

## Security Incident Report – Malware & Lateral Movement Analysis

Analyst: Piyush Bansal

SIEM Platform: Splunk

Incident Type: Malware Infection & Suspected Lateral Movement

Status: Completed Investigation (Simulated Environment)

### Executive Summary

During analysis of simulated security logs using Splunk SIEM, multiple high-severity malware detections were identified across several user accounts and IP addresses. Correlation analysis revealed that the same internal and external IP addresses were associated with multiple user accounts, which is abnormal behavior and indicative of a compromised host or lateral movement within the environment.

Multiple malware families were detected over a short time span, suggesting post-exploitation activity rather than isolated infections. While direct user impersonation cannot be conclusively proven, the evidence strongly supports a coordinated security incident affecting multiple systems.

### Incident Overview

| Field | Details |

Incident Category | Malware / Lateral Movement |

Detection Method | Splunk SIEM Log Analysis |

Affected Users | alice, bob, charlie, david, eve |

Observed Malware | Trojan, Spyware, Rootkit, Worm |

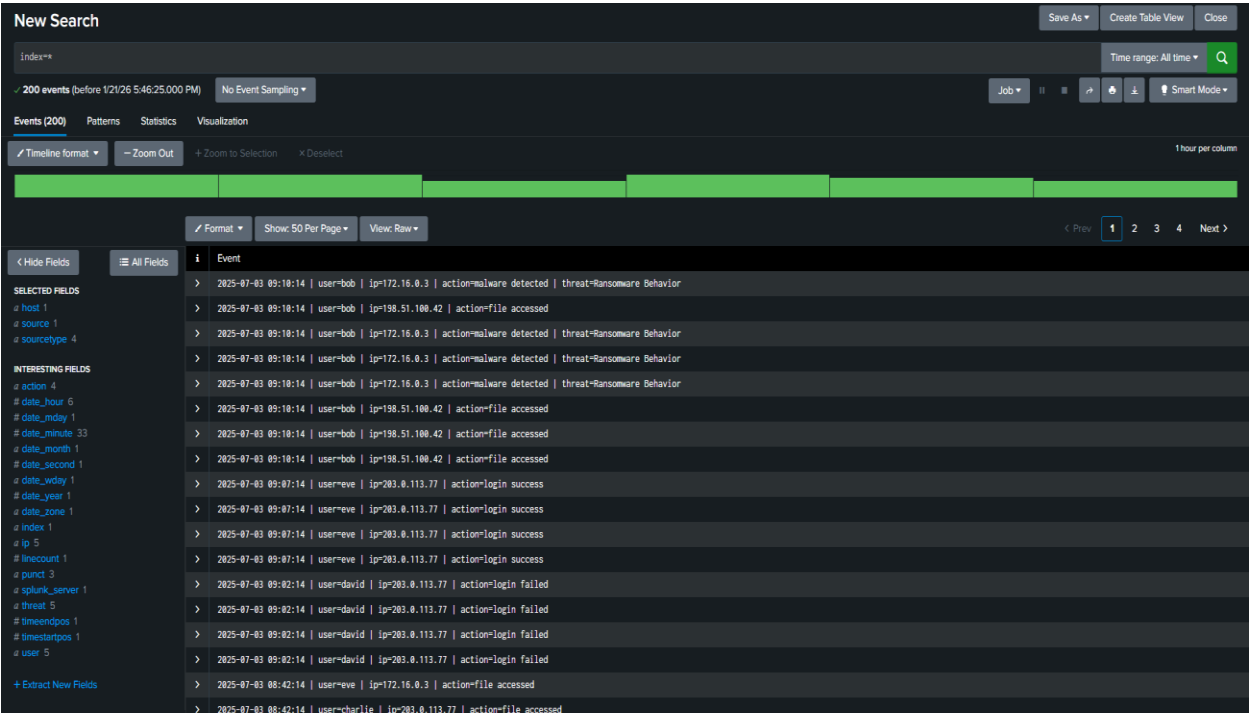
Initial Severity | High |

Final Severity |  High |

Confidence Level | High |

 Data Sources Analyzed

- Authentication logs
- Connection attempt logs
- File access logs
- Malware detection logs



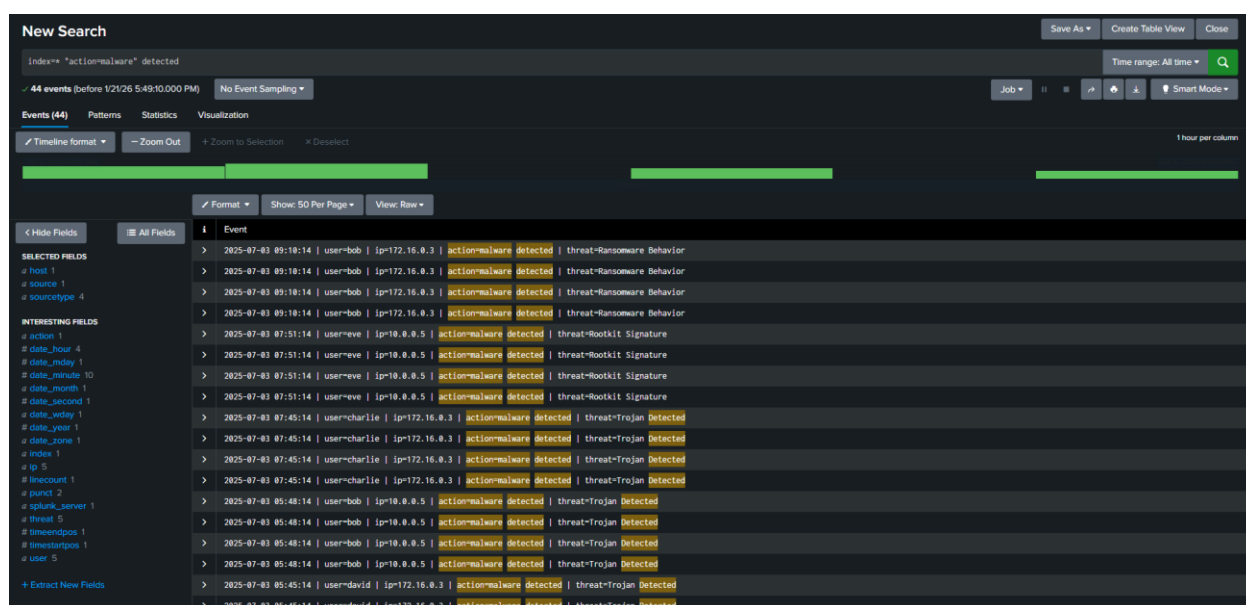
 Key Findings

1. Malware Detections

Multiple malware alerts were detected across different users and IP addresses, including:

- Trojan Detected
- Spyware Alert
- Rootkit Signature
- Worm Infection Attempt

These detections occurred within close time proximity, suggesting an active compromise rather than false positives.



## 2. IP Reuse Across Multiple Users

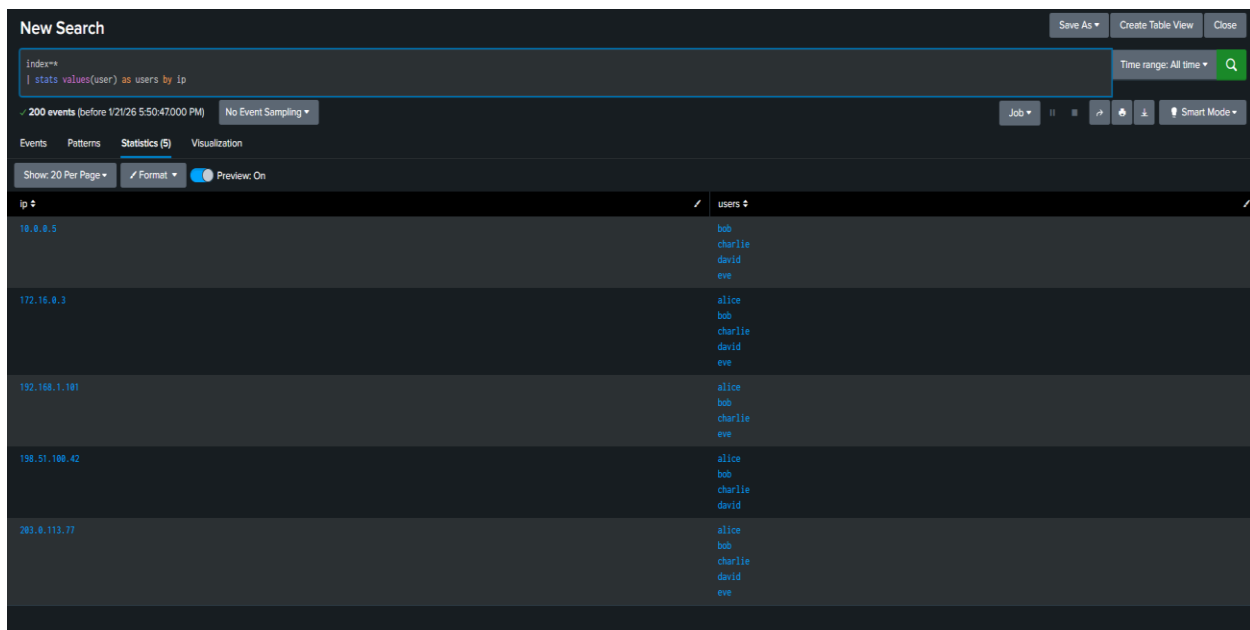
Correlation analysis showed that the same IP addresses were associated with multiple user accounts:

- 10.0.0.5 → bob, charlie, david, eve
- 172.16.0.3 → alice, bob, charlie, david, eve

- 203.0.113.77 → alice, bob, charlie, david, eve

This behavior is inconsistent with normal user activity and strongly suggests:

- A shared compromised host
- Lateral movement within the network
- Or centralized attacker infrastructure



The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Contains the query `index=* | stats values(user) as users by ip`. The time range is set to "All time".
- Results:** 200 events (before 1/21/26 5:50:47000 PM). The table is displayed in "Statistics (5)" view.
- Table Columns:** "ip" and "users".
- Table Data:**

| ip            | users                                   |
|---------------|---|
| 19.0.0.5      | bob<br>charlie<br>david<br>eve          |
| 172.16.0.3    | alice<br>bob<br>charlie<br>david<br>eve |
| 192.168.1.101 | alice<br>bob<br>charlie<br>eve          |
| 198.51.100.42 | alice<br>bob<br>charlie<br>david        |
| 203.0.113.77  | alice<br>bob<br>charlie<br>david<br>eve |

### 3. Malware Sequence Pattern

The order of malware detections indicates a possible attack lifecycle:

1. Initial Trojan infection
2. Spyware deployment for monitoring
3. Rootkit installation for persistence
4. Worm activity indicating spread attempts

This pattern aligns with known post-exploitation techniques.

## Severity Assessment

| Threat Activity | Severity | Reason |

Multiple malware detections | High | Confirmed Compromise

Same IP across users | High | Indicates lateral movement |

Rootkit detection | Critical | Persistence & stealth |

Worm activity | Critical | Propagation risk |

Overall Incident Severity:  High

## Impact Analysis

Potential impacts include:

- Compromise of multiple user accounts
- Persistence via rootkit installation
- Risk of lateral movement across systems
- Potential data exposure (not confirmed in logs)

No direct evidence of data exfiltration was observed in the dataset analyzed.

## Recommended Response Actions

### Immediate Actions

- Isolate affected hosts from the network

- Disable or reset credentials for impacted users
- Block malicious IP addresses

#### Short-Term Actions

- Conduct full endpoint malware scans
- Review authentication and access logs
- Increase SIEM alert sensitivity for malware events

#### Long-Term Actions

- Implement network segmentation
- Enable endpoint detection & response (EDR)
- Deploy automated SIEM alerts and SOC playbooks

#### Stakeholder Communication Summary

##### Summary:

Security monitoring detected coordinated malware activity affecting multiple users and systems. Immediate containment actions are recommended to prevent further spread.

##### Business Impact:

Currently assessed as **moderate to high risk** due to malware persistence and lateral movement potential.



## Conclusion

This investigation demonstrates real-world SOC practices including log analysis, correlation, severity assessment, and incident documentation using Splunk SIEM. The findings indicate a high-confidence security incident involving malware infections and suspected lateral movement across multiple systems. The project reflects practical SOC analyst skills aligned with professional security operations workflows.