TLP:AMBER

PCAP Analysis Report - Sample

Case: Suspicious Network Activity Investigation

ID: CASE-2024-001

Generated: 2025-12-30 11:07

Analyst: Security Analyst

Organization: Security Operations Center

TLP:AMBER

Table of Contents

1. Executive Summary

Executive Summary

This PCAP capture reveals **suspicious network activity** consistent with potential Command & Control (C2) communication patterns.

Key Findings

1. **Beaconing Behavior**: Regular interval connections to external IP `185.220.101.45` every 60 seconds
2. **Data Exfiltration**: Large outbound data transfers (2.3 GB) to unusual destination
3. **DNS Tunneling Indicators**: High-entropy DNS queries to `suspicious-domain.com`
4. **Malicious JA3 Fingerprint**: Detected Cobalt Strike beacon signature

Risk Assessment

Category	Level	Details
Severity	**CRITICAL**	Active C2 communication detected
Confidence	High	Multiple IOCs correlated
Impact	Data Breach	Potential exfiltration in progress

Recommendations

- **Immediate**: Isolate affected host `192.168.1.100`
- **Short-term**: Block IOCs at firewall
- **Long-term**: Conduct forensic investigation

2. Indicators of Compromise

Type	Value	Context
IP Address	185.220.101.45	GreyNoise: malicious
IP Address	93.184.216.34	GreyNoise: benign
IP Address	198.51.100.23	GreyNoise: unknown
Domain	suspicious-domain.com	
Domain	c2-server.net	
Hash (SHA256)	`d41d8cd98f00b204e9800998ecf8427e`	
JA3 Fingerprint	`72a589da586844d7f0818ce684948eea`	

3. OSINT Analysis

IP Address Intelligence

IP	PTR	GreyNoise	VT Rep
185.220.101.45	N/A	malicious	N/A
93.184.216.34	N/A	benign	N/A
198.51.100.23	N/A	unknown	N/A

Domain Intelligence

Domain	Categories
suspicious-domain.com	
c2-server.net	

4. DNS Analysis

2500	156	0
DNS Records	Unique Domains	DNS Servers

DGA Detection: 3 suspicious domains

DNS Tunneling: 1 potential tunneling

DGA Detection Results

Domain	Score	Reason
xk7m2p9q4r8s.com	0.92	High entropy, random characters
a8b2c9d4e5f6.net	0.87	Hexadecimal pattern
qwerty123abc.org	0.75	Dictionary word + numbers

5. TLS Certificate Analysis

0	0	0
Certificates	Self-Signed	Expired

Certificate Details

Subject CN	Issuer CN	Expires	Self-Signed	Risk
N/A	N/A	2025-01-01	Yes	0.00
N/A	N/A	2024-06-01	No	0.00

6. YARA Scan Results

15	3	0
Files Scanned	Matches Found	Rules Loaded

Critical: 1 | High: 1 | Medium: 1 | Low: 0 | Clean: 12

No malicious content detected.

7. Network Flow Analysis

Showing top 5 flows by packet count.

Source	SPort	Destination	DPort	Protocol	Packets
192.168.1.100	49152	185.220.101.45	443	TCP	5000
192.168.1.100	49153	93.184.216.34	80	TCP	3200
192.168.1.100	54321	198.51.100.23	8080	TCP	1500
192.168.1.105	60001	8.8.8.8	53	UDP	850
192.168.1.110	443	10.0.0.50	55555	TCP	420

8. Appendix

Analysis Statistics

- Total Flows: 5
- Unique IPs: 3
- Unique Domains: 2
- File Hashes: 1
- JA3 Fingerprints: 1

Report Generation

- Generated: 2025-12-30 11:07:26
- Classification: TLP:AMBER
- Tool: PCAP Hunter