Incident Response Case Study Report 3

Case Type 3: Malware Beaconing Traffic
SOC Analyst: Parvathy Krishnan
Environment: SOC Home Lab
SIEM: Splunk

---

1. Executive Summary

During continuous SOC monitoring, a **high-severity SIEM alert** was triggered indicating **suspicious periodic outbound network traffic** from a Windows endpoint. The behaviour was consistent with **malware beaconing**, a technique commonly used by compromised hosts to communicate with command-and-control (C2) servers.

The objective of this investigation was to:

- Identify whether the traffic represented malicious C2 communication
- Determine the scope and impact of the activity
- Identify Indicators of Compromise (IOCs)
- Recommend remediation and containment actions

Following a comprehensive investigation, the activity was confirmed as **malware beaconing behaviour**, and the incident was classified as a **True Positive**.

2. Detection & Alert Context

Alert Information

- **Alert Name:** Suspicious Beaconing Network Traffic
- **Severity:** High
- **Detection Source:** Splunk SIEM
- **Affected Host:** WIN10-ENDPOINT-01
- **Source IP:** 192.168.1.101
- **Destination IP:** 185.203.118.45
- **Protocol:** TCP
- **Destination Port:** 443

Why This Alert Matters

Beaconing traffic is a strong indicator of:

- Active malware infection
- Ongoing command-and-control communication
- Potential data exfiltration or tasking from attackers

Such activity typically indicates **post-compromise behaviour** and requires immediate investigation.

3. Initial Triage & Validation

Actions Taken

- Validated the alert source and timestamp
- Confirmed the alert was not a false correlation
- Identified the affected endpoint and user context
- Checked for similar alerts across other hosts

Splunk Query – Alert Validation

```
index=network_logs dest_ip=185.203.118.45
| stats count by src_ip, dest_ip
```

Initial Findings

- Activity was isolated to a single endpoint
- Traffic occurred at consistent time intervals
- No legitimate business justification for the destination IP

The alert was escalated for full investigation.

4. Data Collection & Log Analysis

Log Sources Reviewed

- Network Traffic Logs
- Windows Security Logs
- Sysmon Network Connection Logs
- DNS Logs

Splunk Query – Identify Periodic Connections

```
index=network_logs src_ip=192.168.1.101
| bucket _time span=5m
| stats count by _time, dest_ip
| where count > 5
```

Key Observations

- Outbound connections every 60 seconds
- Consistent destination IP and port
- Small, uniform packet sizes
- Encrypted traffic with no valid application context

These characteristics strongly matched known malware beaconing patterns.

5. Beaconing Pattern & Behaviour Analysis

Behavioural Characteristics Observed

- Regular interval communication
- Low data volume per connection
- No user interaction during activity
- Traffic persisted after user logout

Splunk Query – Beacon Interval Analysis

```
index=network_logs src_ip=192.168.1.101 dest_ip=185.203.118.45
| sort _time
| delta _time as time_diff
| stats avg(time_diff) as avg_beacon_interval
```

Analysis Result

- Average beacon interval: **60 seconds**
- Highly consistent timing suggests automation
- Behaviour consistent with C2 heartbeat traffic

6. Reconstruction

Time (UTC)	Event
11:05	First outbound connection detected
11:10	Repeated periodic traffic observed
11:12	SIEM beaconing alert triggered
11:15	SOC investigation initiated
11:25	Beacon pattern confirmed
11:40	Host identified as compromised
11:55	Incident documented

7. Indicator of Compromise (IOC) Analysis

IOCs Identified

Type	Value
Source IP	192.168.1.101
Destination IP	185.203.118.45
Destination Port	443
Protocol	TCP
Behaviour	Periodic outbound connections

Splunk Query – IOC Enumeration

```
index=network_logs dest_ip=185.203.118.45
| stats count by src_ip, dest_port
```

IOC Enrichment

- Destination IP not associated with known legitimate services
- Pattern matched known C2 infrastructure behaviour
- IP flagged as suspicious within lab threat simulation

8. Scope & Impact Assessment

Scope

- **Affected Hosts:** 1
- **Affected Users:** 1
- **Network Segments:** Local workstation subnet
- **Lateral Movement:** Not detected

Impact Conclusion

- Host confirmed compromised
- Active C2 communication observed
- No confirmed data exfiltration during investigation window

9. Root Cause Analysis

Root Cause

The root cause of the incident was a **malware infection** on the endpoint that established **persistent outbound beaconing communication** to a remote command-and-control server.

Contributing Factors

- Lack of outbound traffic filtering
- No EDR blocking C2 communication
- Limited application-level network visibility

---

10. MITRE ATT&CK Mapping

Tactic	Technique	ID
Command and Control	Application Layer Protocol	T1071
Command and Control	Web Protocols	T1071.001

11.Final Verdict

True Positive – Confirmed Malware Beaconing Activity

The detection successfully identified malicious post-compromise behaviour consistent with active malware communication.

12. Remediation & Recommendations

- Immediately isolate the affected host
- Block destination IP at firewall level
- Reimage or clean the compromised endpoint
- Implement outbound traffic monitoring
- Integrate EDR for endpoint containment
- Enhance SIEM correlation for beaconing patterns

13. Lessons Learned

- Beaconing behaviour is a strong compromise indicator
- Network telemetry is critical for C2 detection
- Interval analysis is effective for identifying malware
- Early detection limits attacker dwell time

14. Analyst Notes

This case demonstrated:

- Effective use of network telemetry
- Behavioural analysis beyond signature-based detection
- Accurate identification of post-exploitation activity
- Proper SOC documentation and escalation handling

15. Summary