



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 shows the Splunk 'Add Data' interface. The top navigation bar includes tabs like 'Page not found!', 'Add Data - Set So...', 'why cant i edit my...', 'how to resolve 40...', 'Your Guide to Trou...', 'gemini - Search', 'Google Gemini', 'Browse Chrome...', and a search bar. Below the navigation is a breadcrumb trail: 'splunk>enterprise' > 'Add Data' > 'Set Source Type'. A progress bar at the top indicates the steps: 'Select Source' (green), 'Set Source Type' (green), 'Input Settings' (white), 'Review' (white), and 'Done' (white). The main content area is titled 'Set Source Type' with a sub-instruction: 'This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".' It shows a table of log entries from 'Source: SOC_Task2_Sample_Logs (1).txt'. The table has columns 'Time' and 'Event'. The log entries are:

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

Below the table are buttons for 'Format', 'Select...', 'Save As', and 'View Event Summary'. The status bar at the bottom shows '88°F Mostly sunny' and the date/time '2:52 AM 12/30/2025'.

```

index='task_two' | eval severity=case[ fieldX='value1', 'high'; fieldX='value2', 'critical'; true(), 'medium' ]

```

50 events (before 12/30/2025 3:51:25:000 AM) No Event Sampling ▾

Events (50) Patterns Statistics Visualization

Time range: All time ▾

1 hour per column

Format Show: 20 Per Page ▾ View: Raw ▾

< Hide Fields ▾ All Fields

SELECTED FIELDS

- ✓ *action* 4
- ✓ *host* 1
- ✓ *ip* 5
- ✓ *severity* 1
- ✓ *source* 1
- ✓ *sourcetype* 1
- ✓ *threat* 5

INTERESTING FIELDS

- ✓ *date_hour* 6
- ✓ *date_minute* 1
- ✓ *date_month* 33
- ✓ *date_second* 1
- ✓ *date_wday* 1
- ✓ *date_year* 1

Event

	Time	Event
>	2025-07-03 04:47:14	user=>bob ip=10.0.0.5 action=login failed
>	2025-07-03 04:46:14	user=>david ip=203.0.113.77 action=login success
>	2025-07-03 04:41:14	user=>alice ip=172.16.0.3 action=malware detected threat=Spyware Alert
>	2025-07-03 04:29:14	user=>alice ip=192.168.1.101 action=malware detected threat=Trojan Detected
>	2025-07-03 04:27:14	user=>david ip=172.16.0.3 action=connection attempt
>	2025-07-03 04:23:14	user=>bob ip=172.16.0.3 action=login failed
>	2025-07-03 04:23:14	user=>charlie ip=198.51.100.42 action=login failed
>	2025-07-03 04:19:14	user=>david ip=10.0.0.5 action=connection attempt
>	2025-07-03 04:19:14	user=>alice ip=198.51.100.42 action=malware detected threat=Rootkit Signature
>	2025-07-03 04:18:14	user=>bob ip=198.51.100.42 action=login success

3:52 AM 12/30/2025

SCOPE OF INCIDENT ANALYSIS

```

source='SOC_Task2_Sample_Logs_(1).txt' host='Grace' index='task_two' 'malware detected'

```

11 events (before 12/30/25 3:00:25:000 AM) No Event Sampling ▾

Events (11) Patterns Statistics Visualization

Time range: All time ▾

1 hour per column

Format Show: 20 Per Page ▾ View: List ▾

< Hide Fields ▾ All Fields

SELECTED FIELDS

- ✓ *host* 1
- ✓ *source* 1
- ✓ *sourcetype* 1

INTERESTING FIELDS

- ✓ *action* 1
- ✓ *date_hour* 4
- ✓ *date_minute* 1
- ✓ *date_month* 10
- ✓ *date_minute* 10
- ✓ *date_month* 1
- ✓ *date_second* 1
- ✓ *date_wday* 1
- ✓ *date_year* 1
- ✓ *date_zone* 1
- ✓ *index* 1
- ✓ *ip* 5
- ✓ *is_instant* 1
- ✓ *is_point* 2
- ✓ *splunk_server* 1
- ✓ *threat* 5

Time

	Time	Event
>	7/3/25 9:10:40:00 AM	user=>bob ip=172.16.0.3 action=malware detected threat=Ransomware Behavior host = Grace source = SOC_Task2_Sample_Logs_(1).txt sourcetype = sample_logs
>	7/3/25 7:51:00:00 AM	2025-07-03 07:51:00 user=> ip=10.0.0.5 action=malware detected threat=Rootkit Signature host = Grace source = SOC_Task2_Sample_Logs_(1).txt sourcetype = sample_logs
>	7/3/25 7:45:10:00 AM	2025-07-03 07:45:10 user=>charlie ip=198.51.100.42 action=malware detected threat=Trojan Detected host = Grace source = SOC_Task2_Sample_Logs_(1).txt sourcetype = sample_logs
>	7/3/25 5:48:10:00 AM	2025-07-03 05:48:10 user=>bob ip=10.0.0.5 action=malware detected threat=Trojan Detected host = Grace source = SOC_Task2_Sample_Logs_(1).txt sourcetype = sample_logs
>	7/3/25 5:45:10:00 AM	2025-07-03 05:45:10 user=> ip=172.16.0.3 action=malware detected threat=Trojan Detected host = Grace source = SOC_Task2_Sample_Logs_(1).txt sourcetype = sample_logs
>	7/3/25 05:42:14	2025-07-03 05:42:14 user=>david ip=172.16.0.3 action=malware detected threat=Trojan Detected host = Grace source = SOC_Task2_Sample_Logs_(1).txt sourcetype = sample_logs
>	7/3/25 5:30:10:00 AM	2025-07-03 05:30:10 user=>eve ip=192.168.1.101 action=malware detected threat=Trojan Detected host = Grace source = SOC_Task2_Sample_Logs_(1).txt sourcetype = sample_logs
>	7/3/25 05:06:14	2025-07-03 05:06:14 user=>bob ip=203.0.113.77 action=malware detected threat=Normal Infection Attempt

3:00 AM 12/30/2025

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
------------------	-------	---------------	-------------------

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `source="SOC_Task2_Sample_Logs (1).txt" host="Grace" index="task_two" action="malware detected" | stats count by ip`. The results table shows 11 events found before 12/30/25 3:18:35.000 AM. The table has columns for IP address and count. The data is as follows:

ip	count
10.0.0.5	2
172.16.0.3	4
192.168.1.101	2
198.51.100.42	1
203.0.113.77	2

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.