SHADOWSERVER

Lighting the way to a more secure Internet

Internet Spelunking

IPv6 Scanning and Device Fingerprinting

Dave De Coster // Piotr Kijewski

decoster@shadowserver.org // piotr@shadowserver.org

30th June, 2022

2022 FIRST Annual Conference, Dublin

SHADOWSERVER.ORG

What is The Shadowserver Foundation

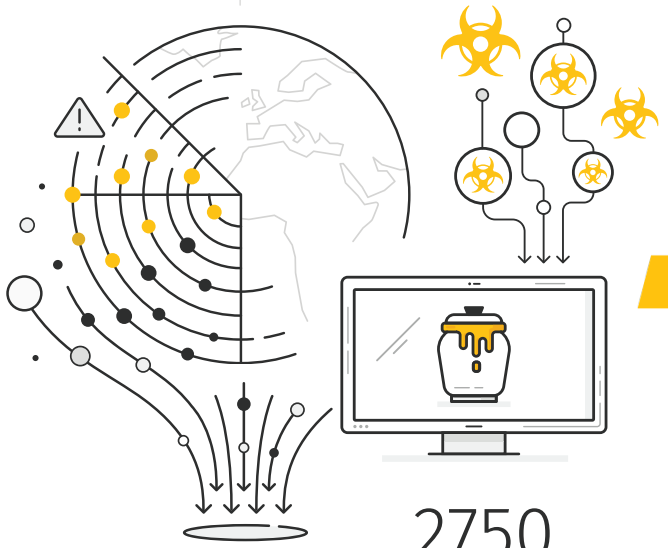
- A not-for-profit organisation (NPO) working to make the Internet more secure for everyone.
- **Unique sources**, a **global vantage point** and **proven partnerships** with:
  - *National Computer Security Incident Response Teams (nCSIRTs)*
  - *Law Enforcement*
  - *Industry and security researchers world-wide*
- **Shares information with Internet defenders at no cost** to mitigate vulnerabilities, detect malicious activity and counter emerging threats.
- An unparalleled combination of position, **trusted information** and **18 years of proven community partnerships** enables Shadowserver to **perform a critical role in Internet security** - **the world's largest provider of free cyber threat intelligence.**

SHADOWSERVER

Shadowserver by (some of the) numbers

3.7 BILLION

IPv4 addresses scanned **103** times per day (**820 Million** IPv6 10 times per day). **381 Million** hosts respond



4-5 MILLION

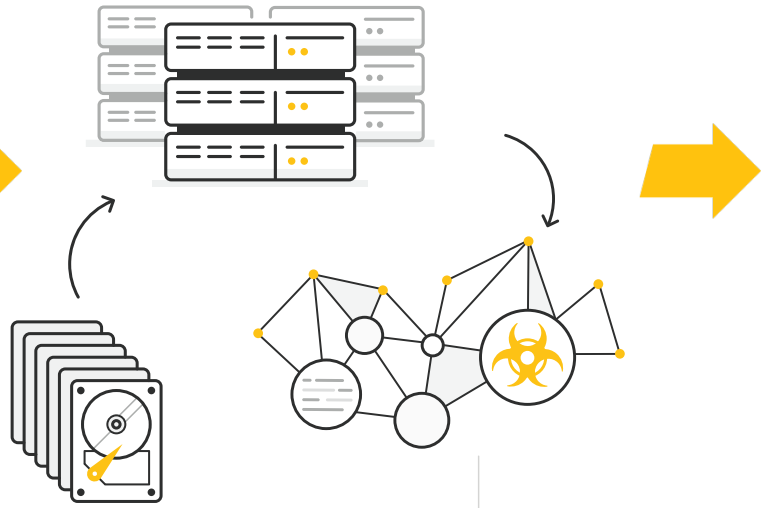
IP addresses per day sinkholed across **400** different malware variants

2750

Class C networks hosting honeypots & spampots

1,115,000

unique malware samples ingested & analyzed **every day** by our sandboxes. Over **1.7 billion samples** in our malware repository



12 PETABYTES

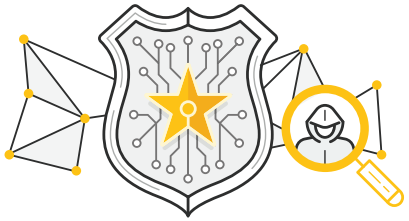
of malware & threat intel stored, **growing at 1+ PB/year**

40 BILLION

SSL certificates, indexed & searchable in our data & analysis clusters

7,000

network owners & **133 National CSIRTs in 175 countries and territories** rely on our **free** daily reports



Behind the scenes support for dozens of international Law Enforcement operations

SHADOWSERVER

So, About Our Scanning …

Big numbers

149,281,685 Reported IPs

107,252,144,957 UDP Probes

225,577,728,428 TCP SYN

407,092,432 Full Handshakes

Ground Rules

Do no harm

Never exploit

Test, test, test, 1/250th test

Test some more

First, do no harm

- Scans will not compromise, harm, or degrade system performance
  - Use the smallest and most minimal packet possible to get the results
  - Test repeatedly before a full Internet scan occurs
  - 1/250th test
- Only scan what is necessary for remediation
  - Vulnerable or misconfigured systems
  - Specific ports used by criminal infrastructures
- Scans will not break any US laws

SHADOWSERVER

How Did We Get Here?

No (good?) deed goes unpunished.

The Origin

You can all thank Christian Rossow for publishing:

"Amplification Hell: Revisiting Network Protocols for DDoS Abuse"

https://christian-rossow.de/publications/amplification-ndss2014.pdf

The Origin

- Started with DNS
  - It was easy
  - Miscreants were already abusing it
  - There were already two open DNS scanners available for us to confirm results against
    - Other data sets were deemed too polluted to be used easily for reporting purposes
    - Cleaning other data sets was difficult and the actual methodology of scanning was flawed by both other scanning entities
    - Better to build something new to meet our more narrow scope and mission

The Origin Story

- First scan took 91 hours to complete
- 16.9 million responses (53/udp only)
- 12.25 million openly recursive

SHADOWSERVER

Fast Forward to curdate()

- The DNS scan now runs in 4 hours
  - 6 million total responses (53/udp only)
  - 1.8 million recursive resolvers

~10.4 million IPs that are no longer abusable

SHADOWSERVER

Hey, It worked!

After discovering that the scanning worked, we:

- Acquired more hardware
- Acquired more bandwidth
- Wrote new scanning tools
- Proceeded to implement scans on the rest of the named UDP targets

SHADOWSERVER

Something Different!

Smooth sailing until October 2014

- POODLE (SSLv3 Downgrade)
  - Padding Oracle On Downgraded Legacy Encryption

SHADOWSERVER

Needed to learn some new tricks..

Discovered that scanning /0 for UDP is *much* easier than TCP

- UDP is just Spray'n'Pray (with some limits)
  - Self DDoS's can hurt if not controlled and rate limited
- TCP you have to track state and scan (at least) twice
  - And you have to talk x509!

SHADOWSERVER

Success! (it took a bit)

- First reported POODLE data:
  - November 2014
  - 15,573,251 IPs vulnerable to a downgrade attack

SHADOWSERVER

Fast Forward to curdate()

POODLE (SSLv3) now:

- 2,365,512

- Still a big number, but better

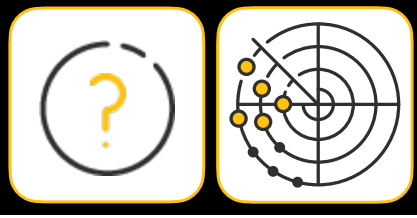
SHADOWSERVER

Expansion of the beast

We couldn’t let all the lessons we learned sit idle, so we added in a *few* more scans..

SHADOWSERVER

Over 100 Full Scans a Day (IPv4)



Protocol	Port	Protocol	Port	Protocol	Port	Protocol	Port	Protocol	Port	Protocol	Port
AMQP	5672/tcp	DVR DHCPDiscover	37810/udp	HTTPS	10443/tcp	LDAP	389/tcp	NTP (Monitor)	123/udp	SMB	445/tcp
Android Debug Bridge	5555/tcp	ElasticSearch	9200/tcp	HTTPS	8010/tcp	mDNS	5353/udp	NTP (Version)	123/udp	SMTP	25/tcp
Apple File Protocol	548/tcp	EPMD	4369/tcp	HTTPS	5001/tcp	MELSEC-Q	5007/tcp	Omron FINS	9600/udp	SMTP (IPv6)	25/tcp
Apple Remote Management	3283/udp	EtherCAT	34980/udp	HTTPS	4433/tcp	MemCacheD	11211/udp	OPC-UA	4840/tcp	SNMPv2	161/udp
BACnet	47808/tcp	EtherNet/IP	44818/tcp	HTTPS	6443/tcp	MemCacheD	11211/tcp	PCWORX	1962/tcp	SOCKS4/5	1080/tcp
CharGEN	19/udp	FTP	21/tcp	HTTPS	447/tcp	Microsoft Exchange	443/tcp	PLEX SSDP	32414/udp	SSDP	1900/udp
cLDAP	389/udp	GE-SRTP	18245/tcp	HTTPS	4117/tcp	Middlebox	80/tcp	Portmapper	111/udp	SSH	22/tcp
CoAP (v1)	5683/udp	Hadoop (DataNode)	50075/tcp	HTTPS	8080/tcp	Mikrotik (Speed Test)	2000/tcp	PostgreSQL	5432/tcp	SSH (IPv6)	22/tcp
CoAP (v2)	5683/udp	Hadoop (NameNode)	50070/tcp	HTTPS	5443/tcp	Mitel	10074/udp	PostgreSQL (IPv6)	5432/tcp	SYNful Knock	80/tcp
CODESYS IEC 61131-3	2455/tcp	HART	5094/tcp	HTTPS	7443/tcp	MODBUS	502/tcp	ProConOS	20547/tcp	Telnet	23/tcp
CODESYS IEC 61131-3	1200/tcp	HTTP	80/tcp	HTTPS (IPv6)	443/tcp	MongoDB	27017/tcp	QOTD	17/udp	Telnet	2323/tcp
CouchDB	5984/tcp	HTTP (IPv6)	80/tcp	HTTPS	443/tcp	MQTT	1883/tcp	QUIC	443/udp	Telnet (IPv6)	23/tcp
Crimson (Red Lion)	789/tcp	HTTP	8080/tcp	ICCP	102/tcp	MQTT SSL	8883/tcp	Radmin	4899/tcp	TFTP	69/udp
CWMP	7547/tcp	HTTP (IPv6)	8080/tcp	IEC 60870-5-104	2404/tcp	MS-SQL	1434/udp	RDP	3389/tcp	Tridium Niagra	1911/tcp
CWMP	30005/tcp	HTTP	8000/tcp	IPMI	623/udp	MySQL	3306/tcp	RDPEUDP	3389/udp	Ubiquiti Discovery Service	10001/udp
DB2	523/udp	HTTPS	8443/tcp	IPP	631/tcp	MySQL (IPv6)	3306/tcp	Redis	6379/tcp	VNC	5900/tcp
DNP3	20000/tcp	HTTPS (IPv6)	8443/tcp	ISAMKP	500/udp	NAT-PMP	5351/udp	rsync	873/tcp	VNC	5901/tcp
DNS	53/udp	HTTPS	9000/tcp	Kubernetes	6443/tcp	NetBIOS	137/udp	S7	102/tcp	XDMCP	177/udp
Docker	2375/tcp	HTTPS	449/tcp	Kubernetes	443/tcp	Netis	53413/udp	SmartInstall	4786/tcp		

SHADOWSERVER

How and Why are the next targets chosen

- Topical – new blog comes out with a vulnerability that can be remotely tested
  - Netis, Synfulknock, ISAKMP, etc
- Looking at legacy protocols that really should not be exposed
  - Telnet, rsh, etc
- Current protocols that really should not be exposed
  - MongoDB, Kubernetes, etc
- Someone asked us to look for it

Fun Facts

We have sent (with daily repeats):

- 209,724,213,326,259 UDP Probes
  - 209.7 Trillion UDP Probes
- 221,639,352,853,200 TCP SYNs
  - 221.6 Trillion TCP Syns
- 508,013,815,018 Full Protocol Connections
  - 508 Billion Connections
- 287,916,573,658 Services for remediation
  - 287.9 Billion Reported

SHADOWSERVER

Sorry for the noise…

The Gear

How the work gets done – Grab the hearing protection

Stack o’ Boxes in a Colo

Just a pile of leftover gear

- 37 x servers
- 2 x 10 Gb/s lines
- 5 x /26 IPv4 blocks (and 1 /24)
- 1 x /64 IPv6 block

SHADOWSERVER

Dirtiest CIDRs on the net?

- We scan from 558 IPv4 addresses:

  [redacted]

- And 1221 IPv6 addresses:

  [redacted]

- Nodes are each assigned 15 IPv4 and 33 IPv6 addrs
- Evenly split across 2x 10 gb lines

Scanning Methodology

- TCP and UDP scans are handled differently
  - TCP Scans are:
    - Broken into shards
      - Shard is 1/250th of the IP space to be scanned
      - IPs in a shard are algorithmically determined by a random seed that is supplied to every shard.
    - Will use the entire cluster to scan
    - Performed using commodity software
  - UDP Scans are:
    - Monolithic
    - Run from a single node
    - Performed using custom software

UDP Scans

- Meet “**railgun**”
  - Designed to send a single UDP packet as randomly as possible and as fast as possible to all 3.4B IPs
  - Tuned for sending small packets
  - Will send packets using all available IPs
  - Has very few safety measures

SHADOWSERVER

UDP Scans

- Railgun can usually scan the internet for one service in around four hours.
  - Highly dependent on the number of responding devices.

SHADOWSERVER

TCP Scans

- Commodity tools
  - Assignment of jobs:
    - HTCondor
  - Actual scanning:
    - Zmap performs the initial sweep
    - Zgrab (mostly) performs the connection
    - Other tools for doing custom things

SHADOWSERVER

TCP Scans

Each service takes between ten minutes and three hours

- Dependent on the complexity of the scan
  - Things with no crypto (Telnet) are fast
    - 8 minutes in human time
    - 3 hours and 57 minutes in machine time
  - Things with crypto (HTTPS) are much slower
    - 2 hours and 29 minutes in human time
    - 82 hours in machine time

SHADOWSERVER

Same From Here

- The raw data is:
  - Parsed (protocol specific)
  - Sanity checked (bad data?)
  - Standardized
  - Shipped off to the Datacenter to get turned into reports

IPv6

You want to scan what?

Surprisingly Familiar

- Like IPv4, just a LOT more of it
- Not feasible to scan it all, so curated lists
  - IPv6 addresses sourced from SSL certificates, IPv6 Hitlist, other.
- Currently scanning 814,675,045 IPv6 addresses

SHADOWSERVER

VARIOT

Blindly Scanning is Infeasible

IPv6 space is 3.48x10^38 unique addresses

Time to scan ~6.33x10^32 seconds

Roughly 2x10^25 years

SHADOWSERVER

VARIOT

Blindly Scanning is Infeasible

- Use curated lists from:
  - DNS AAAA records (passive DNS)
  - IPv6 Hitlist: https://ipv6hitlist.github.io/
  - Certificate transparency streams
  - Sinkholes
  - Partners

Yet Different…

Fewer options for scanning tools

- zmap6: https://github.com/tumi8/zmap
- zgrab/zgrab2 have native IPv6 support
- Other tools.. Not so much

SHADOWSERVER

VARIOT

And Slower…

IPv6 requires more gentle timings than IPv4

- IPv4: Potential packet loss at > 500,000 pps
- IPv6: Potential packet loss at > 100,000 pps

And Slower…

IPv6 requires more gentle timings than IPv4

- IPv4: Packet loss at > 3500 concurrent senders
- IPv6: Packet loss at > 1500 concurrent senders

And Slower…

Average number of IPs/second that can be processed

- IPv4: 243,116 IPs/second
- IPv6: 58,542 IPs/second

SHADOWSERVER

VARIOT

And Doesn’t Like to Share…

IPv4 and IPv6 scans don’t like running at the same time on the same interface

SHADOWSERVER

VARIOT

IPv6 Scans

- SSL (443/tcp, 8443/tcp)
- SMTP (25/tcp)
- TELNET (23/tcp)
- SSH (22/tcp)
- HTTP (80/tcp, 8080/tcp)
- MySQL (3306/tcp)
- FTP (21/tcp)
- PostgreSQL (5432/tcp)

SHADOWSERVER

VARIOT

IPv6 Scan Stats

Scan	Port	Responses
SSL	443/tcp	8 192 360
SSL	8443/tcp	75 432
SMTP	25/tcp	407 521
Telnet	23/tcp	25 267
SSH	22/tcp	839 575
HTTP	80/tcp	109 845 303
HTTP	8080/tcp	415 989
MySQL	3306/tcp	1 424 136
FTP	21/tcp	2 622 208
PostgreSQL	5432/tcp	34 795

SHADOWSERVER

VARIOT

IPv6 Scans (Observations)

SSL

- Fewer hosts with really old ciphers (SSLv3, TLSv1.0, TLSv1.1)
- 3.86% IPv4 vs 0.04% IPv6

FTP

- Far higher ratio of FTP+SSL
- 55% IPv4 vs 91% IPv6

MySQL

- Far fewer hosts with deny rules
- 42% IPv4 vs 4% IPv6

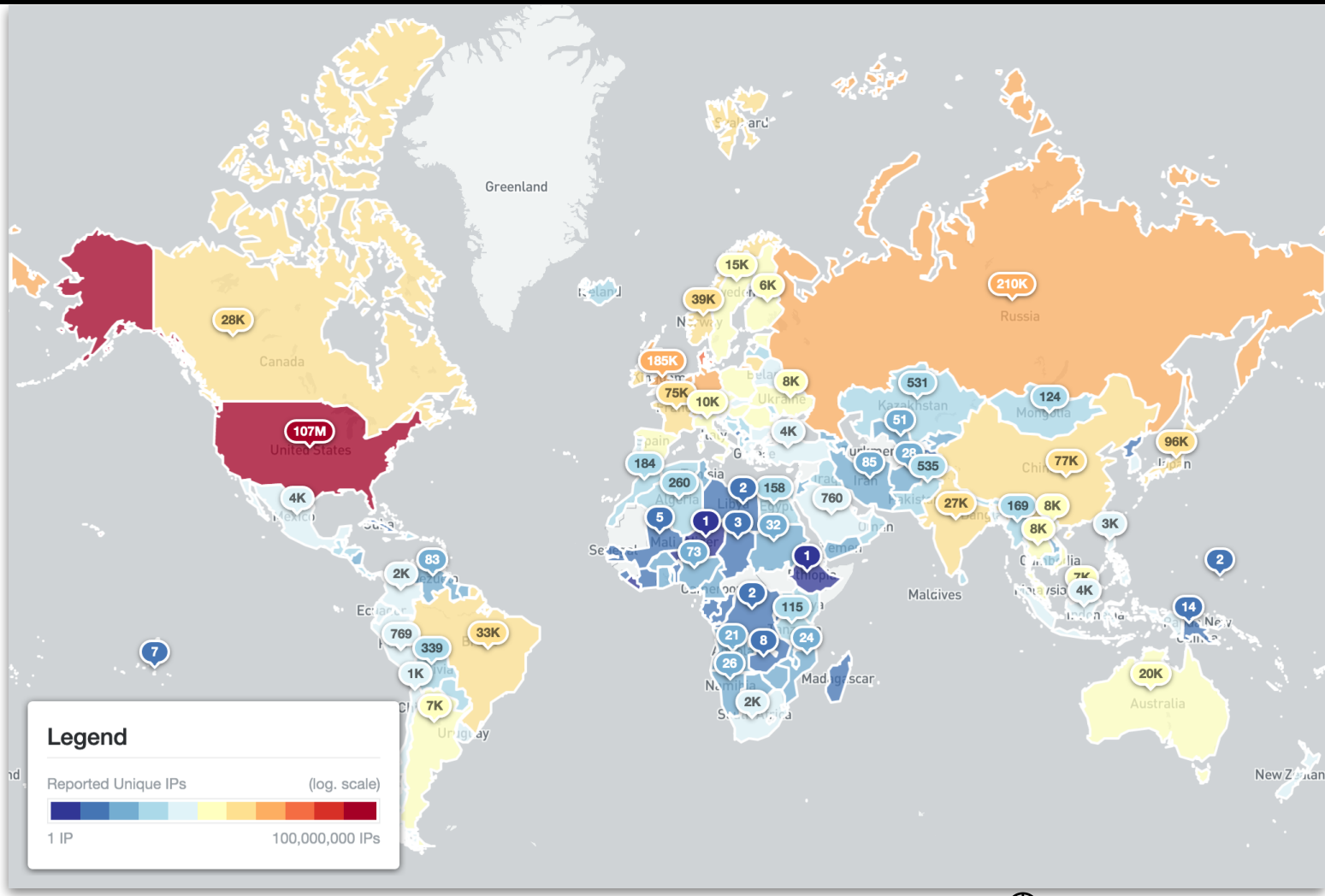
SHADOWSERVER

VARIOT

IPv6 Scans (Population)

Bulk of the “in use” IPv6 is in the United States

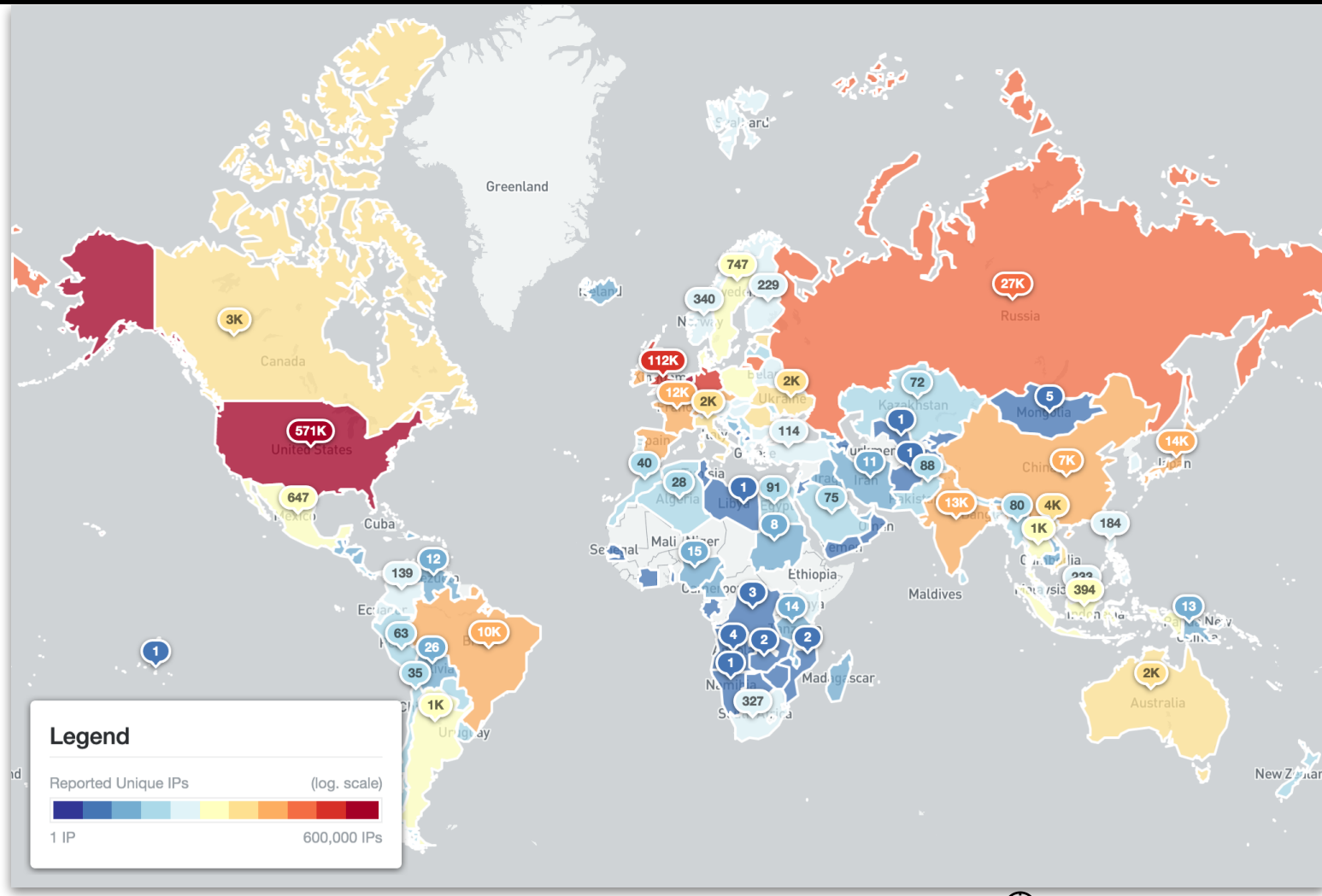
Followed by Denmark, Germany, and Netherlands



IPv6 Scans (Exposed/Vulnerable)

Leader is still the United States.

Followed by Netherlands, Germany, and Singapore.



SHADOWSERVER

VARIOT

IPv6 Scans

Always Looking for More Sources of IPv6 Targets

SHADOWSERVER

VARIOT

Device Identification

Fingerprinting all things!

Device Identification

- Take all data we collect in all our daily scans
  - match fields, banners and responses to identify device make-and-model
- Classify all IPs by:
  - device_type
  - device_vendor
  - device_model
  - device_version
  - device_sector

Device Identification

- Scan rule engine implemented
- Classifies scan data as it is submitted to the Shadowserver backend API
- Currently ~1200 scan rules implemented
- Support for detection of devices from 173 vendors
- Daily successfully classifies over 28M devices (excluding desktops/ servers, web servers etc)
- Findings shared daily with all subscribers in Device Identification Report: https://www.shadowserver.org/what-we-do/network-reporting/device-identification-report/
- More to come!

SHADOWSERVER

VARIOT

Device Identification

Scan rules

Import scan rules | Export scan rules | Advanced filters | Create new | Create in bulk

Action: Go 0 of 20 selected

Contact	Name	Device model	Device type	Device vendor	Group	Order	Test count	Usage	Enabled	State	Created	Actions
Piotr Kije...	Allegro_Software_RomPag...	RomPager	embedded-sys...	Allegro Software	Allegro Software	100			✔		2021-11-14	View | Edit | Delete | Clone
Piotr Kije...	Allegro_Software_RomPag...	RomPager	embedded-sys...	Allegro Software	Allegro Software	200			✔		2021-11-14	View | Edit | Delete | Clone
Piotr Kije...	Realtron_Embedded_Syst...		embedded-sys...	Realtron	Realtron	100			✔		2022-04-24	View | Edit | Delete | Clone
Piotr Kije...	ASUS_httpd_server_http_...		router	ASUS	ASUS	90			✔		2021-01-29	View | Edit | Delete | Clone
Piotr Kije...	ASUS_by_AiCloud_html_title		router	ASUS	ASUS	90			✔		2022-04-13	View | Edit | Delete | Clone
Piotr Kije...	ASUS_catchall_FTP_Banner		router	ASUS	ASUS	95			✔		2021-02-05	View | Edit | Delete | Clone
Piotr Kije...	ASUS_router.asus.com		router	ASUS	ASUS	100			✔		2020-11-13	View | Edit | Delete | Clone
Piotr Kije...	ASUS_by_ASUSTek_cert		router	ASUS	ASUS	100			✔		2022-04-14	View | Edit | Delete | Clone
Piotr Kije...	ASUS_asuscomm_issuer_...		router	ASUS	ASUS	101			✔		2020-11-23	View | Edit | Delete | Clone
Piotr Kije...	ASUS_asuscomm_lets_en...		router	ASUS	ASUS	102			✔		2020-11-23	View | Edit | Delete | Clone
Piotr Kije...	ASUS_asuscomm_lets_en...		router	ASUS	ASUS	105			✔		2021-02-01	View | Edit | Delete | Clone
Piotr Kije...	ASUS_ASUSWRT_issuer_...		router	ASUS	ASUS	120			✔		2020-11-23	View | Edit | Delete | Clone
Piotr Kije...	ASUS_ASUSWRT_HGG_is...		router	ASUS	ASUS	200			✔		2020-11-23	View | Edit | Delete | Clone
Piotr Kije...	ASUS_Merlin_Koolshare_i...		router	ASUS	ASUS	202			✔		2020-11-23	View | Edit | Delete | Clone
Piotr Kije...	ASUS_ASUSWRT_Merlin_i...		router	ASUS	ASUS	203			✔		2020-11-23	View | Edit | Delete | Clone
Piotr Kije...	ASUS_Merlin_Koolshare_r...		router	ASUS	ASUS	204			✔		2020-11-23	View | Edit | Delete | Clone
Piotr Kije...	ASUS_ASUSWRT_Merlin_...		router	ASUS	ASUS	205			✔		2020-11-23	View | Edit | Delete | Clone
Piotr Kije...	ASUS_Merlin_Koolshare_r...	RT-AX88U	router	ASUS	ASUS	206			✔		2020-11-23	View | Edit | Delete | Clone

SHADOWSERVER

Device Identification - Popular matched responses

- SSL Common Names & Organization Names
- HTML body content
- HTTP server names
- HTTP cookies
- SNMP sysdesc, sysname
- FTP, TELNET, SSH banners
- … many more!

SHADOWSERVER

VARIOT

Device Identification - Scan rules

- Rule syntax

```
( boolean expression ) -> statement(s)
```

- Rule operators

Name	Operation
and	boolean and
or	boolean or
=	case sensitive string equality
!=	case sensitive string inequality
=~	regex match
!~	regex difference
:=	assignment

SHADOWSERVER

VARIOT

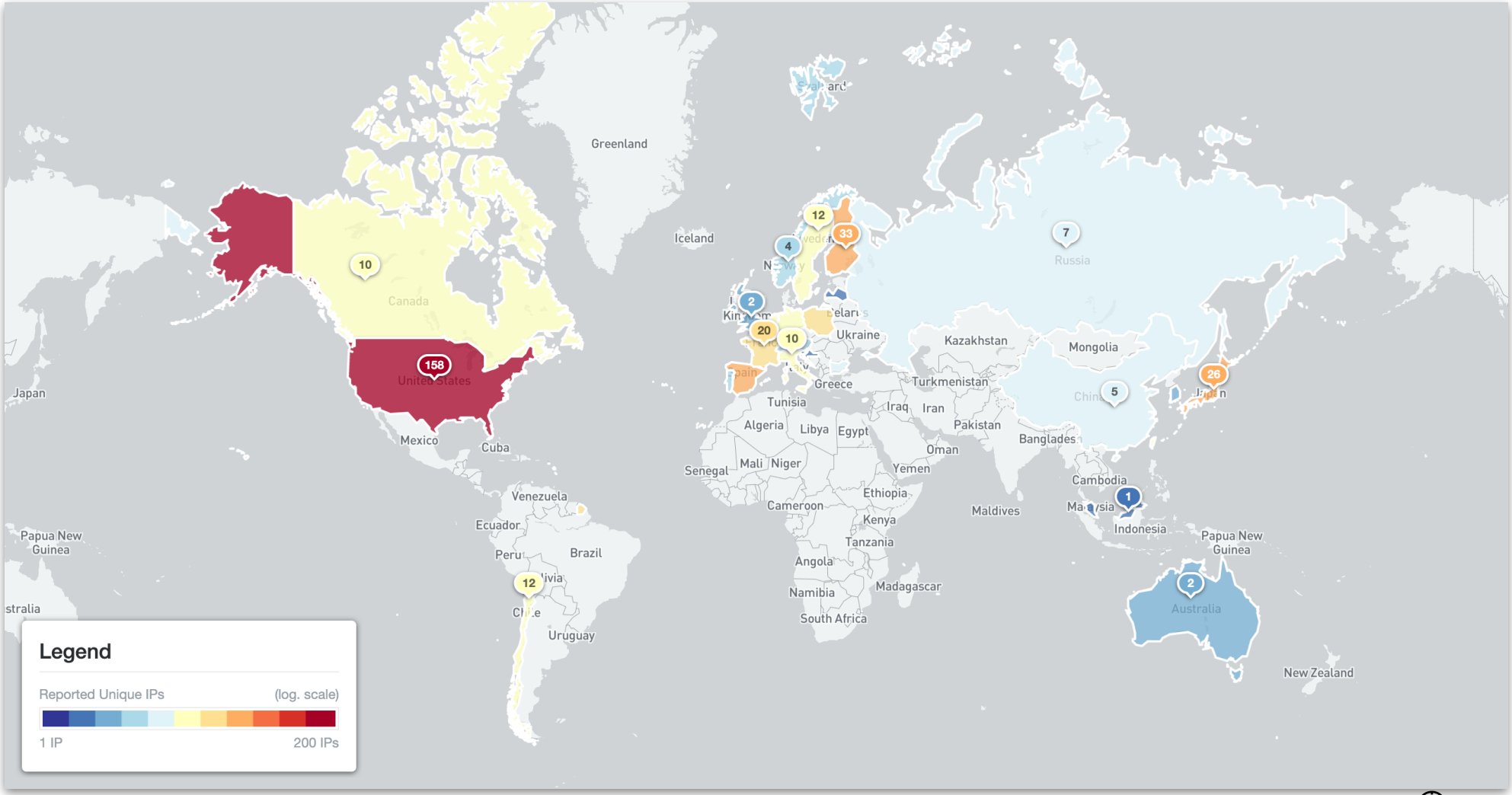
Example fingerprinting rule - iRobot Roomba

```
(issuer_common_name =~ /^Roomba/ and
issuer_organization_name = "iRobot")
-> tag := "iot", device_type :=
"home-appliance", device_vendor :=
"iRobot", device_model := "Roomba",
device_sector := "consumer"
```

SHADOWSERVER

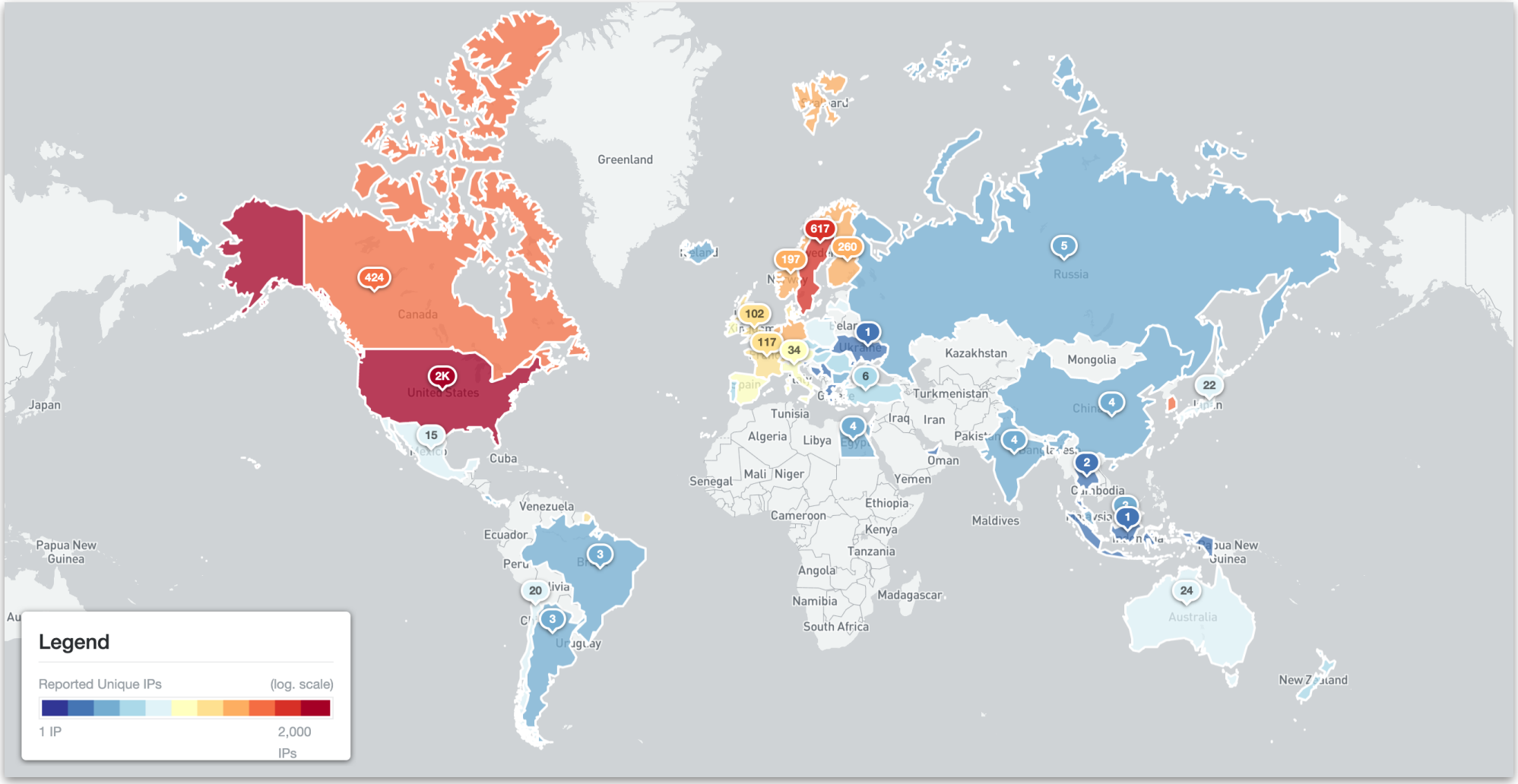
VARIOT

Device Identification - iRobot Roomba (2022-06-21)



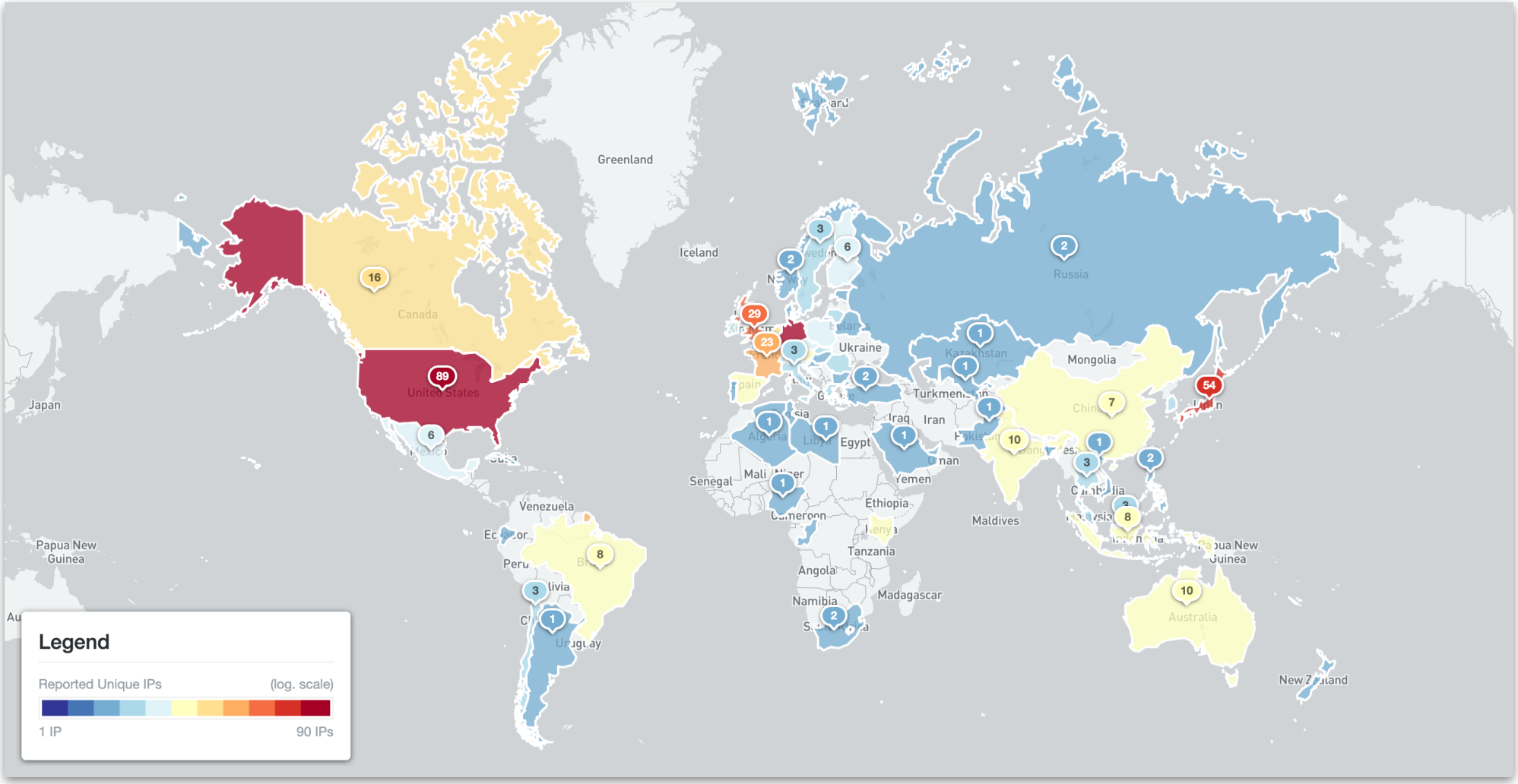
~ 400 devices

Device Identification - Philips HUE (2022-06-21)



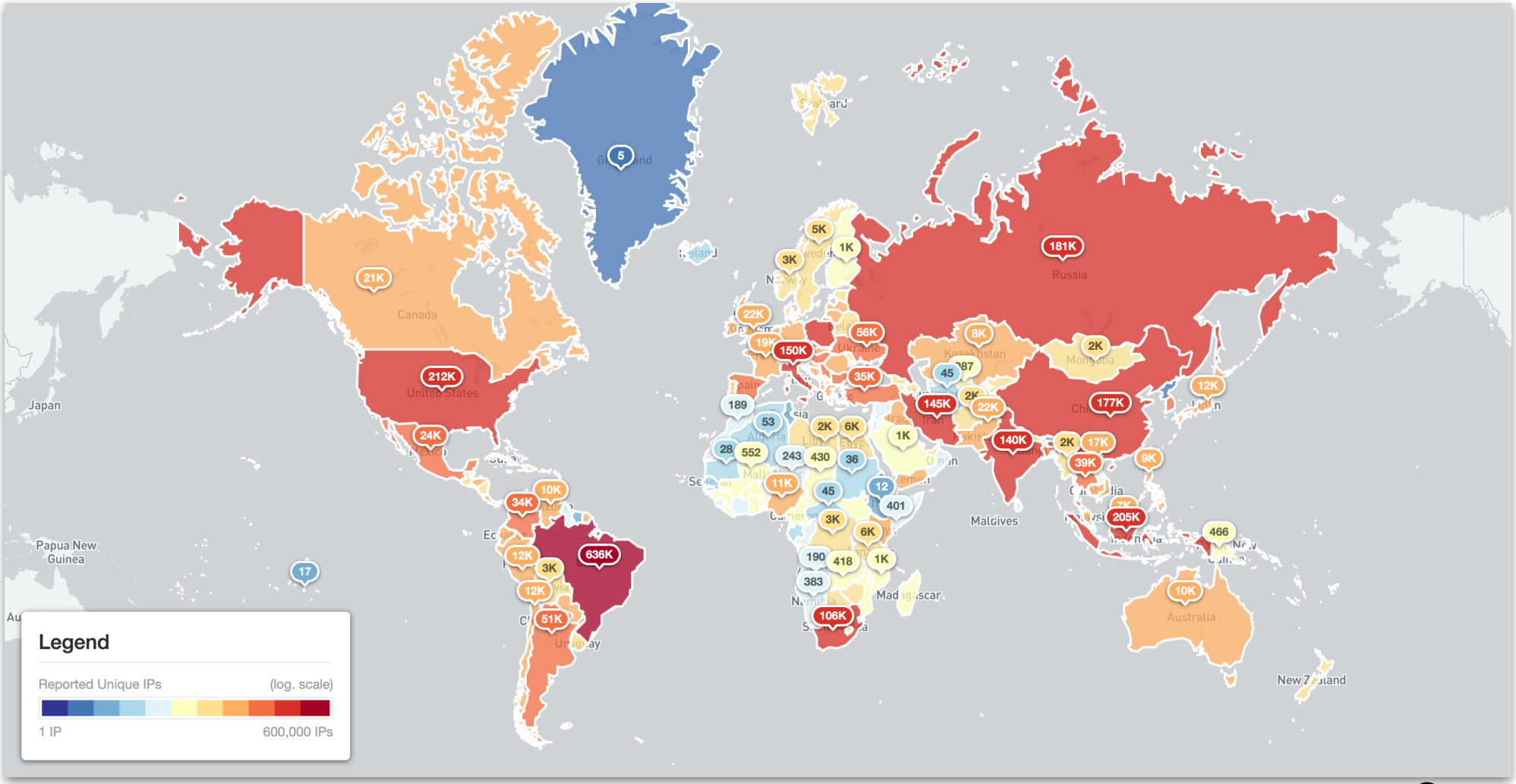
~ 5300 devices

Device Identification - Siemens SIMATIC S7-300 (2022-06-21)



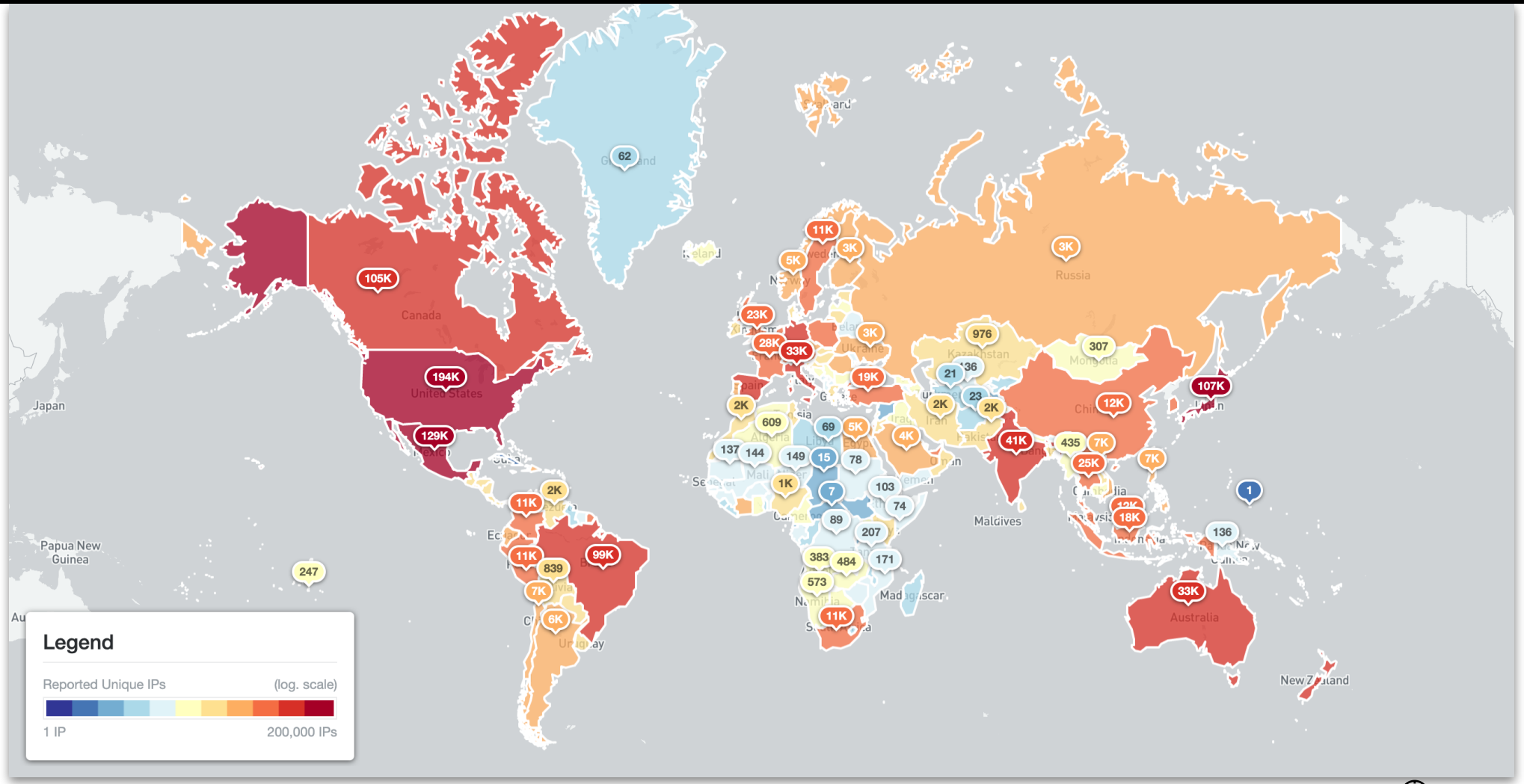
~ 500 devices (based only on non-native ICS scans)

Device Identification - Mikrotik (2022-06-21)



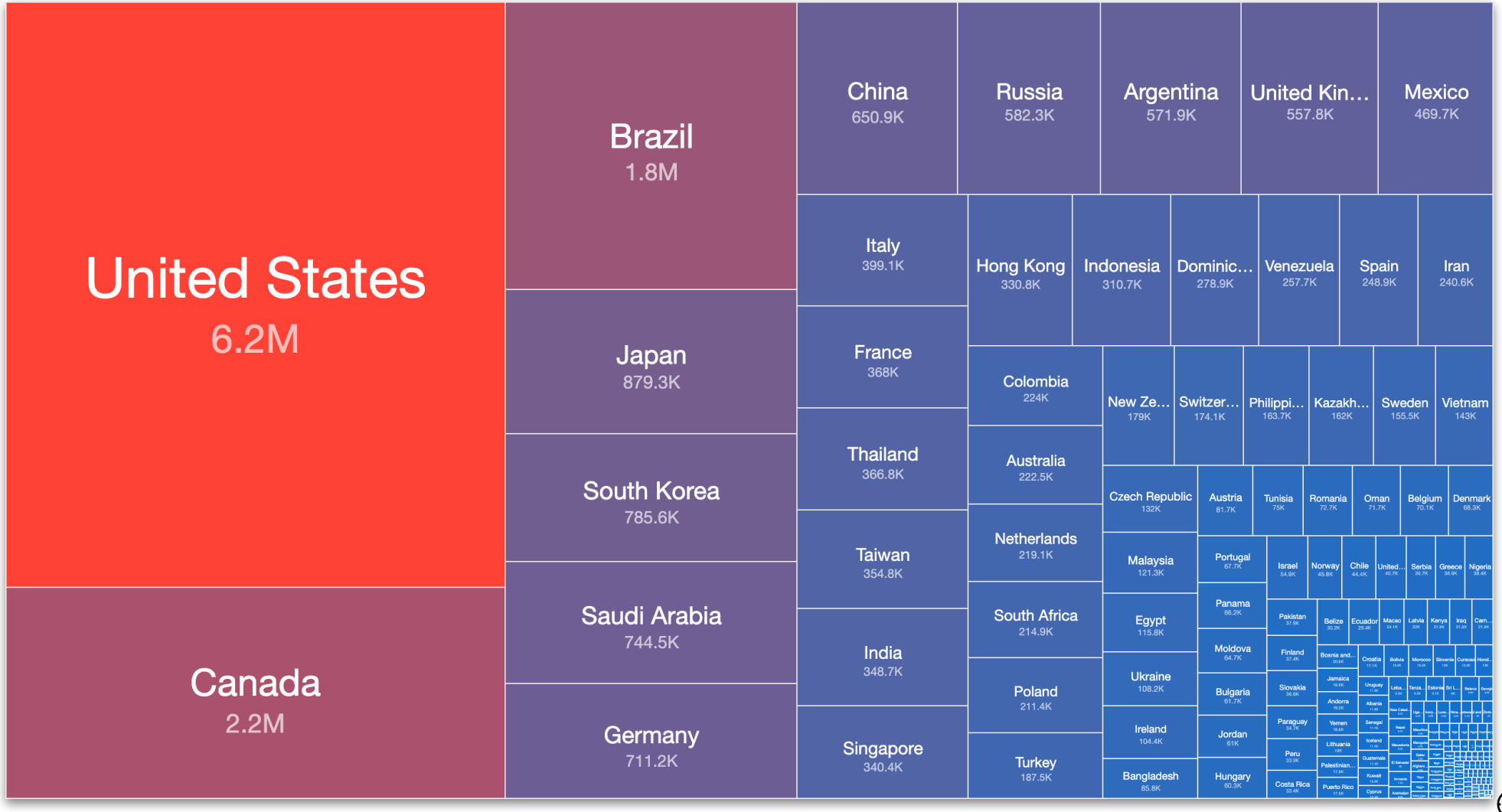
~ 3 200 000 devices

Device Identification - Fortinet (2022-06-21)



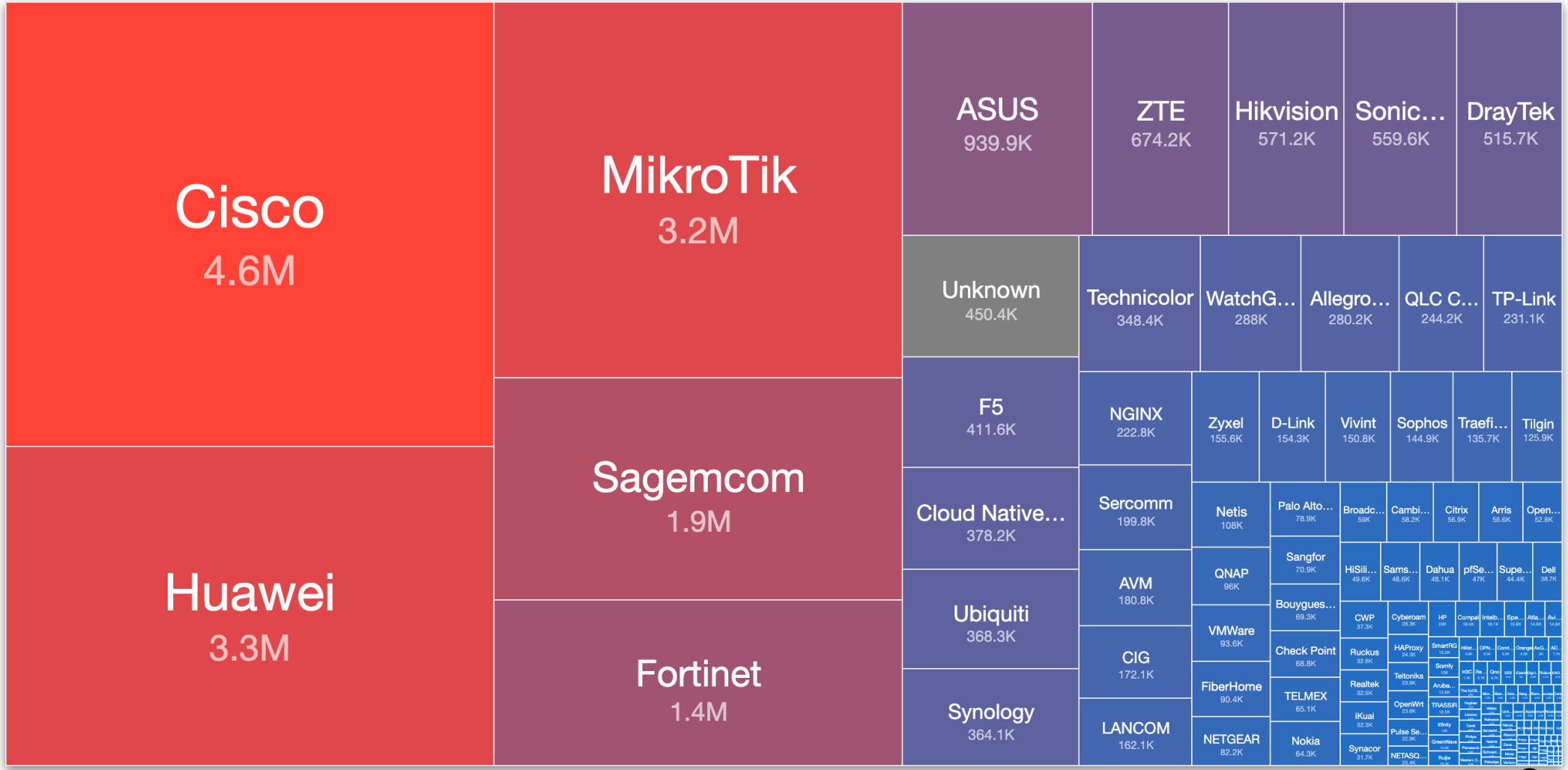
~ 1 400 000 devices

Devices identified by Country (2022-06-21)



(Excluding desktop/servers & web servers)

Device Identification - Vendors (2022-06-21)



(Excluding desktop/servers & web servers)

HaDEA CEF - VARIoT Project

- July 2019 - Oct 2022
- Shadowserver role is focused on improving:
  - scanning of IoT devices
  - observations of IoT attacks
  - collection & analysis of IoT malware
  - sharing of statistics as open data (in the European Data Portal - EDP)

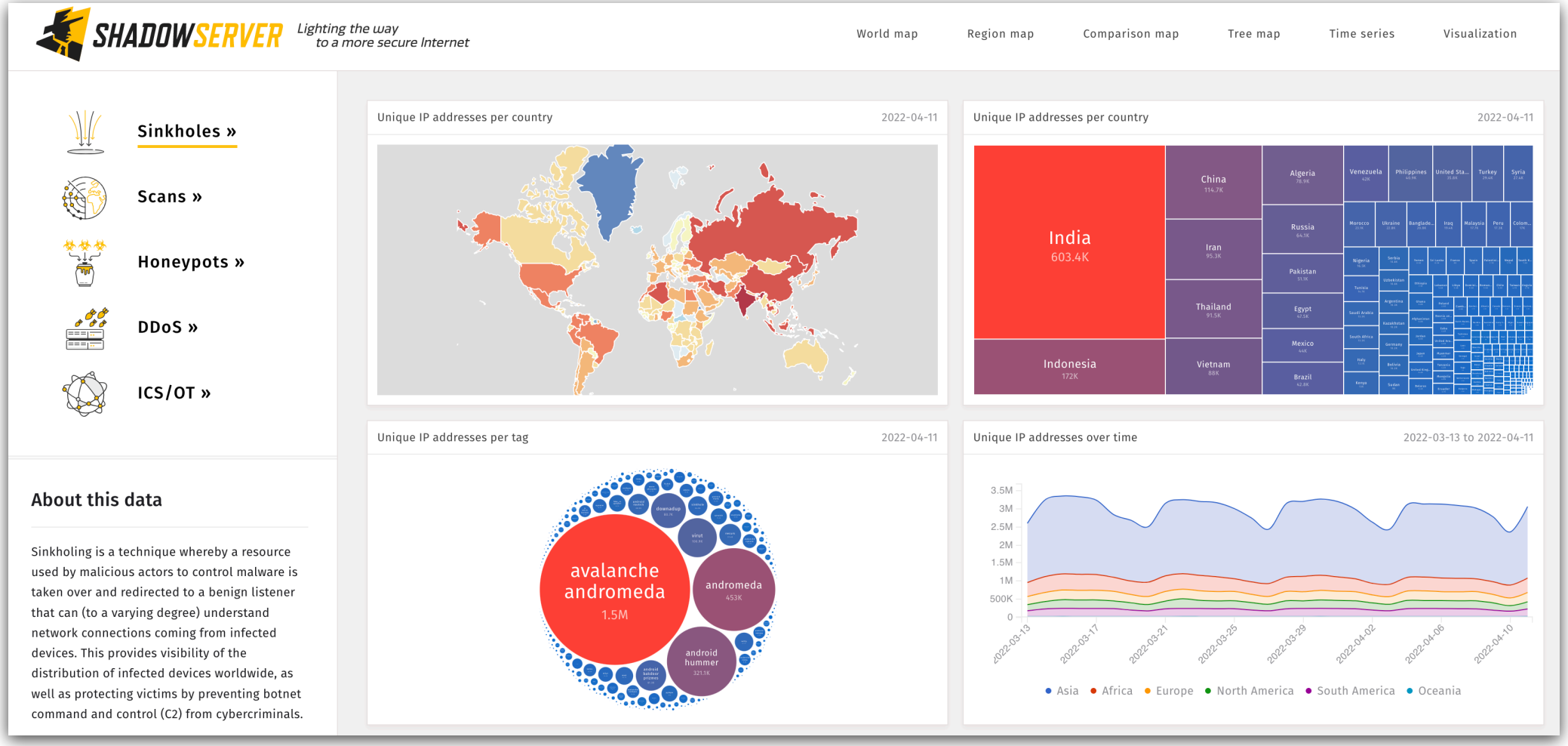
https://variot.eu

SHADOWSERVER

Co-financed by the Connecting Europe Facility of the European Union

VARIOT

Shadowserver Public Dashboard (New)

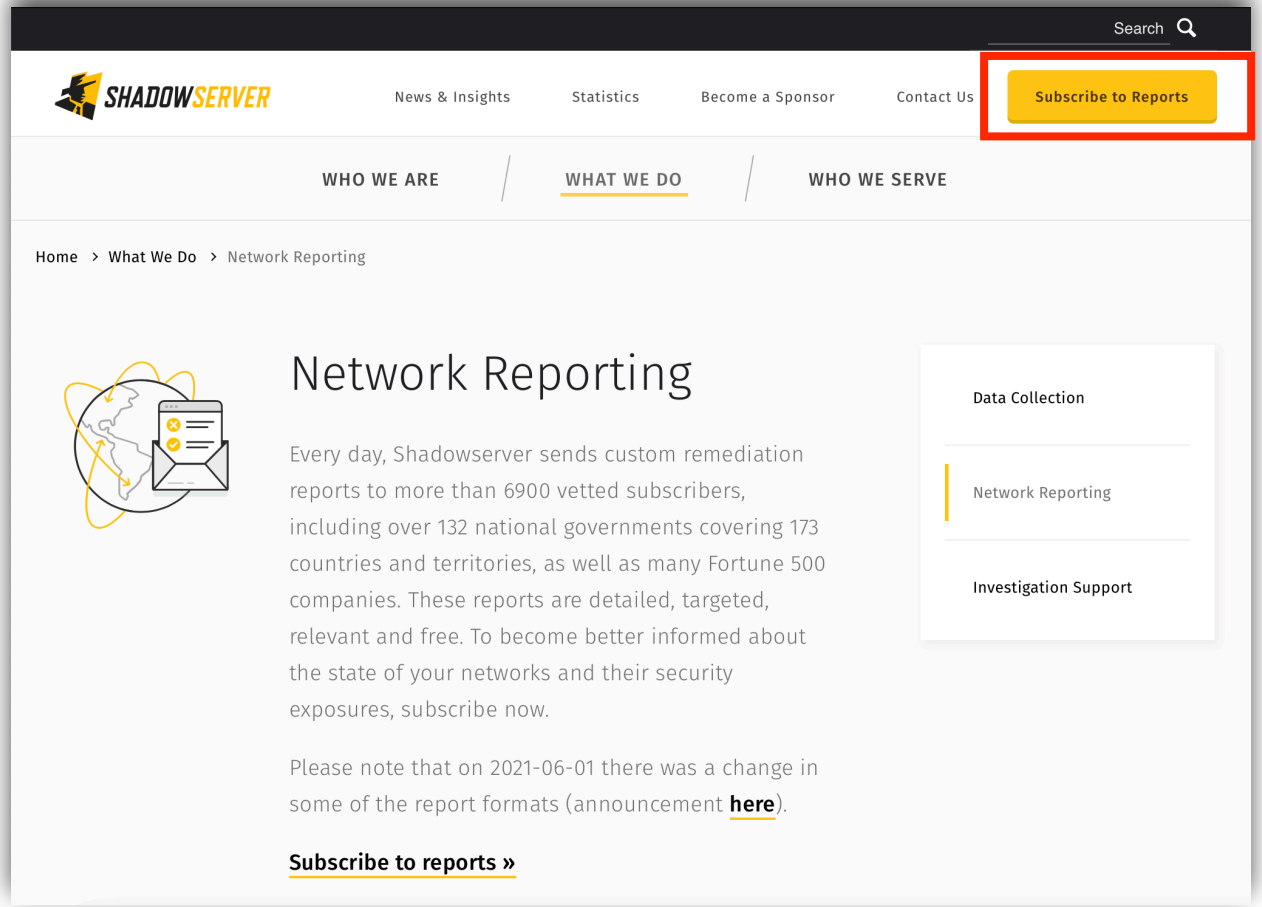


https://dashboard.shadowserver.org

SHADOWSERVER

Preview: Username: **alliance** Password: **SaferInternet**

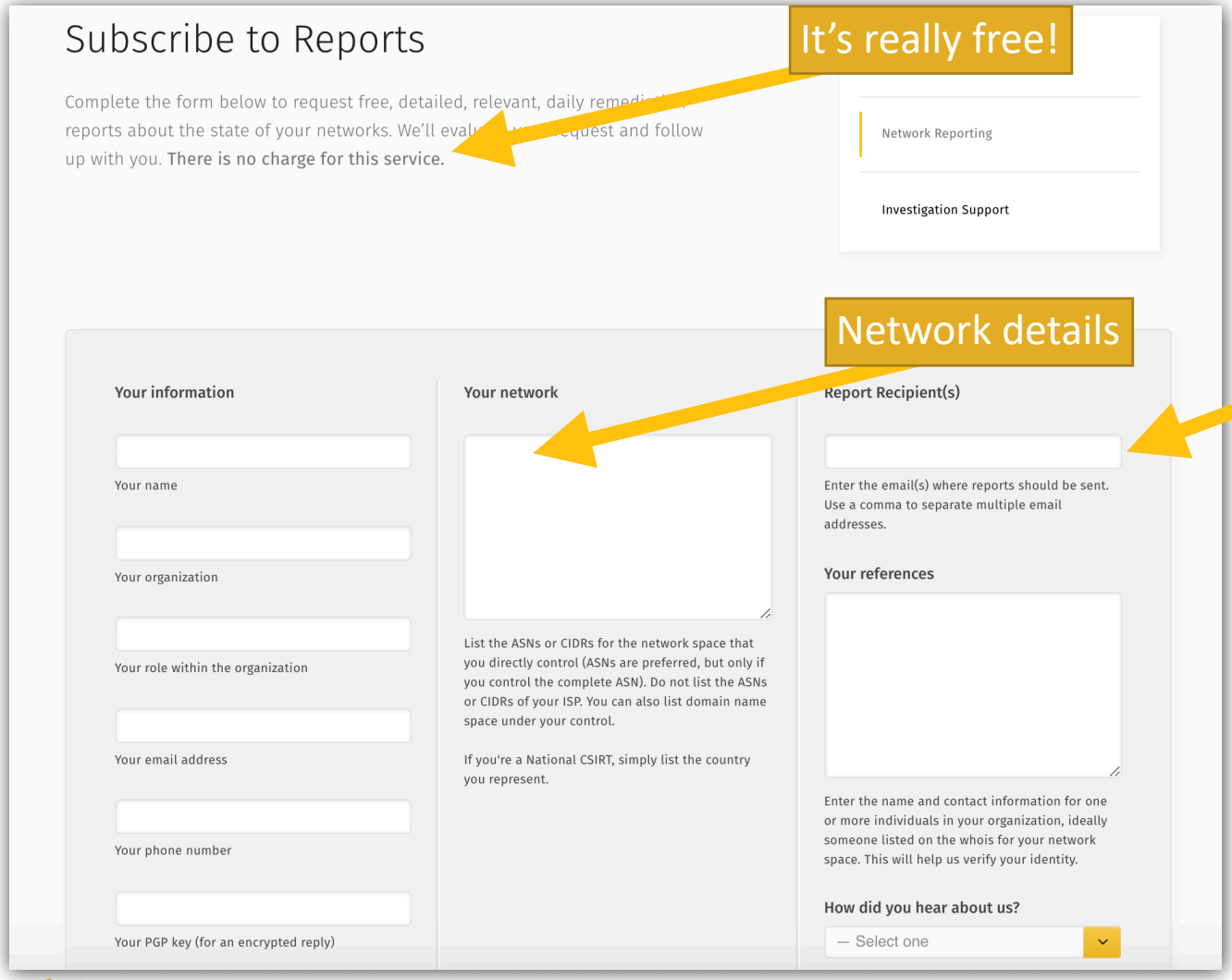
Subscribe to free daily threat feeds!



https://www.shadowserver.org

SHADOWSERVER

Subscribe to free daily threat feeds!



It's really free!

Network details

Email address where reports or download links will be sent

SHADOWSERVER

https://www.shadowserver.org/what-we-do/network-reporting/get-reports/

Questions?

SHADOWSERVER

Lighting the way to a more secure Internet

@shadowserver

decoster@shadowserver.org, piotr@shadowserver.org

SHADOWSERVER.ORG