Incident Response Report

Task 2

Prepared by:
Goutam Adityan M

Tools Used:
Elastic Stack (ELK), Docker

1 Executive Summary

During the monitoring period of July 3, 2025, the Security Operations Center (SOC) detected multiple critical security events indicating a coordinated compromise of internal assets.

Analysis of system logs revealed high-severity threats including **Ransomware behavior**, **Rootkit signatures**, and **Worm infection attempts**. The attacks primarily targeted users *Bob*, *Alice*, and *Eve*, suggesting a spreading infection across the 172.16.x.x and 10.0.x.x subnets. Immediate isolation of affected hosts is recommended.

2 Methodology & Tooling

The analysis was conducted using the **Elastic Stack (ELK)** hosted on a Dockerized environment. Raw log data containing authentication attempts, network connections, and threat signatures were ingested into Kibana.

2.1 Data Parsing

To correctly structure the raw pipe-delimited logs, a custom **Grok Pattern** was developed to extract critical fields such as `threat_type` and `src_ip`:

```
%{TIMESTAMP_ISO8601:timestamp} \| user=%{USERNAME:user_name} \|
   ip=%{IP:src_ip} \| action=%{DATA:action} \| threat=%{
   GREEDYDATA:threat_type}|%{TIMESTAMP_ISO8601:timestamp} \| user
   =%{USERNAME:user_name} \| ip=%{IP:src_ip} \| action=%{
   GREEDYDATA:action}
```

3 Incident Analysis

The following table summarizes the critical alerts identified during the triage phase.

Time	**User**	**Threat Type**	**Priority**	**Impact Analysis**
09:10:14	Bob	Ransomware Behavior	**Critical**	Active file encryption detected on IP 172.16.0.3.
05:30:14	Alice	Rootkit Signature	**Critical**	OS-level compromise on IP 198.51.100.42. Indicates persistent attacker access.
04:53:14	Eve	Rootkit Signature	**Critical**	Second instance of Rootkit detected on internal IP 10.0.0.5.
05:06:14	Bob	Worm Infection	**High**	Attempt to self-propagate malware to other network nodes.
06:10:14	Eve	Trojan Detected	**Medium**	Malware dropped on IP 192.168.1.101.

Table 1: Summary of Detected Threats

3.1 Detailed Findings

- **Compromised Host (Bob - IP 172.16.0.3):** User *Bob* is the primary victim of a destructive attack. Logs show a clear progression of compromise:
  - At **05:06**, a "Worm Infection Attempt" was flagged, suggesting an initial breach trying to spread.
  - By **09:10**, this escalated to "Ransomware Behavior," indicating the payload executed and began encrypting files.
- **Persistence Mechanisms (Alice & Eve):**
  - User *Alice* (IP 198.51.100.42) triggered a "Rootkit Signature" at **05:30**.
  - User *Eve* (IP 10.0.0.5) triggered a separate "Rootkit Signature" at **04:53**.

  Rootkits modify the operating system kernel to hide malicious activity. The presence of rootkits on two separate subnets (External and Internal) indicates a deep network infiltration.
- **Widespread Trojan Activity:** Multiple "Trojan Detected" alerts were observed for users *Eve* (06:10), *Charlie* (05:44), and *David* (05:45). This clustered activity suggests a mass-malware distribution campaign targeting the organization's endpoints.

4 Visualizations

The following dashboard was constructed in Kibana to visualize the threat landscape.

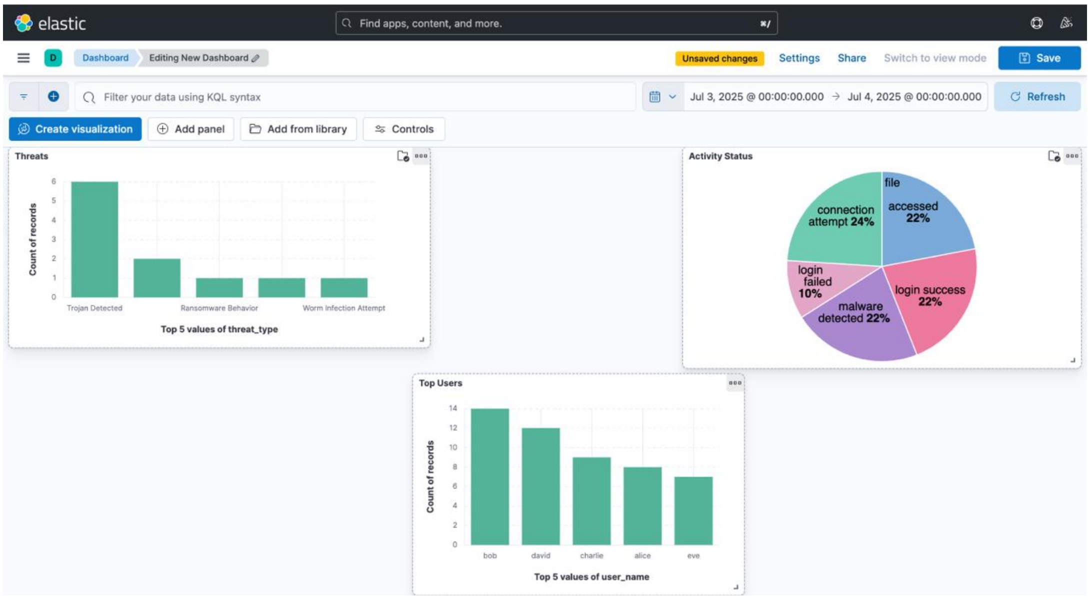

Figure 1: SOC Dashboard showing Threat Distribution and Top Targeted Users

5 Remediation Strategy

1. **Isolate Hosts:** Immediately disconnect endpoints `172.16.0.3` (Bob), `10.0.0.5` (Eve), and `198.51.100.42` (Alice) from the corporate network.

2. **Forensic Snapshot:** Capture memory and disk images of the affected systems before shutting them down to preserve evidence of the Rootkit/Ransomware.

3. **Credential Reset:** Force password resets for users Bob, Alice, Eve, Charlie, and David.

4. **Re-image:** Due to the nature of Rootkits, a complete wipe and reinstall of the operating system is required for Alice and Eve's machines.

Appendix: Stakeholder Communication

Subject: URGENT: Security Incident Detected - Ransomware & Rootkit Activity
To: CISO; IT Management
From: Goutam Adityan, SOC Analyst

Team,

We have detected confirmed malware activity on the network involving Ransomware and Rootkit signatures.

Current Status:

- **User Bob (172.16.0.3):** Flagged for Ransomware behavior. File encryption is likely in progress.
- **User Alice (198.51.100.42) & Eve (10.0.0.5):** Flagged for Rootkit activity, indicating full system compromise.

Actions Taken: We are currently isolating these hosts to prevent lateral movement. We request authorization to take the affected subnets offline immediately for containment.

A full detailed report is attached.

Regards,
Goutam Adityan