Incident Response Report

# 1. Incident Metadata

Incident ID: SOC-2025-07-03-01

Reported By: Nitin Bhatt (SOC Analyst Intern)

Date: 2025-07-03

Tool Used: Splunk (Free Trial)

Log Source: SOC\_Task2\_Sample\_Logs.txt

# 2. Executive Summary

During routine monitoring on July 3, 2025, several suspicious events were identified from simulated log data. These included multiple malware detections, failed login attempts from various users, and access from non-standard IP addresses. The incidents were analyzed and prioritized based on potential impact and threat indicators.

# 3. Indicators of Compromise (IOCs)

|  |  |  |  |
| --- | --- | --- | --- |
| Timestamp | User | IP Address | Alert Type |
| 2025-07-03 05:48:14 | bob | 10.0.0.5 | Malware Detected - Trojan |
| 2025-07-03 07:02:14 | alice | 203.0.113.77 | Login Failed |
| 2025-07-03 04:29:14 | alice | 192.168.1.101 | Malware Detected - Trojan |
| 2025-07-03 07:45:14 | charlie | 172.16.0.3 | Malware Detected - Trojan |
| 2025-07-03 05:06:14 | bob | 203.0.113.77 | Malware Detected - Worm |

# 4. Timeline of Events

- 04:29 - Malware (Trojan) detected on Alice’s machine (192.168.1.101)

- 05:06 - Bob’s system triggered malware alert for Worm infection (203.0.113.77)

- 05:48 - Another malware alert (Trojan) from Bob (10.0.0.5)

- 07:02 - Alice login failed from IP 203.0.113.77

- 07:45 - Charlie’s system detected Trojan (172.16.0.3)

# 5. Impact Assessment

The incidents suggest possible system compromise, especially on Bob and Alice's accounts due to repeated malware alerts. Failed login attempts and suspicious IP usage indicate possible brute-force or lateral movement activities. These incidents should be treated with high priority, especially the malware infections.

# 6. Alert Classification

|  |  |  |
| --- | --- | --- |
| Alert Description | Severity | Reason |
| Multiple malware detections from Bob | High | Indicates active threat on system |
| Login failure from Alice's account | Medium | Possible brute-force attempt |
| Trojan detected on Charlie's system | High | Requires immediate isolation |
| Malware detection on Alice's machine | High | System compromise likely |
| Worm alert on Bob’s IP | High | Propagation risk to network |

# 7. Remediation Recommendations

- Isolate systems showing malware alerts.  
- Conduct full malware scans on affected IPs.  
- Block suspicious external IPs temporarily.  
- Enforce multi-factor authentication (MFA).  
- Update all antivirus and endpoint protection systems.  
- Review user activity and access logs for deeper forensics.

# 8. Stakeholder Communication Summary

An internal communication draft has been prepared to report the above incident to relevant stakeholders, outlining the timeline, severity, and immediate next steps. This ensures transparency and quick containment of potential threats.