Incident Response Report

By: Semer Nuru
Date: 2025-11-08
Tool Used: Splunk Free Trial

Executive Summary

Multiple security alerts were detected including malware infections (Trojan, Rootkit, Ransomware, Worm, Spyware), failed login attempts, and file accesses. Below remediation actions are recommended to reduce the potential impact on data confidentiality, integrity, and availability.

	Alert Type	Count	Description	Severity
2	malware-trojan	6	Trojan malware detected	High
3	malware-ransomware	1	Detected ransomware behavior	High
4	malware-worm	1	Worm malware detected	High
5	malware-spyware	1	Spyware detected	Medium
6	malware-rootkit	2	Rootkit detected	High
7	loginfail	5	Multiple failed login attempts	Medium
8	file accessed	10	Sensitive files accessed	Low
9	connection attempt	12	Connection attempts	Low

Alerts, Impacts and Remediations:

Trojan Malware(6 Alerts)

Timeline: 04:29 – 07:45

Impact: High — Indicates remote control and data theft risk. Systems possibly under attacker control, risk of credential compromise and file exfiltration.

Remediation:Isolate infected hosts immediately (IPs: 10.0.0.5, 192.168.1.101, 172.16.0.3). Run full antivirus and endpoint detection scans. Revoke user sessions and reset credentials. Patch affected systems and remove Trojan executables.

Ransomware Malware(1 Alert)

Timeline: 09:10

Impact: High — Ransomware can encrypt data and disrupt business operations. High risk to availability and potential for financial loss.

Remediation: Disconnect infected devices from the network. Validate data backups and prepare restoration procedures. Conduct forensic analysis to identify entry vectors. Notify management and prepare a user communication plan.

Worm Malware (1 Alert)
Timeline: 05:06
Impact: High — Worms can self-propagate through shared drives or network connections. Could spread rapidly if uncontained.
Remediation: Quarantine affected system. Block network segments showing high outbound traffic. Review firewall and disable unnecessary ports. Update signatures on all endpoints.

Rootkit Malware(2 Alerts)
Timeline: 04:19 – 07:51
Impact: Very High — Rootkits allow stealthy, persistent access and evade traditional antivirus detection. Threat to system integrity and confidentiality.
Remediation: Immediate isolation of hosts. Full OS reinstallation or image restoration. Verify bootloader and kernel integrity. Implement file integrity monitoring for early detection.

Spyware Malware(1 Alert)
Timeline: 04:41
Impact: Medium — Possible credential harvesting or keylogging. May lead to secondary account compromise.
Remediation: Scan endpoint for data-stealing malware. Reset affected user credentials. Educate users on avoiding phishing links. Enforce Two-Factor Authentication.

Multiple Failed Logins (5 Alerts)
Timeline: Throughout 04:23 – 09:02
Impact: Medium — Possible brute-force or credential-stuffing attempts. Repeated failures suggest targeted password guessing.
Remediation: Enable account lockout after 3 failed attempts. Monitor for unusual login patterns. Reset credentials for users with repeated failures. Implement stronger password policies.

File Accessed (10 Alerts)
Timeline: 05:33 – 08:42
Impact: Low — Some file access events may be benign, but in this case, several occurred after malware detection. Possible post-exploit or data exfiltration behavior.
Remediation: Review file integrity and access logs. Identify unauthorized modifications. Restrict access permissions where unnecessary.

Connection Attempts (12 Alerts)
Timeline: 04:19 – 08:42
Impact: Low — Indicates network reconnaissance or lateral movement attempts. Repeated connections to internal subnets suggest scanning behavior.
Remediation: Block suspicious IPs temporarily. Conduct network traffic analysis for unusual outbound patterns. Implement Intrusion Detection System alerts for future attempts.

Conclusion

This incident reveals a multi-stage attack involving various malware types and unauthorized activities across multiple internal IPs. The presence of Trojans, Rootkits, and Ransomware requires urgent system remediation and enhanced monitoring to prevent recurrence. Follow-up investigations and continuous SOC monitoring are essential to maintain a secure environment.