LOG ANALYSIS & THREAT MITIGATION STRATEGY

SUBMITTED TO: CYBER SECURITY INTERNSHIP PROGRAM

FUTURE INTERNS

SUBMITTED BY: ZANNU OPEYEMI EMMANUEL *SOC ANALYST*

CYBERSECURITY INTERN

DATE: DECEMBER 2025

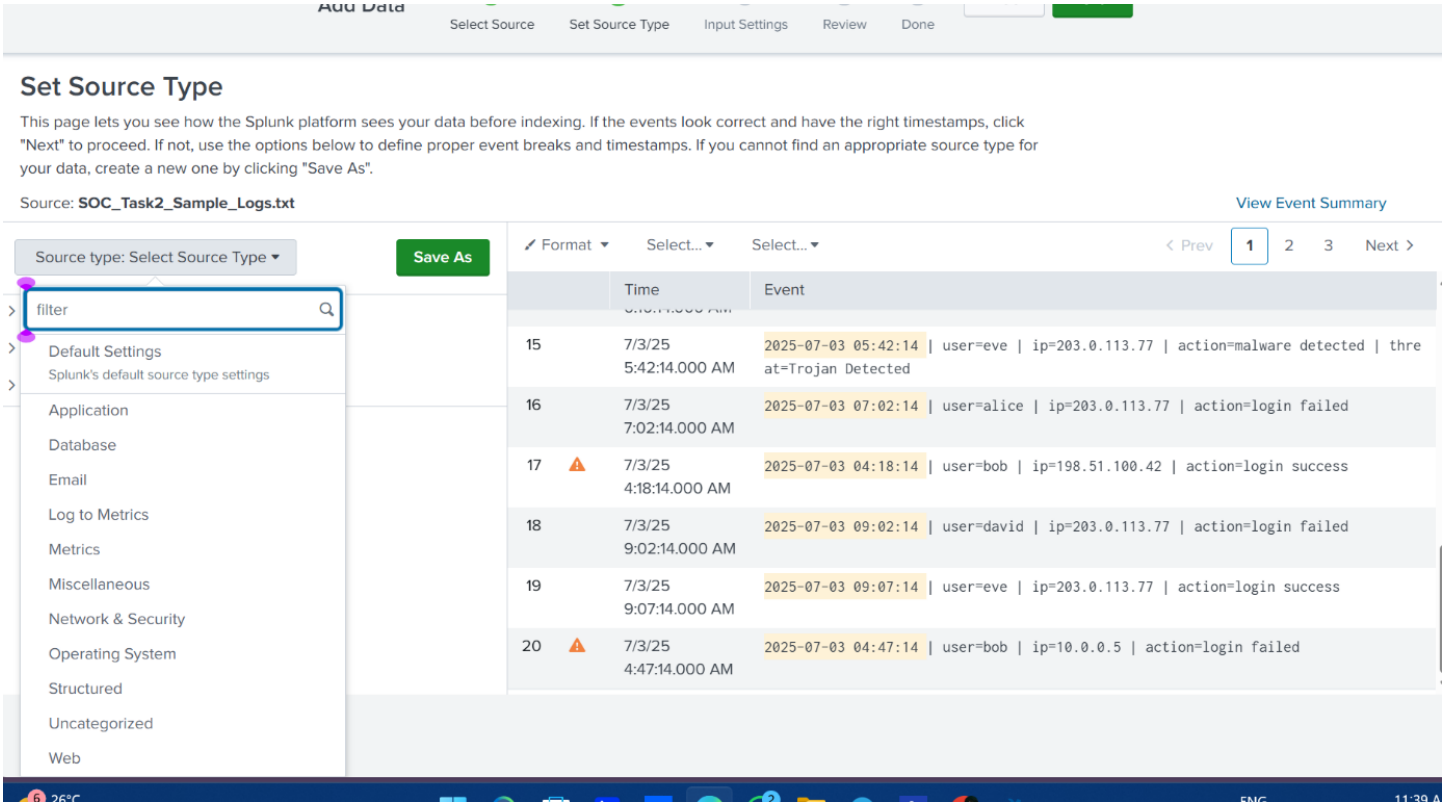
TOOL USED: SPLUNK SIEM

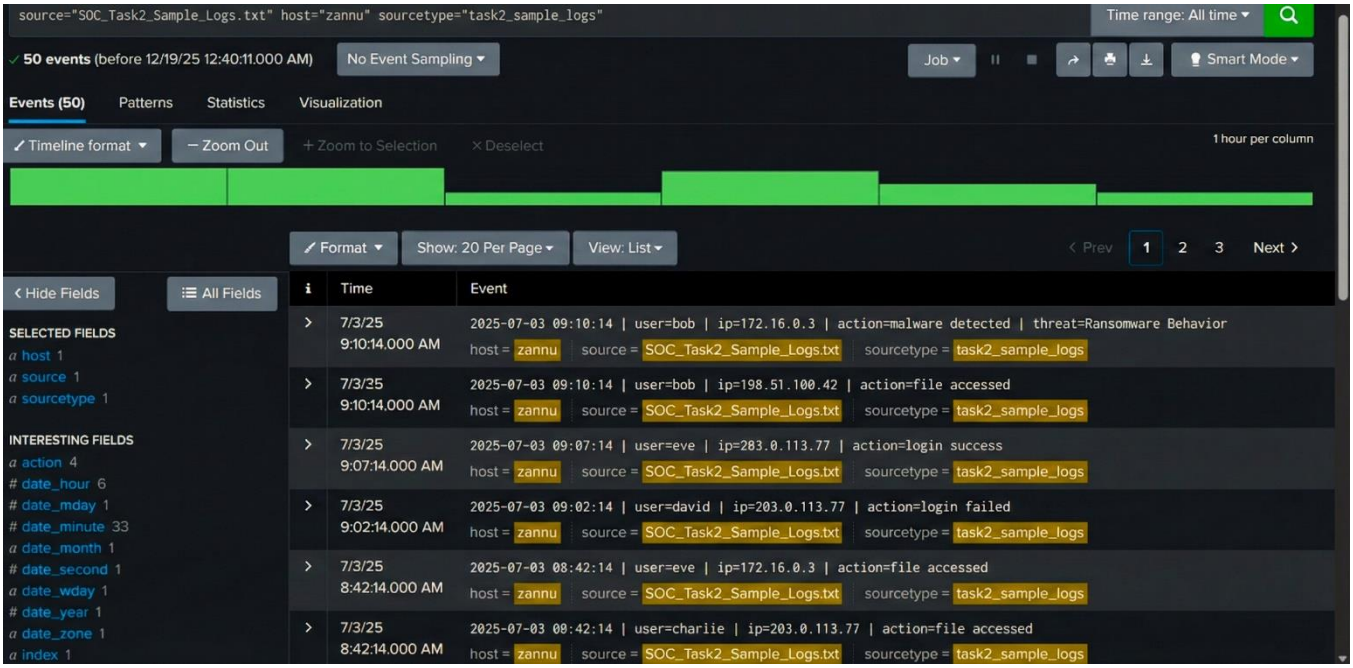
SUBJECT: FORENSIC ANALYSIS OF SIMULATED NETWORK

COMPROMISE (IR-2025-07-03-001)

INTRODUCTION:

This document details the forensic analysis of anomalous system logs captured within the organization's Security Operations Center (SOC). The primary objective is to detect potential security breaches, categorize them by severity level, and formulate effective remediation strategies. Utilizing **Splunk** for log correlation and analysis, this investigation successfully identified various malicious activities, including ransomware behavior, rootkits, Trojans, spyware, and worm propagation attempts.





SCOPE OF DATA ANALYSIS:

- Network & System Logs: Analysis of connection attempts and file access records.
- Authentication Events: Review of successful logins and failed access attempts.
- Security Alerts: Investigation of malware signatures, including Trojans, Rootkits, and Ransomware indicators.

INCIDENT SUMMARY:

A correlation analysis of system logs within the **Splunk SIEM** environment identified a cluster of 22 distinct malware alerts. These alerts, which originated from recurring IP addresses and targeted multiple user accounts, were aggregated and treated as a single, coordinated security incident.

INCIDENT CLASSIFICATION: MALWARE INFECTION

- Severity Level: High
- Detection Vector: Splunk SIEM
- Total Events: 22

KEY FINDINGS:

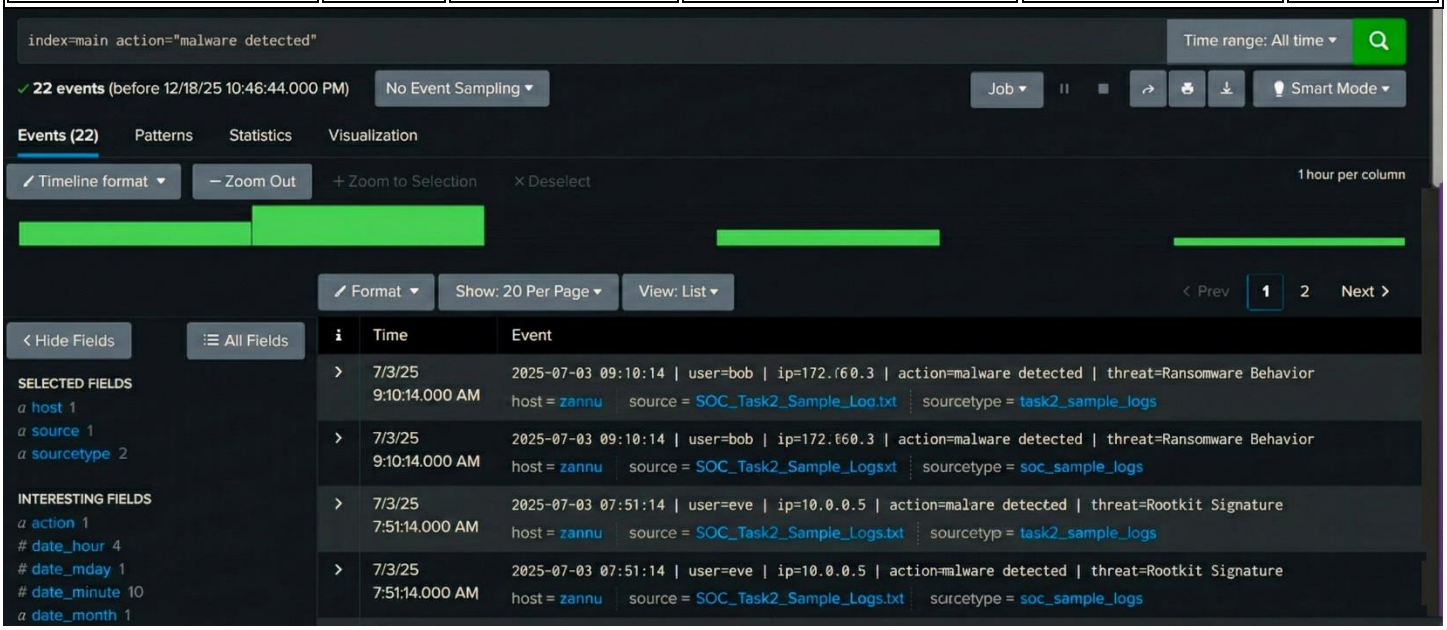
- Malware Detection: Analysis confirmed the presence of distinct malware families, specifically Trojan and Ransomware signatures.
- Indicators of Compromise (IoCs): Traffic analysis highlighted recurrent activity from specific IP addresses, identifying them as compromised endpoints requiring immediate isolation.
- Scope of Impact: The attack was not isolated to a single entity; evidence suggests widespread compromise affecting multiple user accounts across the network.

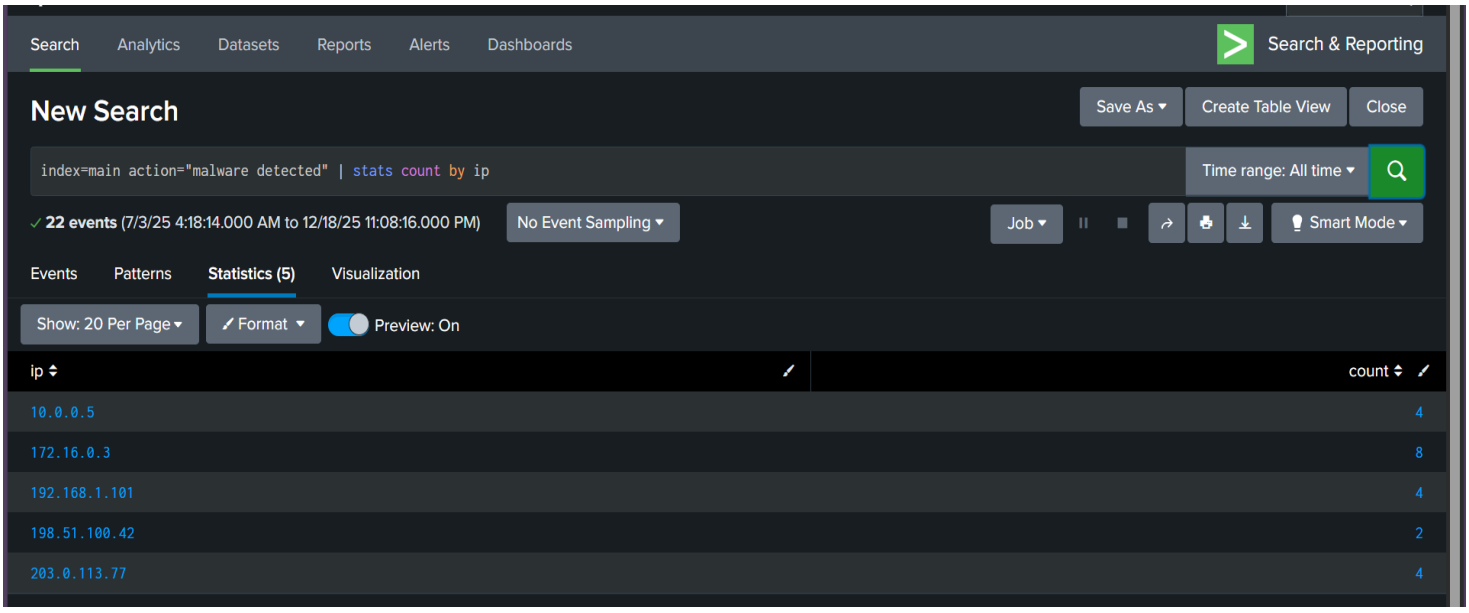
SUSPICIOUS ALERTS IDENTIFIED:

- Suspicious Activity Timeline & Frequency: The forensic analysis focused on log activity recorded between 04:19 AM and 09:10 AM on July 3, 2025.
- Top Suspicious IPs by Alert Volume: The following IP addresses were identified as the primary sources of malicious alerts:
  - 172.16.0.3: 8 Alerts (Highest Volume)
  - 10.0.0.5: 4 Alerts
  - 192.168.1.101: 4 Alerts
  - 203.0.113.77: 4 Alerts
  - 198.51.100.42: 2 Alerts

Timestamp	User	IP Address	Threat Type	Action	Priority
2025-07-03 09:10:14	bob	172.16.0.3	Ransomware Behavior	Malware Detected	High
2025-07-03 07:51:14	eve	10.0.0.5	Rootkit Signature	Malware Detected	High
2025-07-03 07:45:14	charlie	172.16.0.3	Trojan Detected	Malware Detected	Medium

Timestamp	User	IP Address	Threat Type	Action	Priority
2025-07-03 05:48:14	bob	10.0.0.5	Trojan Detected	Malware Detected	Medium
2025-07-03 05:42:14	eve	203.0.113.77	Trojan Detected	Malware Detected	Medium



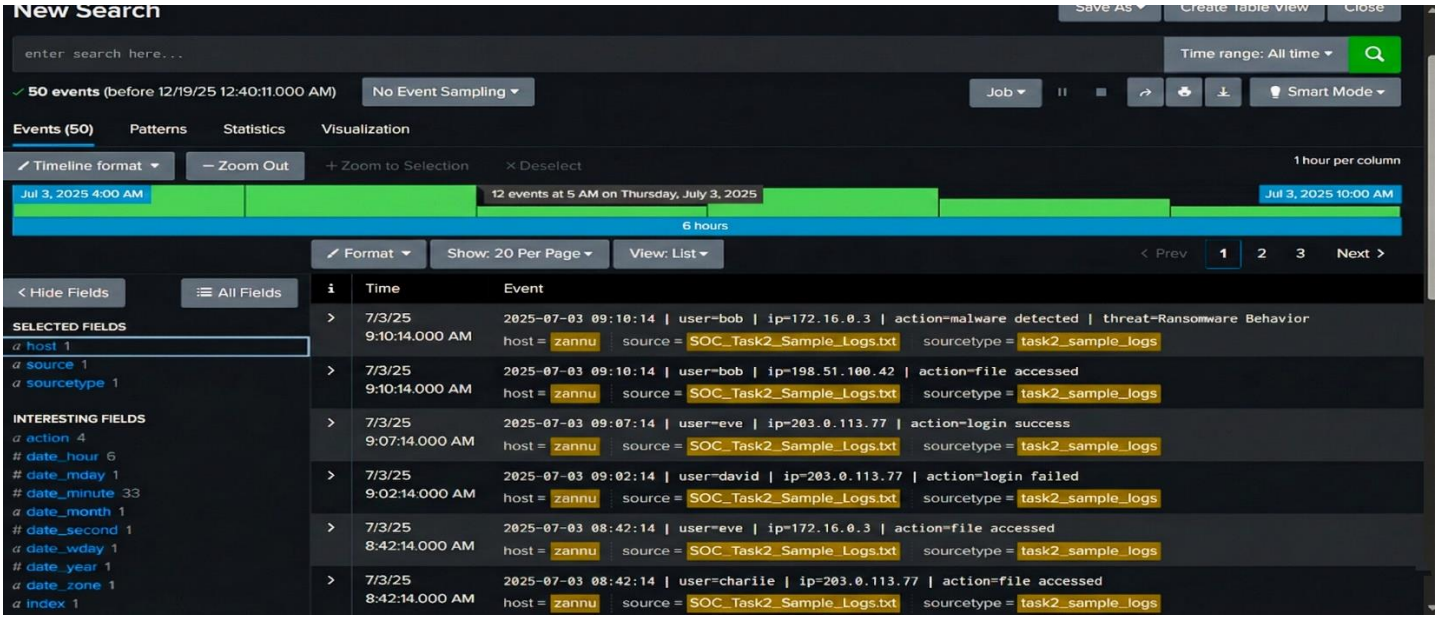


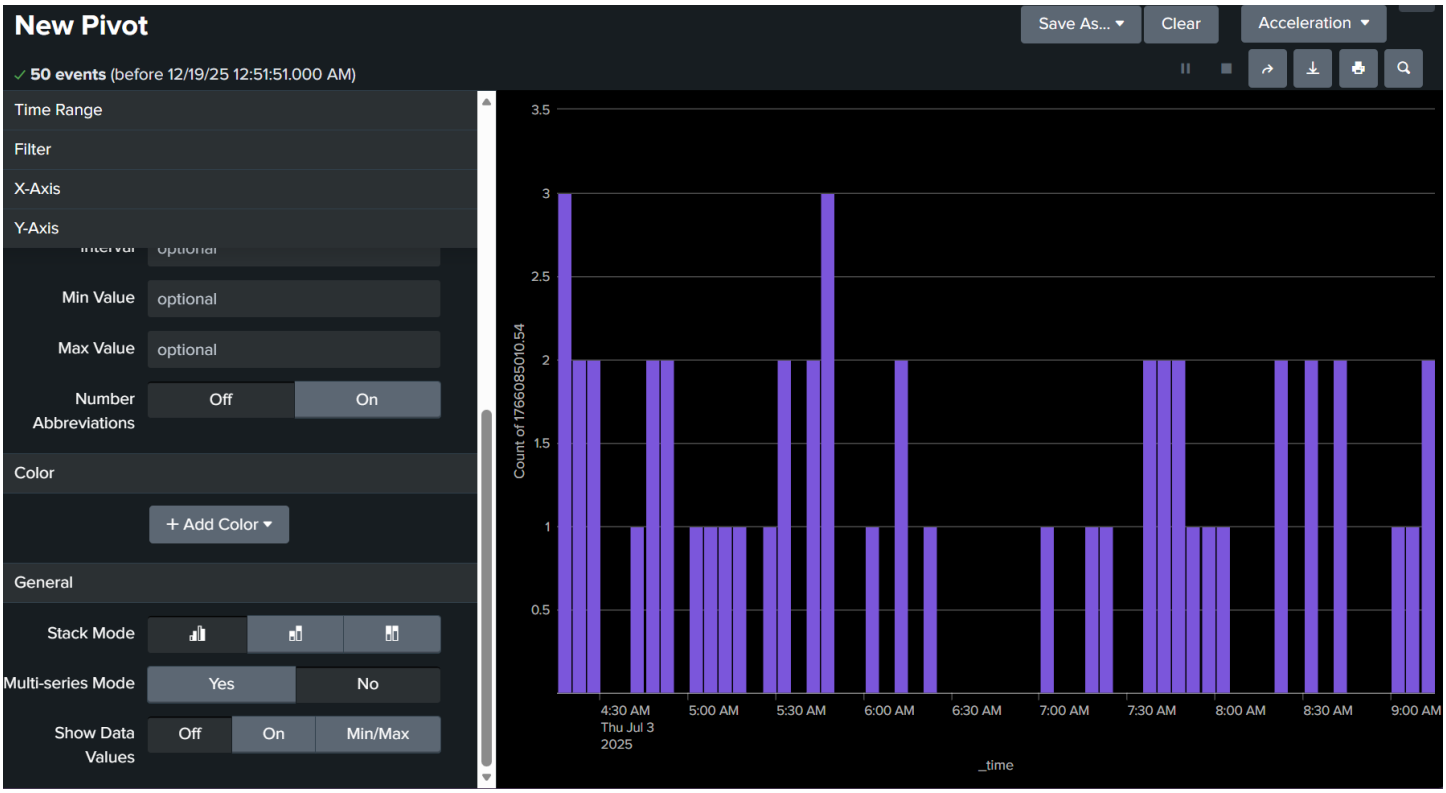
TIMELINE OF INCIDENTS:

Timestamp	Event Description	Source IP	User
2025-07-03 04:19	Rootkit Detected (Initial Access)	198.51.100.42	Alice
2025-07-03 04:29	Trojan Detected (Payload Execution)	192.168.1.101	Alice
2025-07-03 05:06	Worm Infection Attempt (Lateral Movement)	203.0.113.77	Bob
2025-07-03 05:42	Trojan Detected (Persistence)	203.0.113.77	Eve
2025-07-03 09:10	Ransomware Behavior (Action on Objectives)	172.16.0.3	Bob

TIMELINE OF COMPROMISE:

Malicious activity was observed over a continuous period on **July 3, 2025**. The first indicator of compromise (IoC) was logged at **04:19 AM**, with the final critical escalation recorded at **09:10 AM**, demonstrating sustained engagement by the attacker.





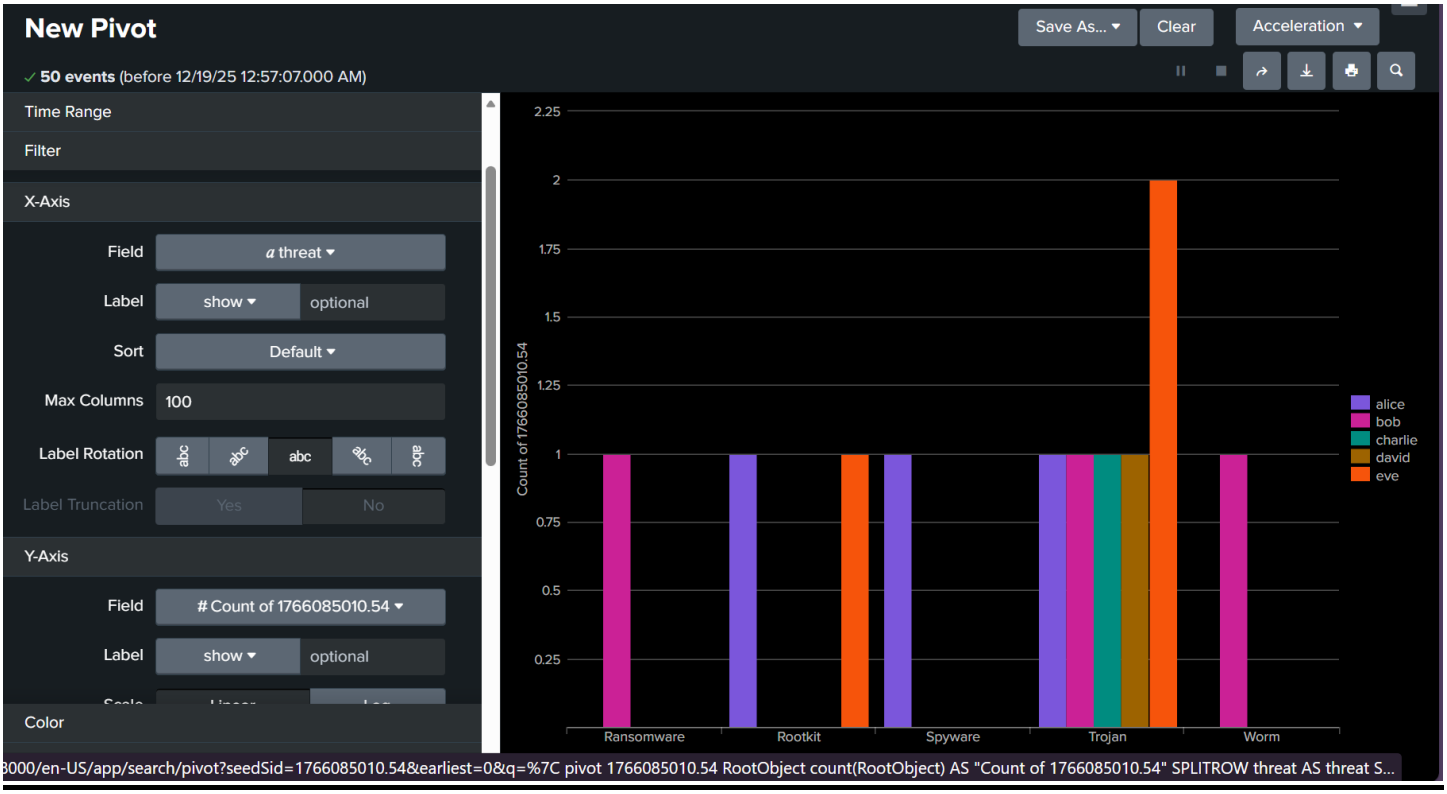
INCIDENT CLASSIFICATION & IMPACT ANALYSIS:

Priority	Threat Type	Impact Assessment	Remediation Strategy
High	Ransomware, Rootkit	Critical System Compromise: High risk of irreversible data encryption (Ransomware) and deep-system persistence (Rootkit), leading to potential full data loss.	Immediate Isolation: Disconnect infected hosts from the network. Force password resets for all affected users. Initiate forensic imaging and restoration from backups.
Medium	Trojan, Worm	Lateral Movement Risk: Evidence of unauthorized backdoor access (Trojan) and attempts to propagate	Containment & Eradication: Block malicious IPs at the firewall. Perform full anti-malware scans on

Priority	Threat Type	Impact Assessment	Remediation Strategy
		across the network (Worm).	**endpoints. Investigate propagation vectors.**
Low	**Spyware**	**Data Privacy Risk: Potential for passive surveillance, keylogging, or unauthorized data collection (Exfiltration).**	**Sanitization: Update antivirus signatures and remove spyware. Review user activity logs for data leakage.**

OPERATIONAL IMPACT ANALYSIS:

The incident resulted in widespread compromise across multiple endpoints and user profiles. The confirmed presence of ransomware and rootkits posed a critical threat to the organization's Confidentiality, Integrity, and Availability (CIA). Specifically, the malicious activity introduced high risks of irreversible data loss (via encryption), deep system compromise, and significant disruption to business services.



REMEDIATION & MITIGATION ACTIONS TAKEN:

- Containment: Immediately isolated compromised endpoints from the corporate network to prevent lateral movement and further data exfiltration.
- Perimeter Defense: Updated firewall configurations to block traffic to and from identified malicious IP addresses.
- Eradication: Executed comprehensive anti-malware and antivirus scans on all affected assets to identify and remove malicious payloads.
- System Hardening: Applied critical system and software security patches to close vulnerabilities exploited during the attack.
- Future Prevention: Initiated targeted user security awareness training to reinforce best practices regarding phishing and suspicious file handling.

CONCLUSION:

The forensic analysis conducted for SOC Task 2 successfully uncovered a complex threat landscape, identifying critical malicious activities including **ransomware behavior**, **rootkit persistence**, **Trojan infections**, and **worm propagation attempts**. Given the severity of these findings, the incidents were classified as **High Priority**, necessitating immediate and targeted remediation strategies. To ensure long-term security and preventing future compromise, the implementation of continuous network monitoring and a rapid incident response framework is strongly recommended.