SOC Incident Response Report

Date: 2025-07-10

Analyst: Anubhav

SIEM Tool: Splunk

Incident ID: IR-2025-07-10-001

1. Executive Summary

On July 10th, 2025, the Security Operations Center identified and responded to a coordinated cyber incident affecting multiple internal and external network endpoints. The event combined several types of malicious activity, including repeated unauthorized connection attempts, confirmed malware detections of varying severity, and suspicious file access patterns across multiple user accounts.

Analysis of SIEM data revealed that the attack involved multiple malware strains such as Trojans, Rootkits, Spyware, Worms, and even early-stage ransomware behavior. The simultaneous occurrence of different threats strongly suggests that this was not an isolated infection, but rather a multi-vector intrusion aimed at gaining persistence, harvesting sensitive data, and potentially encrypting critical systems.

The SOC team initiated containment procedures shortly after detection, mitigating the spread and securing the compromised accounts.

2. Timeline of Events

The earliest suspicious activity was recorded at 04:18 UTC when the user account “bob” successfully logged in from an external IP address 198.51.100.42. Within the next minute, the account “alice” triggered a Rootkit detection from the same IP, indicating either a shared compromised endpoint or an immediate malware dropper execution following login.

By 04:29 UTC, the same user “alice” was involved in another malware detection, this time from the internal IP 192.168.1.101, showing evidence that the infection had already begun moving laterally within the network.

Throughout the next hour, additional users—david, charlie, and eve—began exhibiting both connection attempts from unusual locations and direct malware detections. At 05:06 UTC, a Worm infection attempt was identified on “bob”’s account from IP 203.0.113.77, followed by Trojan detections on multiple internal IPs. By 05:45 UTC, at least three separate internal machines had registered confirmed malware infections.

The situation escalated at 07:45 UTC when the user “charlie” triggered yet another Trojan detection on IP 172.16.0.3. Less than two hours later, at 09:10 UTC, “bob”’s account was flagged for ransomware behavior from the same internal IP, suggesting that the attacker’s objective had shifted towards system encryption.

3. Incident Classification

This incident has been classified as a High-Severity Multi-Vector Malware Attack. The threat profile includes both external intrusion attempts and internal lateral movement. The confirmed presence of ransomware indicators elevates the criticality, as this represents an imminent risk to system availability in addition to the already high risks to confidentiality and integrity.

4. Affected Assets and Accounts

The compromise impacted multiple internal IP addresses, notably 10.0.0.5, 192.168.1.101, and 172.16.0.3, as well as external addresses including 198.51.100.42 and 203.0.113.77. At least five separate user accounts—alice, bob, charlie, david, and eve—were involved in either malicious login attempts, confirmed malware detections, or suspicious file access.

5. Root Cause Analysis

Preliminary analysis indicates that the incident likely began with the compromise of one or more privileged user accounts via stolen credentials, possibly obtained through phishing or prior credential leaks. Once inside the network, attackers deployed multiple malware payloads in quick succession, enabling persistence mechanisms and initiating lateral movement to additional endpoints.

The appearance of distinct malware families across different hosts within such a short time frame suggests that the attackers used automated tools or scripts to deploy malicious binaries en masse. The ransomware behavior detected later in the timeline implies that the attack followed a deliberate kill chain: initial compromise, reconnaissance, malware deployment, and finally, attempted encryption.

6. Impact Assessment

The confidentiality of organizational data is considered to be at high risk, given the presence of spyware and rootkits that are typically used for credential harvesting and covert surveillance. Integrity risks are moderate but tangible due to the presence of Trojans and worms capable of modifying system files. Availability risks have risen significantly with the detection of ransomware indicators, which, if executed fully, could have rendered multiple systems inoperable.

At present, there is no confirmed evidence of large-scale data exfiltration, but forensic investigation is ongoing to verify this.

7. Remediation Actions Taken

Immediately after confirming the incident, the SOC initiated network isolation procedures for all affected hosts. Compromised accounts were disabled, and password resets were enforced across the organization. Malware samples were quarantined, and affected machines were subjected to deep scans using updated antivirus and endpoint detection rules. Security patches were applied to vulnerable systems, and network traffic from suspicious IPs was blocked at the firewall level.

Additionally, SIEM rules have been adjusted to trigger earlier alerts for similar threat patterns, aiming to reduce response times in the event of future attacks.

8. Recommendations

To prevent recurrence, the SOC advises the implementation of multi-factor authentication for all accounts, particularly those with remote access privileges. Network segmentation should be enhanced to limit lateral movement in case of a breach, and an endpoint detection and response (EDR) solution should be deployed across all devices. Firewall policies should be reviewed to ensure minimal exposure to external threats.

Finally, a targeted phishing awareness campaign is recommended to reduce the likelihood of credential theft through social engineering, as human error remains a critical entry point in most cyber intrusions.