📂 SOC Incident Report | Case Study 01 (CS-01)

Malware Execution and Persistence Analysis

Incident ID: IR-2025-01-Malware-Contained
Alert/Case Name: Suspicious Process Execution Detected
Analyst: Roshan Kumar
Date & Time of Detection: 2025-11-14 10:45:00 UTC
Final Status: TRUE POSITIVE – CONTAINED

I. Executive Summary

A high-severity alert was generated by the Endpoint Detection and Response (EDR) system, indicating the execution of a file with a known malicious signature on endpoint **HR-LPT-04** belonging to the **Human Resources** department. Immediate actions were executed to isolate the host and prevent data exfiltration or lateral movement. The root cause was identified as execution via a macro-enabled document. The incident was successfully contained and eradicated with **no** confirmed data loss.

II. Technical Analysis & Investigation (S-T-A-R Situation & Task)

The alert was triggered by EDR detecting abnormal process behavior associated with common credential-stealing malware. The investigation confirmed the following technical details:

Field	**Detail Found**	**Evidence Source**
Source of Compromise	Malicious document with embedded macro (T1566.001 - Phishing)	EDR/Email Logs
Infected Hostname	**HR-LPT-04**	EDR Telemetry
Malicious File Hash (SHA256)	**d28e75f1a9b2b5c0e1d0f3a4b9c8d7e6**	EDR Telemetry, VirusTotal
Persistence Mechanism	Scheduled Task Creation (T1053.005)	Windows Event Logs (Event ID 4698/4702)
Attempted C2 Communication	Outbound TCP connection to **192.168.20.10:4444**	Firewall/Proxy Logs

MITRE ATT&CK Classification:

- **Tactic:** Execution (TA0002) - Running the malicious payload.
- **Tactic:** Persistence (TA0003) - Establishing a foothold via Scheduled Task (**T1053.005**).

III. Containment, Eradication, and Recovery (S-T-A-R Action)

Action Taken:

1. **Isolation (Containment):** The affected host, **HR-LPT-04**, was immediately isolated from the network using EDR functionality to prevent Command and Control (C2) communication and lateral movement.
2. **Forensics & Analysis:** The malicious file was quarantined and confirmed via VirusTotal. Memory dumps were analyzed to ensure no other malicious processes were running.
3. **Eradication:** The malicious file, associated registry entries, and the unauthorized Scheduled Task were successfully removed from the host.
4. **Recovery:** The host was patched against known macro vulnerabilities and returned to the network with heightened monitoring enabled.

IV. Post-Incident Recommendations (S-T-A-R Result)

The successful containment of this incident provides crucial intelligence for bolstering future defenses.

Recommendations:

1. **Endpoint Security:** Update the EDR policy to block execution of all Office Macros unless digitally signed by an authorized enterprise source.
2. **Email Security:** Implement stricter filtering rules to block compressed attachments (.zip, .rar) containing Office documents for high-risk departments.
3. **Training:** Mandate immediate, targeted security awareness training for the **Human Resources** department on the dangers of enabling macros and phishing attempts.