LOG ANALYSIS & THREAT MITIGATION STRATEGY

SUBMITTED TO: CYBER SECURITY INTERNSHIP PROGRAM

FUTURE INTERNS

SUBMITTED BY: ENI GRACE ODEN SOC ANALYST

CYBERSECURITY INTERN

DATE: DECEMBER 2025

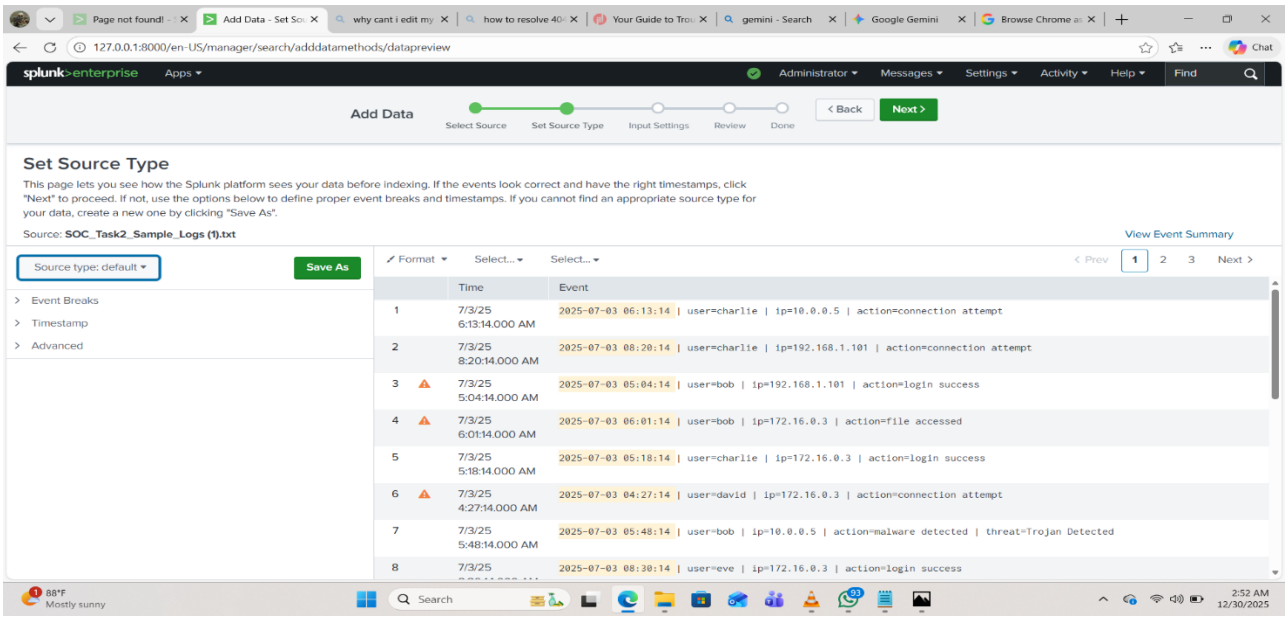
TOOL USED: SPLUNK SIEM

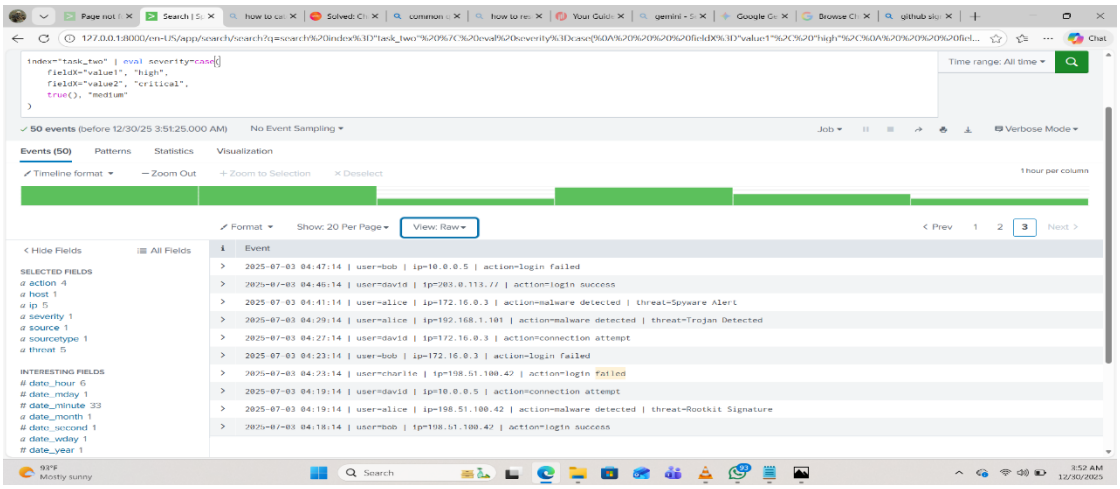
SUBJECT: FORENSIC ANALYSIS OF SIMULATED NETWORK

COMPROMISE (IR-2025-07-03-001)

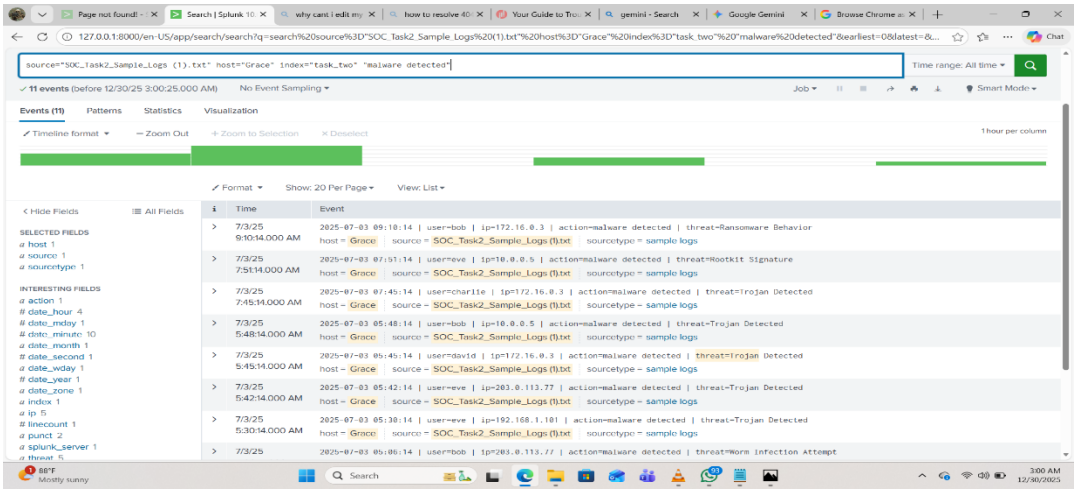
INTRODUCTION

This document presents the forensic analysis of anomalous system logs collected within the organization's Security Operations Center (SOC). The primary objective is to identify potential security incidents, classify them by severity, and develop effective remediation strategies. Using Splunk for log correlation and analysis, the investigation identified multiple malicious activities, including ransomware behavior, rootkits, Trojans, spyware, and worm propagation attempts.





SCOPE OF INCIDENT ANALYSIS



SOC Case Report

Case ID: SOC-IR-2025-07-003-001

Case Title: Multiple Malware Detections Across User Endpoints

Status: Closed (Post-Incident Review)

Priority: High

Summary

Multiple malware-related alerts were identified through Splunk SIEM during routine monitoring. The alerts indicated malicious activity across several user endpoints, involving both internal and external IP addresses. Detected threats included ransomware behavior, rootkits, Trojans, spyware, and worm infection attempts.

Detection Source

- **SIEM Platform:** Splunk
- **Log Source:** Sample system logs
- **Detection Method:** Keyword-based search and log correlation
- **Trigger Keyword**: malware

Affected Assets

Users:

- bob
- eve
- alice
- charlie
- david

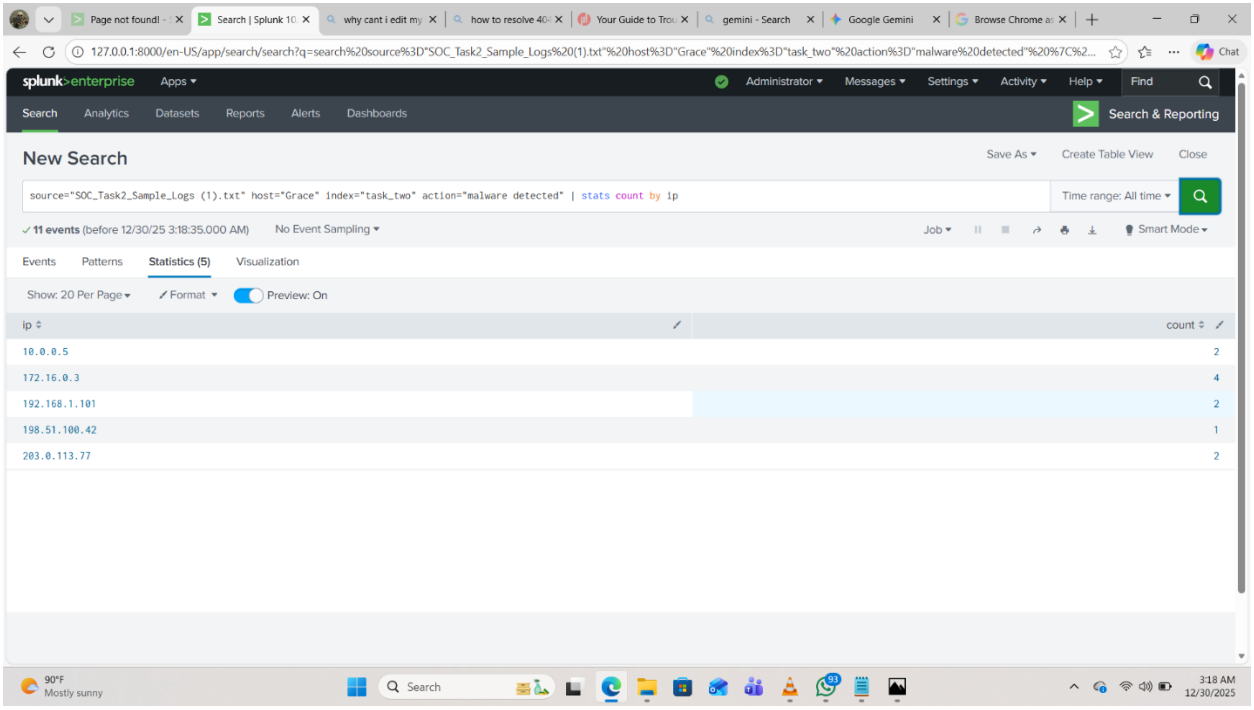
IP Addresses:

- Internal: 172.16.0.3, 10.0.0.5, 192.168.1.101
- External: 203.0.113.77, 198.51.100.42

Indicators of Compromise (IOCs)

Timestamp (UTC)	User	IP Address	Threat Detected
2025-07-03 09:10	bob	172.16.0.3	Ransomware Behavior
2025-07-03 07:51	eve	10.0.0.5	Rootkit Signature
2025-07-03 07:45	charlie	172.16.0.3	Trojan Detected

Timestamp (UTC)	User	IP Address	Threat Detected
2025-07-03 05:06	bob	203.0.113.77	Worm Infection Attempt
2025-07-03 04:41	alice	172.16.0.3	Spyware Alert
2025-07-03 04:19	alice	198.51.100.42	Rootkit Signature



Severity Assessment

Threat Type	Severity
Rootkit Signature	Critical
Ransomware Behavior	High
Trojan Malware	High
Worm Infection Attempt	High
Spyware Alert	Medium

Incident Timeline

Initial Detection: Malware alerts observed in Splunk during log review

- **Analysis:** Correlation confirmed multiple malware types across endpoints
- **Containment:** Affected systems flagged and isolated
- **Remediation:** Endpoint scans and credential reviews initiated
- **Closure:** No further malicious activity observed after controls applied

Remediation Actions

- Full antivirus and EDR scans executed
- Systems with rootkit and ransomware indicators recommended for reimaging
- Security patches applied to affected hosts
- User credentials reset and MFA enforcement recommended

Recommendations

- Deploy advanced Endpoint Detection and Response (EDR) solutions
- Improve network segmentation
- Conduct regular malware-focused threat hunting
- Provide user awareness training on malicious downloads and phishing

CONCLUSION

The forensic analysis for SOC Task 2 identified high-severity threats, including ransomware, rootkits, Trojans, and worm activity. These incidents were classified as **High Priority**, requiring immediate remediation and continuous monitoring to prevent future compromise.