INCIDENT RESPONSE REPORT

Subject:Malware Behavior Detection (Kali → Kali)

Incident ID: IR-2025-1227-010

PREPARED BY:

Vignesh K.

SOC Analyst / Security Researcher

CERTIFICATIONS: Google Cybersecurity Professional

REPORT DATE: December 27, 2025

Incident ID	IR-2025-1227-010
Date	December 27, 2025
Severity	Medium
Status	Closed (Lab Simulation)

1. Project Overview and Goal

- This project demonstrates malware detection using a behavior-based approach without deploying real malware. A simulated malicious script was executed on a Kali Linux system to mimic common malware behaviors such as hidden file creation, persistence mechanisms, and beaconing activity. The investigation was conducted from a Security Operations Center (SOC) perspective.

2. Lab Architecture

- **Attacker System: Kali Linux (simulated adversary behavior)**
- **Victim System: Kali Linux (host under investigation)**
- **Detection Method: Host-based behavioral analysis**

3. Objectives:

- Simulate realistic malware behavior in a controlled environment
- Identify indicators of compromise through system behavior
- Map observed activity to the MITRE ATT&CK framework
- Perform containment and remediation actions

4.Malware Behavior Simulation

A benign shell script was created to emulate malware behavior. The script performed the following actions:

- Creation of hidden files in a temporary directory
- Persistence via cron job scheduling
- Continuous background execution (beacon-like behavior)

5. Detection & Analysis

The system was analyzed using standard Linux administrative and monitoring commands. Detection relied on behavioral indicators rather than traditional SIEM alerts.

- Hidden files detected using directory listing commands
- Unauthorized cron job identified as a persistence mechanism
- Suspicious long-running background process discovered
- Periodic activity consistent with beaconing observed in log files

6. MITRE ATT&CK Mapping

- T1059 – Command and Scripting Interpreter
- T1053 – Scheduled Task / Cron
- T1547 – Persistence Mechanisms
- T1071 – Application Layer Protocol (Beaconing)

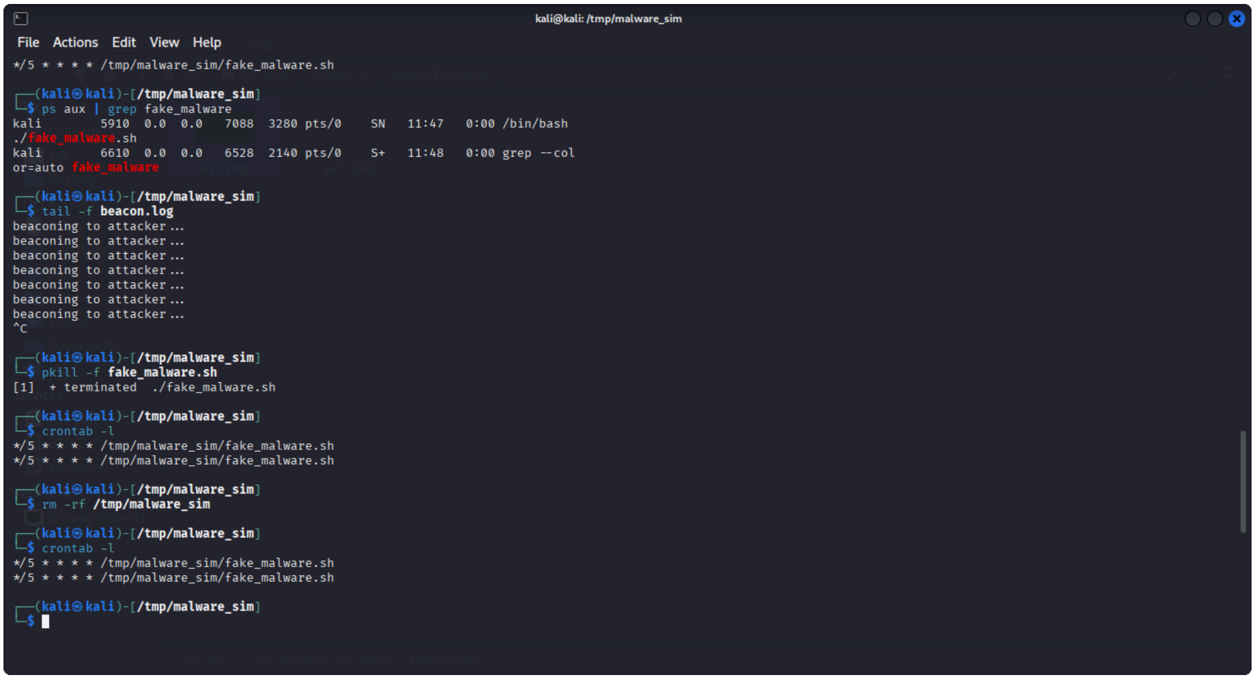
7. Incident Response & Remediation

- Terminated the malicious process
- Removed unauthorized cron job
- Deleted all malicious artifacts
- Verified system integrity post-cleanup

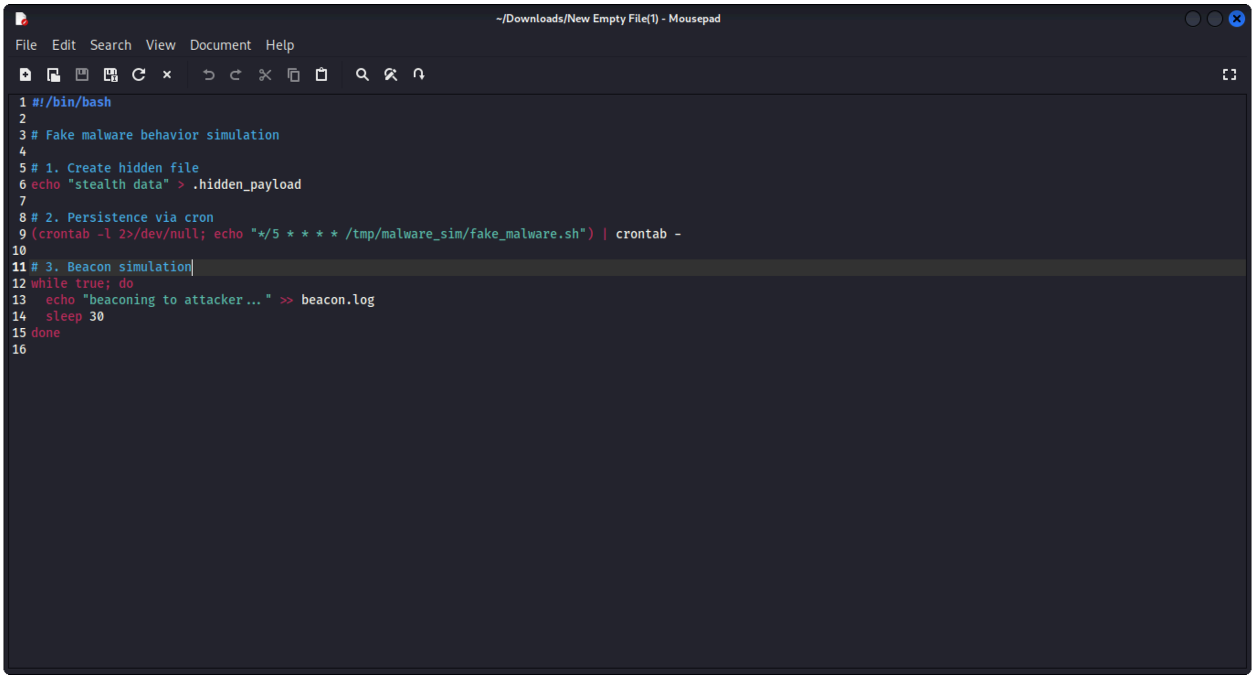
8. Conclusion

This project highlights the importance of behavior-based malware detection, especially in scenarios where traditional logs or signatures may be absent or evaded. The investigation reflects real-world SOC workflows and demonstrates strong foundational skills in threat detection, analysis, and response.

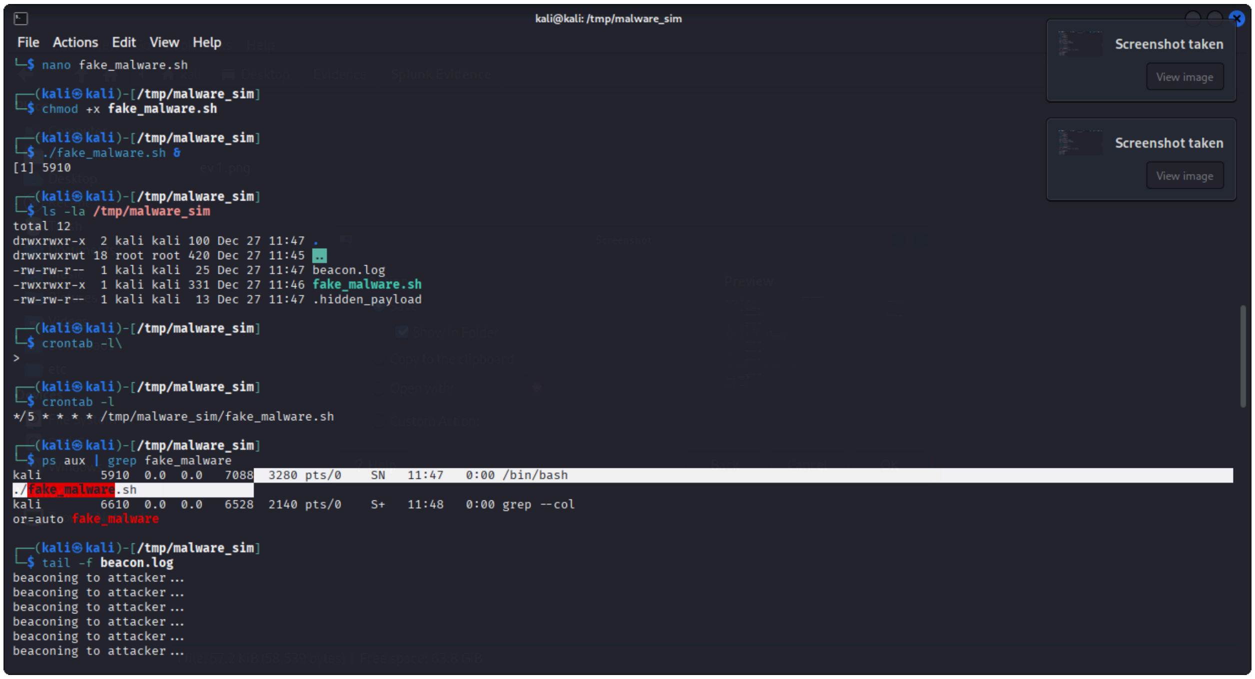
9. Evidence



```
*/5 * * * * /tmp/malware_sim/fake_malware.sh

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ ps aux | grep fake_malware
kali        5910  0.0  0.0   7088  3280 pts/0    SN   11:47   0:00 /bin/bash
./fake_malware.sh
kali        6610  0.0  0.0   6528  2140 pts/0    S+   11:48   0:00 grep --col
or=auto fake_malware

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ tail -f beacon.log
beaconing to attacker...
beaconing to attacker...
beaconing to attacker...
beaconing to attacker...
beaconing to attacker...
beaconing to attacker...
beaconing to attacker...
^C

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ pkill -f fake_malware.sh
[1]  + terminated  ./fake_malware.sh

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ crontab -l
*/5 * * * * /tmp/malware_sim/fake_malware.sh
*/5 * * * * /tmp/malware_sim/fake_malware.sh

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ rm -rf /tmp/malware_sim

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ crontab -l
*/5 * * * * /tmp/malware_sim/fake_malware.sh
*/5 * * * * /tmp/malware_sim/fake_malware.sh

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ 
```


~/Downloads/New Empty File(1) - Mousepad
File Edit Search View Document Help

```bash
#!/bin/bash

# Fake malware behavior simulation

# 1. Create hidden file
echo "stealth data" > .hidden_payload

# 2. Persistence via cron
(crontab -l 2>/dev/null; echo "*/5 * * * * /tmp/malware_sim/fake_malware.sh") | crontab -

# 3. Beacon simulation
while true; do
  echo "beaconing to attacker..." >> beacon.log
  sleep 30
done
```



```
└─$ nano fake_malware.sh

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ chmod +x fake_malware.sh

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ ./fake_malware.sh &
[1] 5910

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ ls -la /tmp/malware_sim
total 12
drwxrwxr-x  2 kali kali 100 Dec 27 11:47 .
drwxrwxrwt 18 root root 420 Dec 27 11:45 ..
-rw-rw-r--  1 kali kali  25 Dec 27 11:47 beacon.log
-rwxrwxr-x  1 kali kali 331 Dec 27 11:46 fake_malware.sh
-rw-rw-r--  1 kali kali  13 Dec 27 11:47 .hidden_payload

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ crontab -l\
>

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ crontab -l
*/5 * * * * /tmp/malware_sim/fake_malware.sh

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ ps aux | grep fake_malware
kali        5910  0.0  0.0   7088  3280 pts/0    SN   11:47   0:00 /bin/bash
./fake_malware.sh
kali        6610  0.0  0.0   6528  2140 pts/0    S+   11:48   0:00 grep --col
or=auto fake_malware

┌──(kali㉿kali)-[/tmp/malware_sim]
└─$ tail -f beacon.log
beaconing to attacker ...
beaconing to attacker ...
beaconing to attacker ...
beaconing to attacker ...
beaconing to attacker ...
beaconing to attacker ...
```