# Incident Response Report – SOC_Task2_Sample_Logs

## 1. Executive Summary

During log analysis in Splunk, multiple suspicious activities were detected including failed login attempts, malware infections, and repeated activity from a suspicious IP (203.0.113.77). These findings suggest an active attack and potential system compromise requiring immediate response.

## 2. Timeline of Events

- 07/03/2025 04:23–09:02 → Multiple failed logins from different IPs (10.0.0.5, 172.16.0.3, 198.51.100.42) - 07/03/2025 05:42–09:10 → Malware detected (Trojan, Rootkit, Ransomware) affecting multiple users (bob, eve, david, charlie) - 07/03/2025 07:02–09:07 → IP 203.0.113.77 showed failed logins, connection attempts, file access, and malware activity

## 3. Threats Identified

1. Failed logins (Brute-force attempts) → Severity: Medium 2. Malware detected (Trojan/Rootkit/Ransomware) → Severity: High 3. Malicious IP 203.0.113.77 activity → Severity: Critical

## 4. Impact Assessment

- Risk of credential compromise due to brute-force attempts. - Malware infections suggest system breach and persistence mechanisms. - Malicious IP activity indicates potential lateral movement.

## 5. Recommendations

- Block IP 203.0.113.77 at the firewall immediately. - Reset credentials for compromised users (bob, eve, david, charlie). - Run endpoint malware scans and isolate infected machines. - Monitor Splunk dashboards for further anomalies. - Escalate incident to IR team for containment and forensics.

## 6. Stakeholder Communication (Sample Email)

**Subject:** Urgent Security Alert – Malware & Unauthorized Login Attempts Detected

Dear Team,

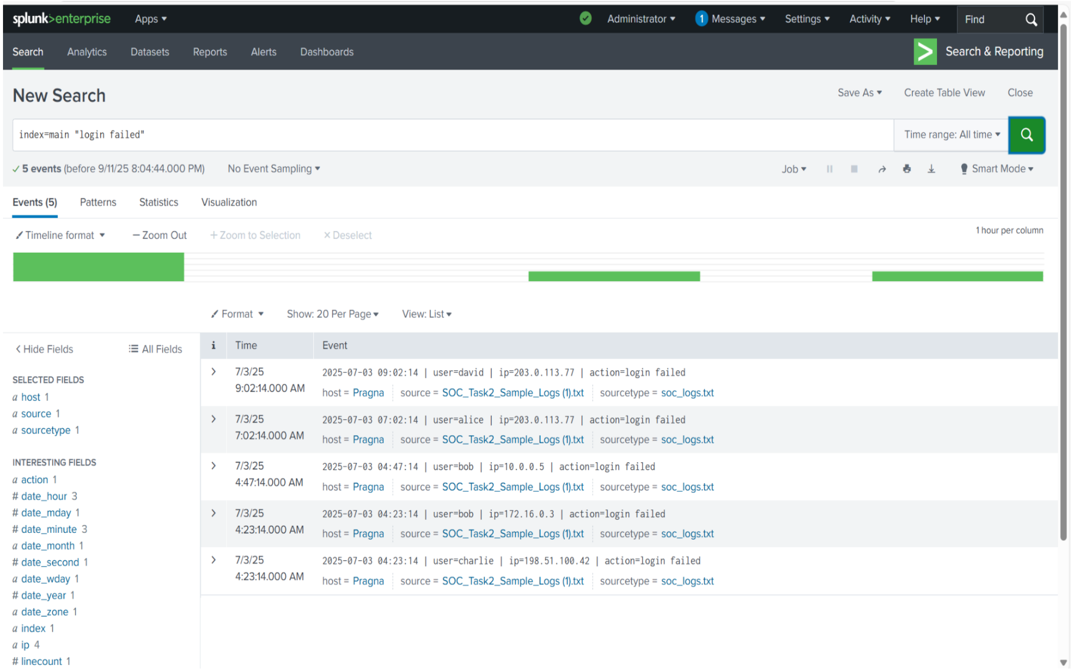
Our monitoring system (Splunk) detected multiple incidents:
1. Repeated failed logins across several user accounts.
2. Malware alerts (Trojan, Rootkit, Ransomware) on multiple endpoints.
3. Malicious activity traced to IP 203.0.113.77.

**Impact:** Potential compromise of user accounts and infected systems.
**Action Taken:** Initial containment steps include IP blocking, credential resets, and malware scans.

**Next Steps:** Recommend isolation of affected systems, forensic investigation, and escalation.

Best regards,
SOC Analyst

# Appendix – Evidence Screenshots



New Search

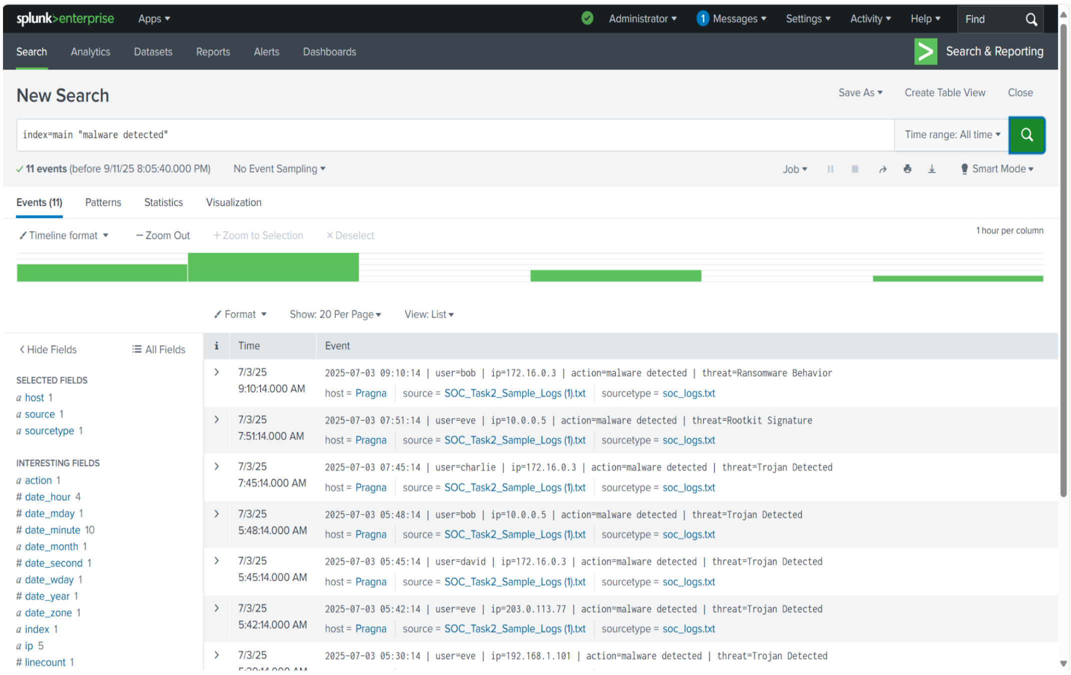
```
index=main "login failed"
```

✓ 5 events (before 9/11/25 8:04:44.000 PM)   No Event Sampling

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a action 1
- # date_hour 3
- # date_mday 1
- # date_minute 3
- a date_month 1
- # date_second 1
- a date_wday 1
- # date_year 1
- a date_zone 1
- a index 1
- a ip 4
- # linecount 1

```
i  Time              Event
>  7/3/25            2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
   9:02:14.000 AM    host = Pragna | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = soc_logs.txt
>  7/3/25            2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
   7:02:14.000 AM    host = Pragna | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = soc_logs.txt
>  7/3/25            2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed
   4:47:14.000 AM    host = Pragna | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = soc_logs.txt
>  7/3/25            2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login failed
   4:23:14.000 AM    host = Pragna | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = soc_logs.txt
>  7/3/25            2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed
   4:23:14.000 AM    host = Pragna | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = soc_logs.txt
```



New Search

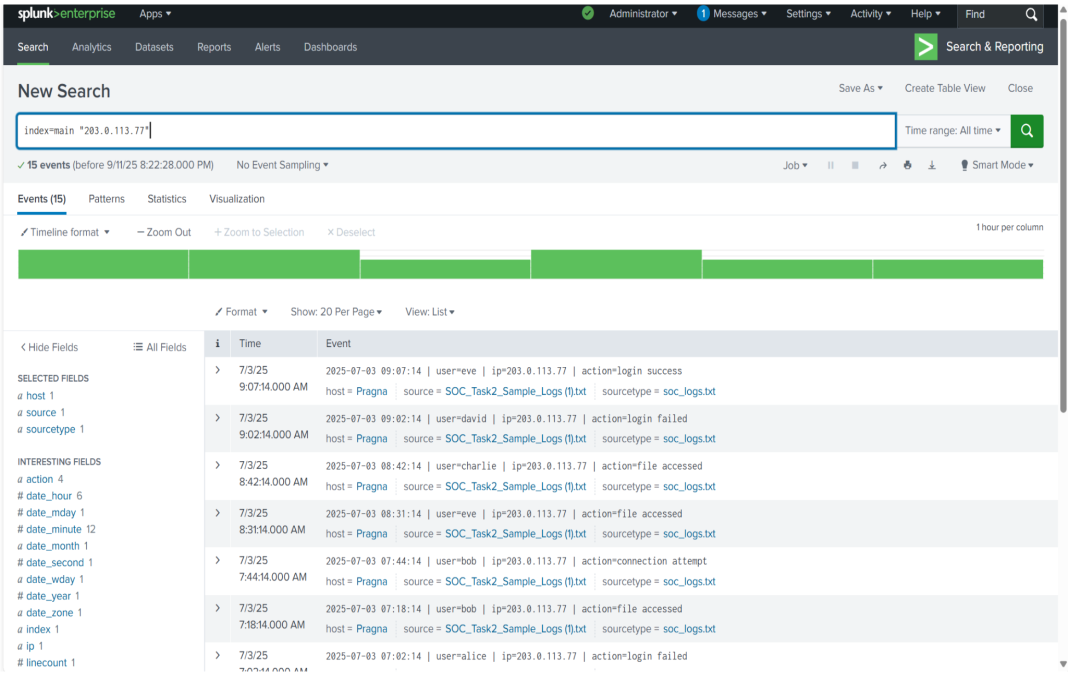
```
index=main "malware detected"
```

✓ 11 events (before 9/11/25 8:05:40.000 PM)   No Event Sampling

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a action 1
- # date_hour 4
- # date_mday 1
- # date_minute 10
- a date_month 1
- # date_second 1
- a date_wday 1
- # date_year 1
- a date_zone 1
- a index 1
- a ip 5
- # linecount 1

```
i  Time              Event
>  7/3/25            2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
   9:10:14.000 AM    host = Pragna | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = soc_logs.txt
>  7/3/25            2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
   7:51:14.000 AM    host = Pragna | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = soc_logs.txt
>  7/3/25            2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
   7:45:14.000 AM    host = Pragna | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = soc_logs.txt
>  7/3/25            2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
   5:48:14.000 AM    host = Pragna | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = soc_logs.txt
>  7/3/25            2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
   5:45:14.000 AM    host = Pragna | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = soc_logs.txt
>  7/3/25            2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
   5:42:14.000 AM    host = Pragna | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = soc_logs.txt
>  7/3/25            2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
```



New Search

```
index=main "203.0.113.77"
```

Time range: All time

✓ **15 events** (before 9/11/25 8:22:28.000 PM) No Event Sampling

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a action 4
- # date_hour 6
- # date_mday 1
- # date_minute 12
- a date_month 1
- # date_second 1
- a date_wday 1
- # date_year 1
- a date_zone 1
- a index 1
- a ip 1
- # linecount 1

| i | Time | Event |
|---|---|---|
| › | 7/3/25<br>9:07:14.000 AM | `2025-07-03 09:07:14 \| user=eve \| ip=203.0.113.77 \| action=login success`<br>host = Pragna source = SOC_Task2_Sample_Logs (1).txt sourcetype = soc_logs.txt |
| › | 7/3/25<br>9:02:14.000 AM | `2025-07-03 09:02:14 \| user=david \| ip=203.0.113.77 \| action=login failed`<br>host = Pragna source = SOC_Task2_Sample_Logs (1).txt sourcetype = soc_logs.txt |
| › | 7/3/25<br>8:42:14.000 AM | `2025-07-03 08:42:14 \| user=charlie \| ip=203.0.113.77 \| action=file accessed`<br>host = Pragna source = SOC_Task2_Sample_Logs (1).txt sourcetype = soc_logs.txt |
| › | 7/3/25<br>8:31:14.000 AM | `2025-07-03 08:31:14 \| user=eve \| ip=203.0.113.77 \| action=file accessed`<br>host = Pragna source = SOC_Task2_Sample_Logs (1).txt sourcetype = soc_logs.txt |
| › | 7/3/25<br>7:44:14.000 AM | `2025-07-03 07:44:14 \| user=bob \| ip=203.0.113.77 \| action=connection attempt`<br>host = Pragna source = SOC_Task2_Sample_Logs (1).txt sourcetype = soc_logs.txt |
| › | 7/3/25<br>7:18:14.000 AM | `2025-07-03 07:18:14 \| user=bob \| ip=203.0.113.77 \| action=file accessed`<br>host = Pragna source = SOC_Task2_Sample_Logs (1).txt sourcetype = soc_logs.txt |
| › | 7/3/25<br>7:02:14.000 AM | `2025-07-03 07:02:14 \| user=alice \| ip=203.0.113.77 \| action=login failed` |