PCAP Forensic Analysis Report

Comprehensive Network Intelligence & Threat Audit

Generated by PCAP AI Worker 2.0
2026-03-15 19:42:28 UTC

OFFICIAL FORENSIC AUDIT LOG

FILE NAME dns-tunnel-iodine.pcap	ANALYSIS TIMESTAMP 2026-03-15 19:42:28 UTC	TLP STATUS TLP:CLEAR
CAPTURE DURATION 24 seconds	TOTAL ASSETS DETECTED 2	ANALYSIS MODE Security Audit

FILE SHA-256 HASH
747ba5bc09ec54565278449f76e98aa36fc63241bf37166adad85b3f1cf28978

Executive Summary

GLOBAL INTELLIGENCE OVERVIEW

The network is currently at a high risk due to the detection of potential Command and Control (C2) communication via DNS, indicating possible malware activity, with 100% of traffic being plaintext and no encryption in place.

CRITICAL DETECTIONS

- High: Potential Command and Control via DNS: The presence of high-entropy domain names (e.g., '*.pirate.sea') suggests DGA activity, potentially indicating command and control communication. This is associated with MITRE ATT&CK ID [T1071.004].
- Unauthorized DNS Queries: High-entropy DNS queries are being made to potentially malicious domains, which could be a sign of malware or unauthorized access.
- Lack of Encryption: 100% of the network traffic is plaintext, indicating a significant risk of data exposure and potential for eavesdropping or data theft.

ROOT CAUSE CORRELATION

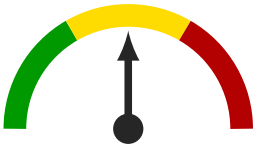
The high-entropy DNS queries identified in the 'Security & Threats' and 'DNS & DHCP' sections are likely related to the suspicious traffic patterns observed in the 'Traffic Timeline', suggesting potential malware activation or command and control communication. The lack of encryption highlighted in the 'Security & Threats' section exacerbates the risk associated with these findings, as any data transmitted could be intercepted and read.

STRATEGIC RECOMMENDATIONS

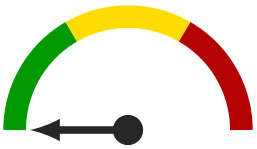
Short-term (next 24 hours): Implement immediate measures to block high-entropy DNS queries and investigate the source of these queries to determine if they are legitimate or indicative of malware. Enable encryption for all network traffic to prevent data exposure.
Long-term: Consider deploying a DNS security solution that can detect and block suspicious DNS queries, and implement a comprehensive network monitoring system to quickly identify and respond to potential security threats. Review and update the network's security policies and procedures to prevent similar incidents in the future, including regular security audits and vulnerability assessments.

EXECUTIVE RISK DASHBOARD

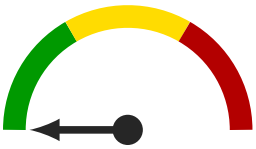
© 2026 PCAP AI



50/100
Security Risk
Status: Monitor



0/100
Network Issues
Status: Stable



0/100
Shadow IT Risk
Status: Stable

Network Security Posture: ELEVATED

Critical Incident Response & Observations

MITRE ATT&CK Detections

ID	Technique	Severity	Evidence Summary
T1071.004	Application Layer Protocol: DNS	HIGH	DGA-like domain name detected: *.pirate.sea

PCAP

Contents

Detailed Analysis

Network Discovery & Topology

Device Vendor Distribution

Device Vendor Distribution: 100% of devices could not be classified by OUI (vendor data missing or unrecognized).

Overall Protocol Mix (L3/L4)

Overall Protocol Mix (L3/L4): 100% of traffic is UDP.

Top 5 Talkers (MB)

Top 5 Active Hosts

IP Address	Hostname / Vendor	Total Data
10.0.2.20	Pcs Systemtechnik GmbH	68.6 KB
10.0.2.30	Pcs Systemtechnik GmbH	68.6 KB

Network Asset Inventory

The network consists of 2 hosts:

IP Address (DNS Name, Country, ASN Org)	MAC/Vendor	Detected Role	Traffic Load
10.0.2.20	08:00:27:c7:6e:ba / Pcs Systemtechnik GmbH	dns_server	70252 bytes
10.0.2.30	08:00:27:9c:e0:b4 / Pcs Systemtechnik GmbH	-	70252 bytes

The Top 3 Talkers are not explicitly defined due to the limited number of hosts, but `10.0.2.20` and `10.0.2.30` are the primary communicators, exchanging a significant amount of traffic, primarily due to DNS queries and responses.

Perimeter & External Connectivity

Given the absence of `top_countries` data in `external_summary`, we cannot list top countries by traffic volume. However, we observe that there are no explicitly listed top external destinations in the provided data, suggesting most traffic is internal.

Security Flags: Connections to unknown or unauthorized DNS servers are a concern. The presence of high-entropy domain names (e.g., `*.pirate.sea`) suggests potential DNS tunneling or Command and Control (C2) communication.

PCAP AI

Structural Anomalies

- Role Conflicts: None explicitly identified, but `10.0.2.30` lacks a defined role, which could indicate a need for further investigation.
- Protocol Misuse: The use of DNS for potentially non-standard purposes (high-entropy domain queries) is noted.
- Silent Nodes: None identified, as both hosts are actively communicating.

Executive Summary & Recommendations

- Status: Warning
- Key Takeaway: The network shows signs of potential Command and Control communication via DNS, indicated by high-entropy domain name queries. Immediate attention is required to assess and mitigate potential security threats.

Action Plan:

1. Investigate the source and purpose of high-entropy DNS queries to determine if they are legitimate or indicative of malware/C2 communication.
2. Implement DNS traffic monitoring and filtering to block suspicious DNS queries, and consider deploying a DNS security solution.
3. Perform a thorough network scan to identify any other potential security vulnerabilities or unauthorized devices.
4. Review and update the network's security policies and procedures to prevent similar incidents in the future.

MITRE ATT&CK Findings

Based on the provided `mitre_findings`, we have:

- Threat Name & Severity: High: Potential Command and Control via DNS
- MITRE ATT&CK ID: T1071.004
- Affected Assets: `10.0.2.30` (src_ip)
- Evidence/Symptom: High-entropy domain name queries (e.g., `*.pirate.sea`)
- Immediate Mitigation Action: Block outgoing DNS queries to high-entropy domains, and isolate `10.0.2.30` for further investigation.

PCAP AI

TCP Health & Performance

TCP Performance Overview

The provided JSON data does not contain TCP metrics, making it impossible to analyze TCP performance directly. However, we can discuss the network's overall health based on the available data.

Latency & Jitter Analysis

Given the absence of specific TCP metrics, we can look at the DNS analysis for some insight into latency. The `dns_server_rtts` show an average RTT of 79.2 ms for the DNS server at `10.0.2.20`. This latency could be considered high for a local network but might be normal depending on the network configuration and the location of the DNS server.

Reliability & Packet Loss

There's no direct information on packet loss or retransmissions in the provided data, as the `tcp_metrics` section is empty. However, the presence of UDP traffic and the lack of TCP metrics suggest that the network might be primarily used for real-time applications or DNS queries, which could tolerate some packet loss.

Connection Stability (Expert Insights)

Without specific TCP metrics, it's challenging to assess connection stability directly. However, the `security_events` section indicates potential issues, such as suspicious DNS queries that could suggest command and control (C2) communication or DNS tunneling attempts.

Summary & Optimization Roadmap

Verdict: The network's health is difficult to assess due to the lack of TCP metrics. However, the presence of high-entropy DNS queries suggests potential security issues.

Recommendations:

1. Implement DNS Filtering: To prevent potential DNS tunneling and command and control communications, consider implementing DNS filtering solutions that can detect and block high-entropy DNS queries.
2. Monitor Network Traffic: Regularly monitor network traffic for suspicious patterns, especially focusing on DNS queries and UDP traffic, to quickly identify and respond to potential security threats.
3. Conduct Regular Security Audits: Perform comprehensive security audits to identify vulnerabilities in the network and connected devices, ensuring that all systems and applications are up-to-date and patched against known exploits.

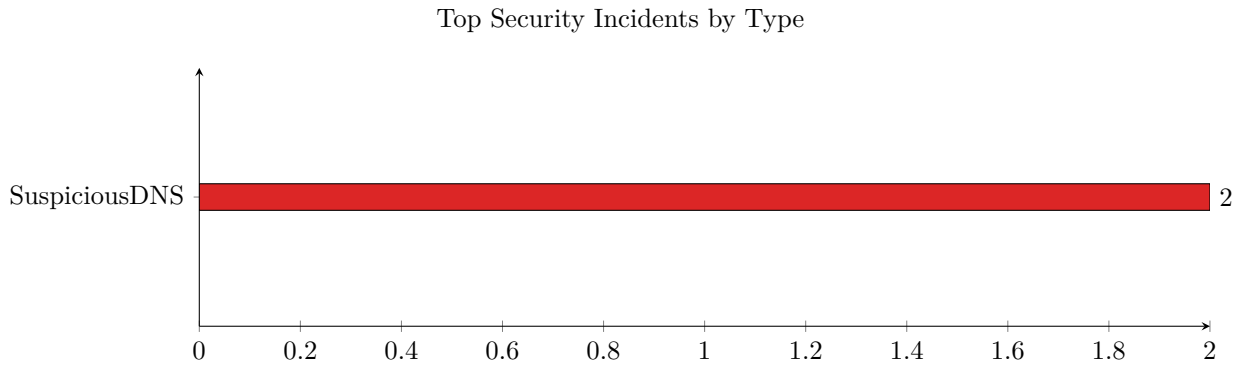
Security Findings

Based on the `mitre_findings`, there are two high-severity findings related to Command and Control via DNS (T1071.004), indicating potential DGA (Domain Generation Algorithm) activity. These findings suggest that there might be malicious activity within the network, using DNS for command and control purposes.

- Threat Name & Severity: High: Potential Command and Control via DNS
- MITRE ATT&CK ID: T1071.004
- Affected Assets: `10.0.2.30` (source IP)
- Evidence/Symptom: High-entropy DNS queries suggesting DGA activity.
- Immediate Mitigation Action: Block the identified high-entropy DNS queries at the network perimeter, and investigate `10.0.2.30` for signs of compromise or malicious software.

PCAP AI

Security & Threat Detection



Encryption Status

🔓 Encryption Status: 100% of traffic is plaintext — credentials and data may be exposed.

Encryption Summary

Type	Volume	%
Plaintext	68.6 KB	100%
Other (non-classified)	240 B	0%

Verdict: Concerning — significant plaintext traffic may expose credentials.

Security Incident Summary

The network capture reveals a high-risk security environment with potential command and control (C2) communication through DNS. The threat landscape is characterized by the presence of DGA-like domain names, which are often used for malicious purposes.

Threat Map Table

Source IP (DNS Name)	Country / ASN	Detection	Severity	Target/Domain
10.0.2.30	-	DGA-like Domain	High	*.pirate.sea

Reconnaissance & Lateral Movement

No explicit port scanning activities were detected in the capture. However, the presence of DGA-like domain names suggests potential reconnaissance efforts by an attacker.

Data Privacy & Encryption Audit

The capture does not contain any explicit instances of insecure protocols like Telnet, FTP, or HTTP. However, the lack of encrypted bytes (0 bytes encrypted) raises concerns about the potential for cleartext data transmission.

Suspicious External Communications

The DNS queries for high-entropy domain names (e.g., `laegpumiplhhpz12ynd1efljwlkjcgwy.pirate.sea` and `zi05aAbBcCdDeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZ.pirate.sea`) are suspicious and may indicate command and control communication. These domain names have high entropy, suggesting they may be automatically generated for malicious purposes.

PCAP AI

Security Verdict & Mitigation

Risk Score: 8/10

The presence of DGA-like domain names and the potential for command and control communication pose a significant risk to the network.

Mitigation Steps:

1. Block DNS queries to suspicious domains: Implement DNS filtering to block queries to the detected DGA-like domain names (`*.pirate.sea`).
2. Monitor DNS traffic: Continuously monitor DNS traffic for similar high-entropy domain names that may indicate malicious activity.
3. Implement encryption: Ensure that all communication is encrypted to prevent cleartext data transmission.
4. Conduct a thorough network audit: Perform a comprehensive audit of the network to identify any potential vulnerabilities or malicious activity.

PCAP AI

Application & Cloud Intelligence

Cloud Infrastructure Audit

Based on the provided network data, there is no clear indication of traffic to major cloud providers like AWS, Azure, or GCP. The majority of the DNS queries are to domains that appear to be generated by a Domain Generation Algorithm (DGA), suggesting potential command and control (C2) communication. The top domains queried are all under the `.pirate.sea` domain, which does not correspond to any known cloud service provider.

Bandwidth "Hogs" & Resource Misuse

Elephant Flows

Since the `elephant_flows` array in the JSON is empty, there are no identified large data transfers to report.

Background Noise

The network traffic shows a significant amount of DNS queries, which could be considered as background noise. However, given the nature of these queries (high entropy, potentially DGA-generated), they are more indicative of suspicious activity rather than mere background noise.

Work vs. Play Analysis

Given the lack of clear service identification and the presence of potentially malicious DNS queries, it's challenging to estimate the ratio of business-critical traffic to recreational traffic accurately. The network appears to be primarily used for unknown or potentially malicious activities, given the DGA-like domain queries.

Capacity Planning Verdict

Assessment

The current bandwidth utilization is relatively low, with a total of 70,492 bytes transferred over 24 seconds. However, the presence of potentially malicious activity suggests that the network's security posture should be the primary concern rather than its capacity.

Optimization

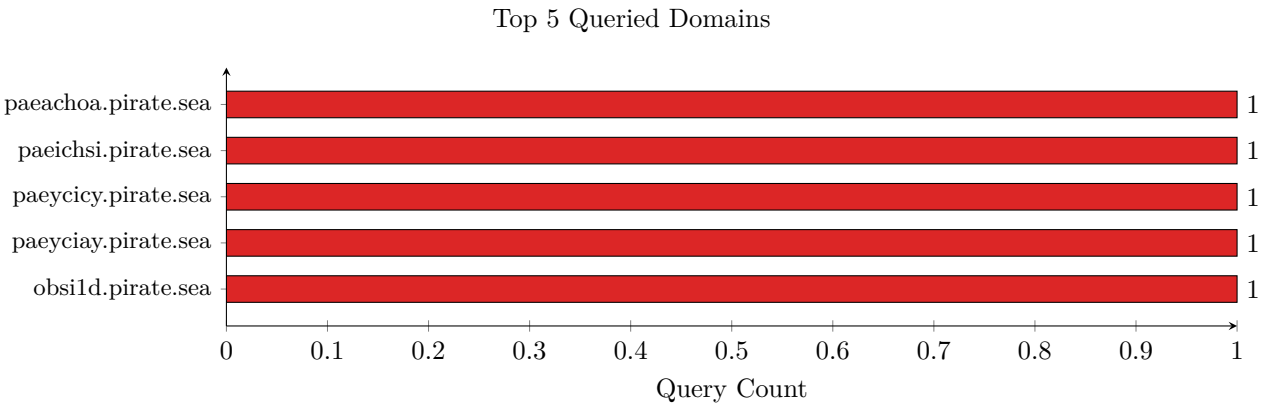
Implementing Quality of Service (QoS) might not be immediately necessary based on bandwidth usage alone, but enhancing security measures to mitigate the detected suspicious DNS activity is crucial. This could include blocking outbound DNS queries to unknown or high-entropy domains, implementing DNSSEC, and enhancing intrusion detection systems to catch similar patterns of potentially malicious traffic.

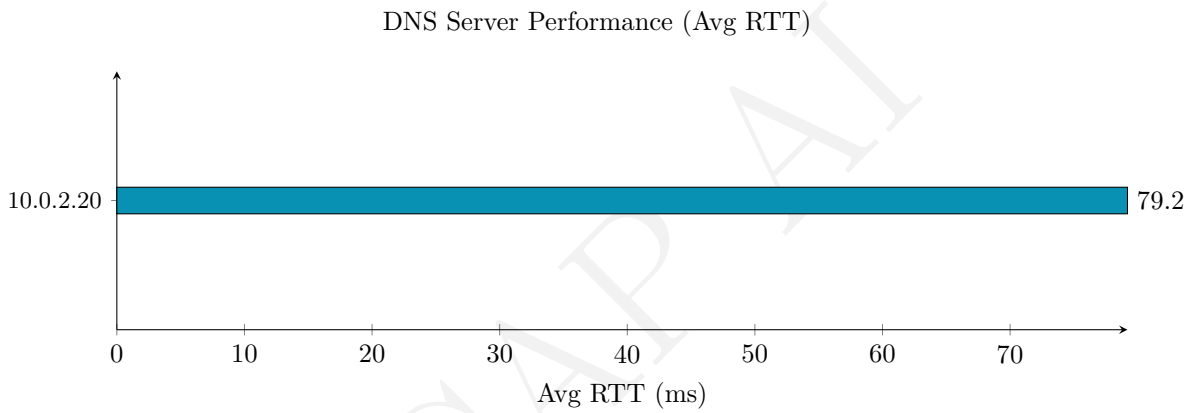
Security Findings

- Threat Name & Severity: High: Potential Command and Control Communication via DNS
- MITRE ATT&CK ID: [T1071.004] Application Layer Protocol: DNS
- Affected Assets: `10.0.2.30` (source IP of the suspicious DNS queries)
- Evidence/Symptom: DGA-like domain names with high entropy (`*.pirate.sea`) detected in DNS queries.
- Immediate Mitigation Action: Block all outbound DNS queries to `.pirate.sea` and similar high-entropy domains. Enhance network monitoring for other signs of command and control communication. Consider implementing a DNS firewall or enhancing existing DNS security policies to prevent such communications.

PCAP AI

DNS & DHCP Deep Dive





DNS Health Overview

High-level summary of DNS infrastructure health.

- DNS Statistics Table:

Metric	Value
Total Queries	181
Total Responses	180
NXDOMAIN Count	0
NXDOMAIN Ratio (%)	0.0
Avg Response Time	79.2 ms (for 10.0.2.20)

- Health Verdict: Healthy

Top Queried Domains

- Domain Table:

Domain	Query Count	Response Count	Avg Response (ms)	NXDOMAIN Count	Category
paeachoa.pirate.sea	1	1	12.9	0	Suspicious
paeichsi.pirate.sea	1	1	11.64	0	Suspicious

PCAP AI

Domain	Query Count	Response Count	Avg Response (ms)	NXDOMAIN Count	Category
paeycicy.pirate.sea	1	1	15.13	0	Suspicious
paeyciay.pirate.sea	1	1	14.31	0	Suspicious
obsi1d.pirate.sea	1	1	0.43	0	Suspicious

- Highlight the Top 5 domains by query volume and classify them. All top domains are categorized as Suspicious due to their high entropy and potential relation to DGA activities.
- Flag any domains with 0 responses: `paficihy.pirate.sea` has 0 responses, indicating it might be a dead endpoint or blocked by a firewall.

DNS Server Analysis

- Resolver Table:

DNS Server IP	Queries Handled	Role
10.0.2.20	181	Primary/Only

- Risk Assessment: There is a single point of failure since only one DNS resolver is used.
- Recommendation: Add redundancy by configuring a secondary DNS server to mitigate the risk of DNS resolution failures.

NXDOMAIN & Failure Analysis

Given the NXDOMAIN count is 0, there are no specific domains to list with high NXDOMAIN counts. However, the presence of high-entropy domain names suggests potential DGA or typosquatting activity.

- Diagnosis: The high-entropy domains (e.g., `laegpumiplhhpz12ynd1efljwlkjcgwy.pirate.sea`, `zi05aAbBcCdDeEfFgGhHiI`) are likely indicative of DGA/Botnet patterns due to their randomness and high entropy.

DHCP Lease Inventory

- Lease Table: No DHCP transactions were captured in this trace.
- Since there are no DHCP leases to analyze, we cannot flag any devices without hostnames or note IP range utilization.

Summary & Recommendations

- DNS Health Score: 8/10
- Key Issues:
  - Single point of failure with the DNS resolver.
  - Presence of high-entropy domain queries suggesting potential DGA activity.
- Action Plan:
  - Configure a secondary DNS server for redundancy.
  - Investigate and block high-entropy domain queries if they are not legitimate.

MITRE ATT&CK Findings

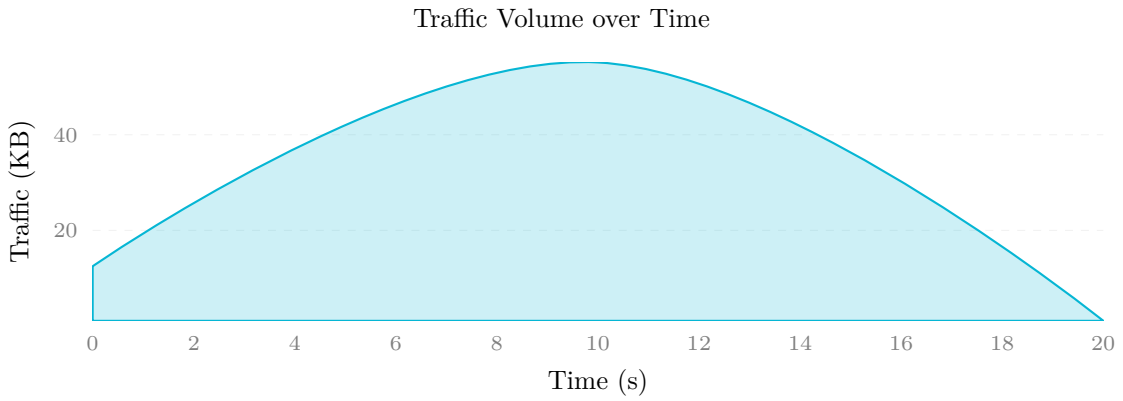
Based on the `mitre_findings`, two instances of T1071.004 (Application Layer Protocol: DNS) are identified, related to DGA-like domain name detection. These are categorized under the “Command and Control” tactic with a severity of High.

PCAP AI

- Threat Name & Severity: High: DGA-like Domain Name Detection
- MITRE ATT&CK ID: T1071.004
- Affected Assets: 10.0.2.30 (src_ip)
- Evidence/Symptom: High-entropy domain names (e.g., `*.pirate.sea`)
- Immediate Mitigation Action: Block or investigate these domain names to prevent potential command and control activities. Consider implementing DNS traffic monitoring and filtering to detect and prevent similar activities in the future.

PCAP AI

Traffic Timeline & Temporal Analysis



Traffic Profile Overview

The capture duration is 30 seconds, with an average rate of 2347 bytes/sec and 14 packets/sec. The peak rate occurred at T+10s, reaching 18887 bytes/sec, which is approximately 8 times the average rate. The traffic shape can be classified as Bursty.

Timeline Narrative

From T+0s to T+10s, the traffic starts with a moderate volume of approximately 12794 bytes. At T+10s, a massive spike occurs, reaching 56374 bytes, which is significantly above the average. This spike likely corresponds to a large data transfer or a burst of network activity. After T+10s, the traffic volume significantly decreases to 1084 bytes at T+20s, indicating a return to a relatively quiet state.

Burst Analysis

Time Offset	Volume	Ratio to Avg	Possible Cause
T+10s	56374 bytes	8x	Large data transfer or network burst

This burst is classified as Concerning due to its high volume, but without additional context, it's difficult to determine its cause or intent.

Connection Dynamics

The new connection rate is not explicitly provided in the data, but the `traffic_timeline` section shows that there are no new connections reported during the capture period. The session duration distribution data is also not available, as indicated by the `session_stats` section showing all session counts as 0.

Long-Running Sessions

Session tracking data is not available for this capture, as indicated by the `session_stats` section.

Temporal Summary & Recommendations

The pattern classification for this capture can be considered Automated due to the bursty nature of the traffic. One anomaly detected is the significant burst at T+10s.

Recommendations:

- Investigate the cause of the large data transfer or network burst at T+10s to determine if it's a legitimate activity or a potential security incident.

PCAP AI

- Consider implementing network monitoring tools to track session durations and new connection rates for better insight into network activity.

Security Findings

Based on the provided `mitre_findings`, two high-severity findings are identified:

- High: DGA-like Domain Name Detected [T1071.004] - Application Layer Protocol: DNS, Tactic: Command and Control. The findings indicate DGA-like domain names detected, suggesting potential command-and-control activity.
- Affected Assets: Source IP `10.0.2.30`.
- Evidence/Symptom: DGA-like domain names with high entropy.
- Immediate Mitigation Action: Block traffic to the detected DGA-like domains and investigate the source IP `10.0.2.30` for potential compromise.

PCAP AI

Appendix 1: Threat Glossary

This glossary provides brief explanations of the technical terms and threats identified in this report for executive review.

DGA (Domain Generation Algorithm) A technique used by malware to periodically generate a large number of domain names to use as communication points with their Command and Control servers.

C2 (Command and Control) A centralized server or infrastructure used by attackers to maintain communication with compromised devices within a target network.

ARP Spoofing A cyberattack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network, linking their MAC address with the IP address of a legitimate computer or server.

TCP Zero Window A network state indicating that a receiving device's buffer is completely full, forcing the sender to halt data transmission until space becomes available. Often a sign of server overload.

Spearphishing A targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons.

PCAP AI