**INCIDENT RESPONSE REPORT**

**SOC Task 2 - Security Alert Analysis**

**Date: 15th October, 2025**

**Analyst: Olaiya Ireoluwatomiwa.**

**SUMMARY**

Between 04:19 and 09:10 on July 3, 2025, the Security Operations Centre detected multiple high-severity security incidents, including 11 malware infections across 5 user accounts and 5 failed login attempts from suspicious IP addresses. Immediate containment actions are required.

**KEY FINDINGS**

• 11 malware infections detected across all monitored users

• Multiple malware types: Trojan (6), Rootkit (2), Ransomware (1),

Spyware (1), Worm (1)

• 5 failed login attempts from suspicious IP addresses

• All monitored users (Alice, Bob, Charlie, David, Eve) affected

• Suspicious IPs: 203.0.113.77, 10.0.0.5, 198.51.100.42

**INCIDENT TIMELINE - TOP 8 ALERTS**

**HIGH PRIORITY ALERTS:**

2025-07-03 04:19:14 - user=alice @ 198.51.100.42 - Rootkit Signature

2025-07-03 04:29:14 - user=alice @ 192.168.1.101 - Trojan Detected

2025-07-03 04:41:14 - user=alice @ 172.16.0.3 - Spyware Alert

2025-07-03 05:45:14 - user=david @ 172.16.0.3 - Trojan Detected

2025-07-03 05:48:14 - user=bob @ 10.0.0.5 - Trojan Detected

**MEDIUM PRIORITY ALERTS:**

2025-07-03 07:02:14 - user=alice @ 203.0.113.77 - Login Failed

2025-07-03 09:02:14 - user=david @ 203.0.113.77 - Login Failed

2025-07-03 04:47:14 - user=bob @ 10.0.0.5 - Login Failed

**IMPACT ASSESSMENT**

**RISK LEVEL: HIGH**

• Data Exfiltration Risk: Multiple file access events from compromised accounts

• System Integrity: Rootkits and ransomware pose critical system threats

• Business Continuity: Ransomware detection indicates potential service disruption

• Credential Security: Multiple failed logins suggest brute-force attempts

**REMEDIATION RECOMMENDATIONS**

**IMMEDIATE CORRECTIVE ACTIONS (0-2 Hours)**

**CONTAINMENT MEASURES:**

**✅ 1. Network Isolation**

• Block malicious IP 203.0.113.77 at firewall

• Quarantine systems with IPs: 10.0.0.5, 172.16.0.3

• Disable network access for compromised accounts

**✅ 2. Account Security**

• Force immediate password reset for users: Alice, Bob, Charlie, David, Eve

• Temporarily suspend accounts with multiple malware detections

• Revoke active sessions for affected users

✅ **3. Endpoint Protection**

• Isolate endpoints with ransomware detection immediately

• Initiate full system scans on infected machines

• Deploy emergency antivirus signatures

**SHORT-TERM CORRECTIVE MEASURES (2-8 Hours)**

**INVESTIGATION & REMEDIATION:**

**🔍 4. Forensic Analysis**

• Capture memory dumps from infected systems

• Analyze rootkit infection depth and persistence mechanisms

• Determine initial attack vector and entry point

**🔍 5. Malware Eradication**

• Deploy specialized rootkit removal tools

• Execute ransomware decryption tools if available

• Remove Trojan backdoors and spyware components

**🔍 6. System Restoration**

• Restore clean systems from known good backups

• Rebuild compromised endpoints with updated images

• Verify system integrity before reconnecting to the network

**LONG-TERM CORRECTIVE MEASURES (24-72 Hours)**

**PREVENTION & HARDENING:**

**🛡️ 7. Security Controls Enhancement**

• Implement multi-factor authentication for all user accounts

• Deploy advanced endpoint detection and response (EDR) solutions

• Enhance firewall rules to block known malicious IP ranges

**🛡️ 8. Access Control Improvements**

• Implement principle of least privilege for user accounts

• Deploy application whitelisting policies

• Enhance monitoring of privileged account usage

**🛡️ 9. Network Security**

• Segment network to limit lateral movement

• Implement intrusion prevention system (IPS) rules

• Deploy network traffic analysis tools

**POST-INCIDENT CORRECTIVE MEASURES (1 Week)**

**ORGANIZATIONAL IMPROVEMENTS:**

**📊 10. Security Awareness**

• Conduct mandatory security training for affected users

• Implement phishing awareness campaigns

• Establish clear incident reporting procedures

**📊 11. Process Improvements**

• Update incident response playbook with lessons learned

• Enhance SIEM alerting rules for similar attack patterns

• Establish regular security control reviews

**📊 12. Continuous Monitoring**

• Implement 24/7 SOC monitoring for similar indicators

• Deploy threat intelligence feeds for emerging threats

• Establish a regular vulnerability assessment schedule