SOC Internship Task
Prepared by: Yehya Hamdy Sayed-Ahmed Mohammed
Date: October 20, 2025
Submitted to: Future Interns Task Two

Executive Summary

On July 3, 2025, between 07:45 AM and 09:10 AM, the Security Operations Center (SOC) identified five critical security incidents, including three malware detections (Ransomware, Rootkit, and Trojan) and a failed login attempt from an external IP address. These incidents pose a severe threat to system integrity, data confidentiality, and operational continuity. Immediate containment actions have been executed, and this report delivers a detailed analysis, remediation plan, and strategic recommendations.

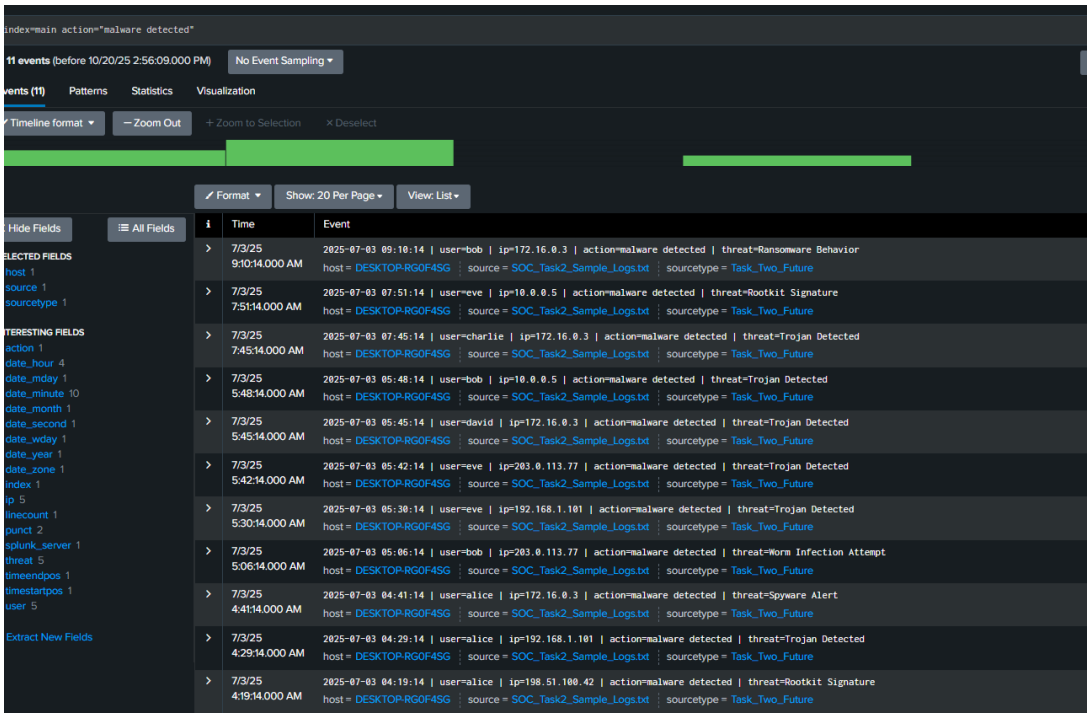
Incident Details

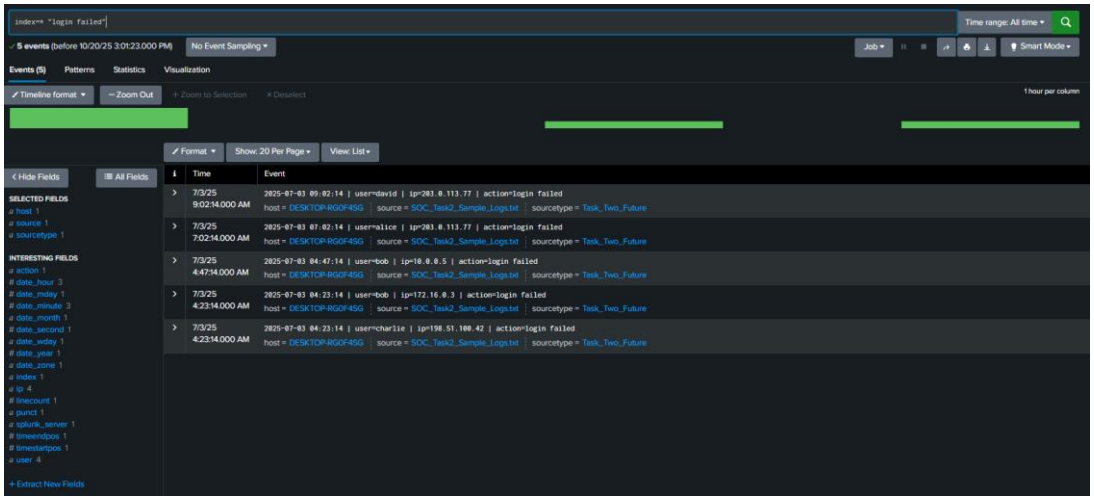
Timeline of Events

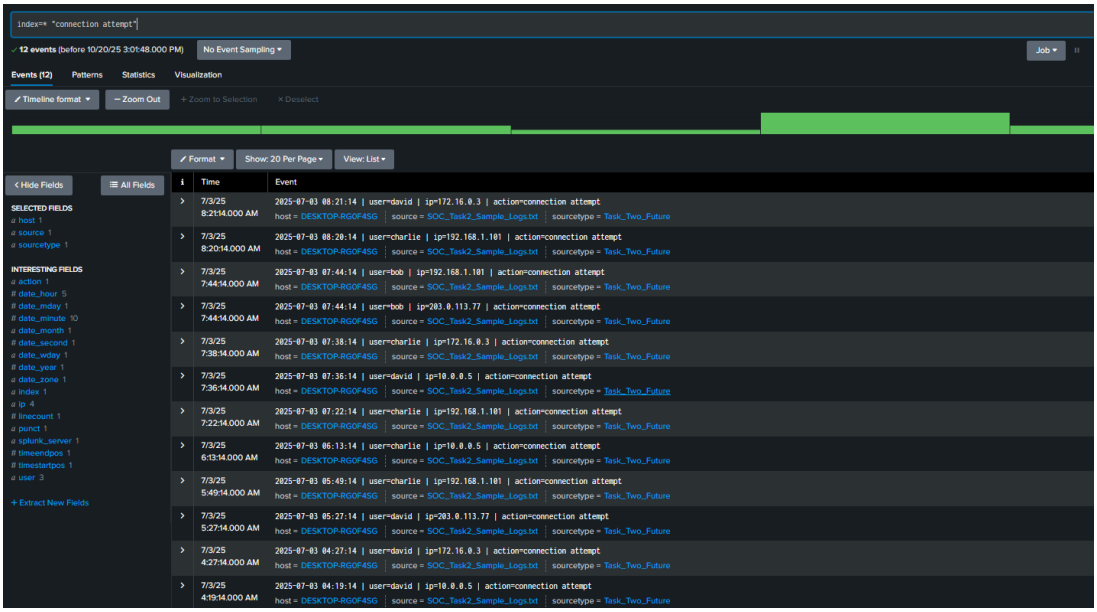
- **07:45:14 AM: Trojan malware detected on user *charlie* (IP: 172.16.0.3).**
- **07:51:14 AM: Rootkit signature detected on user *eve* (IP: 10.0.0.5).**
- **09:02:14 AM: Failed login attempt for user *david* (IP: 203.0.113.77).**
- **09:10:14 AM: Ransomware behavior detected on user *bob* (IP: 172.16.0.3).**
- **07:44:14 AM - 08:21:14 AM: Multiple connection attempts observed from various IP addresses.**

Impact Assessment

The identified malware variants (Ransomware, Rootkit, Trojan) present significant risks, including data encryption, unauthorized remote access, and persistent system compromise. The failed login attempt suggests a potential brute force attack, while recurring connection attempts indicate reconnaissance activities by a malicious actor. These incidents could result in substantial data loss, financial repercussions, and operational downtime if not addressed effectively.


index=main action="malware detected"
11 events (before 10/20/25 2:56:09.000 PM)
No Event Sampling
Events (11)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
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_mday 1
date_minute 10
date_month 1
date_second 1
date_wday 1
date_year 1
date_zone 1
index 1
ip 5
linecount 1
punct 2
splunk_server 1
threat 5
timeendpos 1
timestartpos 1
user 5
Extract New Fields
Time
Event
7/3/25 9:10:14.000 AM
2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 7:51:14.000 AM
2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 7:45:14.000 AM
2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
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
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 5:45:14.000 AM
2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 5:42:14.000 AM
2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 5:30:14.000 AM
2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 5:06:14.000 AM
2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 4:41:14.000 AM
2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 4:29:14.000 AM
2025-07-03 04:29:14 | user=alice | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 4:19:14.000 AM
2025-07-03 04:19:14 | user=alice | ip=198.51.100.42 | action=malware detected | threat=Rootkit Signature
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future


index=* "login failed"
Time range: All time
5 events (before 10/20/25 3:01:23.000 PM)
No Event Sampling
Job
Smart Mode
Events (5)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
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 3
date_mday 1
date_minute 3
date_month 1
date_second 1
date_wday 1
date_year 1
date_zone 1
index 1
ip 4
linecount 1
punct 1
splunk_server 1
timeendpos 1
timestartpos 1
user 4
Extract New Fields
Time
Event
7/3/25 9:02:14.000 AM
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 7:02:14.000 AM
2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 4:47:14.000 AM
2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 4:23:14.000 AM
2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login failed
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 4:23:14.000 AM
2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future


index=* "connection attempt"
12 events (before 10/20/25 3:01:48.000 PM)
No Event Sampling
Job
Events (12)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
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 5
date_mday 1
date_minute 10
date_month 1
date_second 1
date_wday 1
date_year 1
date_zone 1
index 1
ip 4
linecount 1
punct 1
splunk_server 1
timeendpos 1
timestartpos 1
user 3
Extract New Fields
Time
Event
7/3/25 8:21:14.000 AM
2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 8:20:14.000 AM
2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 7:44:14.000 AM
2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection attempt
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 7:44:14.000 AM
2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 7:38:14.000 AM
2025-07-03 07:38:14 | user=charlie | ip=172.16.0.3 | action=connection attempt
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 7:36:14.000 AM
2025-07-03 07:36:14 | user=david | ip=10.0.0.5 | action=connection attempt
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 7:22:14.000 AM
2025-07-03 07:22:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 6:13:14.000 AM
2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 5:49:14.000 AM
2025-07-03 05:49:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 5:27:14.000 AM
2025-07-03 05:27:14 | user=david | ip=203.0.113.77 | action=connection attempt
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 4:27:14.000 AM
2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future
7/3/25 4:19:14.000 AM
2025-07-03 04:19:14 | user=david | ip=10.0.0.5 | action=connection attempt
host = DESKTOP-RG0F4SG | source = SOC_Task2_Sample_Logs.txt | sourcetype = Task_Two_Future

---

Root Cause Analysis

The malware infections are likely the result of a successful exploit, potentially delivered through phishing emails or malicious attachments. The failed login attempt from an external IP (203.0.113.77) aligns with patterns of a brute force attack. Multiple connection attempts across different IPs suggest a reconnaissance phase, possibly preceding a larger-scale attack.

Remediation Steps

Immediate Actions

- **Block malicious IPs: 172.16.0.3, 10.0.0.5, and 203.0.113.77.**
- **Isolate affected systems associated with users *bob*, *eve*, and *charlie*.**
- **Initiate comprehensive antivirus scans to eradicate malware.**

Long-Term Measures

- **Update antivirus software with the latest threat definitions.**
- **Enforce multi-factor authentication (2FA) across all user accounts.**
- **Enhance SIEM monitoring with custom rules to detect similar anomalies.**

Recommendations

- **Implement mandatory phishing awareness training for all employees.**
- **Strengthen SIEM detection rules to identify failed login attempts and unusual connection patterns.**
- **Review and tighten network access controls to restrict external IP activity.**
- **Conduct a thorough post-incident review to assess vulnerabilities and enhance security posture.**

Alert Classification Log

Alert ID	Timestamp	Type	Source IP	User/Target	Severity
1	2025-07-03 09:10:14	Malware	172.16.0.3	bob	High
2	2025-07-03 07:51:14	Malware	10.0.0.5	eve	High
3	2025-07-03 07:45:14	Malware	172.16.0.3	charlie	High
4	2025-07-03 09:02:14	Failed Login	203.0.113.77	david	Medium
5	2025-07-03 07:44:14	Connection Attempt	203.0.113.77	bob	Medium

---