.0.0.5). Rootkits allow attackers to maintain persistent access and often go undetected by standard security tools.
- At 09:10 AM, Ransomware Behavior was flagged on user bob's machine, again associated with IP 172.16.0.3, indicating that the same machine was targeted or reinfected.

The reuse of the IP address 172.16.0.3 for both the Trojan and ransomware detections suggests that the host was likely compromised early and later used as a launchpad for the final payload. This progression, from Trojan to Rootkit then to Ransomware, indicates a coordinated attack with stages of infection.

No alerts indicated any form of automated mitigation or containment, so it's likely that the infection chain was allowed to proceed unchecked.

Root Cause Analysis

Based on the timing and nature of the alerts, the likely root cause of this incident is an initial compromise of the host at 172.16.0.3, possibly via a phishing email or malicious file download by user charlie. The Trojan detected at 07:45 AM suggests that this host was the first point of entry.

The subsequent detection of a Rootkit on a different system (10.0.0.5) shortly after indicates potential lateral movement or further exploitation of vulnerable systems within the network.

Finally, the detection of Ransomware Behavior on bob's device, which shares the same IP as charlie, suggests that the malware escalated privileges and deployed its final payload. The logs show no signs of automatic mitigation or user intervention, implying a lack of active endpoint protection or delayed response.

This incident highlights the risks of inadequate threat isolation, missing endpoint defenses, and low user awareness.

Containment & Mitigation

To contain the incident and minimize further damage, the following actions should be taken:

- Immediate Isolation of Affected Hosts – Disconnect the host at 172.16.0.3 (used by both charlie and bob) from the network to prevent ransomware spread. Isolate 10.0.0.5 (eve's system) to halt any rootkit persistence or command & control traffic.
- Malware Removal & System Scans – Run a full malware and rootkit scan using enterprise-grade antivirus and EDR tools. Remove all detected malicious files and binaries. Check for signs of persistence (e.g., autorun entries, scheduled tasks, registry changes).
- Credential Resets – Reset user passwords for charlie, bob, and eve. Check logs for any lateral movement or privilege escalation.
- System Restoration – Re-image systems showing ransomware behavior (if files are encrypted or compromised). Restore clean backups where possible.
- Log Review & Threat Hunting – Review SIEM logs for indicators of compromise on other hosts. Hunt for similar patterns across the network.

Recommendations

Based on the analysis of this incident, the following recommendations are proposed to strengthen the organization's cybersecurity posture:

- User Awareness Training – Educate users about phishing attacks and safe handling of email attachments, especially targeting users like charlie, eve, and bob.
- Endpoint Protection & EDR Tools – Deploy modern endpoint detection and response (EDR) tools to detect and isolate malware in real-time. Enable automatic quarantine for malicious activity.
- Network Segmentation – Isolate critical systems to prevent lateral movement of malware within the network.
- Regular Patching and Updates – Apply OS and software patches promptly to close vulnerabilities that malware might exploit.
- Multi-Factor Authentication (MFA) - Enforce MFA on all user accounts to reduce the risk of credential misuse.
- Advanced SIEM Alerting & Playbooks – Improve SIEM alert logic to detect abnormal behaviors faster. Develop incident response playbooks for malware events to reduce response time.
- Periodic Security Audits - Conduct regular vulnerability assessments and penetration tests.