Traffic Analysis Essentials

# 📝 ****Full Incident Report – Traffic Analysis Essentials****

**Lab Name:** Traffic Analysis Essentials  
**Category:** Network Security & Traffic Analysis – Full Report

## **1. Executive Summary**

This investigation involved analyzing **network packet captures (PCAPs)** to identify malicious activity within enterprise traffic.  
The objective was to detect suspicious network behaviors, extract indicators of compromise (IOCs), and determine the attacker’s tactics, techniques, and procedures (TTPs).

The analysis revealed:

* Malicious HTTP and HTTPS connections to known C2 servers.
* File downloads containing malware payloads.
* Signs of lateral movement attempts via SMB.

## **2. Incident Timeline**

| **Time (UTC)** | **Event** |
| --- | --- |
| 09:14 | Network IDS alerts on suspicious domain request. |
| 09:15 | PCAP extracted from IDS logs for deeper inspection. |
| 09:20 | Analyst begins filtering traffic for suspicious hosts. |
| 09:35 | Malware payload identified in HTTP GET request. |
| 09:42 | C2 communication established over HTTPS. |
| 09:50 | SMB traffic analyzed for lateral movement. |
| 09:55 | SOC recommends containment actions. |

## **3. Technical Investigation**

### **3.1 Tools Used**

* **Wireshark** – PCAP filtering, packet inspection.
* **NetworkMiner** – IOC extraction (domains, IPs, file hashes).
* **Zeek** – HTTP and SSL log analysis.

### **3.2 Key Findings**

**a. Malicious Domain Requests**

* Example IOC: malicious-updates[.]com (HTTP GET request to /payload.exe)
* Matched to threat actor infrastructure in MISP database.

**b. Command & Control Communication**

* HTTPS connections to 203.0.113.45 on port 443 with regular beacon intervals.
* TLS handshake indicated suspicious self-signed certificate.

**c. Payload Delivery**

* Extracted binary hash:
  + SHA256: 8d2f6b2ac6f4dfe1b77d4b2f4fbdcfae62123456789abcd1234567890abcdef
  + VirusTotal: Trojan Downloader (linked to known campaign).

**d. Lateral Movement Attempts**

* SMB traffic from infected workstation to multiple internal hosts.
* Signs of brute-force attempts using NTLM authentication.

## **4. MITRE ATT&CK Mapping**

| **Technique ID** | **Technique Name** | **Observation** |
| --- | --- | --- |
| T1071.001 | Application Layer Protocol: Web Traffic | C2 over HTTPS |
| T1105 | Ingress Tool Transfer | Download of payload.exe |
| T1021.002 | Remote Services: SMB/Windows Admin Shares | Lateral movement attempts |
| T1041 | Exfiltration Over C2 Channel | Potential data exfiltration over HTTPS |

## **5. Containment & Mitigation**

1. **Immediate Actions:**
   * Block malicious IP and domain at firewall.
   * Isolate infected workstation.
2. **Long-Term Measures:**
   * Update IDS/IPS rules with new IOCs.
   * Enhance email filtering to prevent delivery of malicious links.
   * Implement stricter SMB authentication policies.

## **6. Conclusion**

This case demonstrated the importance of **packet-level inspection** in SOC operations.  
By correlating PCAP findings with threat intelligence feeds, we were able to quickly identify malicious infrastructure and prevent further compromise.



