Incident Response Report

1. Executive Summary

On 3rd July 2025, multiple security events were detected across internal IP ranges and external access points. These events included successful and failed logins, malware detections (Trojan, Worm, Rootkit, Ransomware, Spyware), and suspicious file access activity. The incidents involve multiple users and raise concerns of lateral movement and data compromise.

2. Scope of Investigation

Date Range: 3 July 2025

Users Involved: alice, bob, charlie, david, eve

Assets/IPs Involved: 10.0.0.5, 172.16.0.3, 192.168.1.101, 198.51.100.42, 203.0.113.77

3. Key Indicators of Compromise (IoCs)

Time (UTC)	User	IP Address	Action	Details
05:48:14	bob	10.0.0.5	malware detected	Trojan Detected
05:30:14	eve	192.168.1.101	malware detected	Trojan Detected
04:19:14	alice	198.51.100.42	malware detected	Rootkit Signature
05:06:14	bob	203.0.113.77	malware detected	Worm Infection Attempt
07:45:14	charlie	172.16.0.3	malware detected	Trojan Detected
05:45:14	david	172.16.0.3	malware detected	Trojan Detected
07:51:14	eve	10.0.0.5	malware detected	Rootkit Signature
04:41:14	alice	172.16.0.3	malware detected	Spyware Alert
09:10:14	bob	172.16.0.3	malware detected	Ransomware Behavior

4. Suspicious Login and Access Patterns

- Multiple login successes from different users on same IPs (e.g., 203.0.113.77 and 172.16.0.3), indicating possible shared access or compromise.
- Failed logins and subsequent success raise concerns of brute-force or credential stuffing.
- Frequent file access by potentially infected users like bob, david, eve.

5. Initial Containment Actions

Incident Response Report

- Isolated affected IPs (10.0.0.5, 172.16.0.3, 198.51.100.42) from the network.
- Revoked access credentials for users: bob, eve, charlie.
- Notified incident response team for forensic analysis.

6. Malware Details

- Trojan Detected: High severity, capable of data exfiltration.
- Rootkit: Stealthy persistence threat.
- Ransomware Behavior: High impact, data encryption.
- Spyware: Potential data leak via surveillance.
- Worm Infection: Propagation concern across internal network.

7. Recommendations

- Perform full malware scan across all endpoints involved.
- Enforce multi-factor authentication (MFA) for all users.
- Conduct password resets for impacted accounts.
- Patch systems and update antivirus signatures.
- Review audit logs for lateral movement and privilege escalation.

8. Lessons Learned

- Early malware detection mechanisms worked but response delay allowed lateral movement.
- Segmentation of internal network could have limited spread.
- Need to review access controls and implement behavior-based monitoring.