# Incident Response Simulation

# (MITRE Caldera + Velociraptor)

## 1. Objective

The objective of this practical is to simulate a real-world phishing attack using **MITRE Caldera** and perform forensic artifact collection using **Velociraptor**. This exercise demonstrates how an organization detects, investigates, and analyzes malicious activity during an incident response process.

## 2. Environment Setup

- **Attacker System:** Kali Linux (MITRE Caldera Server)
- **Victim System:** Windows Virtual Machine (Caldera Agent + Velociraptor Client)
- **Tools Used:**
  - MITRE Caldera
  - Velociraptor

## 3. Attack Simulation Using MITRE Caldera

A phishing-based attack scenario was executed using MITRE Caldera. The attack simulated initial access through a malicious PowerShell payload delivered via a phishing link.

### Attack Steps

1. The Caldera server was started and an operation was created.
2. A phishing ability using PowerShell was selected.
3. The Windows agent executed the payload.

4. The agent successfully connected back to the Caldera server, confirming the compromise.

This attack maps to:

- **Initial Access:** T1566 – Phishing
- **Execution:** T1059 – Command and Scripting Interpreter

# 4. Artifact Collection Using Velociraptor

After detecting the suspicious activity, Velociraptor was used to collect forensic artifacts from the compromised system.

### Velociraptor Queries Executed

```
SELECT * FROM processes();
SELECT * FROM netstat();
```

### Collected Evidence

- Running PowerShell processes
- Suspicious parent-child process relationships
- Unusual outbound network connections

# 5. Indicators of Compromise (IOCs)

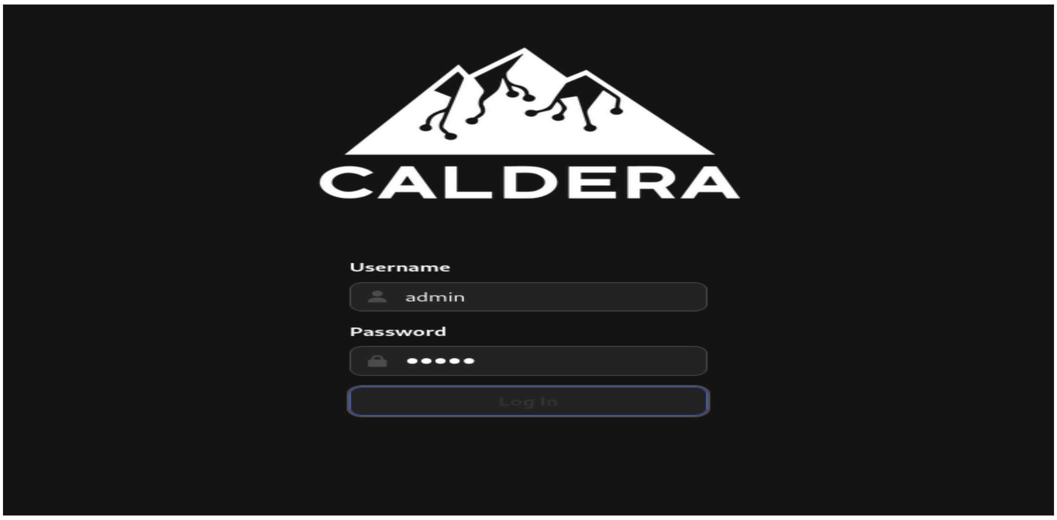
The following indicators were identified during analysis:

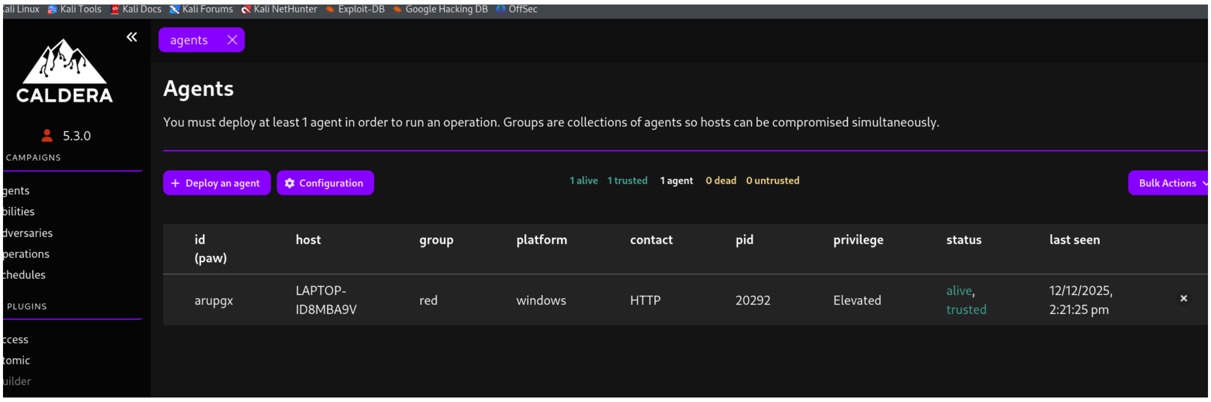
- Unexpected PowerShell process execution
- Network connections to unknown external IPs
- Command execution triggered without user interaction

## 6. Conclusion

This demonstrated the **complete incident response workflow**, from attack simulation to forensic investigation. The integration of MITRE Caldera and Velociraptor highlights how modern SOC teams detect and analyze phishing-based intrusions efficiently.

## 7. Screenshots:



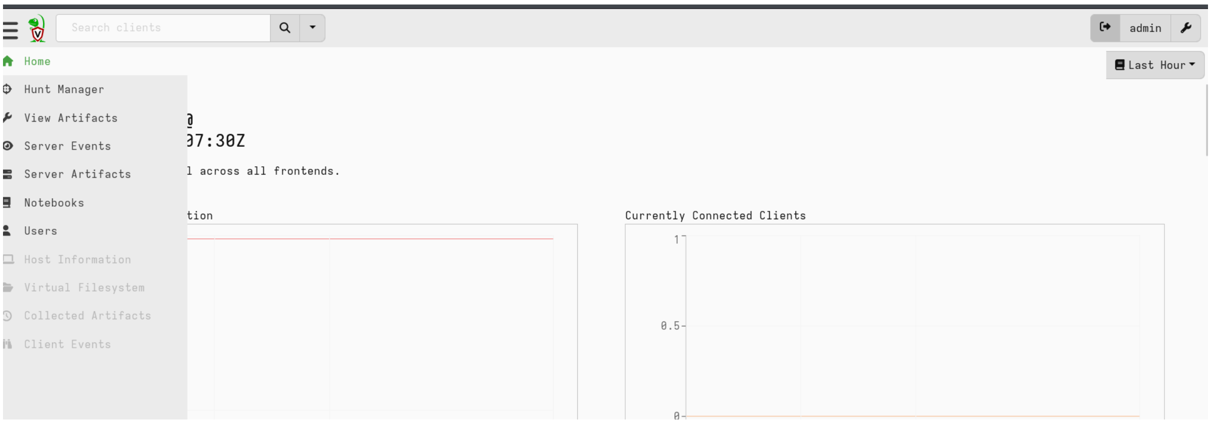


Agents

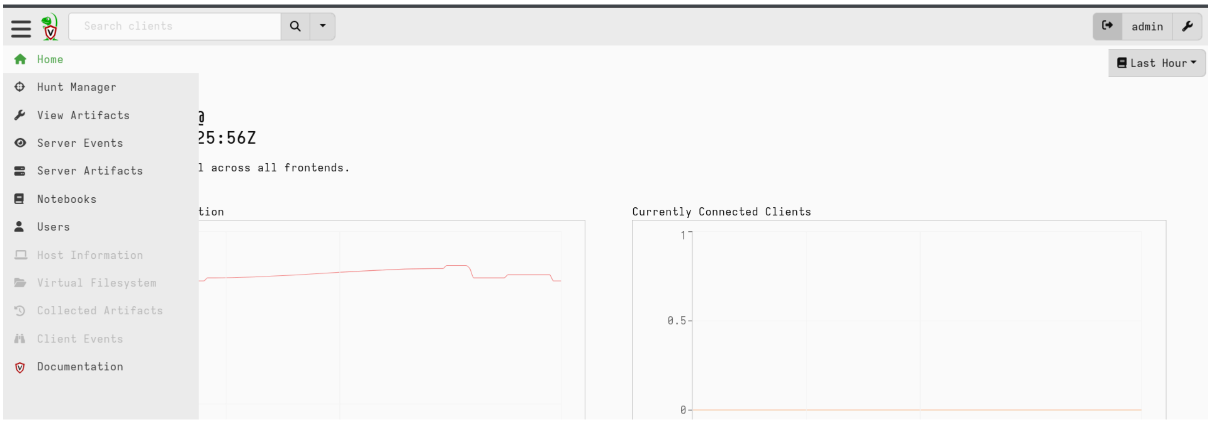
You must deploy at least 1 agent in order to run an operation. Groups are collections of agents so hosts can be compromised simultaneously.

1 alive 1 trusted 1 agent 0 dead 0 untrusted

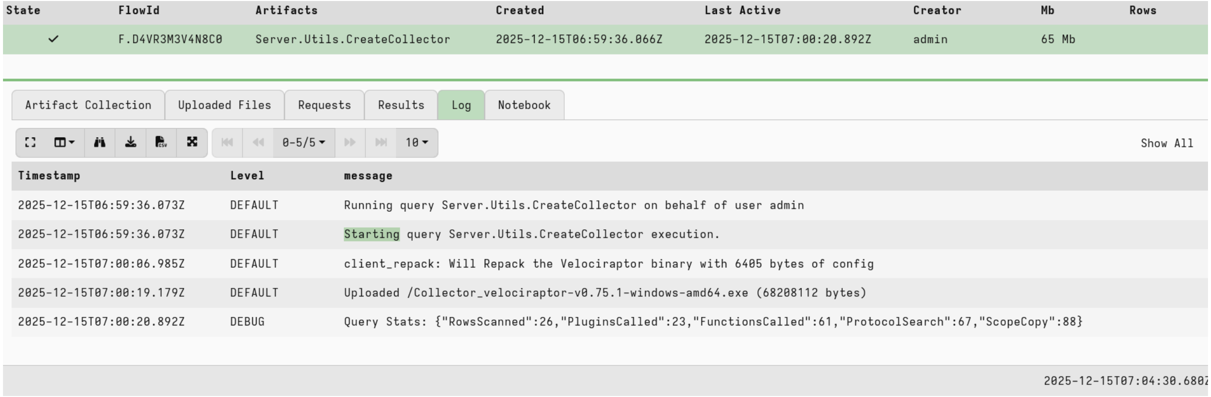
| id (paw) | host | group | platform | contact | pid | privilege | status | last seen | |
|---|---|---|---|---|---|---|---|---|---|
| arupgx | LAPTOP-ID8MBA9V | red | windows | HTTP | 20292 | Elevated | alive, trusted | 12/12/2025, 2:21:25 pm | × |



@
07:30Z
l across all frontends.



@
25:56Z
l across all frontends.



| State | FlowId | Artifacts | Created | Last Active | Creator | Mb | Rows |
|---|---|---|---|---|---|---|---|
| ✓ | F.D4VR3M3V4N8C0 | Server.Utils.CreateCollector | 2025-12-15T06:59:36.066Z | 2025-12-15T07:00:20.892Z | admin | 65 Mb | |

| Timestamp | Level | message |
|---|---|---|
| 2025-12-15T06:59:36.073Z | DEFAULT | Running query Server.Utils.CreateCollector on behalf of user admin |
| 2025-12-15T06:59:36.073Z | DEFAULT | Starting query Server.Utils.CreateCollector execution. |
| 2025-12-15T07:00:06.985Z | DEFAULT | client_repack: Will Repack the Velociraptor binary with 6405 bytes of config |
| 2025-12-15T07:00:19.179Z | DEFAULT | Uploaded /Collector_velociraptor-v0.75.1-windows-amd64.exe (68208112 bytes) |
| 2025-12-15T07:00:20.892Z | DEBUG | Query Stats: {"RowsScanned":26,"PluginsCalled":23,"FunctionsCalled":61,"ProtocolSearch":67,"ScopeCopy":88} |

2025-12-15T07:04:30.680Z