Incident Response Report

Name: Nilesh Kisan Chavan

Date: 23 August 2025

Incident Title: Multiple Security Alerts Detected Through Splunk SIEM

Monitoring

Summary:

During routine log monitoring using Splunk SIEM, multiple suspicious activities were detected.

Findings & Evidence:

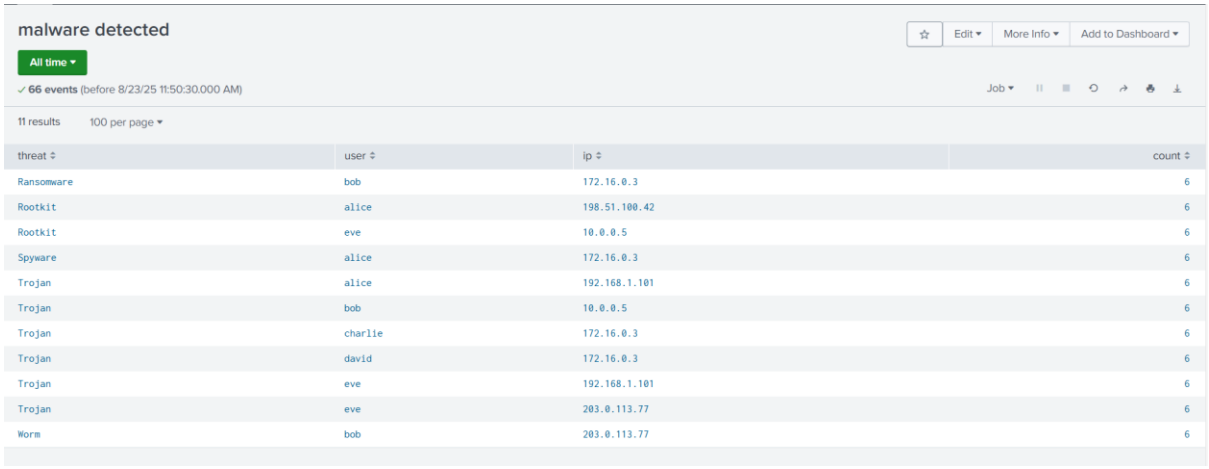
Malware detection alert:

Threat(ransomware,Rootkit,Trojan,Worm)

User(bob,alice,eve,)

IP(172.16.0.3),(198.51.100.42),(192.168.1.101),(203.0.113.77)

Count(6.6.6.6)



malware detected

All time ▾

✓ 66 events (before 8/23/25 11:50:30.000 AM)

☆ Edit ▾ More Info ▾ Add to Dashboard ▾

Job ▾

11 results 100 per page ▾

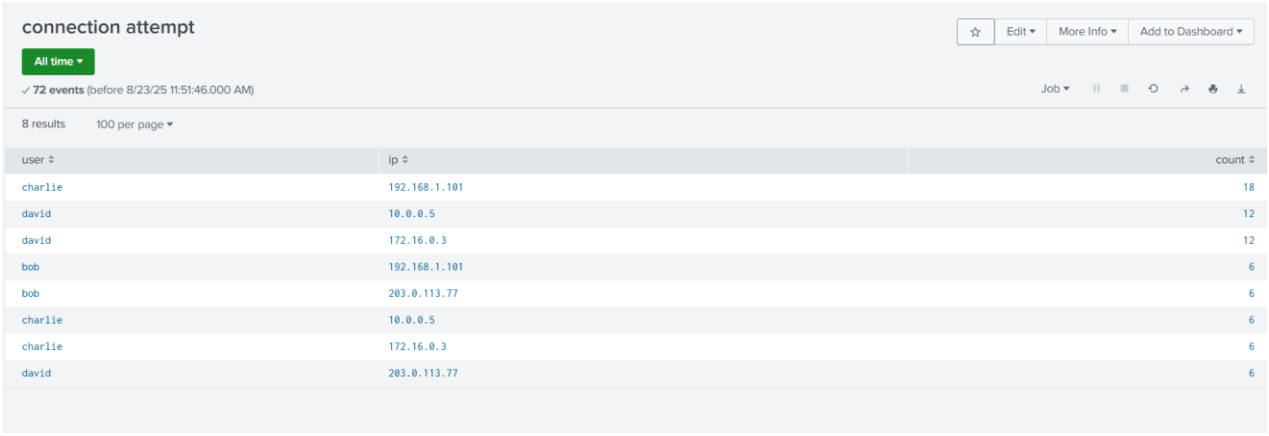
threat ≎	user ≎	ip ≎	count ≎
Ransomware	bob	172.16.0.3	6
Rootkit	alice	198.51.100.42	6
Rootkit	eve	10.0.0.5	6
Spyware	alice	172.16.0.3	6
Trojan	alice	192.168.1.101	6
Trojan	bob	10.0.0.5	6
Trojan	charlie	172.16.0.3	6
Trojan	david	172.16.0.3	6
Trojan	eve	192.168.1.101	6
Trojan	eve	203.0.113.77	6
Worm	bob	203.0.113.77	6

Connection attempt:

User(Charlie,David,bob)

IP(192.168.1.101),(10.0.0.5),(192.168.1.10 1)

Count(18,12,6)

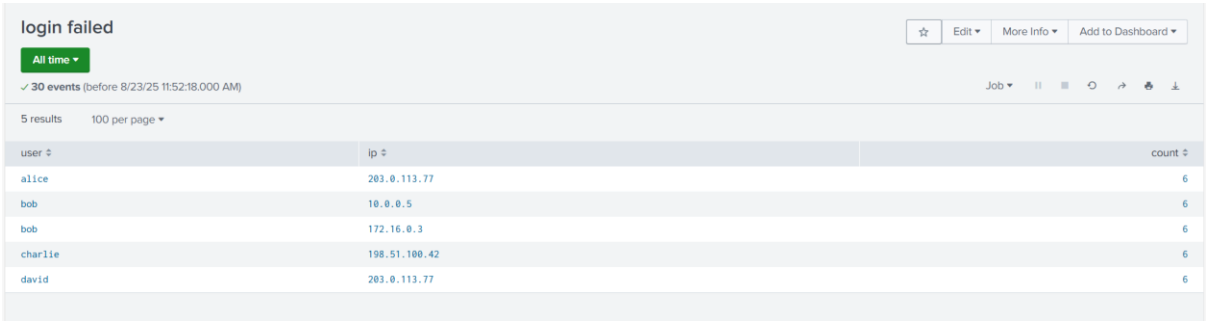


Login failed:

User(alice,bob,charlie,david)

IP(203.0.113.77),(10.0.0.5),(198.51.100.42),(203.0.113.77)

Count(6,6,6,6)



Impact & Risk Assessment:

Ransomware (bob – 172.16.0.3): High risk – could lead to encryption and data loss.

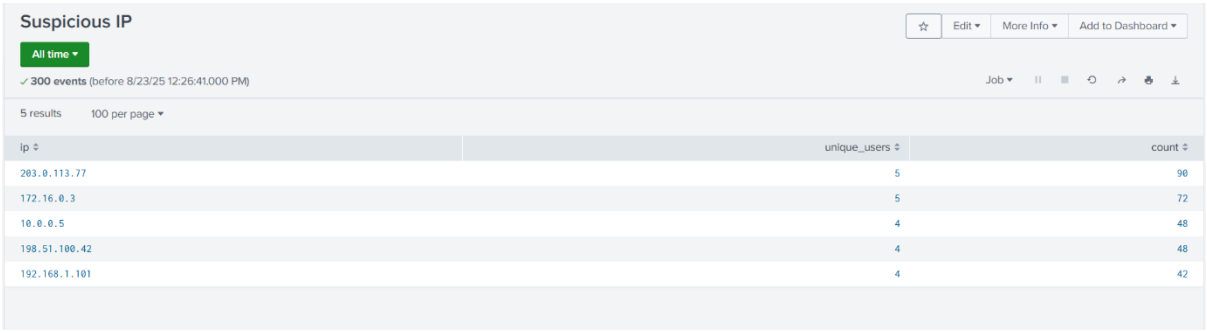
Rootkit (alice – 198.51.100.42, eve – 10.0.0.5): High risk – indicates stealthy persistence and privilege escalation.

Suspicious IP:

IP(203.0.113.77),(172.16.0.3),(10.0.0.5),(198.51.100.42),(192.168.1.101)

Unique_users(5,5,4,4,4)

Count(90,72,48,48,42)



ip	unique_users	count
203.0.113.77	5	90
172.16.0.3	5	72
10.0.0.5	4	48
198.51.100.42	4	48
192.168.1.101	4	42

➢ *Impact & Risk Assessment:*

- **Ransomware (bob – 172.16.0.3):** High risk – could lead to encryption and data loss.
- **Rootkit (alice – 198.51.100.42, eve – 10.0.0.5):** High risk – indicates stealthy persistence and privilege escalation
- **Charlie (192.168.1.101 – 18 attempts):** High risk – indicates repeated unauthorized access attempts on internal network.
- **David (10.0.0.5 & 172.16.0.3 – 12 attempts each):** Medium–High risk – possible brute-force or probing activity.
- **Alice (203.0.113.77 – 6 attempts):** Medium risk – possible unauthorized login attempt from external IP.
- **Bob (10.0.0.5 & 172.16.0.3 – 6 attempts each):** Medium–High risk – repeated failed attempts may indicate brute-force testing on internal systems.
- **203.0.113.77 (5 users – 90 events):** High risk – repeated suspicious activity from external IP across multiple accounts, possible brute-force or coordinated attack.
- **172.16.0.3 (5 users – 72 events):** High risk – internal IP generating multiple suspicious events, may indicate compromised host.

➢ Recommendations / Remediation:

- Isolate infected systems immediately (bob: 172.16.0.3 & 203.0.113.77, alice: 198.51.100.42, eve: 10.0.0.5 & 192.168.1.101, etc.).
- Perform full malware removal and forensic analysis on compromised endpoints.
- Block suspicious IPs (especially 203.0.113.77 – external source).
- Implement account lockout policies after repeated failed attempts.
- Reset credentials for affected accounts (Alice, Bob, Charlie, David).
- Enforce MFA on all critical user accounts to reduce brute-force success chances.
- Immediately block/blacklist external suspicious IPs (**203.0.113.77, 198.51.100.42**).
- Investigate internal hosts (**172.16.0.3, 10.0.0.5, 192.168.1.101**) for compromise indicators.

➢ **Conclusion:**

Splunk monitoring identified multiple security incidents requiring immediate mitigation steps.

Prepared by: Nilesh kisan Chavan