SECURITY INCIDENT RESPONSE REPORT

2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success
2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed
2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success
2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt
2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success
2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success
2025-07-03 04:19:14 | user=alice | ip=198.51.100.42 | action=malware detected | threat=Rootkit Signature
2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 06:10:14 | user=david | ip=203.0.113.77 | action=file accessed
2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
2025-07-03 04:18:14 | user=bob | ip=198.51.100.42 | action=login success
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed
2025-07-03 07:38:14 | user=charlie | ip=172.16.0.3 | action=connection attempt
2025-07-03 07:57:14 | user=david | ip=10.0.0.5 | action=file accessed
2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt
2025-07-03 05:33:14 | user=david | ip=198.51.100.42 | action=file accessed
2025-07-03 04:19:14 | user=david | ip=10.0.0.5 | action=connection attempt
2025-07-03 04:29:14 | user=alice | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
2025-07-03 04:53:14 | user=david | ip=203.0.113.77 | action=login success
2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed
2025-07-03 05:27:14 | user=david | ip=203.0.113.77 | action=connection attempt
2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success

2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert
2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
2025-07-03 07:36:14 | user=david | ip=10.0.0.5 | action=connection attempt
2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
2025-07-03 05:49:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 06:21:14 | user=alice | ip=203.0.113.77 | action=login success
2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection attempt
2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login failed
2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed
2025-07-03 05:12:14 | user=alice | ip=198.51.100.42 | action=login success
2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt
2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login success
2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
2025-07-03 07:22:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 04:53:14 | user=alice | ip=203.0.113.77 | action=file accessed
2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
2025-07-03 05:44:14 | user=bob | ip=198.51.100.42 | action=file accessed

SECURITY INCIDENT RESPONSE REPORT

Date: November 2, 2025

Incident ID: SOC-2025-001

Report Type: Malware Outbreak & Account Compromise

Analyst: Karina de Oliveira Silva

EXECUTIVE SUMMARY

Multiple malware infections detected across corporate network involving 5 users and 4 suspicious IP addresses. The incident involves ransomware, rootkits, trojans, and spyware with evidence of potential brute force attacks and account compromise.

INCIDENT TIMELINE

04:19-04:41 - Initial malware detections (Rootkit, Spyware)

05:06-05:48 - Multiple Trojan infections across users

07:02-09:02 - Failed login attempts and suspicious connections

09:10 - Ransomware behavior detected - CRITICAL

INCIDENT CLASSIFICATION

Severity: HIGH

Priority: HIGH

Category: Malware Infection & Account Compromise

DETAILED FINDINGS

1. Malware Infections Identified

- Ransomware Behavior (HIGH) - User: bob
- Rootkit Signature (HIGH) - Users: alice, eve
- Worm Infection Attempt (HIGH) - User: bob
- Spyware Alert (MEDIUM) - User: alice
- Trojan Detected (MEDIUM) - Users: bob, david, eve, charlie

2. Compromised Accounts

- bob: 5 malware alerts - Highly compromised
- alice: 3 malware alerts - Compromised
- david: 2 malware alerts - Compromised
- eve: 2 malware alerts - Compromised
- charlie: 1 malware alert - Potentially compromised

3. Suspicious Network Activity

- IP 203.0.113.77: 11 occurrences - Highly suspicious
- IP 172.16.0.3: 9 occurrences - Suspicious
- IP 10.0.0.5: 7 occurrences - Suspicious
- Failed Logins: 4 attempts across 3 users

IMPACT ASSESSMENT

- HIGH RISK: Data encryption threat from ransomware
- MEDIUM RISK: Data exfiltration from spyware and trojans
- HIGH RISK: Persistent access from rootkits
- MEDIUM RISK: Credential compromise from brute force attempts

REMEDIATION RECOMMENDATIONS

1. IMMEDIATE: Isolate infected machines (bob, alice, david, eve)
2. IMMEDIATE: Reset passwords for all compromised accounts
3. HIGH PRIORITY: Block malicious IP 203.0.113.77 at firewall
4. MEDIUM PRIORITY: Scan entire network for worm propagation
5. LONG TERM: Implement multi-factor authentication

CONCLUSION

This coordinated malware attack requires immediate containment. The presence of ransomware and rootkits indicates a sophisticated threat actor. Quick isolation of compromised systems and credential reset is critical to prevent further damage.