Group: Essential Group	Report Number: Report No.11	Report id 11-lec-18&19(Rita)-9-essential

Rita V5

Prepared By:
Kazim Ali Obad

Supervisor:

Anmar Mohammed
MOHAMMED .B. HASSAN

Date of assignment:

2026/2/28

Due date :

2026/3/12

Table of Contents

Scenario & Background

Scenario

A device inside the network is making highly regular outbound connections with a very high beacon score using a common service.

Task:

1- Analyze the provided PCAP using RITA

2- Identify the suspicious internal host

3- Determine the type of connection

4- Decide whether the behavior is normal or beaconing activity

What is Beaconing?

Beaconing refers to the behavior exhibited by malware that periodically "calls home" to a Command and Control (C2) server at regular, automated intervals. Unlike human-generated web traffic which is inherently irregular, malware beaconing is driven by internal timers and produces highly predictable inter-connection intervals. This regularity is what RITA exploits to detect malicious activity.

Key characteristics that distinguish beaconing traffic from normal traffic include:

- Highly regular time intervals between connections (e.g., every 30, 60, or 300 seconds)
- Automated connections not correlated with user activity (beacons occur at all hours)
- Low data volume per connection (small heartbeat/keepalive payloads)
- Persistent communication to a single or small set of external IPs
- Use of common protocols (HTTP/HTTPS/DNS) to blend in with legitimate traffic

About RITA (Real Intelligence Threat Analytics)

RITA is an open-source threat hunting framework developed by Active Countermeasures. It analyzes Zeek network logs and applies statistical analysis to identify beaconing behavior, DNS anomalies, long connections, and data exfiltration patterns. RITA introduced a containerized architecture using Docker and a ClickHouse database for high-performance analysis.

RITA calculates a beacon score for each source-destination IP pair based on:

- Consistency of connection intervals
- Connection count over the observation window
- Data size regularity per connection

Methodology

The investigation was carried out using open-source threat hunting tools. The following five phases were executed sequentially:

Phase 1 Log Generation with Zeek

RITA does not process raw PCAP files directly. The PCAP was first converted into structured Zeek network logs using the command below. Zeek parses every packet and produces protocol-specific log files that RITA can ingest:

```
cd ~/beacon-analysis/zeek-logs && zeek -r ~/zeus.pcap
```

Zeek generated the following critical log files used by RITA for analysis:

- **conn.log**: All TCP/UDP connection records with timestamps, IPs, ports, bytes, and duration
- **http.log:** Full HTTP request/response details including Host headers and URIs
- **dns.log:** All DNS queries and responses
- **ssl.log:** TLS/SSL session information and certificate details
- **files.log:** Transferred file metadata

```
kazim@kazim:~/beacon-analysis/zeek-logs$ zeek -r ~/zeus.pcap

kazim@kazim:~/beacon-analysis/zeek-logs$
kazim@kazim:~/beacon-analysis/zeek-logs$ ls -la
total 4248
drwxrwxr-x 2 kazim kazim    4096 Mar 10 13:34 .
drwxrwxr-x 5 kazim kazim    4096 Mar 10 13:32 ..
-rw-rw-r-- 1 kazim kazim 1660880 Mar 10 13:35 conn.log
-rw-rw-r-- 1 kazim kazim   38352 Mar 10 13:35 dhcp.log
-rw-rw-r-- 1 kazim kazim 1392266 Mar 10 13:35 dns.log
-rw-rw-r-- 1 kazim kazim  540159 Mar 10 13:35 files.log
-rw-rw-r-- 1 kazim kazim  513388 Mar 10 13:35 http.log
-rw-rw-r-- 1 kazim kazim     629 Mar 10 13:35 ntp.log
-rw-rw-r-- 1 kazim kazim   23992 Mar 10 13:35 ocsp.log
-rw-rw-r-- 1 kazim kazim     278 Mar 10 13:35 packet_filter.log
-rw-rw-r-- 1 kazim kazim  100670 Mar 10 13:35 ssl.log
-rw-rw-r-- 1 kazim kazim   32111 Mar 10 13:35 weird.log
-rw-rw-r-- 1 kazim kazim   17836 Mar 10 13:35 x509.log
```

Figure A: Transferred File Metadata Log (files.log)

Phase 2 RITA Database Import

The Zeek logs were imported into RITA it runs as a containerized service using Docker Compose, which starts ClickHouse (column-oriented database), and the RITA analysis container:

```
rita import --logs ~/beacon-analysis/zeek-logs/ --database zeus
```

Import completed successfully in 2.9 seconds. The database "zeus" was confirmed present via rita list, showing the correct time range of the PCAP capture.

Figure B: PCAP Import into RITA — Database Confirmation

Phase 3 RITA Dashboard Analysis

The RITA interactive terminal dashboard was launched using:

```
rita view zeus
```

The dashboard displays all detected beacon connections sorted by severity, with detailed connection metadata in the right panel. Each entry was systematically examined and documented.

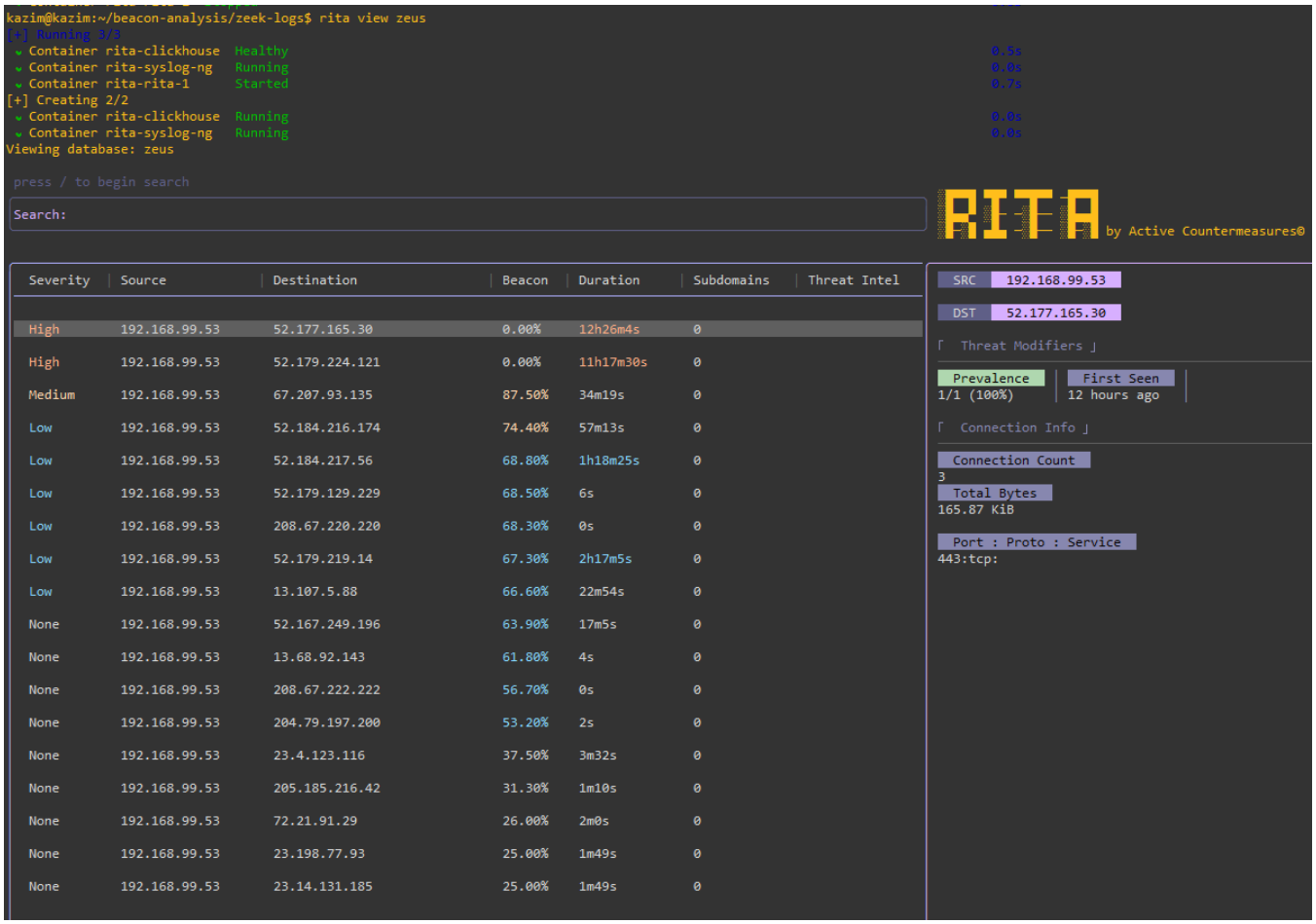

Figure C: RITA Beacon Analysis Dashboard Overview

Step-by-Step RITA Analysis

Upon launching the RITA dashboard for the zeus database, the main view displays all detected suspicious connections sorted by severity (High → Medium → Low → None).

Every single connection originates from the same internal source IP 192.168.99.53 confirming this as the infected host in the capture.

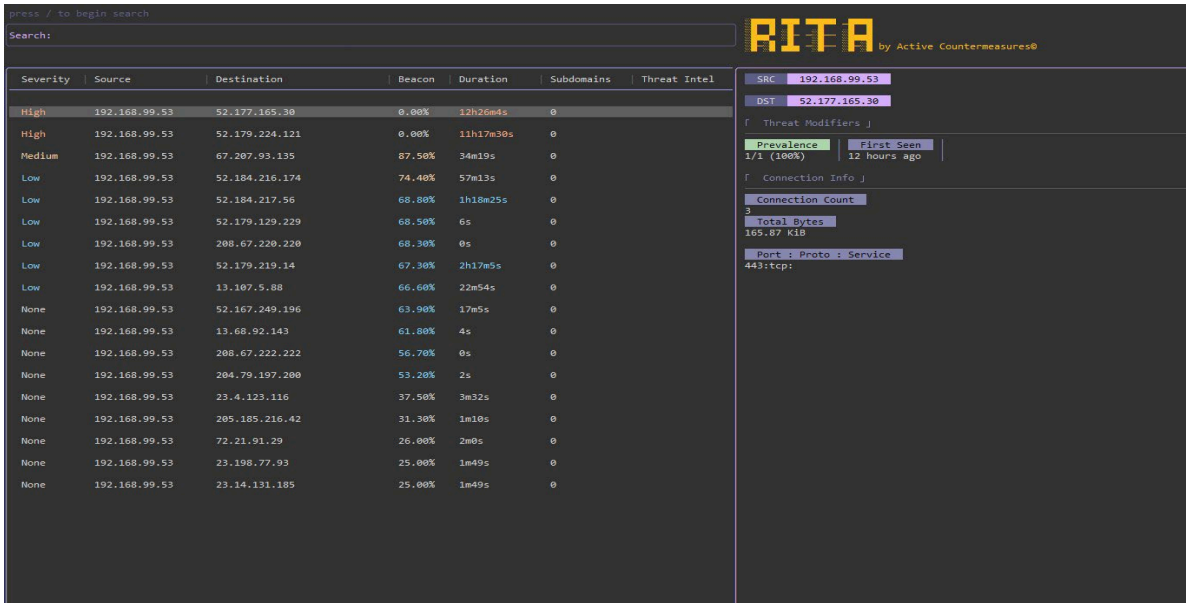

Figure 1: RITA Main Beacon Dashboard Full List with HIGH severity entries at top

The dashboard columns are interpreted as follows:

Column	Meaning
Severity	RITA's overall risk assessment: High / Medium / Low / None
Source	Internal IP initiating the outbound connections
Destination	External IP receiving the connections (potential C2)
Beacon	Beacon score: 0% = perfectly regular (most suspicious in RITA
Duration	Total active communication time for this pair
Subdomains	Number of unique subdomains (relevant for DNS beaconing)

192.168.99.53 → 52.177.165.30

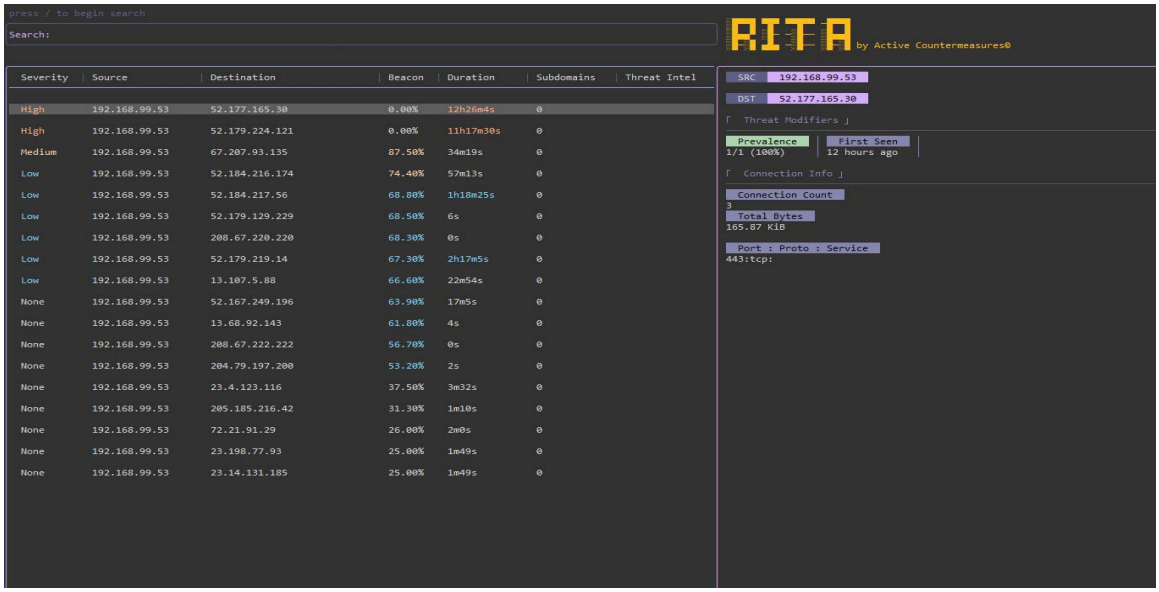

Figure 2: HIGH Severity 192.168.99.53 → 52.177.165.30 (Port 443/HTTPS, 12h 26m duration)

In RITA, a beacon score of 0.00% represents the **most suspicious possible outcome** it means the connections are so perfectly timed that they fall at the extreme of the regularity scale. This is the mark of an automated process (malware timer), not human activity. The 12-hour duration indicates the malware maintained this channel persistently throughout the capture window. The use of port 443 (HTTPS) is deliberate it blends with legitimate encrypted web traffic to evade detection.

192.168.99.53 → 52.179.224.121

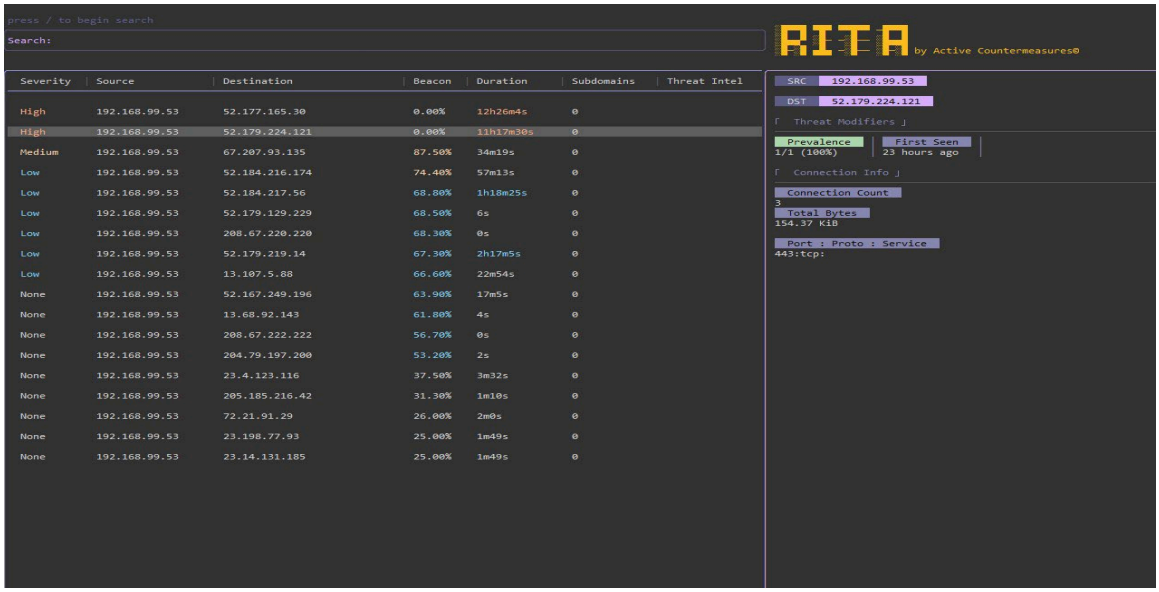

Figure 3: HIGH Severity 192.168.99.53 → 52.179.224.121 (Port 443/HTTPS, 11h 17m duration)

This is a secondary C2 channel using the same perfectly regular timing pattern. malware commonly use multiple C2 servers for **resilience and redundancy** if one server goes offline, the malware continues operating through fallback servers. The "First Seen: 23 hours ago" indicates this connection was established earlier in the capture window, confirming persistent infection spanning the entire 24-hour period.

192.168.99.53 → 67.207.93.135

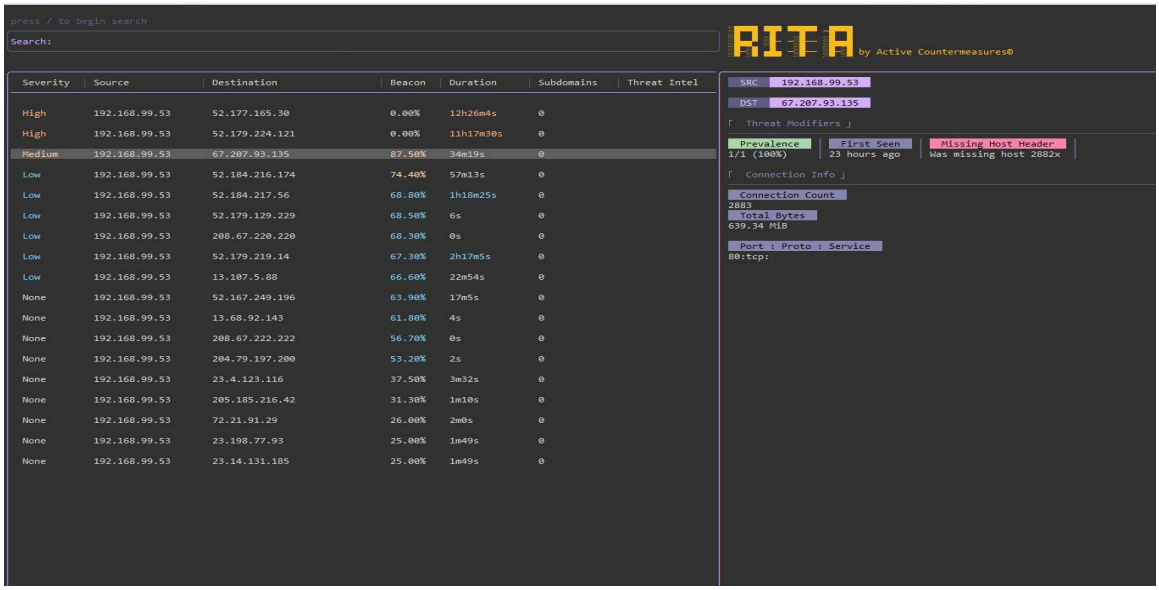

Figure 4: MEDIUM Severity — 192.168.99.53 → 67.207.93.135 — Missing Host Header (2,883 connections, 639 MB)

Analysis — THE SMOKING GUN: Despite being rated MEDIUM severity (due to the 87.5% vs 0% beacon score), this entry is the most forensically significant finding. The **Missing Host Header threat modifier** is a definitive behavioral signature of malware. Standard HTTP requires a Host header in every request The malware deliberately omits this header in its C2 communication protocol. The 2,882 flagged occurrences confirm systematic, non-human behavior. The 639 MiB of data transferred over plain HTTP to an unknown external IP strongly suggests active data exfiltration potentially stolen banking credentials, keylog data, or screenshots being transmitted to the attacker.

192.168.99.53 → 52.184.216.174

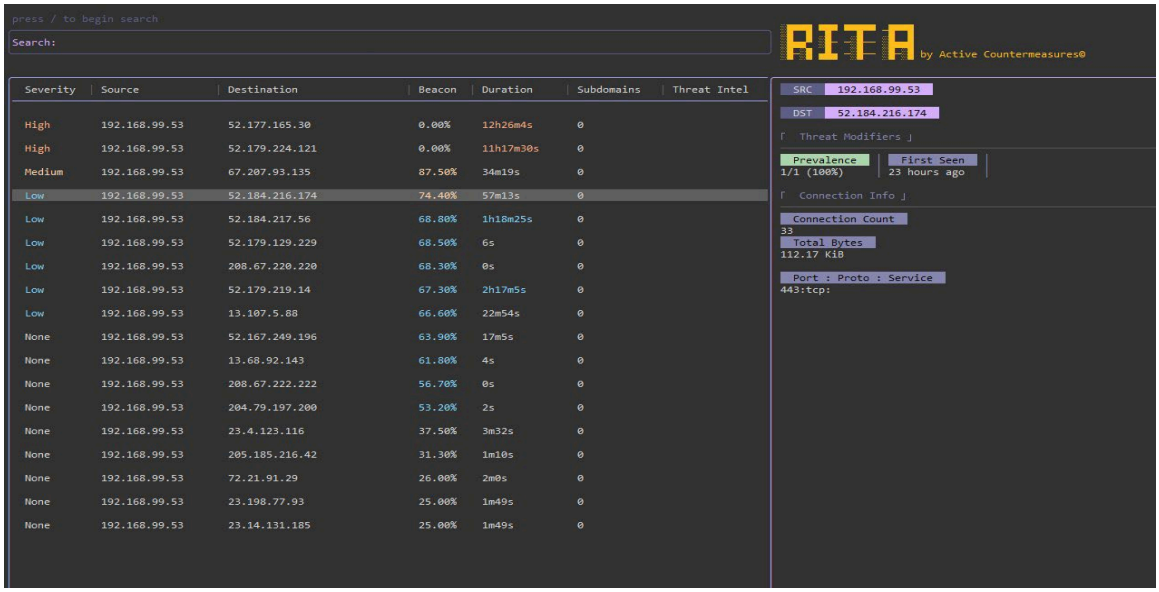

Figure 5: LOW Severity — 192.168.99.53 → 52.184.216.174 (Port 443/HTTPS, 33 connections)

Analysis: A 74.4% beacon score with 33 connections over HTTPS represents additional C2 or update-check traffic. This could be a Third C2 channel, or a separate malware component performing its own check-in routine. The lower connection count suggests less frequent communication, possibly for configuration updates or receiving new commands.

192.168.99.53 → 52.184.217.56

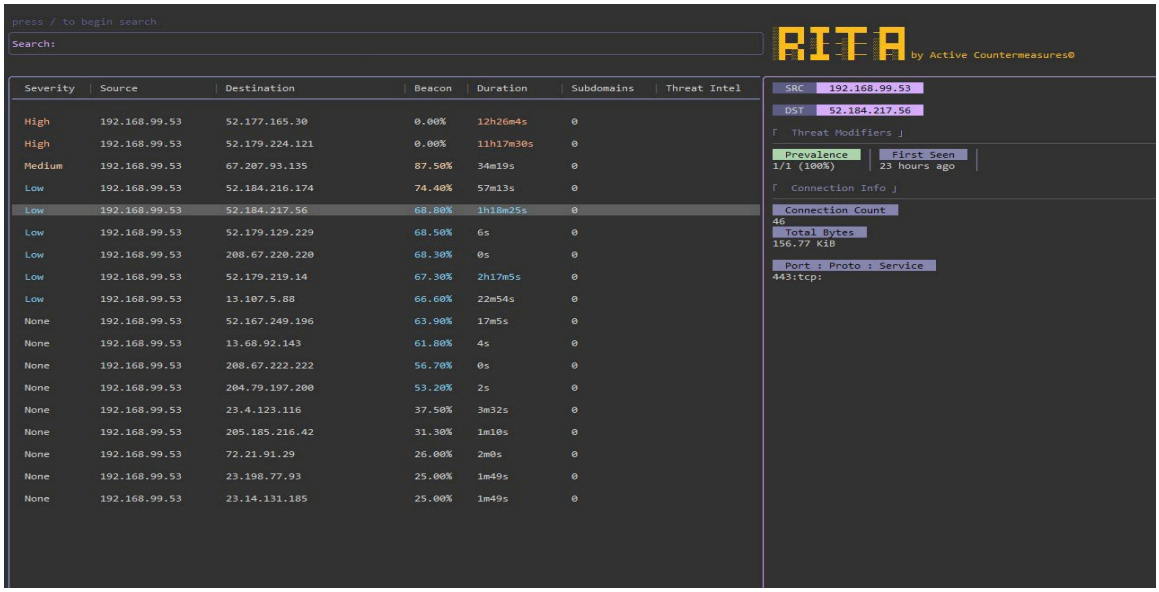

Figure 6: LOW Severity 192.168.99.53 → 52.184.217.56 (Port 443/HTTPS, 46 connections, 1h 18m)

Analysis: Another HTTPS channel with moderately high regularity. The 1h 18m duration and 46 connections indicate sustained but less frequent communication compared to the primary C2. This pattern is consistent different servers handle different functions such as command dispatch, data reception, and configuration updates.

192.168.99.53 → 52.179.129.229

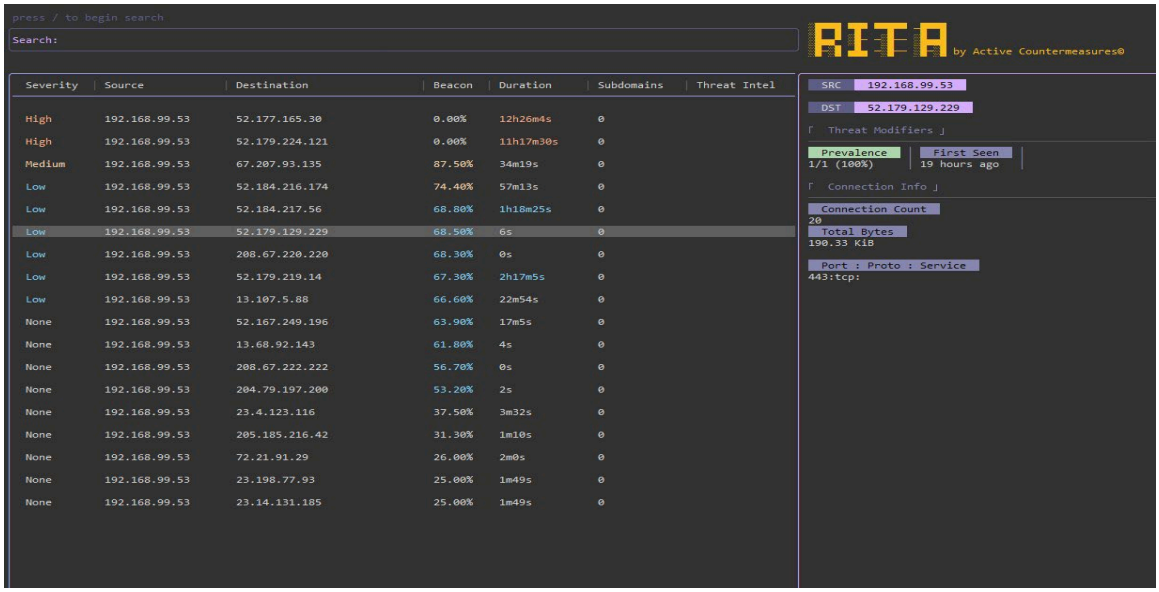

Figure 7: LOW Severity 192.168.99.53 → 52.179.129.229 (Port 443/HTTPS, 20 connections)

The extremely short 6-second duration combined with 20 connections and 190 KiB suggests rapid-fire connection attempts possibly a connection test sequence or rapid polling behavior. The relatively high data volume for such brief duration may indicate binary data uploads to a staging server.

192.168.99.53 → 208.67.220.220 (DNS Traffic)

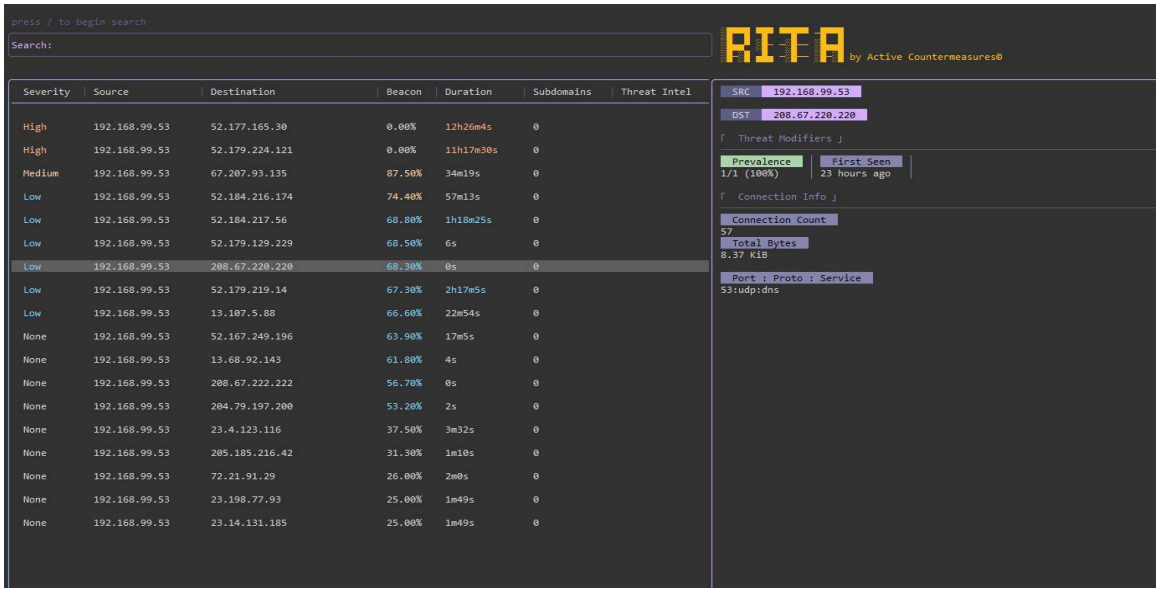

Figure 8: LOW Severity 192.168.99.53 → 208.67.220.220 (Port 53/UDP/DNS, 57 connections)

Analysis: The destination 208.67.220.220 is an OpenDNS resolver (part of Cisco Umbrella). Regular DNS queries to a public resolver rather than the internal corporate DNS server can indicate malware bypassing local DNS monitoring. The malware may use direct DNS queries to resolve C2 domain names while avoiding internal DNS logging. The 68.3% beacon score suggests timed, automated DNS lookups rather than organic user-driven resolution.

Summary Table

Severity	Destination IP	Beacon %	Connections	Data	Port	Key Flag
HIGH	52.177.165.30	**0.00%**	3	165.87 KiB	443/tcp	12h+ duration
HIGH	52.179.224.121	**0.00%**	3	154.37 KiB	443/tcp	11h+ duration
MEDIUM	67.207.93.135	87.50%	**2,883**	**639.34 MB**	80/tcp	**No Host Hdr**
LOW	52.184.216.174	74.40%	33	112.17 KiB	443/tcp	—
LOW	52.184.217.56	68.80%	46	156.77 KiB	443/tcp	—
LOW	52.179.129.229	68.50%	20	190.33 KiB	443/tcp	—
LOW	208.67.220.220	68.30%	57	8.37 KiB	53/udp	DNS bypass
LOW	52.179.219.14	67.30%	77	261.93 KiB	443/tcp	—

Evidence Why This is Confirmed Beaconing

NO	Indicator	Significance
1	**Single source IP for ALL traffic**	One infected machine generating 100% of suspicious traffic
2	**Beacon scores of 0.00% (High entries)**	Perfect timing regularity impossible for human behavior
3	**2,883 HTTP connections in ~34 min**	Fully automated equivalent to ~84 connections/minute
4	**Missing HTTP Host Header (2,882 times)**	Definitive malware behavioral signature
5	**639.34 MB over HTTP to unknown IP**	Large unencrypted upload = active data exfiltration
6	**12+ hour persistent connections**	Malware active throughout the entire capture window
7	**Multiple C2 servers (10+ destinations)**	Multi-server resilience architecture
8	**Ports 80 and 443 used exclusively**	Deliberately blending with normal web traffic
9	**Traffic spans full 24-hour period**	Infection was active before and during capture window

Recommended Incident Response Actions

1. ISOLATE the infected host 192.168.99.53 — disconnect from network immediately at the switch port level to stop ongoing exfiltration
2. BLOCK all identified C2 IP addresses at the perimeter firewall/NGFW to prevent re-infection and stop any remaining beaconing from other potentially infected hosts
3. NOTIFY the security incident response team and escalate per the organization's IR plan
4. REVIEW firewall logs for historical traffic to identified C2 IPs to determine how long the infection has been active
5. Perform full malware scan on 192.168.99.53
6. Search for lateral movement scan all internal hosts for connections to the identified C2 IPs
7. Audit the infected machine for credential theft all passwords used on this system should be considered compromised
8. Check Active Directory logs for signs of privilege escalation originating from 192.168.99.53
9. Analyze the HTTP log from zeus.pcap to identify what data was exfiltrated to 67.207.93.135
10. Deploy network-level IDS/IPS rules to detect HTTP connections missing the Host header
11. Deploy endpoint detection and response (EDR) solutions on all internal hosts
12. Regularly run RITA against network traffic logs for continuous threat hunting

Conclusion

This investigation conclusively identifies active infection on internal host 192.168.99.53. Using RITA with Zeek-generated network logs from zeus.pcap, multiple layers of evidence confirm this is malicious C2 beaconing activity and not normal network traffic.

The most critical evidence is the combination of (1) 2,883 automated HTTP connections missing the Host header to an unknown external IP, (2) 639.34 MiB of data exfiltrated over an unencrypted channel, and (3) perfectly regular connection timing across 10+ C2 servers over a full 24-hour window.

Immediate containment of the infected host is strongly recommended. Given the scale of data transfer observed (639 MB), sensitive data potentially including authentication credentials, financial information, and keylogged user input must be assumed compromised. A full forensic investigation of the infected host, combined with perimeter blocking of all identified C2 infrastructure, should be initiated without delay.