



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

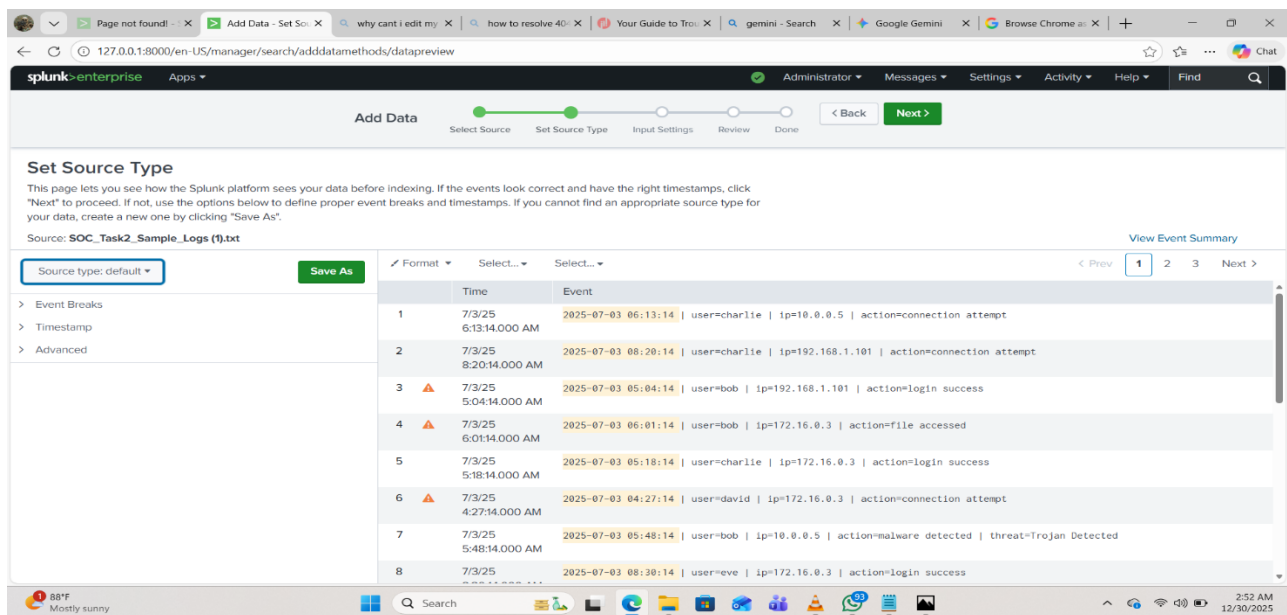
TOOL USED: SPLUNK SIEM

SUBJECT: FORENSIC ANALYSIS OF SIMULATED NETWORK

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

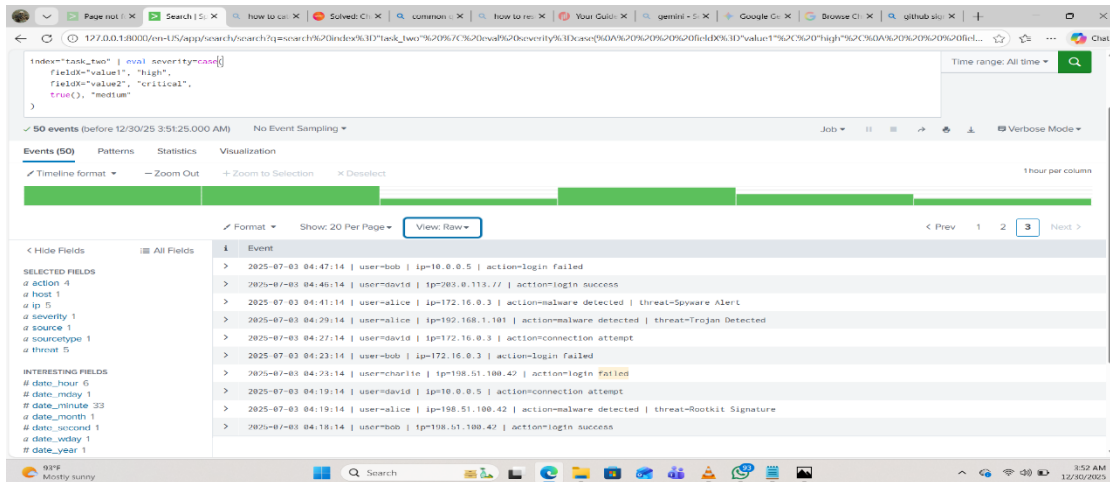
INTRODUCTION

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.

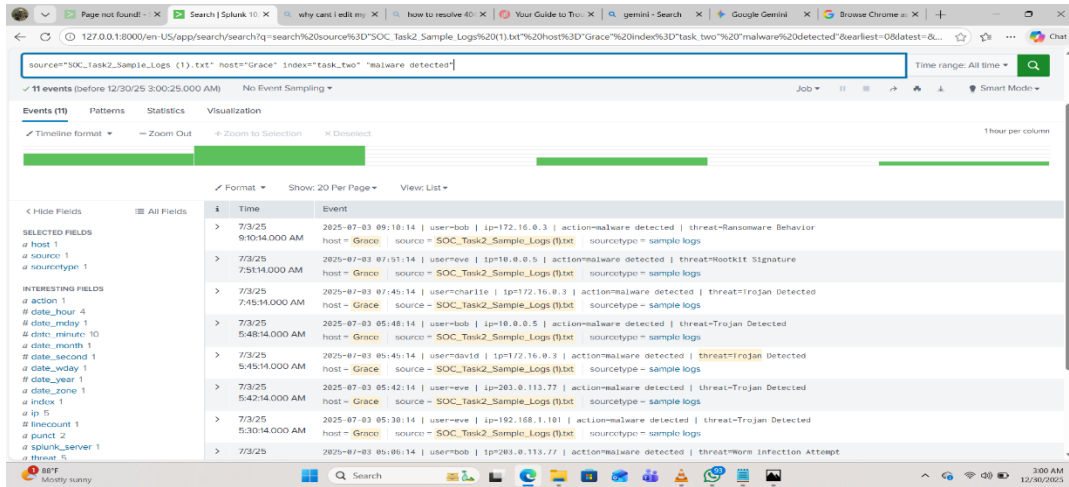


The screenshot displays the Splunk 'Set Source Type' configuration page. The source is identified as 'SOC_Task2_Sample_Logs (1).txt'. The interface includes a 'Source type: default' dropdown and a 'Save As' button. A table of log events is shown, with columns for 'Time' and 'Event'. The events are numbered 1 through 8, with some marked as warnings (yellow triangles). The events include connection attempts, login successes, file accesses, and malware detection.

	Time	Event
1	7/3/25 6:13:14.000 AM	2025-07-03 06:13:14 user=charlie ip=10.0.0.5 action=connection attempt
2	7/3/25 8:20:14.000 AM	2025-07-03 08:20:14 user=charlie ip=192.168.1.101 action=connection attempt
3	7/3/25 5:04:14.000 AM	2025-07-03 05:04:14 user=bob ip=192.168.1.101 action=login success
4	7/3/25 6:01:14.000 AM	2025-07-03 06:01:14 user=bob ip=172.16.0.3 action=file accessed
5	7/3/25 5:18:14.000 AM	2025-07-03 05:18:14 user=charlie ip=172.16.0.3 action=login success
6	7/3/25 4:27:14.000 AM	2025-07-03 04:27:14 user=david ip=172.16.0.3 action=connection attempt
7	7/3/25 5:48:14.000 AM	2025-07-03 05:48:14 user=bob ip=10.0.0.5 action=malware detected threat=Trojan Detected
8	7/3/25 8:30:14.000 AM	2025-07-03 08:30:14 user=eve ip=172.16.0.3 action=login success



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

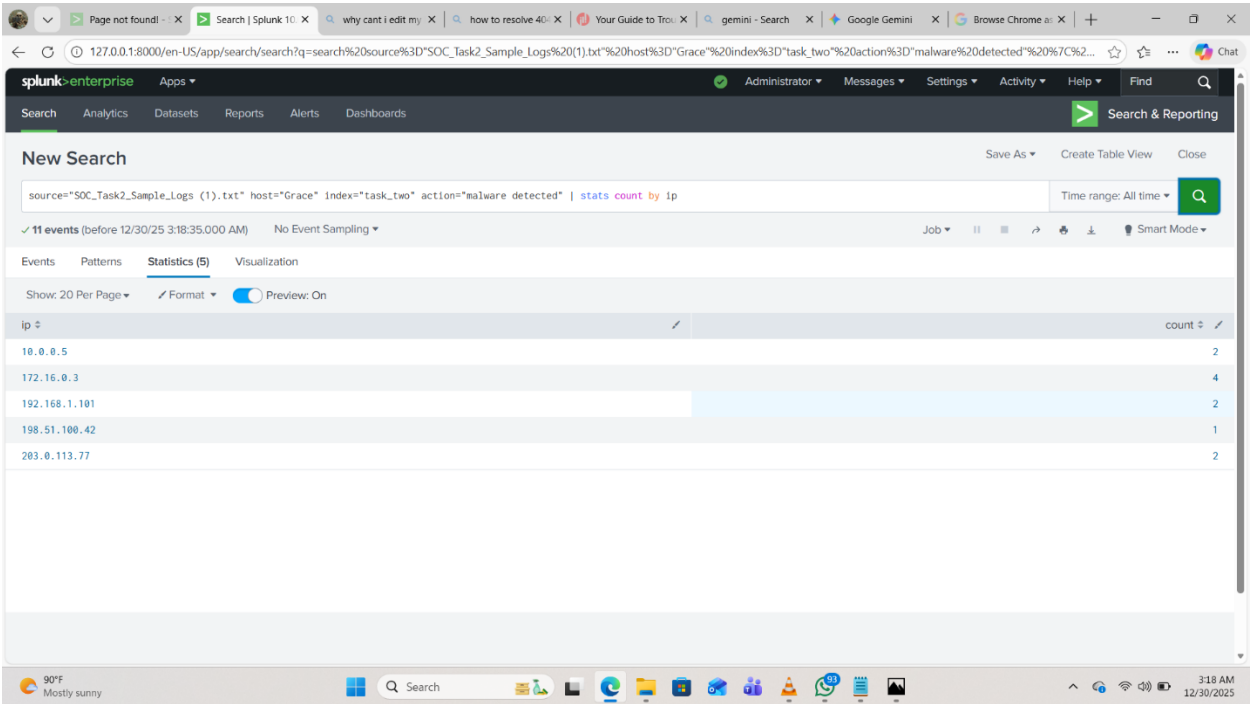
IP Addresses:

- 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.