The Attack Surface Landscape in Brazil - An Overview

Piotr Kijewski, @piotrkijewski
piotr@shadowserver.org

29th July 2024
12º Fórum Brasileiro de CSIRTs, São Paulo

SHADOWSERVER.ORG

TLP CLEAR

whoami

- **Piotr Kijewski (NL)** - US CEO, US Board of Trustees, EU Director, Programme Manager
  - 20+ years experience in the operational security community
  - Sysadmin (Unix) background
  - National CSIRT background - Previously Head of CERT Polska (CERT.PL)
  - Previously a Director at the Honeynet Project (honeypots!)
  - Authored large scale threat detection systems and threat information sharing systems
  - Botnet takedown, disruption, sinkholing …
  - Still active with research into above!

SHADOWSERVER

TLP CLEAR

What is The Shadowserver Foundation?

A US 501c3 and Dutch Stichting **not-for-profit** organisation that works to try and make the Internet more secure for all by providing quality intelligence about threats for **free**

SHADOWSERVER
Lighting the way to a more secure Internet

We share information with Internet defenders at no cost
We work to help mitigate vulnerable systems, detect malicious activity and counter emerging threats with greatest effect internationally.

We tell people **for free** what risks we see they are holding

We punch **seriously** above our weight - with our own **Unique sources**, a **global vantage point** and **proven partnerships** with the people who can make the necessary security updates

We have been quietly building this unique position of trust for **20 years** of **proven community partnerships.** We are the **world's largest provider** of **free cyber threat intelligence** (and most people have never heard of us!)

SHADOWSERVER

TLP CLEAR

3 Target Audiences - to make **Everybody** Safer

National Level

We pass the data every day to the National bodies responsible for 175 countries, so they can help protect their citizens & companies

Network Level

We pass the data to over 8,000 Network Owners, including most Fortune 500 companies, so they can better protect their own networks (plus their customers where they are service providers)

Law Enforcement

Law Enforcement lack our data, scale or insight and can benefit from the global trust network we have built - so we (quietly) support top tier law enforcement operations in their efforts to protect citizens from the actions of the online criminals

SHADOWSERVER

TLP CLEAR

What does The Shadowserver Foundation do?

- **Sinkholes:**
  We take control of domain names and addresses used by criminals to log the IP address of infected devices for over 400 malware families

- **Scanning:**
  We call out to nearly every IPv4 (~3.7 billion) and ~1.9 billion IPv6 addresses many times a day looking for different types of vulnerable, compromised, abusable systems, attacker infra

- **Sensors:**
  We build and deploy systems to the Internet that pretend to be vulnerable computers, and log cyber criminals trying to abuse them

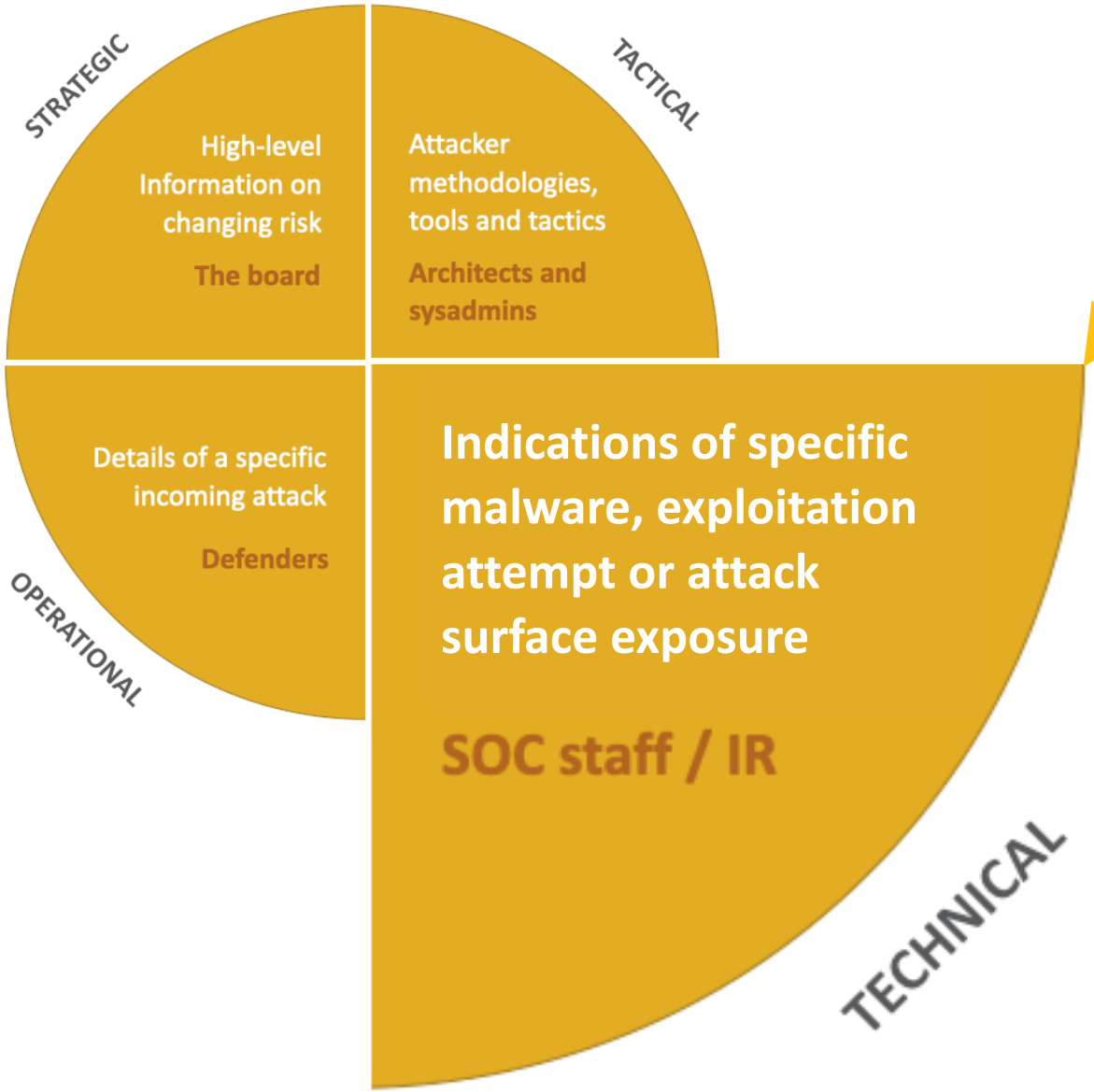
- **Sandboxes:**
  We collect malicious software samples at industrial scale (often 1 million+ per day, for nearly 2 billion total) and run them to see what they do

For network owners + focus on CSIRT & LE support

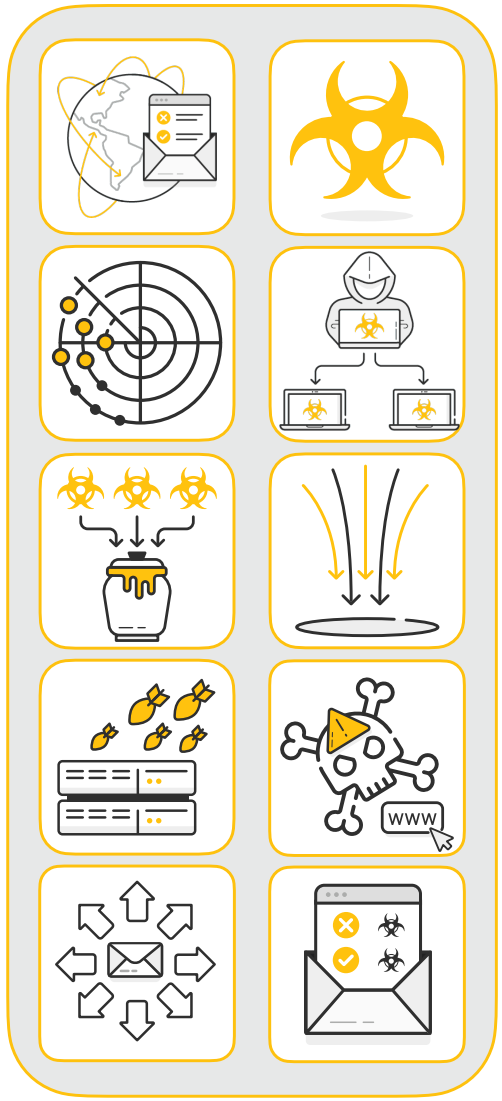
+ a host of other interesting things!

SHADOWSERVER

TLP CLEAR



Core Shadowserver offering



Free Daily Remediation Reports - National CSIRTs and Network Owners

Network Reporting

Every day, Shadowserver sends custom remediation reports to more than 8000 vetted subscribers, including over 201 national CSIRTs in 175 countries and territories and many Fortune 500 companies. These reports are detailed, targeted, relevant and free.

DNS Open Resolvers	Accessible Telnet	Command and Control	Netcore/Netis Router Vulnerability	Open LDAP TCP	Open Redis	Scan Report
Accessible XDMCP Service	Accessible VNC	Darknet	NTP Monitor	Open mDNS	Open SNMP	Sinkhole6 HTTP Drone
ASN Summary Report	Accessible Rsync	DDoS	NTP Version	Open Memcached	Open SSDP	Sinkhole6 HTTP Referer
Botnet URL	Amplification DDoS Victim	Drone/Botnet-Drone	Open CWMP	Open MongoDB	Open/Accessible TFTP	Spam URL
Sinkhole HTTP Drone	Botnet Drone Hadoop	Geographical Summary	Open DB2 Discovery Service	Open MS-SQL Server Resolution	Open Ubiquiti	SSL Freak
Accessible ADB	Brute Force Attack	Honeypot URL	Open Chargen	Open NAT-PMP	Proxy	SSL Poodle
Accessible AFP	Blacklist	HTTP Scanners	Open Elasticsearch	Open Netbios	Sandbox URL	Synful Scan
Accessible Hadoop	Click-fraud	ICS Scanners	Accessible HTTP	Open Portmapper	Sandbox Connection	Vulnerable ISAKMP
Accessible SMB	Compromised Host	IRC Port Summary	Open IPMI	Open Proxy	Sandbox IRC	Accessible Cisco Smart Install
Accessible SSH	Compromised Website	Microsoft Sinkhole	Open LDAP	Open QOTD	Sandbox SMTP	Accessible FTP/RDP

Much of the world uses these reports to receive rapid notification when computer networks globally are exposed, misconfigured, vulnerable, abusable, compromised, become a source of attacks, host malicious C2 or other attacker infrastructure …

<u>Everyone</u> can get <u>free</u> daily reports about who/what is at risk in their <u>own</u> network/country.

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

TLP CLEAR

Use Report Event Severity for Triage

Severity Levels

Level	Description
critical	Highly critical vulnerabilities that are being actively exploited, where failure to remediate poses a very high likelihood of compromise. For example, a pre-auth RCE or modification or leakage of sensitive data.
high	End of life systems, systems that you can log into with authentication that are meant to be internal (SMB, RDP), some data can be leaked. Sinkhole events end up in this category.
medium	Risk that does not pose an immediate threat to the system but can over time escalate to a higher severity. For example, risk of participating in DDoS, unencrypted services requiring login, vulnerabilities requiring MITM to exploit, attacker will need to know internal systems/infrastructure in order to exploit it.
low	Deviation from best practice - little to no practical way to exploit, but setup is not ideal. For example, SSL POODLE reports may end up in this category.
info	Informational only. Typically no concerns. However, this category includes the Device Identification report, which may include information on device types that should not be accessible on the public Internet, in which case the individual events in the report may be assigned higher severity levels. Review in accordance with your security policy.

SHADOWSERVER

https://github.com/The-Shadowserver-Foundation/report_schema

TLP CLEAR

Automation

The-Shadowserver-Foundation / **api_utils**

Type / to search

Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights

api_utils Public

Unwatch 9 | Fork 4 | Starred 42

main | 1 Branch | 0 Tags | Go to file t | Add file | Code

elsif2 Update README.md — c9bc483 · last week — 21 Commits

cef	Escape special characters.	3 months ago
elasticsearch	README update	6 months ago
splunk	Update README.md	last week
LICENSE	Initial commit	2 years ago
README.md	update link	2 years ago
call-api-json.py	add call-api-json.py	last year
call-api.pl	publish	2 years ago
call-api.py	switch encoding to utf-8	2 years ago
report-manager.py	add report-manager	2 years ago

About

Sample programs to access the API

Readme
GPL-3.0 license
Activity
Custom properties
42 stars
9 watching
4 forks
Report repository

Releases

No releases published

Packages

No packages published

SHADOWSERVER

TLP CLEAR

Automation

certtools / intelmq

Type / to search

Code | Issues 181 | Pull requests 16 | Discussions | Actions | Projects 2 | Security | Insights

intelmq

Public

Watch 76 | Fork 290 | Star 900

develop | 18 Branches | 69 Tags | Go to file t | Add file | Code

aaronkaplan update docs to reflect mkdocs ✓ b257f04 · 4 days ago 7,920 Commits

.github	DOC: Updates links to new documentation.	5 days ago
.reuse	DOC: n6: add more illustrations	3 years ago
LICENSES	DOC: n6: add more illustrations	3 years ago
contrib	DOC: Updates links to new documentation.	5 days ago
debian	REL: release 3.3.0	4 days ago
docs	update docs to reflect mkdocs	4 days ago
intelmq	REL: release 3.3.0	4 days ago
scripts	DOC: Changes documentation to mkdocs.	4 months ago
.codecov.yml	DOC: add license information to all the files	3 years ago
.gitattributes	DOC: add license information to all the files	3 years ago
.gitignore	Merge branch 'develop' into entry_point_enum	4 months ago

About

IntelMQ is a solution for IT security teams for collecting and processing security feeds using a message queuing protocol.

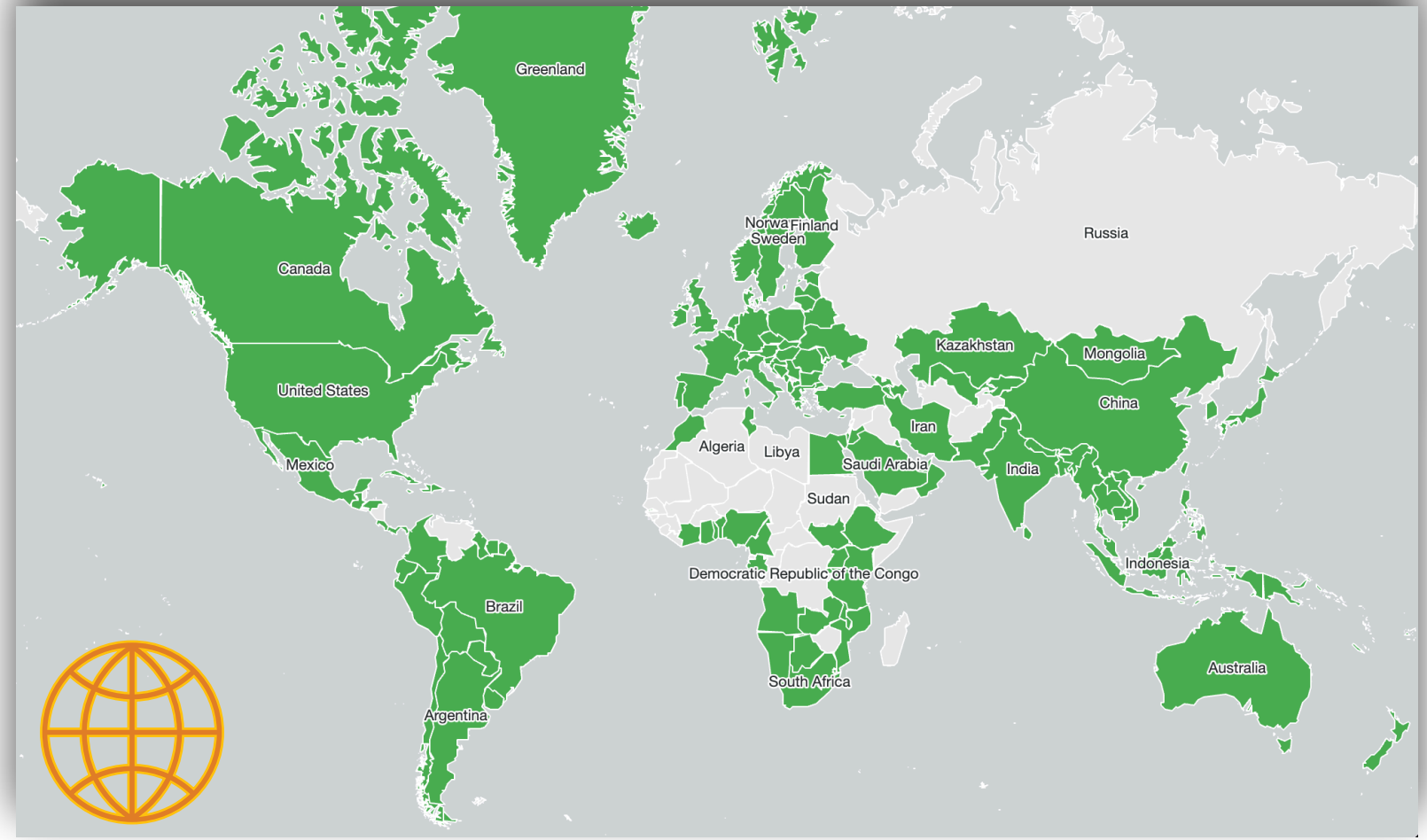
docs.intelmq.org/latest/

python | ioc | intelligence | alerts | automation | incident-response | malware | phishing | threat | cybersecurity | cert | csirt | feeds | handling | incident | ihap

Readme
AGPL-3.0 license
Security policy
Activity
Custom properties
900 stars
76 watching

TLP CLEAR

“Global Plumbing” - nCSIRT Coverage



201 nCSIRTs
(175 Countries)
+
8000+ Network Owners (Direct)
+ many more (Indirect)

Every Day
Free!

SHADOWSERVER

TLP CLEAR

Shadowserver ASN Coverage By Continent

Europe	63%
North America	57%
Oceania	65%
Africa	42%
South America	35%
Asia	29%

SHADOWSERVER

TLP CLEAR

Shadowserver ASN Subscribers - Brazil

Statistics At geo-level	**90,972,218** IPs **62,429** CIDRs **10,241** ASNs
Statistics At ASN-level	**151,609,216** IPs **62,221** CIDRs **10,240** ASNs
	180 ASNs with a report **54,939,776** IPs (60%)
	10,061 ASNs without a report **36,032,442** IPs (40%)

SHADOWSERVER

TLP CLEAR

Direct Report Recipients (LAC)

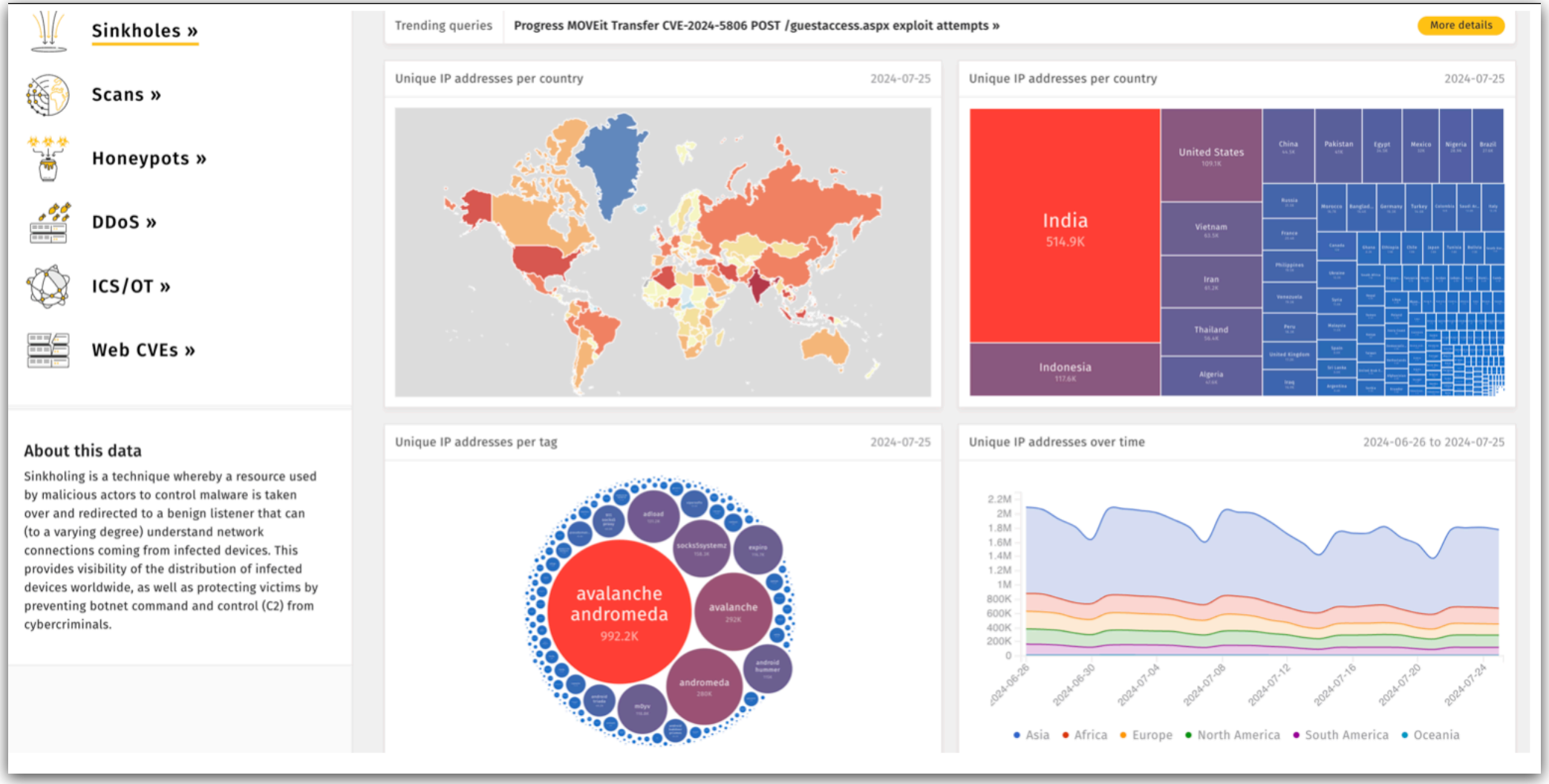
SHADOWSERVER

The Shadowserver Foundation Dashboard

A Free Tool for the Community

TLP CLEAR

Shadowserver Public Dashboard

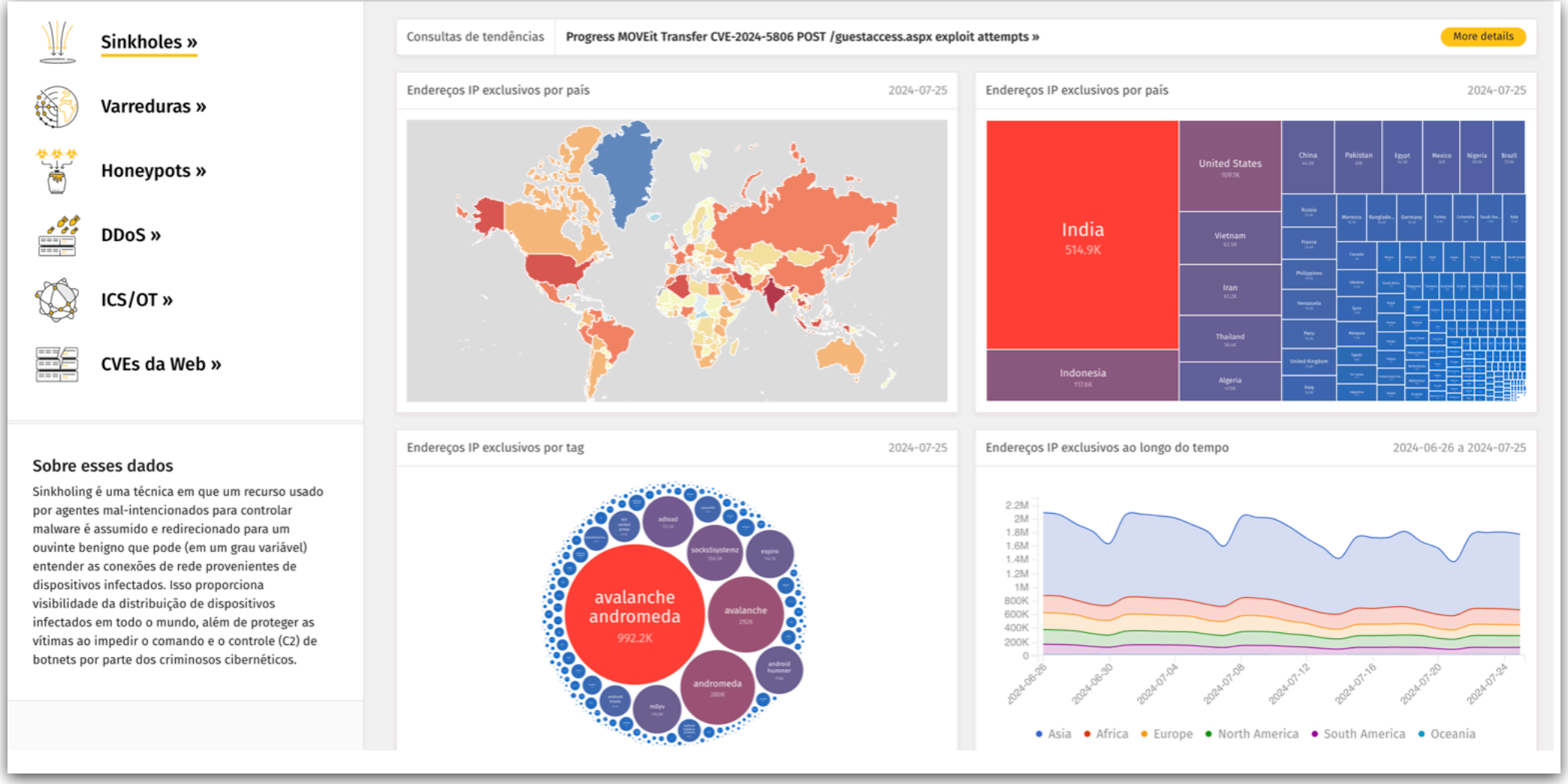


SHADOWSERVER

https://dashboard.shadowserver.org

TLP CLEAR

Shadowserver Public Dashboard - Multiple Language Support



SHADOWSERVER

https://dashboard.shadowserver.org/pt-br/

Brazil

As seen by Shadowserver

Device Attack Surface

As seen in our scans (only for cases where we identify a device!)

TLP CLEAR

Remote Device Identification

- Take all data we collect in all our daily scans
  - Match returned content with regularly updated signatures to identify devices
- Classify all IPs by:
  - device_type
  - device_vendor
  - device_model
  - device_version
  - device_sector

SHADOWSERVER

VARIOT

TLP CLEAR

Remote Device Identification

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

SHADOWSERVER

VARIOT

TLP CLEAR

Remote Device Identification

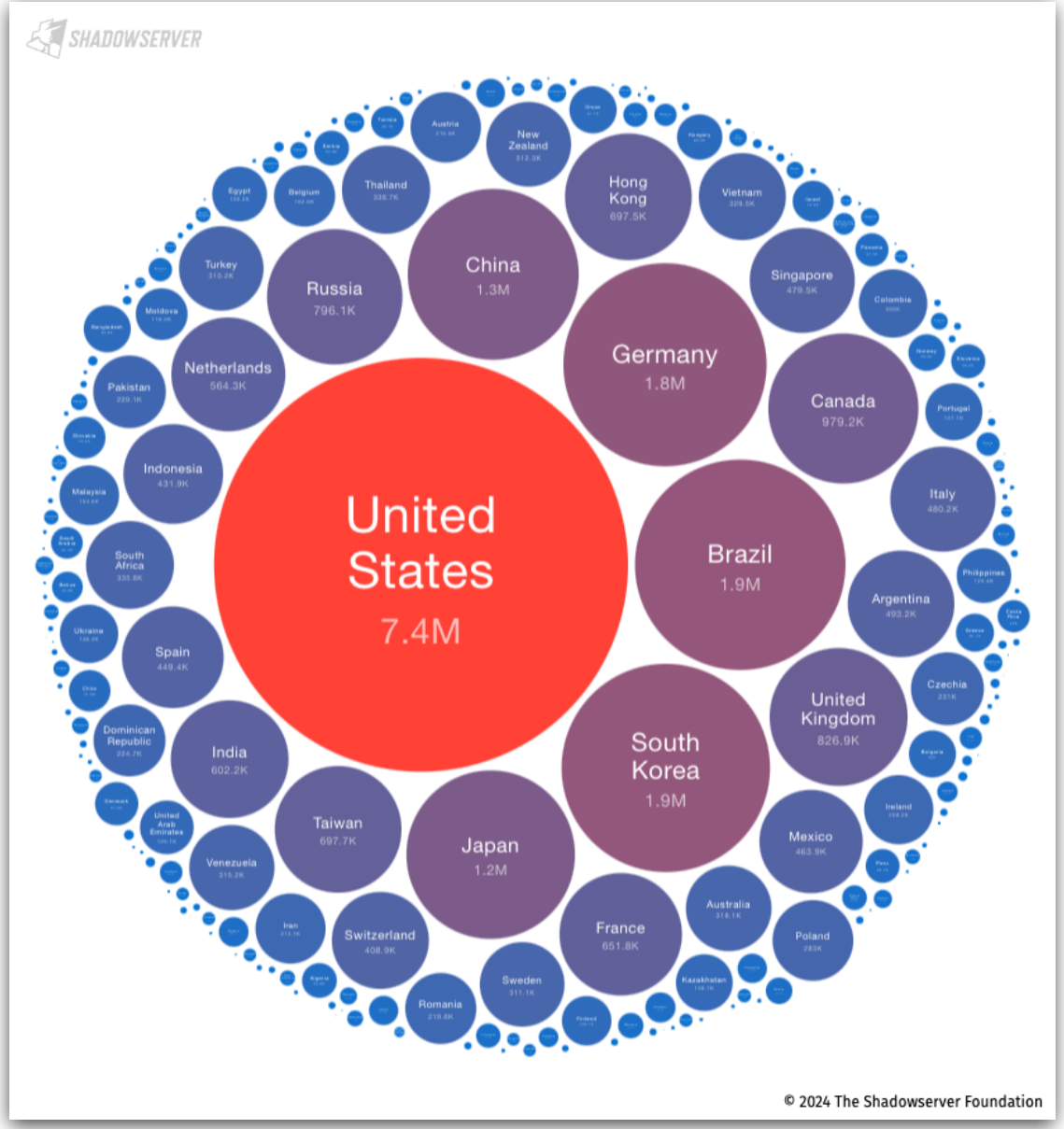
- Scan rule engine implemented
- Classifies scan data as it is submitted to the Shadowserver backend API
- Currently ~2800 scan rules implemented - June 2024
- Support for detection of devices from ~700 vendors - June 2024
- Daily successfully classifies over 50M devices (excluding desktops/ servers, web servers etc) - June 2024

SHADOWSERVER

VARIOT

TLP CLEAR

Daily Device Attack Surface Volume - World & South America

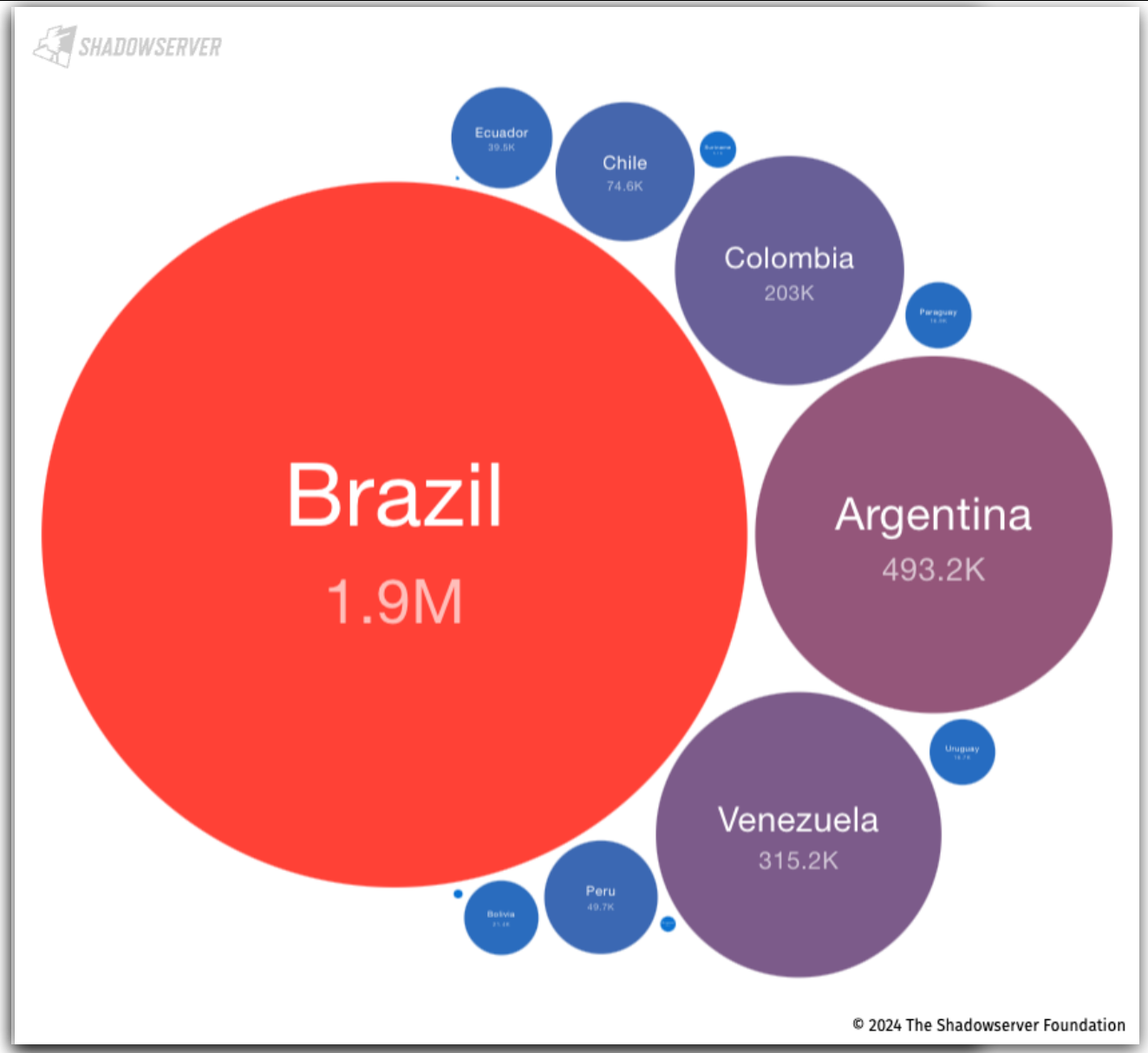


Note: Only cases where we identify a device

SHADOWSERVER

TLP CLEAR

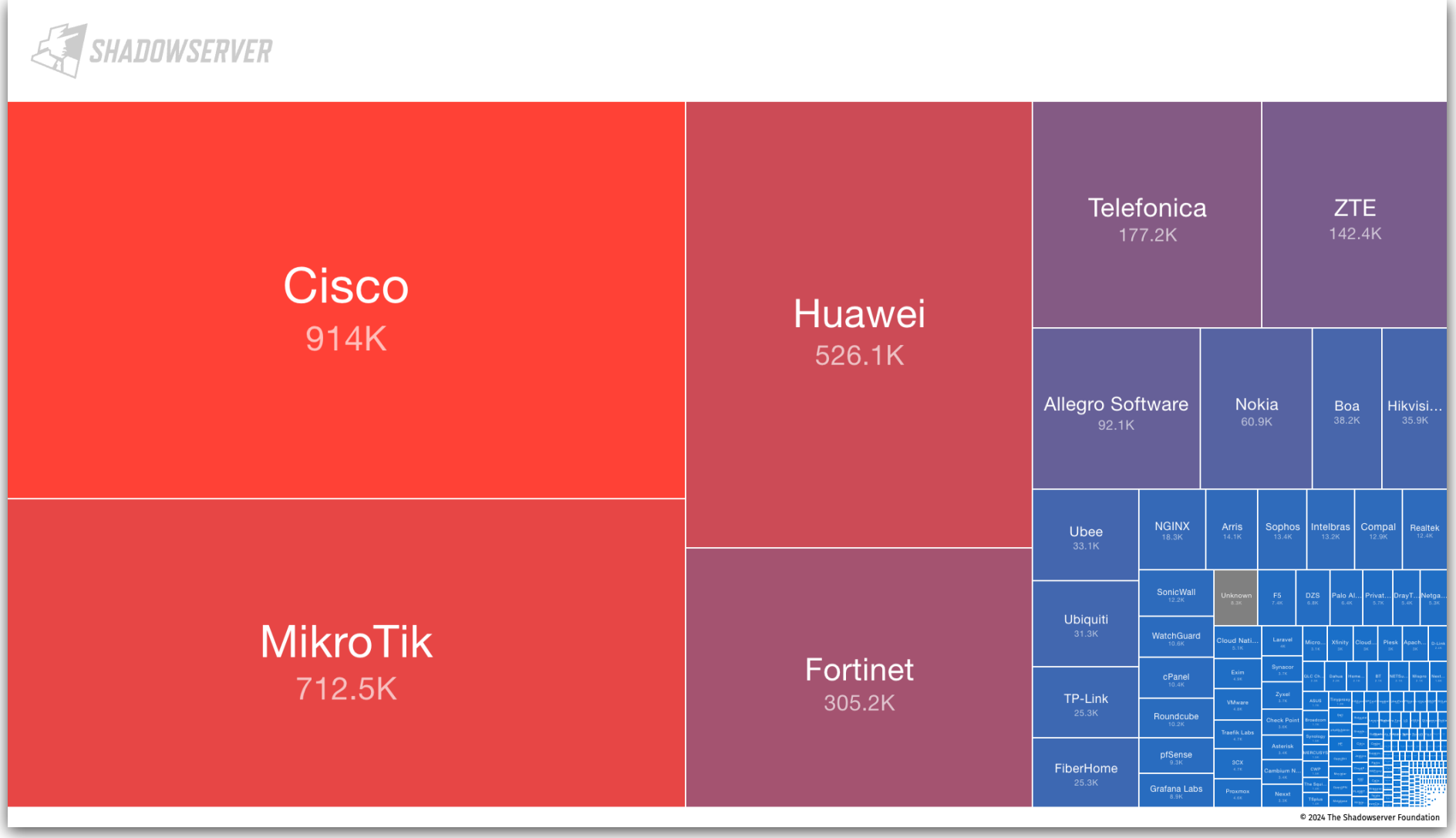
Daily Device Attack Surface Volume - World & South America



Note: Only cases where we identify a device

SHADOWSERVER

Device Exposure by Vendor - South America & Brazil (2024-07-24)

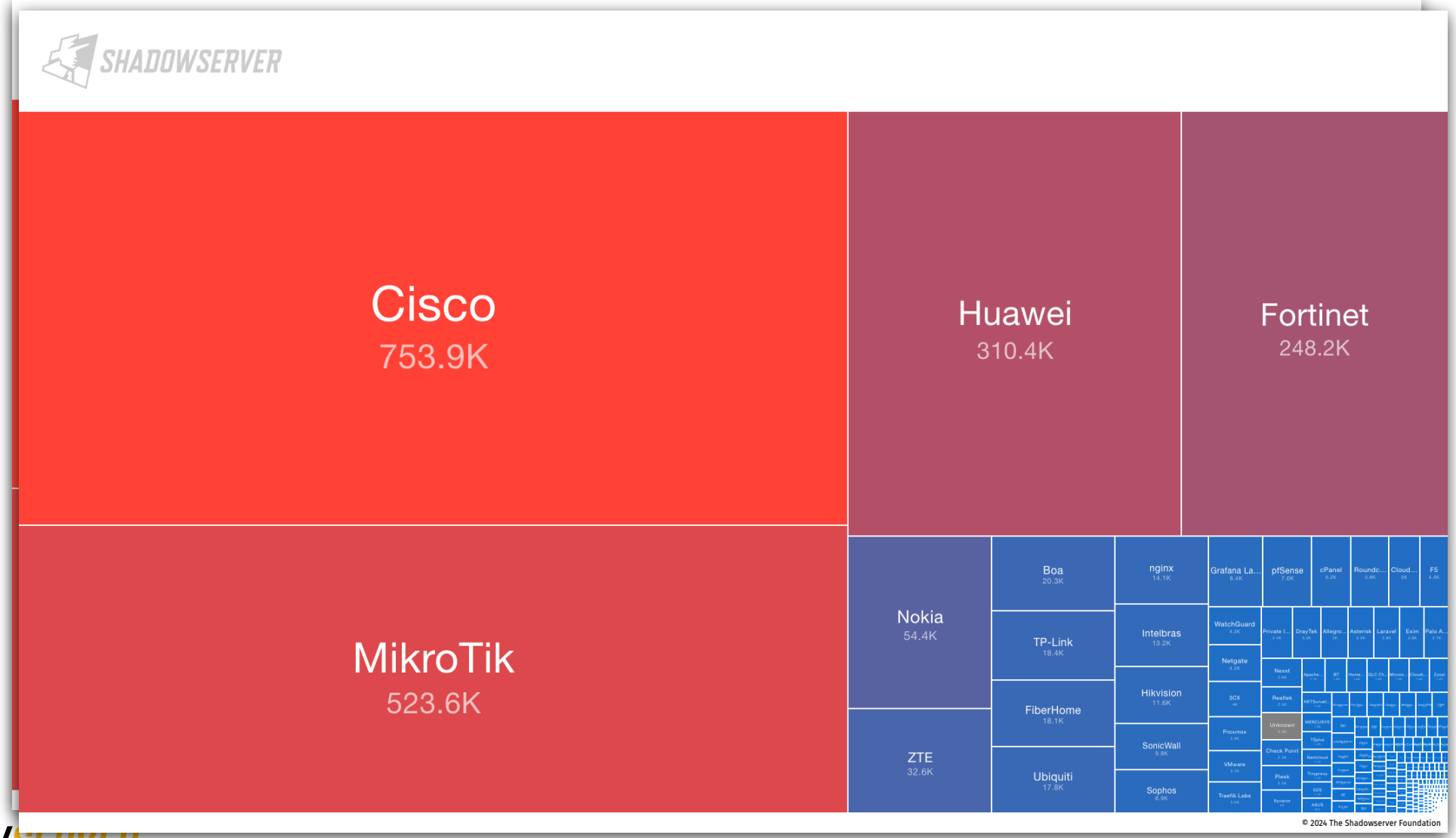


© 2024 The Shadowserver Foundation

Note: Only cases where we identify a device

TLP CLEAR

Device Exposure by Vendor - South America & Brazil (2024-07-24)

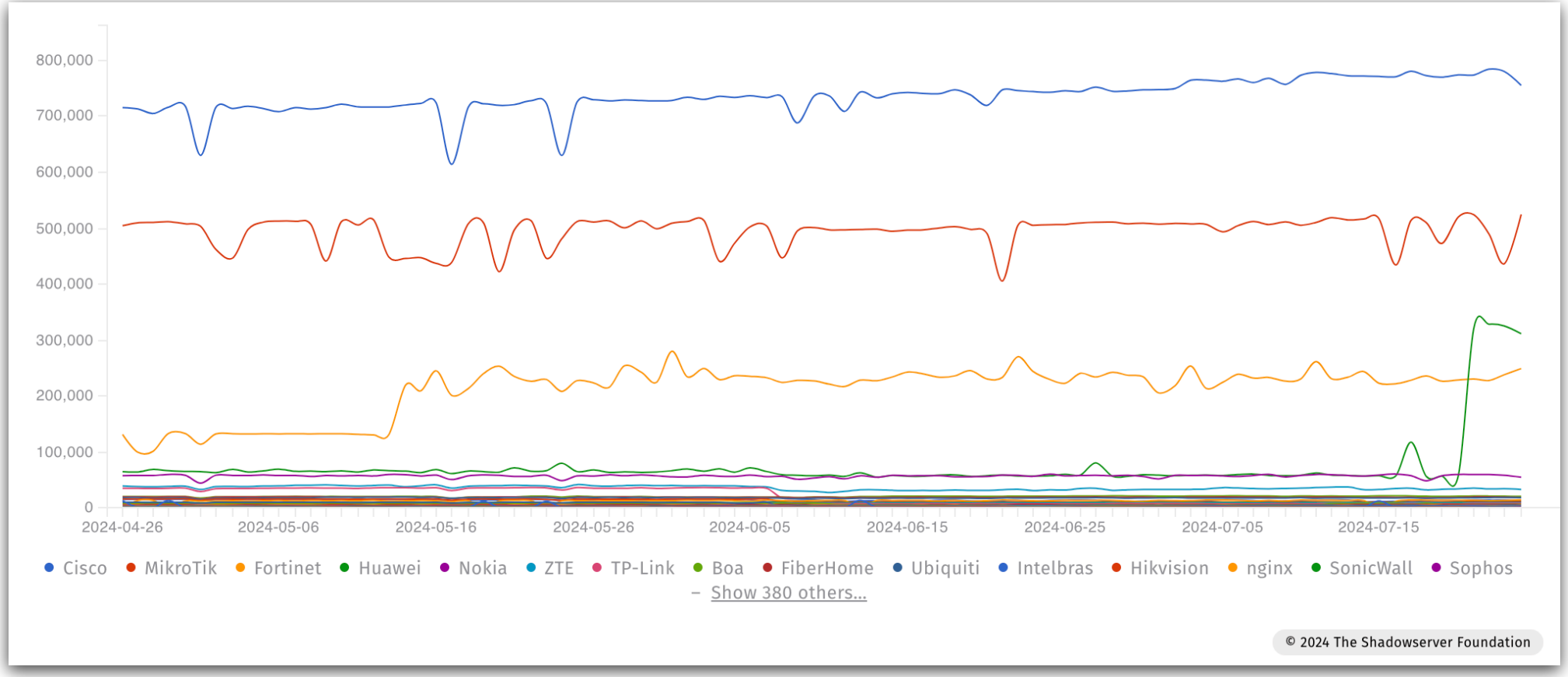


© 2024 The Shadowserver Foundation

Note: Only cases where we identify a device

TLP CLEAR

Device Exposure by Vendor - BR (Last 3 months)

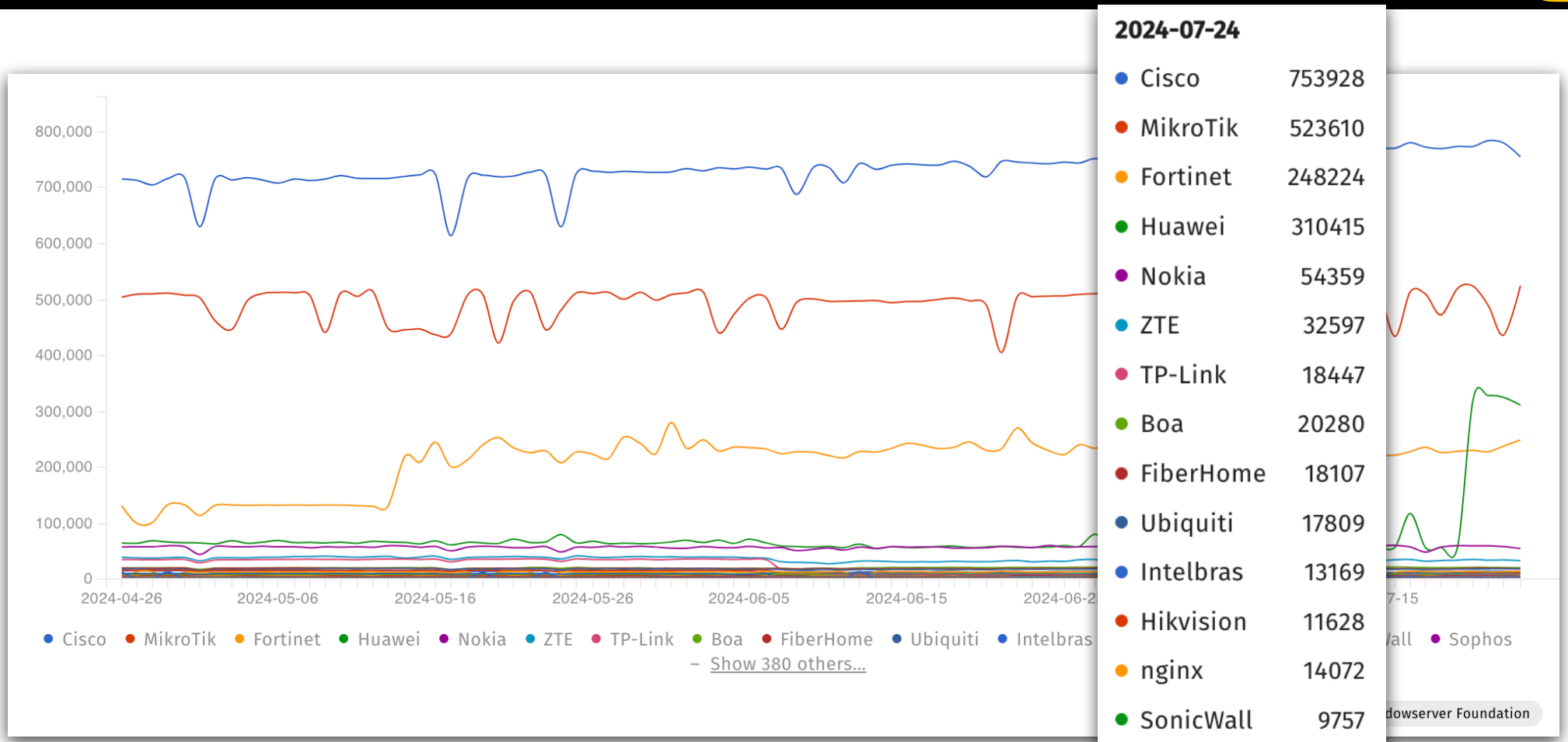


Note: Only cases where we identify a device

SHADOWSERVER

TLP CLEAR

Device Exposure by Vendor - BR (Last 3 months)



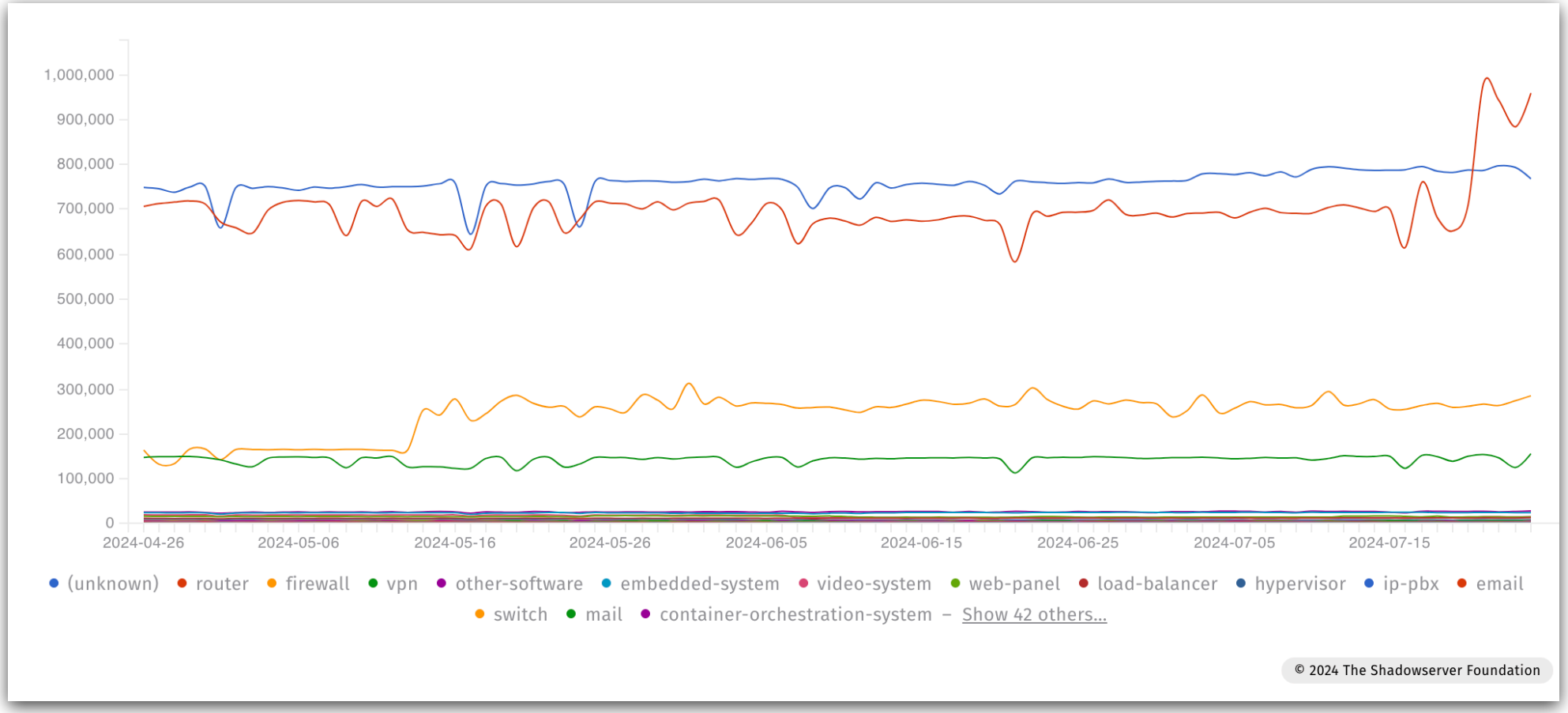
2024-07-24	
Cisco	753928
MikroTik	523610
Fortinet	248224
Huawei	310415
Nokia	54359
ZTE	32597
TP-Link	18447
Boa	20280
FiberHome	18107
Ubiquiti	17809
Intelbras	13169
Hikvision	11628
nginx	14072
SonicWall	9757
Sophos	8918
And 337 others...	

Note: Only cases where we identify a device

SHADOWSERVER

TLP CLEAR

Device Exposure by Type - BR (Last 3 months)

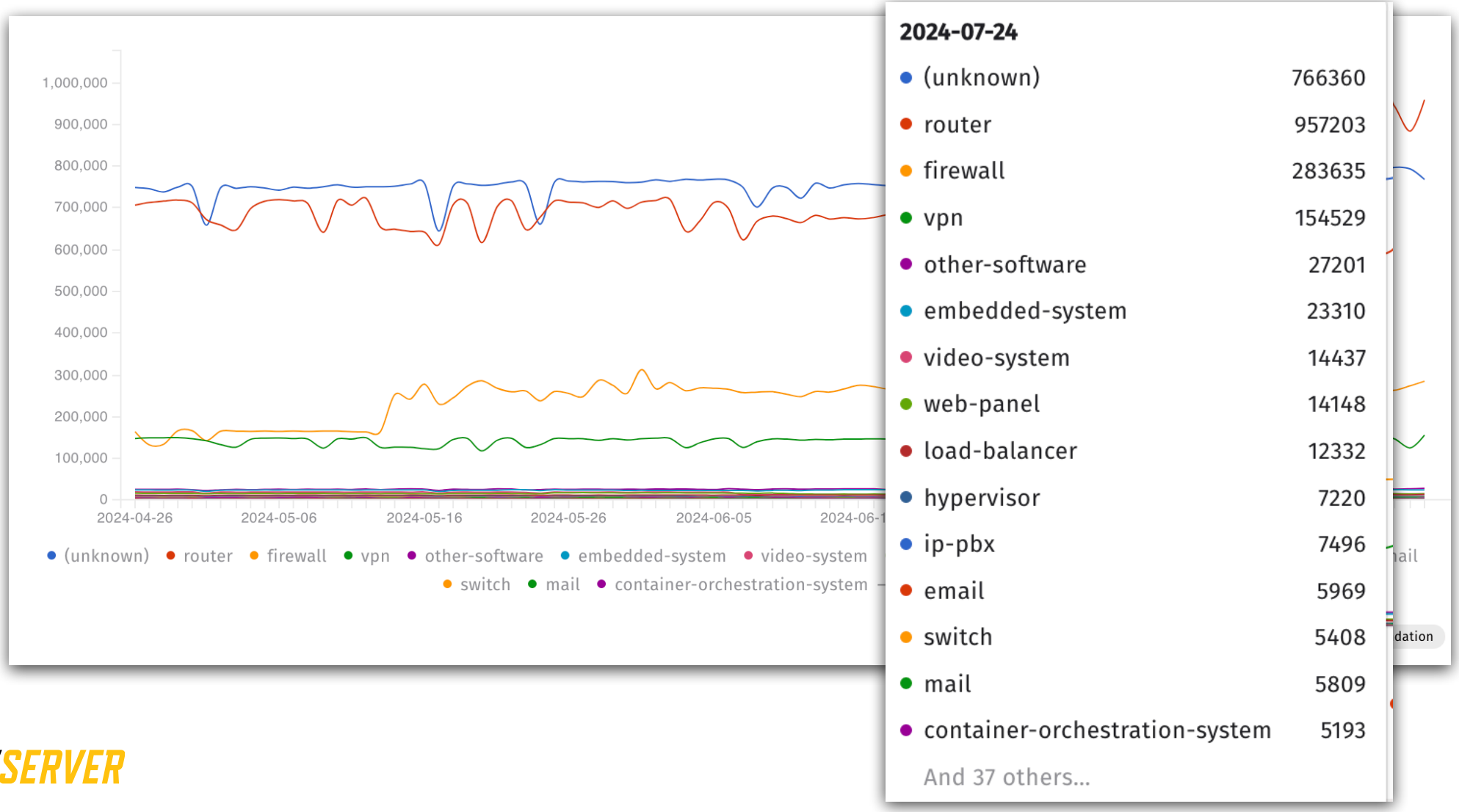


Note: Only cases where we identify a device

SHADOWSERVER

TLP CLEAR

Device Exposure by Type - BR (Last 3 months)

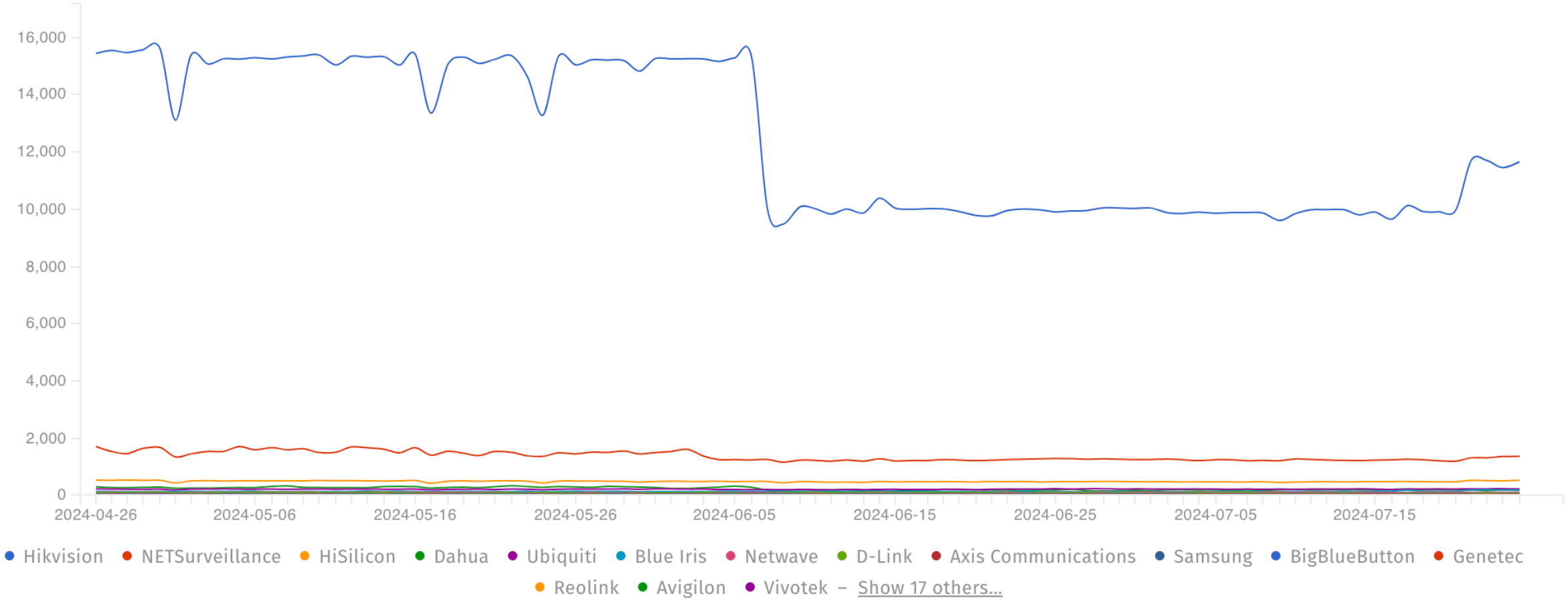


Note: Only cases where we identify a device

SHADOWSERVER

TLP CLEAR

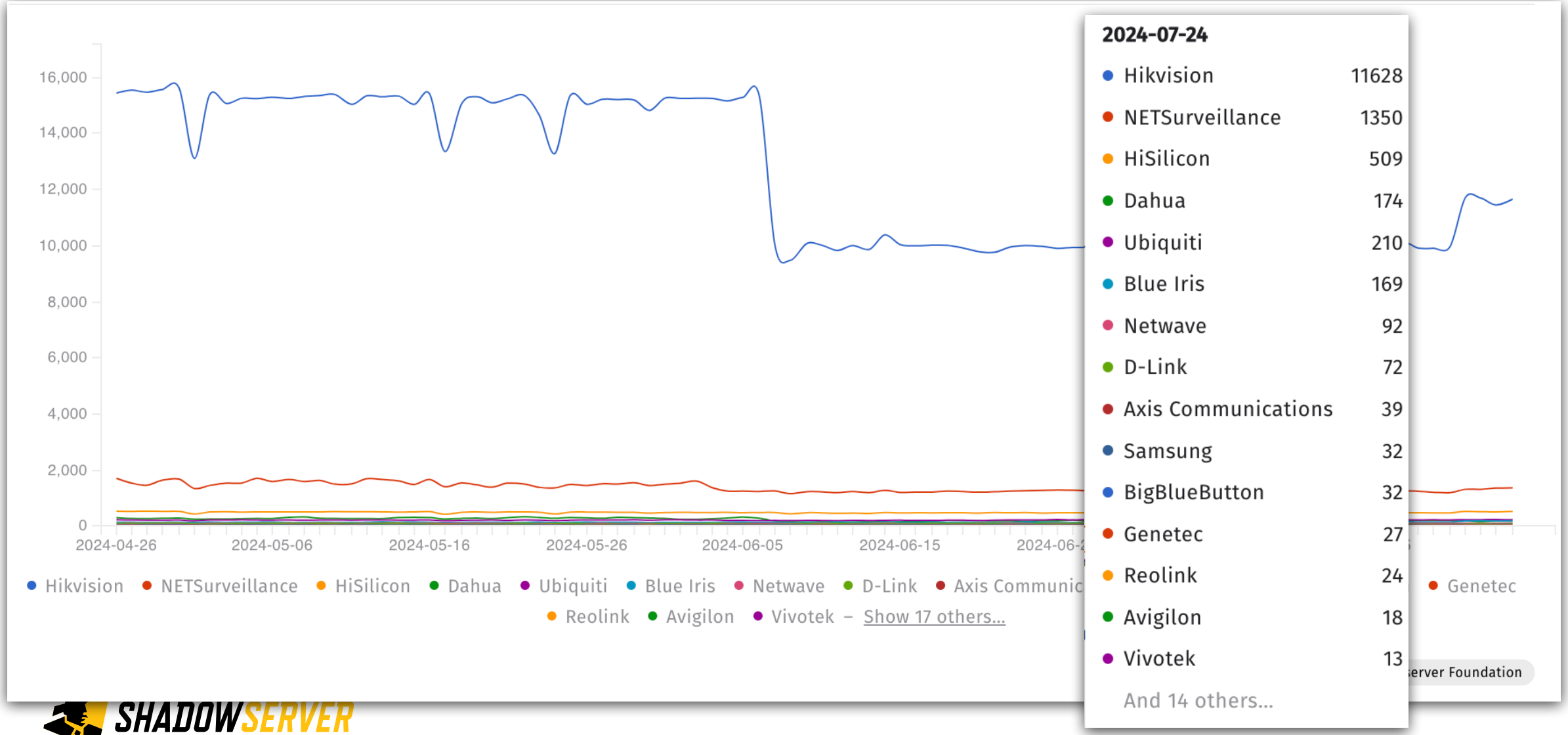
Video System Exposure - BR (Last 3 months)



SHADOWSERVER

TLP CLEAR

Video System Exposure - BR (Last 3 months)



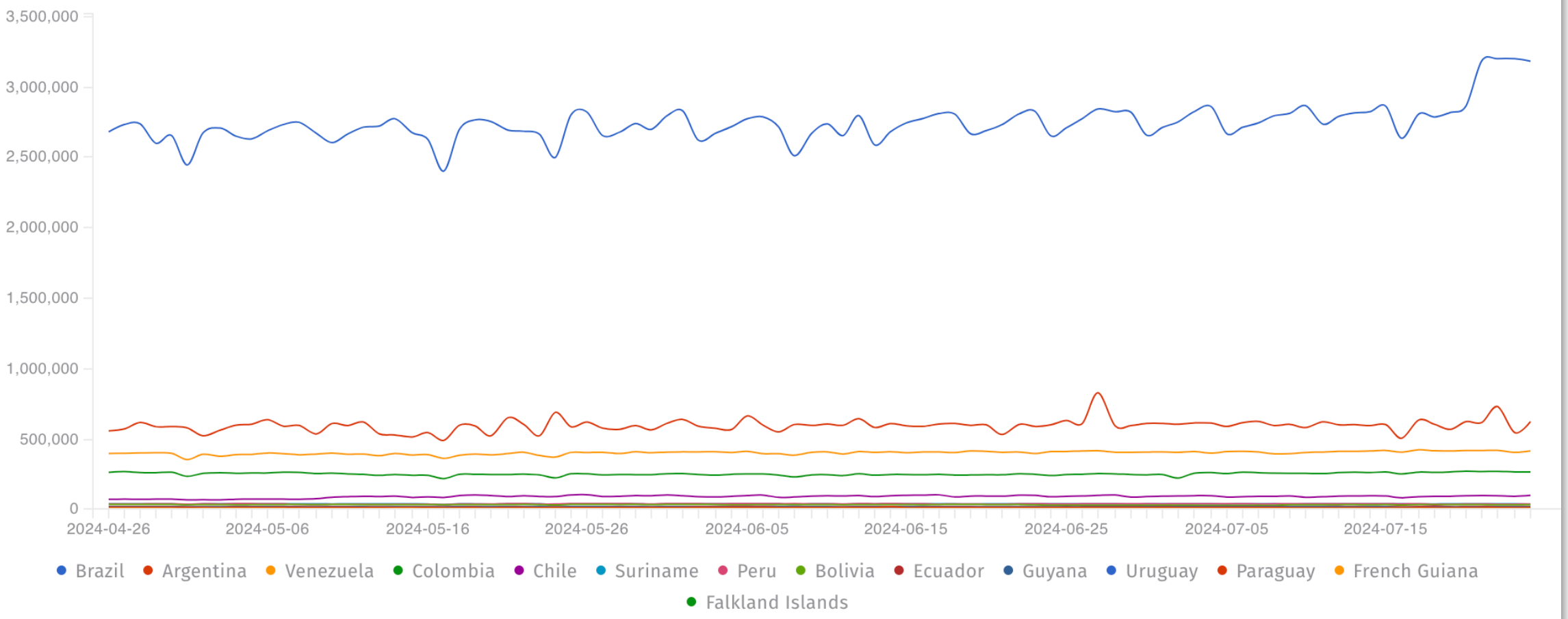
SHADOWSERVER

Exposed Services

Unnecessary attack surface

TLP CLEAR

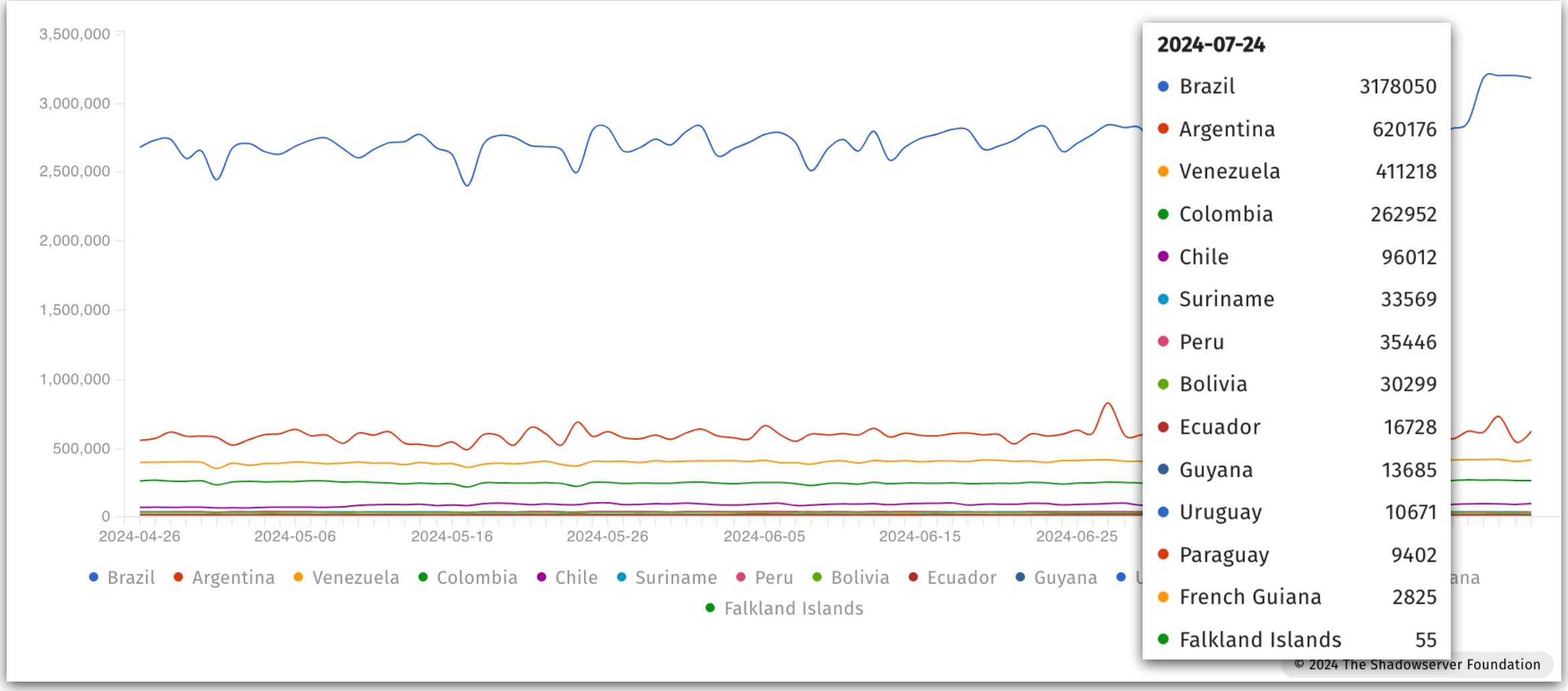
Problematic Exposed Server-side Applications (South America)



SHADOWSERVER

TLP CLEAR

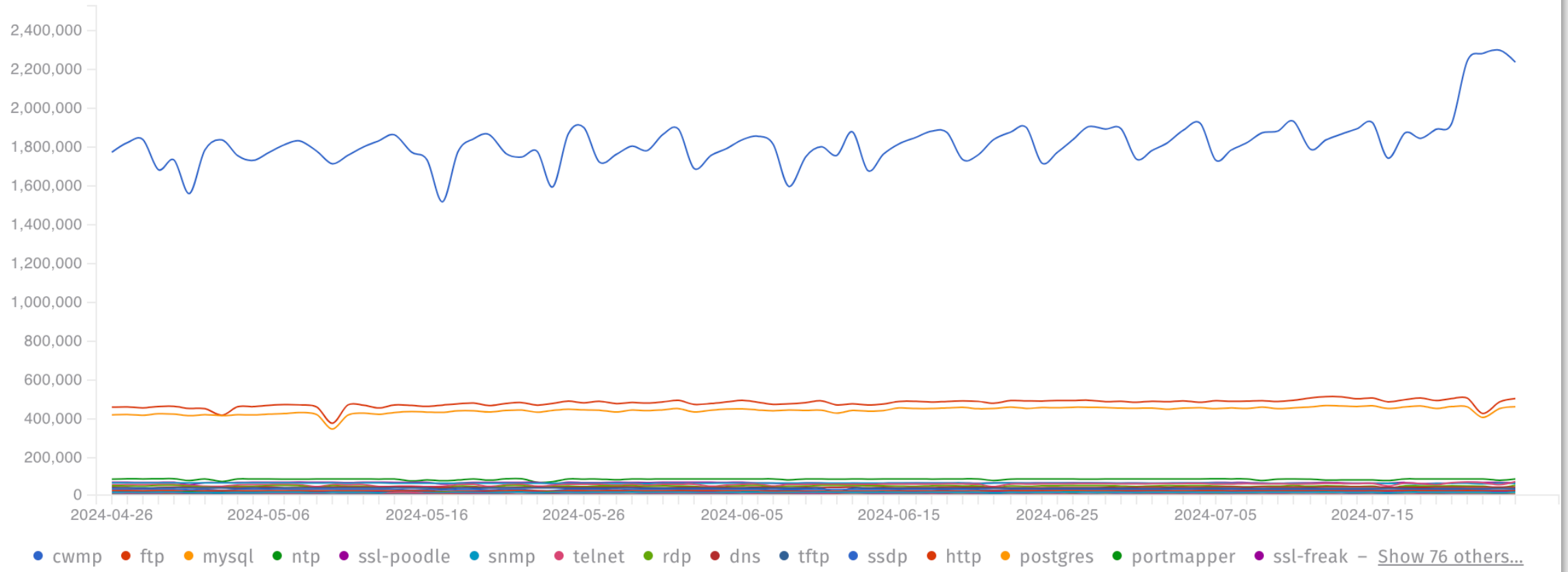
Problematic Exposed Server-side Applications (South America)



SHADOWSERVER

TLP CLEAR

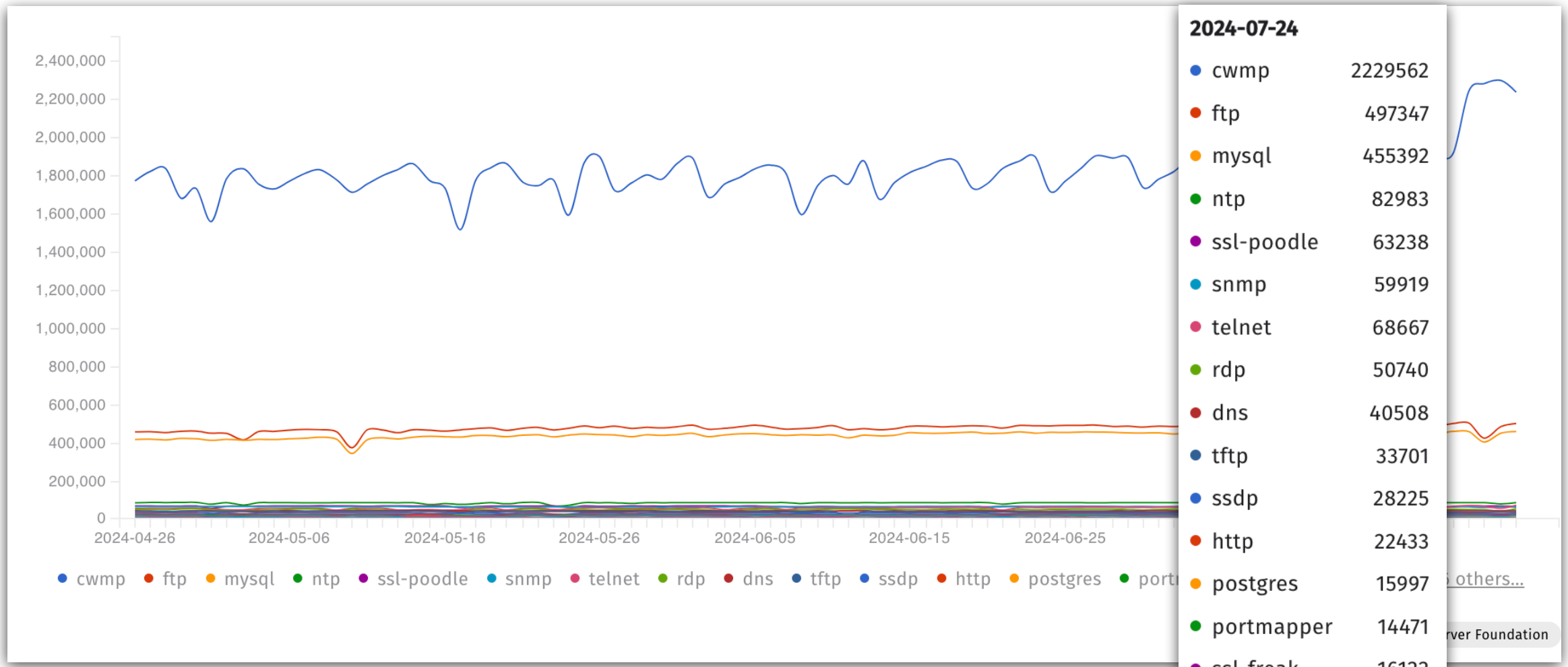
Problematic Exposed Server-side Applications by Type - BR



SHADOWSERVER

TLP CLEAR

Problematic Exposed Server-side Applications by Type - BR



SHADOWSERVER

TLP CLEAR

SCADA/ICS - Unitronics, Modbus & more

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Alert

ALERT

Exploitation of Unitronics PLCs used in Water and Wastewater Systems

Release Date: November 28, 2023

RELATED TOPICS: CYBERSECURITY BEST PRACTICES

CISA is responding to active exploitation of Unitronics programmable logic controllers (PLCs) used in the Water and Wastewater Systems (WWS) Sector. Cyber threat actors are targeting PLCs associated with WWS facilities, including an identified Unitronics PLC, at a U.S. water facility. In response, the affected municipality's water authority immediately took the system offline and switched to manual operations—there is no known risk to the municipality's drinking water or water supply.

WWS Sector facilities use PLCs to control and monitor various stages and processes of water and wastewater treatment, including turning on and off pumps at a pump station to fill tanks and reservoirs, flow pacing chemicals to meet regulations, gathering compliance data for monthly regulation reports, and announcing critical alarms to operations.

DRAGOS

Intelligence Brief: Impact of FrostyGoop ICS Malware on Connected OT Systems

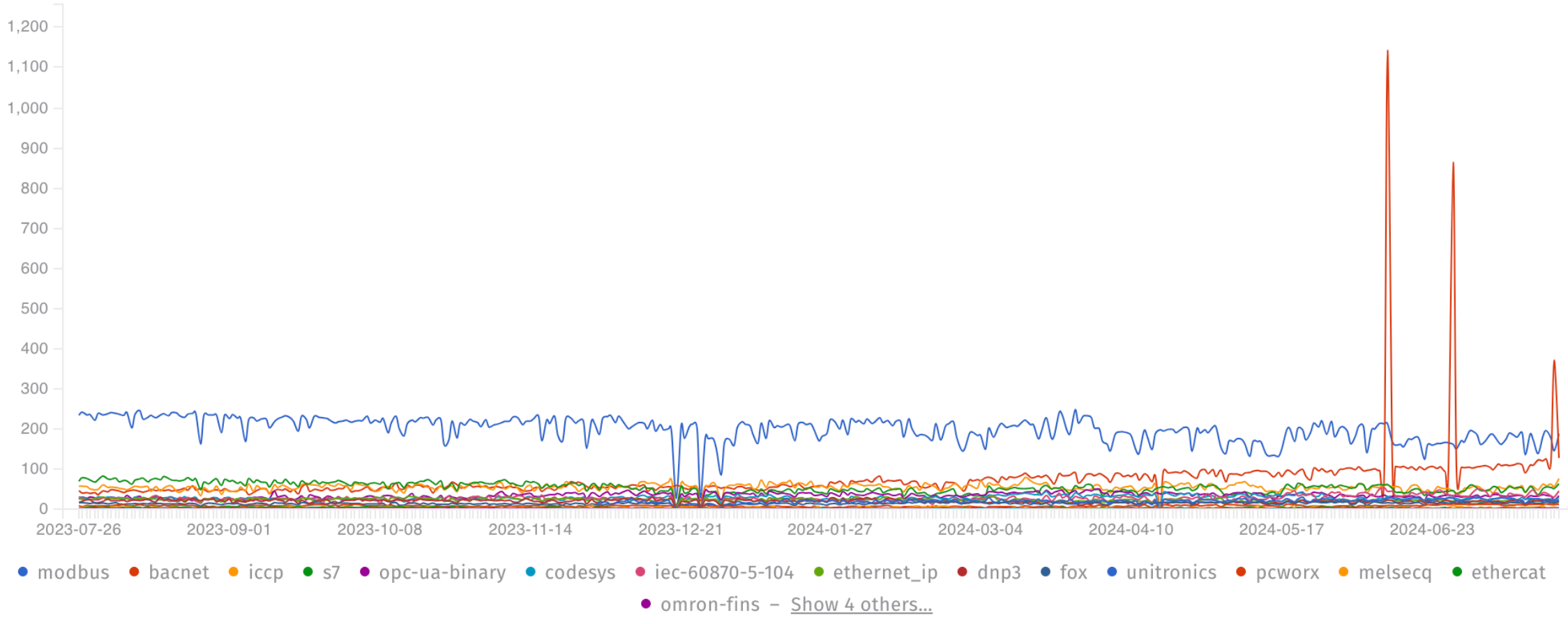
In April 2024, FrostyGoop, an ICS malware, was discovered in a publicly available malware scanning repository. FrostyGoop can target devices communicating over Modbus TCP to manipulate control, modify parameters, and send unauthorized command messages. Modbus TCP is a commonly used protocol across all industrial sectors.

The Cyber Security Situation Center (CSSC), a part of the Security Service of Ukraine, shared details with Dragos about a cyber attack that impacted a municipal district energy company in Ukraine in January 2024. At the time of the attack, this facility fed over 600 apartment buildings, supplying customers with central heating. Remediation of the incident took almost two days, during which time the civilian population had to endure sub-zero temperatures. Dragos assessed that FrostyGoop and internet-exposed ICS devices facilitated this attack.

SHADOWSERVER

TLP CLEAR

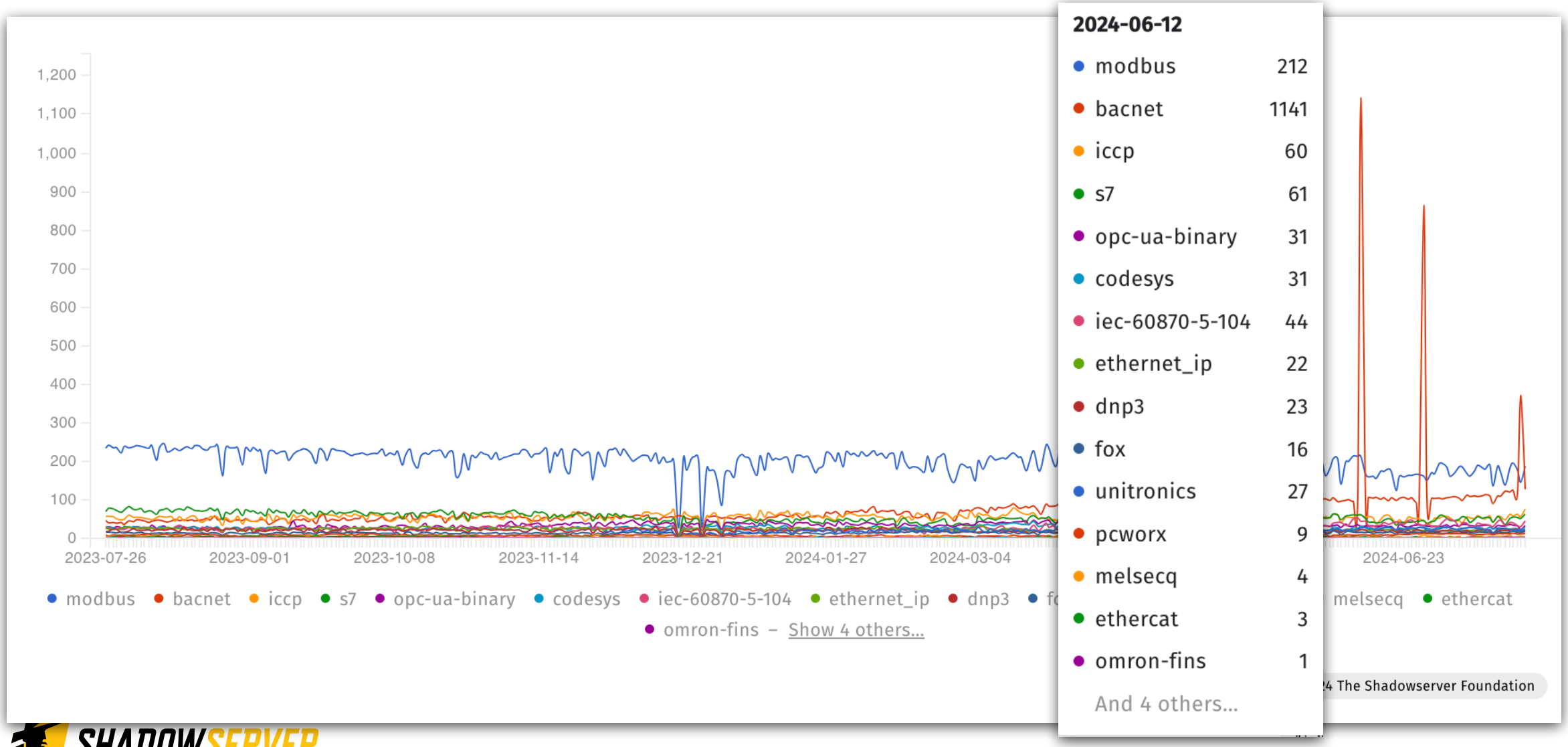
Exposed Native ICS Applications - South America



SHADOWSERVER

TLP CLEAR

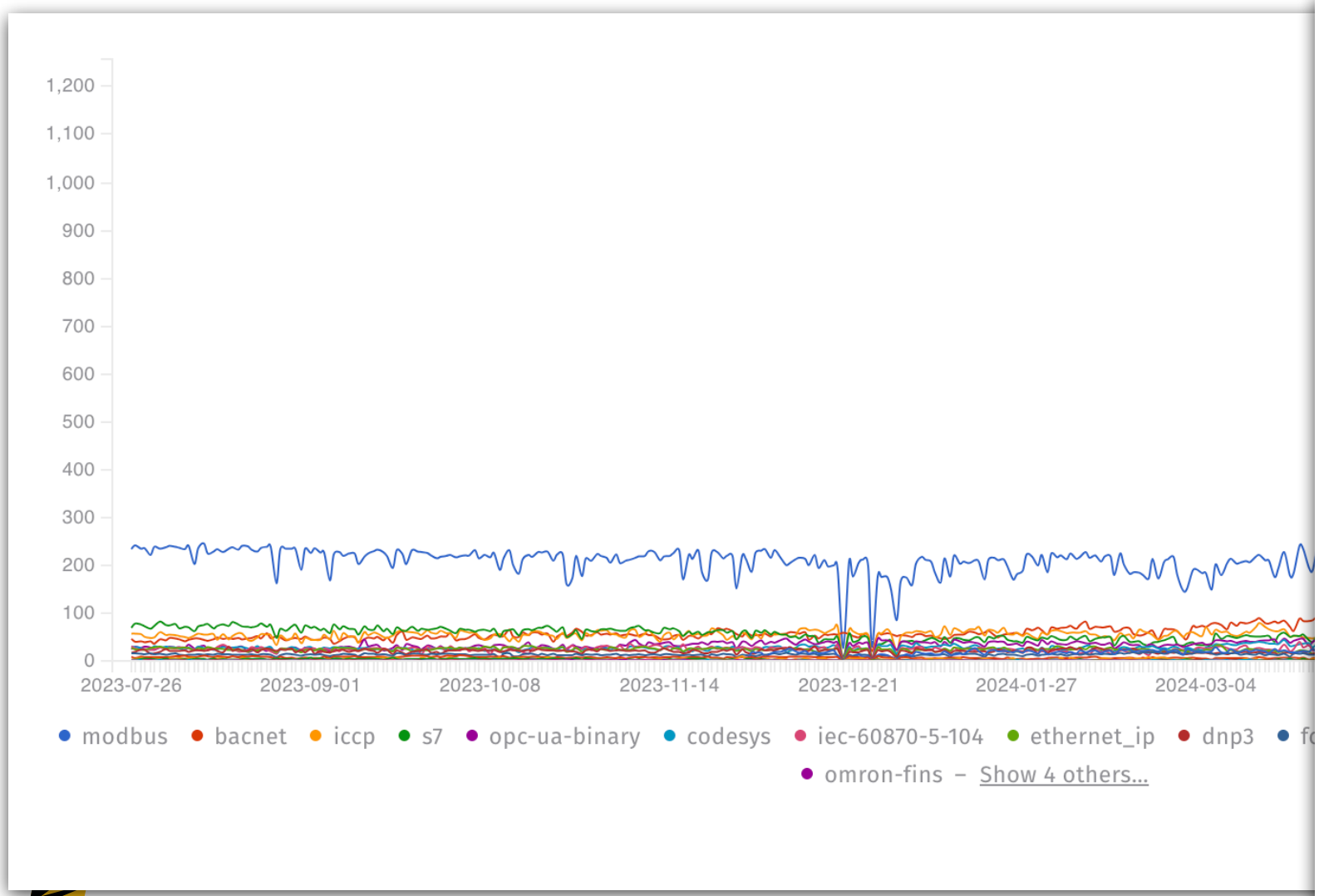
Exposed Native ICS Applications - South America



SHADOWSERVER

TLP CLEAR

Exposed Native ICS Applications - South America



2024-06-12

modbus	212
bacnet	1141
iccp	60
s7	61
opc-ua-binary	31
codesys	31
iec-60870-5-104	44
ethernet_ip	22
dnp3	23
fox	16
unitronics	27
pcworx	9
melsecq	4
ethercat	3
omron-fins	1

And 4 others...

2024-07-23

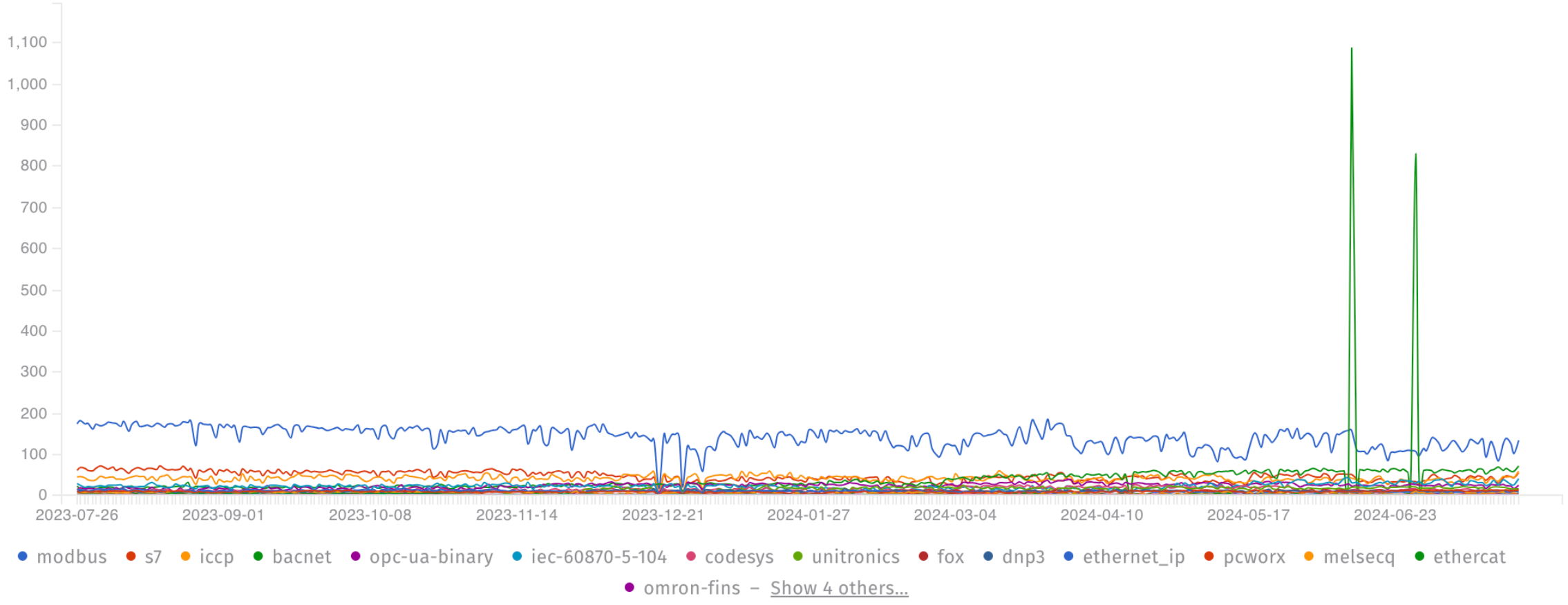
modbus	145
bacnet	370
iccp	56
s7	51
opc-ua-binary	23
codesys	22
iec-60870-5-104	30
ethernet_ip	14
dnp3	17
fox	15
unitronics	20
pcworx	11
melsecq	5
ethercat	1
omron-fins	2

And 2 others...

SHADOWSERVER

TLP CLEAR

Exposed Native ICS Applications - BR



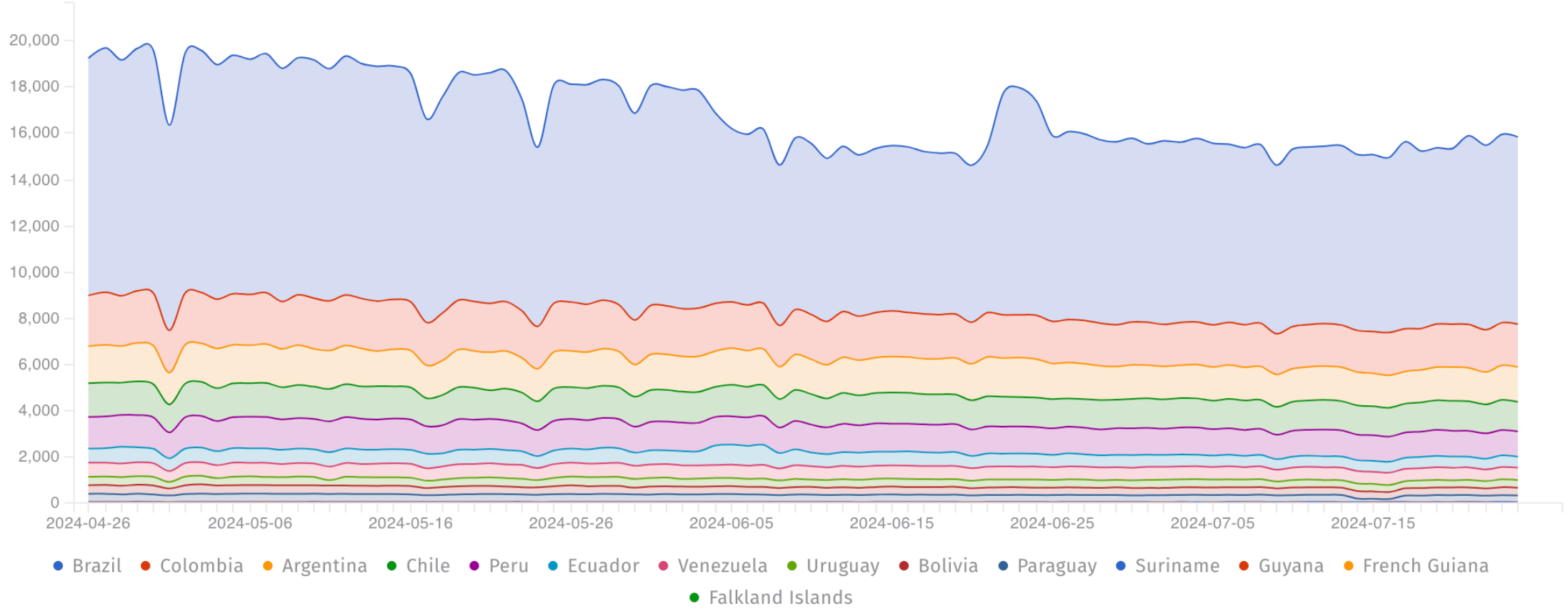
SHADOWSERVER

Critical Vulnerabilities

Infrastructure Vulnerable to Unauthenticated Remote Code Execution (via Web-based attacks)

TLP CLEAR

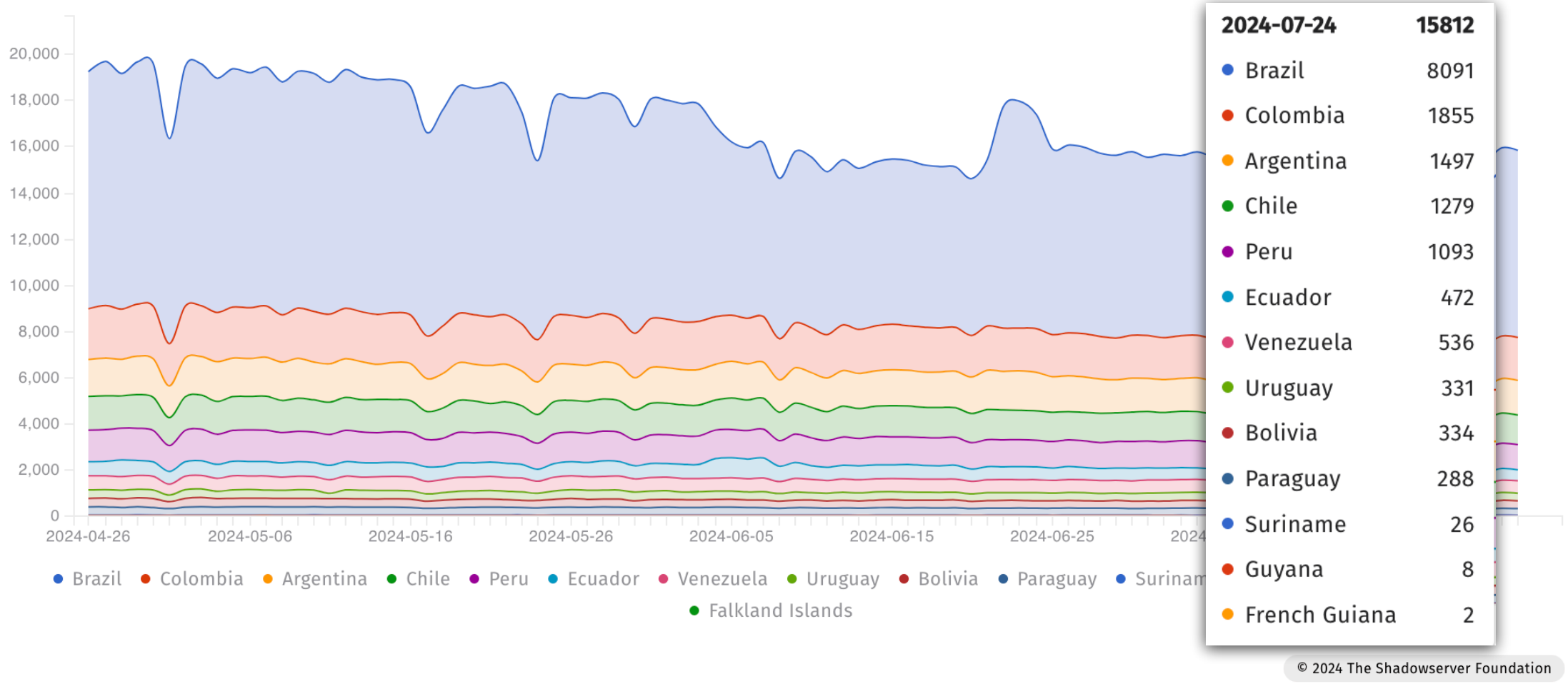
Exposed Assets (in Critical Applications) Vulnerable to RCE - South America



SHADOWSERVER

TLP CLEAR

Exposed Assets (in Critical Applications) Vulnerable to RCE - South America



SHADOWSERVER

TLP CLEAR

Top RCE exposure - South America & Brazil (Last 3 months)

Tag	Counted IP addresses	
cve-2024-21762	7,286	Fortinet
cve-2023-27997	4,227	Fortinet
cve-2020-3992	2,879	VMware ESXi
cve-2021-21974	2,879	VMware ESXi
cve-2019-5544	2,663	VMware ESXi
cve-2023-5631	1,782	Roundcube
cve-2022-37042	1,268	Zimbra Collaboration Suite
cve-2023-43770	869	Roundcube
cve-2024-22252	415	VMware ESXi
cve-2022-42475	340	Fortinet
cve-2023-33308	340	Fortinet

South America

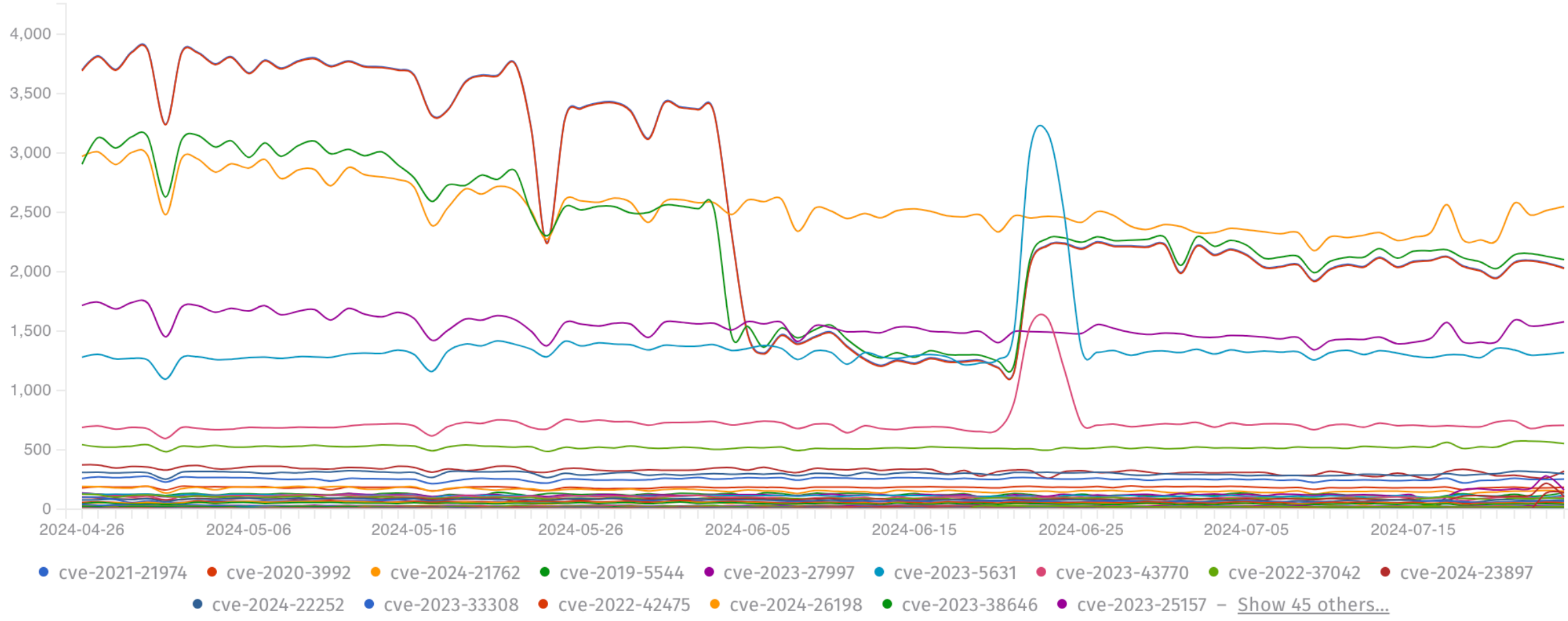
Tag	Counted IP addresses	
cve-2020-3992	2,556	VMware ESXi
cve-2021-21974	2,556	VMware ESXi
cve-2024-21762	2,475	Fortinet
cve-2019-5544	2,287	VMware ESXi
cve-2023-27997	1,464	Fortinet
cve-2023-5631	1,282	Roundcube
cve-2023-43770	726	Roundcube
cve-2022-37042	521	Zimbra Collaboration Suite
cve-2024-22252	278	VMware ESXi
cve-2022-42475	182	Fortinet
cve-2023-33308	182	Fortinet

Brazil

SHADOWSERVER

TLP CLEAR

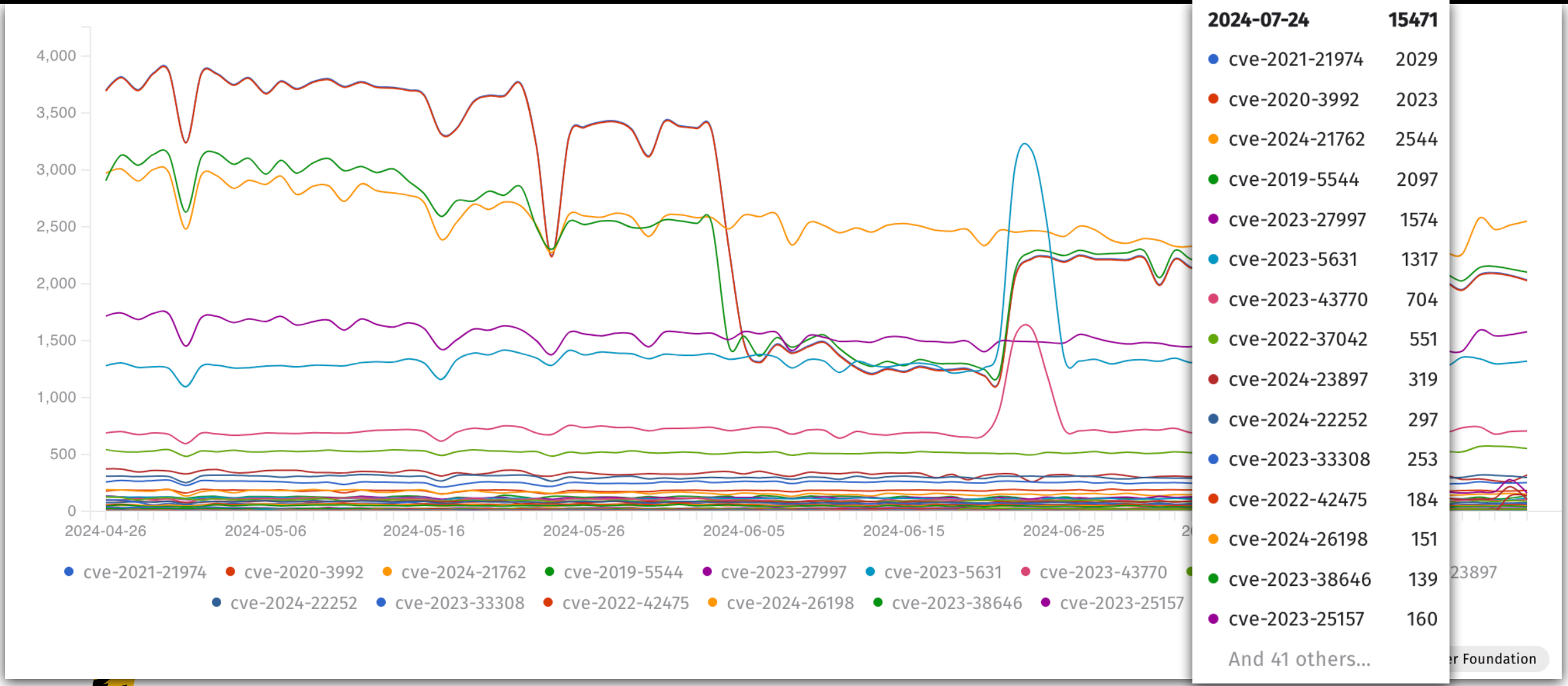
Exposed Assets (in Critical Applications) Vulnerable to RCE - BR



SHADOWSERVER

TLP CLEAR

Exposed Assets (in Critical Applications) Vulnerable to RCE - BR



SHADOWSERVER

Citrix NetScaler

CVE-2023-3519

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

CTX561482

Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467

Security Bulletin | Severity: Critical | 137 found this helpful | Created: 18 Jul 2023 | Modified: 18 Jul 2023 | Status: Final

Applicable Products

Citrix ADC Citrix Gateway

Description of Problem

Multiple vulnerabilities have been discovered in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway).

The following supported versions of NetScaler ADC and NetScaler Gateway are affected by the vulnerabilities:

- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13
- NetScaler ADC and NetScaler Gateway 13.0 before 13.0-91.13
- NetScaler ADC 13.1-FIPS before 13.1-37.159
- NetScaler ADC 12.1-FIPS before 12.1-55.297
- NetScaler ADC 12.1-NDcPP before 12.1-55.297

Note: NetScaler ADC and NetScaler Gateway version 12.1 is now End Of Life (EOL) and is vulnerable.

Start Chat

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

CTX561482

Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467

Security Bulletin | Severity: Critical | 137 found this helpful | Created: 18 Jul 2023 | Modified: 18 Jul 2023 | Status: Final

Shadowserver already had Device Identification rules in place for Citrix NetScaler. This helped free daily report constituents in multiple sectors to quickly identify where Citrix devices were located in their networks, which allowed local Incident Response (IR) teams to start immediate investigations as soon as the vendor advisory was made public, and in some cases feed their discoveries back to us, as part of our existing scan/report/feedback cycle with some constituents.

- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13
- NetScaler ADC and NetScaler Gateway 13.0 before 13.0-91.13
- NetScaler ADC 13.1-FIPS before 13.1-37.159
- NetScaler ADC 12.1-FIPS before 12.1-55.297
- NetScaler ADC 12.1-NDcPP before 12.1-55.297

Note: NetScaler ADC and NetScaler Gateway version 12.1 is now End Of Life (EOL) and is vulnerable.

Start Chat

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

CTX561482

Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467

Security Bulletin | Severity: Critical | 137 found this helpful | Created: 18 Jul 2023 | Modified: 18 Jul 2023 | Status: Final

Shadowserver already had Device Identification rules in place for Citrix NetScaler. This helped free daily report constituents in multiple sectors to quickly identify where Citrix devices were located in their networks, which allowed local Incident Response (IR) teams to start immediate investigations as soon as the vendor advisory was made public, and in some cases feed their discoveries back to us, as part of our existing scan/report/feedback cycle with some constituents.

Fingerprinting was consistently improved in the following days, based on feedback

- NetScaler ADC 13.1-FIPS before 13.1-37.159
- NetScaler ADC 12.1-FIPS before 12.1-55.297
- NetScaler ADC 12.1-NDcPP before 12.1-55.297

Note: NetScaler ADC and NetScaler Gateway version 12.1 is now End Of Life (EOL) and is vulnerable.

Start Chat

SHADOWSERVER

Citrix NetScaler: CVE-2023-3519

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 19th: CISA Adds Citrix NetScaler CVE-2023-3519 to its KEV list

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 19th: CISA Adds Citrix NetScaler CVE-2023-3519 to its KEV list

July 19th: Shadowserver develops first CVE-2023-3519 vulnerability scan (based on hash version presence in html body content)

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 19th: CISA Adds Citrix NetScaler CVE-2023-3519 to its KEV list

July 19th: Shadowserver develops first CVE-2023-3519 vulnerability scan (based on hash version presence in html body content)

July 20th: Shadowserver shares vulnerable instance information in its daily reports (Vulnerable HTTP report)

SHADOWSERVER

TLP CLEAR

Citrix NetS

July 19th: CISA Adds Citrix Net

July 19th: Shadowserver devel presence in html body content)

July 20th: Shadowserver share TTP report)

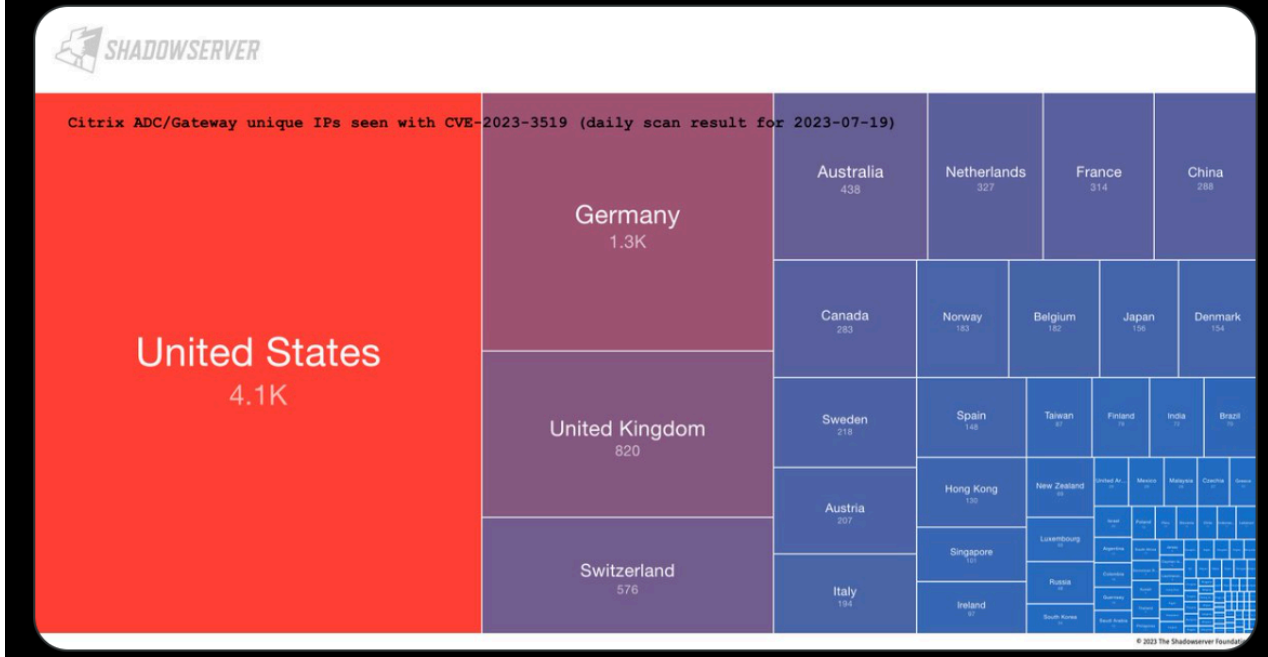
The Shadowserver Foundation
@Shadowserver

Now sharing info on likely CVE-2023-3519 vulnerable Citrix ADC/Gateway instances in our Vulnerable HTTP report: shadowserver.org/what-we-do/net...

At least 11170 unique IPs found, most in the US (4.1K).

Make sure to patch: support.citrix.com/article/CTX561...

Dashboard stats: dashboard.shadowserver.org/statistics/com...



3:39 PM · Jul 20, 2023 · **14.8K** Views

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 19th: CISA Adds Citrix NetScaler CVE-2023-3519 to its KEV list

July 19th: Shadowserver develops first CVE-2023-3519 vulnerability scan (based on hash version presence in html body content)

July 20th: Shadowserver shares vulnerable instance information in its daily reports (Vulnerable HTTP report)

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 19th: CISA Adds Citrix NetScaler CVE-2023-3519 to its KEV list

July 19th: Shadowserver develops first CVE-2023-3519 vulnerability scan (based on hash version presence in html body content)

July 20th: Shadowserver shares vulnerable instance information in its daily reports (Vulnerable HTTP report)

July 20th: CISA Advisory on CVE-2023-3519 with information on exploitation and webshells

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 19th: CISA Adds Citrix NetScaler CVE-2023-3519 to its KEV list

July 19th: Shadowserver develops first CVE-2023-3519 vulnerability scan (based on hash version presence in html body content)

July 20th: Shadowserver shares vulnerable instance information in its daily reports (Vulnerable HTTP report)

July 20th: CISA Advisory on CVE-2023-3519 with information on exploitation and webshells

July 21st: Shadowserver improves scans for vulnerable instances - based on feedback

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 19th: CISA Adds Citrix Net

July 19th: Shadowserver devel ml body content)

July 20th: Shadowserver share

July 20th: CISA Advisory on CV

July 21st: Shadowserver impro

The Shadowserver Foundation
@Shadowserver

Update on CVE-2023-3519 vulnerable IPs: we now tag 15K Citrix IPs as vulnerable to CVE-2023-3519. We extended the tagging logic to tag as vulnerable all that return Last Modified headers with a date before July 1, 2023 00:00:00Z. We also improved NetScaler AAA detection coverage.

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 19th: CISA Adds Citrix NetScaler CVE-2023-3519 to its KEV list

July 19th: Shadowserver develops first CVE-2023-3519 vulnerability scan (based on hash version presence in html body content)

July 20th: Shadowserver shares vulnerable instance information in its daily reports (Vulnerable HTTP report)

July 20th: CISA Advisory on CVE-2023-3519 with information on exploitation and webshells

July 21st: Shadowserver improves scans for vulnerable instances - based on feedback

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 19th: CISA Adds Citrix NetScaler CVE-2023-3519 to its KEV list

July 19th: Shadowserver develops first CVE-2023-3519 vulnerability scan (based on hash version presence in html body content)

July 20th: Shadowserver shares vulnerable instance information in its daily reports (Vulnerable HTTP report)

July 20th: CISA Advisory on CVE-2023-3519 with information on exploitation and webshells

July 21st: Shadowserver improves scans for vulnerable instances - based on feedback

July 21st: Initial analysis by AssetNote in their search for CVE-2023-3519 details

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 19th: CISA Adds Citrix NetScaler CVE-2023-3519 to its KEV list

July 19th: Shadowserver develops first CVE-2023-3519 vulnerability scan (based on hash version presence in html body content)

July 20th: Shadowserver shares vulnerable instance information in its daily reports (Vulnerable HTTP report)

July 20th: CISA Advisory on CVE-2023-3519 with information on exploitation and webshells

July 21st: Shadowserver improves scans for vulnerable instances - based on feedback

July 21st: Initial analysis by AssetNote in their search for CVE-2023-3519 details

July 21st: Honeypot profile added

SHADOWSERVER

Citrix NetScaler: CVE-2023-3519

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

July 24th: First Exploitation attempts observed by honeypots - CVE-2024-3519 tagging added by Shadowserver

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

July 24th: First Exploitation attempts observed by honeypots - CVE-2024-3519 tagging added by Shadowserver

July 26th: First CVE-2024-3519 tagged exploitation attempts

SHADOWSERVER

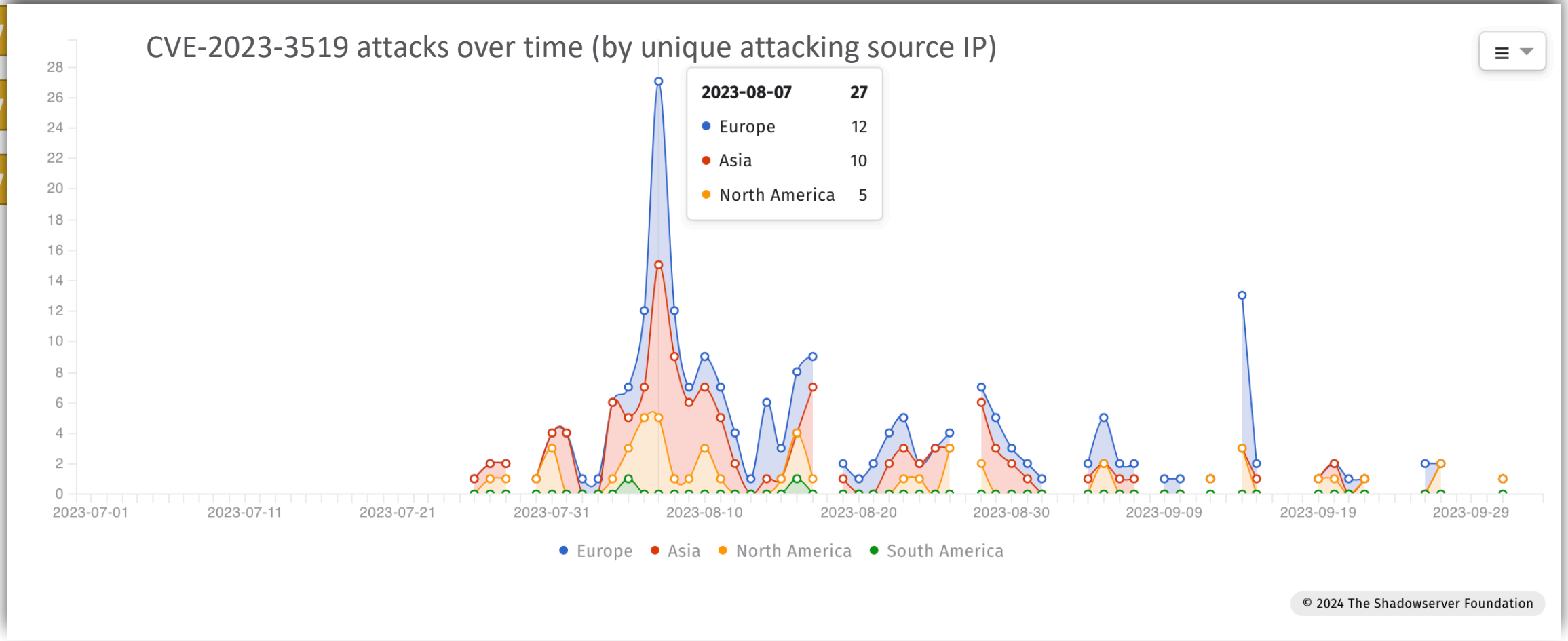
TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July

July

July



SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

July 24th: First Exploitation attempts observed by honeypots - CVE-2024-3519 tagging added by Shadowserver

July 26th: First CVE-2024-3519 tagged exploitation attempts

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

July 24th: First Exploitation attempts observed by honeypots - CVE-2024-3519 tagging added by Shadowserver

July 26th: First CVE-2024-3519 tagged exploitation attempts

July 27th: Trusted partner reaches out to us that they found China Chopper webshells installed on compromised instances

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

July 24th: First Exploitation attempts observed by honeypots - CVE-2024-3519 tagging added by Shadowserver

July 26th: First CVE-2024-3519 tagged exploitation attempts

July 27th: Trusted partner reaches out to us that they found China Chopper webshells installed on compromised instances

July 28th: First full scan for webshells conducted based on developed methodology: 691 found

SHADOWSERVER

TLP CLEAR

Citrix NetSc

July 24th: CVE-2024-3519 PoC pub

July 24th: First Exploitation attemp by Shadowserver

July 26th: First CVE-2024-3519 tag

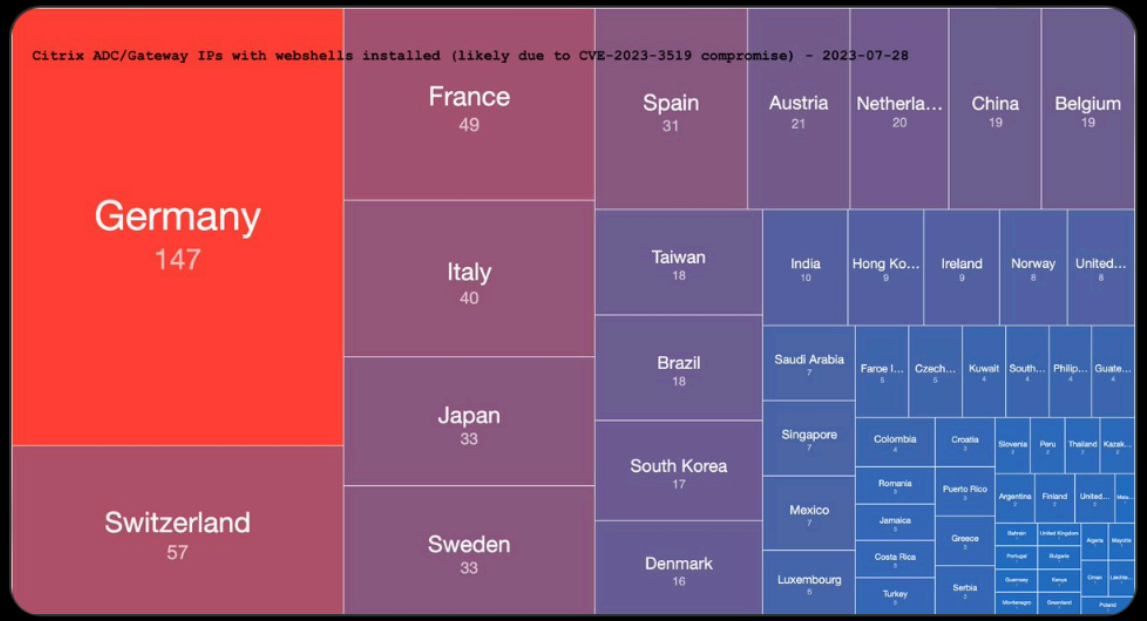
July 27th: Trusted partner reaches d on compromised instances

July 28th: First full scan for webshe d

The Shadowserver Foundation
@Shadowserver

We are reporting out webshells installed on Citrix ADC/Gateway IPs likely compromised as part of CVE-2023-3519 attacks. We found 691 instances on 2023-07-28. If you received a report today for your network/constituency, please make sure to investigate.

shadowserver.org/what-we-do/net...



3:32 PM · Jul 29, 2023 · **10.4K** Views

View post engagements

1 25 41 5

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

July 24th: First Exploitation attempts observed by honeypots - CVE-2024-3519 tagging added by Shadowserver

July 26th: First CVE-2024-3519 tagged exploitation attempts

July 27th: Trusted partner reaches out to us that they found China Chopper webshells installed on compromised instances

July 28th: First full scan for webshells conducted based on developed methodology: 691 found

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

July 24th: First Exploitation attempts observed by honeypots - CVE-2024-3519 tagging added by Shadowserver

July 26th: First CVE-2024-3519 tagged exploitation attempts

July 27th: Trusted partner reaches out to us that they found China Chopper webshells installed on compromised instances

July 28th: First full scan for webshells conducted based on developed methodology: 691 found

Aug 7th: We publish a technical blog in collaboration with trusted partners. TLP:AMBER version shared Aug 4th

SHADOWSERVER

TLP CLEAR

Citrix NetSc

July 24th: CVE-2024-3519 PoC pub

July 24th: First Exploitation attemp by Shadowserver

July 26th: First CVE-2024-3519 tag

July 27th: Trusted partner reaches d on compromised instances

July 28th: First full scan for webshe d

Aug 7th: We publish a technical bl n shared Aug 4th

Technical Summary of Observed Citrix CVE-2023-3519 Incidents

AUGUST 7, 2023

INTRODUCTION

The Shadowserver Foundation and trusted partners have observed three different malicious campaigns that have exploited **CVE-2023-3519**, a code injection vulnerability rated **CVSS 9.8** critical in **Citrix NetScaler ADC and NetScaler Gateway**. The summary below is based on collaboration with the individual compromised organizations, as well as their commercial incident response teams. All timestamps in this write-up are in **UTC timezone**, and they have all been slightly adjusted to not disclose the actual times. **Please ensure you follow the detection and hunting steps provided for signs of possible compromise and webshell presence**.

Citrix released an advisory along with a patch on July 18th 2023 – **CTX561482 Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467**. Initial CVE-2023-3519 attacks were well documented by CISA in their **Cybersecurity Advisory Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells** on July 20th 2023.

To assist National CSIRTs and system defenders in identifying which organizations and Citrix instances they should focus on and investigate/remediate, Shadowserver provides – amongst others – the **Device Identification report** and the **Vulnerable HTTP report**. These proved very useful as Partners could use the **Shadowserver Device Identification report** to look for Citrix NetScaler/Gateway devices very rapidly in their constituency. The Shadowserver **Vulnerable HTTP report** was expanded quickly to tag vulnerable Citrix NetScaler/Gateway devices with "cve-2023-3519" starting July 20th, which enabled Partners to quickly gain insight into which devices needed particular attention. As a result of the work documented in this summary, **Shadowserver have reported over 600 hosts** that have webshells installed through the **Shadowserver Compromised Website report**. The real number of compromised/webshelled hosts will be significantly higher, as any host patched/updated after July 20th will not be included in the report.

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

July 24th: First Exploitation attempts observed by honeypots - CVE-2024-3519 tagging added by Shadowserver

July 26th: First CVE-2024-3519 tagged exploitation attempts

July 27th: Trusted partner reaches out to us that they found China Chopper webshells installed on compromised instances

July 28th: First full scan for webshells conducted based on developed methodology: 691 found

Aug 7th: We publish a technical blog in collaboration with trusted partners. TLP:AMBER version shared Aug 4th

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

July 24th: First Exploitation attempts observed by honeypots - CVE-2024-3519 tagging added by Shadowserver

July 26th: First CVE-2024-3519 tagged exploitation attempts

July 27th: Trusted partner reaches out to us that they found China Chopper webshells installed on compromised instances

July 28th: First full scan for webshells conducted based on developed methodology: 691 found

Aug 7th: We publish a technical blog in collaboration with trusted partners. TLP:AMBER version shared Aug 4th

Aug 13th: Mandiant update their blogs/tooling to include Shadowserver contribution

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

July 24th: First Exploitation attempts observed by honeypots - CVE-2024-3519 tagging added by Shadowserver

July 26th: First CVE-2024-3519 tagged exploitation attempts

July 27th: Trusted partner reaches out to us that they found China Chopper webshells installed on compromised instances

July 28th: First full scan for webshells conducted based on developed methodology: 691 found

Aug 7th: We publish a technical blog in collaboration with trusted partners. TLP:AMBER version shared Aug 4th

Aug 13th: Mandiant update their blogs/tooling to include Shadowserver contribution

Aug 18th: Share further reports on compromised devices based on Fox-IT/DIVD NL collaboration

SHADOWSERVER

TLP CLEAR

Citrix NetS

July 24th: CVE-2024-3519 PoC p

July 24th: First Exploitation atte

July 26th: First CVE-2024-3519 t

July 27th: Trusted partner reach

July 28th: First full scan for web

Aug 7th: We publish a technical

Aug 13th: Mandiant update the

Aug 18th: Share further reports

Shadowserver

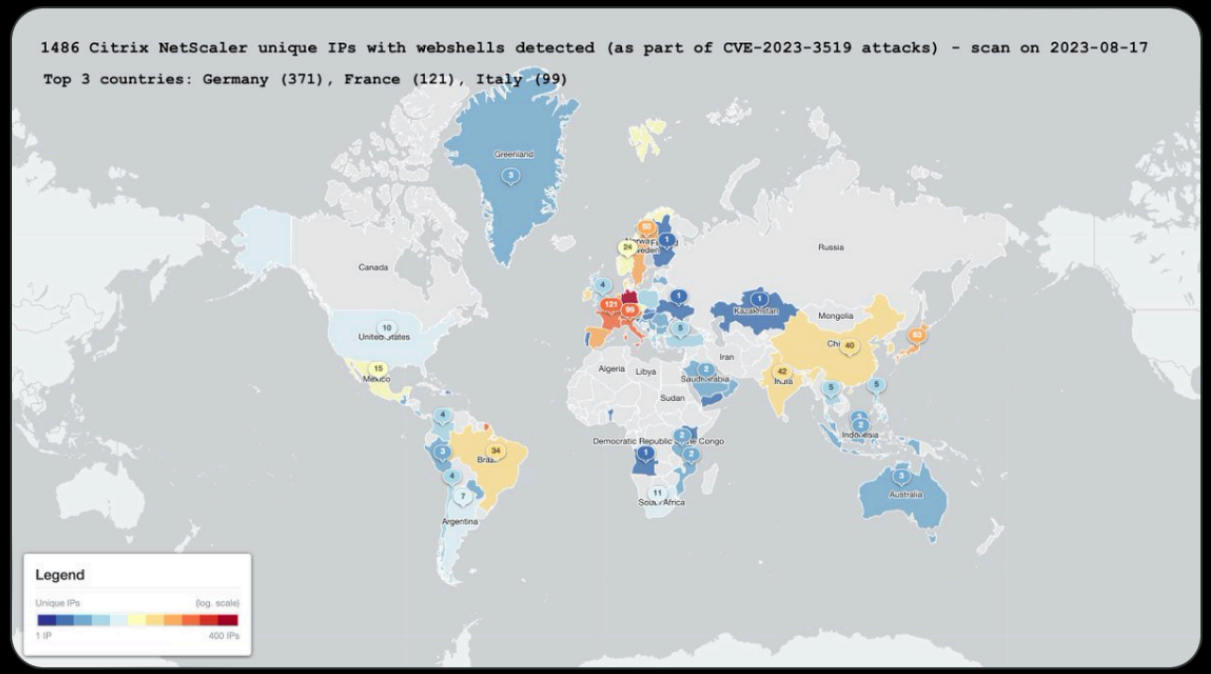
n compromised instances

shared Aug 4th

The Shadowserver Foundation
@Shadowserver

We continue to report out daily lists of Citrix ADC/Gateway IPs that are known to be compromised with webshells installed (CVE-2023-3519 attacks). We now see 1486 instances on 2023-08-17. Big thank you to @DIVDnl & @foxit for the collaboration.

Data in shadowserver.org/what-we-do/net...



8:12 PM · Aug 18, 2023 · **7,436** Views

View post engagements

1 22 42 7

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

July 24th: First Exploitation attempts observed by honeypots - CVE-2024-3519 tagging added by Shadowserver

July 26th: First CVE-2024-3519 tagged exploitation attempts

July 27th: Trusted partner reaches out to us that they found China Chopper webshells installed on compromised instances

July 28th: First full scan for webshells conducted based on developed methodology: 691 found

Aug 7th: We publish a technical blog in collaboration with trusted partners. TLP:AMBER version shared Aug 4th

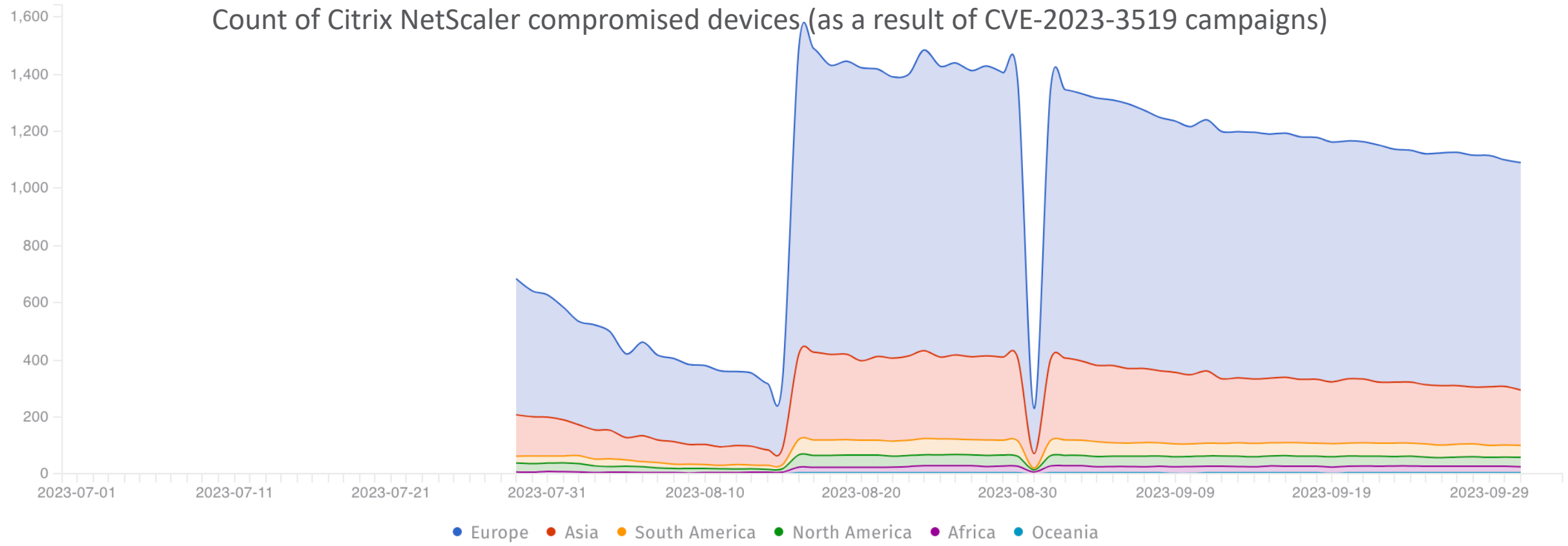
Aug 13th: Mandiant update their blogs/tooling to include Shadowserver contribution

Aug 18th: Share further reports on compromised devices based on Fox-IT/DIVD NL collaboration

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519



SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

July 24th: First Exploitation attempts observed by honeypots - CVE-2024-3519 tagging added by Shadowserver

July 26th: First CVE-2024-3519 tagged exploitation attempts

July 27th: Trusted partner reaches out to us that they found China Chopper webshells installed on compromised instances

July 28th: First full scan for webshells conducted based on developed methodology: 691 found

Aug 7th: We publish a technical blog in collaboration with trusted partners. TLP:AMBER version shared Aug 4th

Aug 13th: Mandiant update their blogs/tooling to include Shadowserver contribution

Aug 18th: Share further reports on compromised devices based on Fox-IT/DIVD NL collaboration

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519

July 24th: CVE-2024-3519 PoC published by AssetNote

July 24th: First Exploitation attempts observed by honeypots - CVE-2024-3519 tagging added by Shadowserver

July 26th: First CVE-2024-3519 tagged exploitation attempts

July 27th: Trusted partner reaches out to us that they found China Chopper webshells installed on compromised instances

July 28th: First full scan for webshells conducted based on developed methodology: 691 found

Aug 7th: We publish a technical blog in collaboration with trusted partners. TLP:AMBER version shared Aug 4th

Aug 13th: Mandiant update their blogs/tooling to include Shadowserver contribution

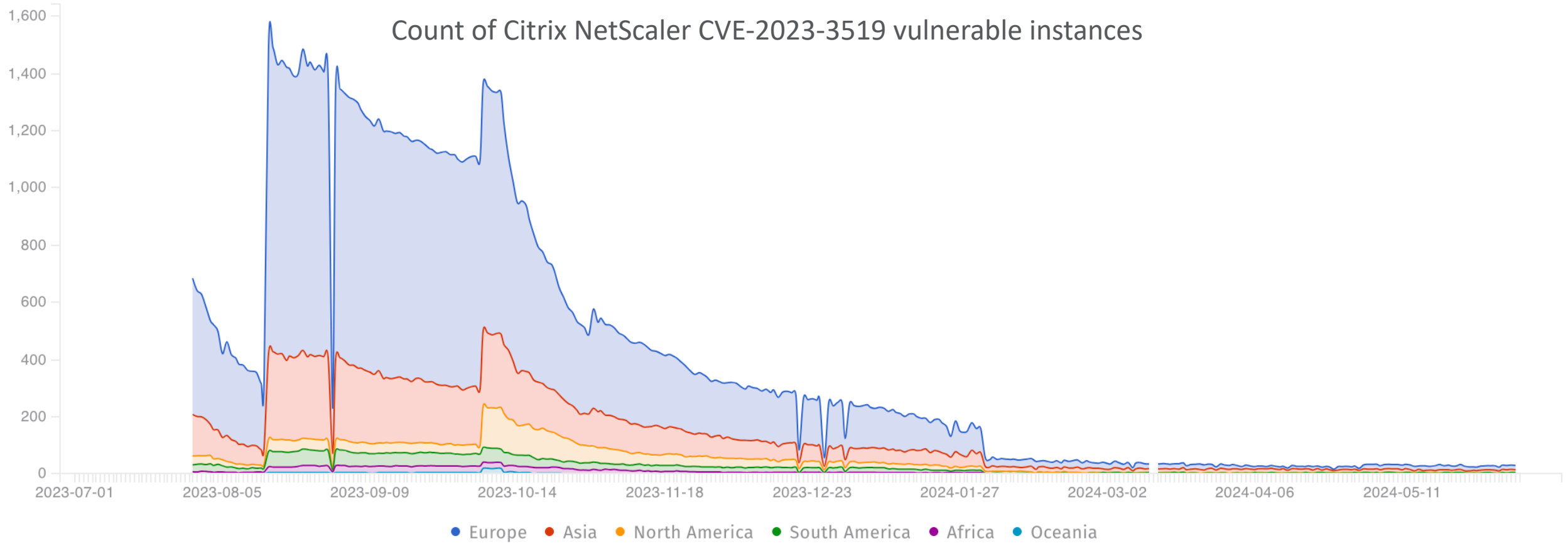
Aug 18th: Share further reports on compromised devices based on Fox-IT/DIVD NL collaboration

Sep 6th: CISA updates Citrix advisory based on input from partners, including Shadowserver (part of JCDC collaboration)

SHADOWSERVER

TLP CLEAR

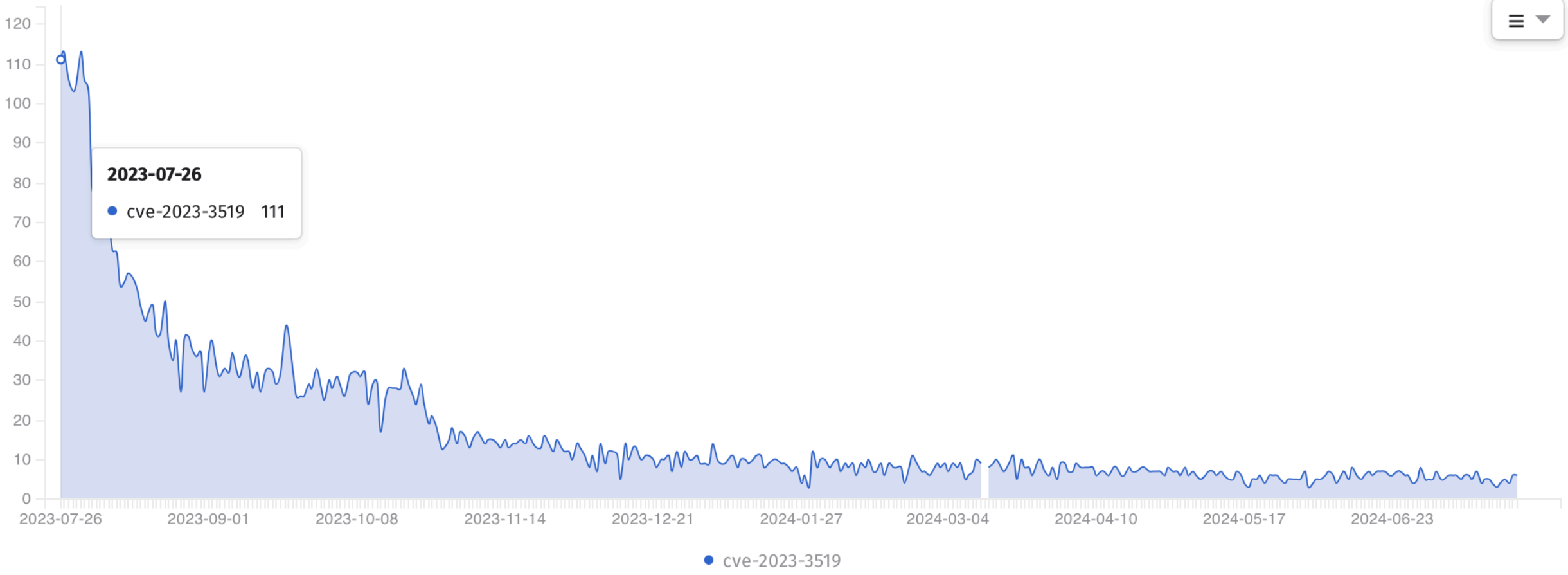
Citrix NetScaler: CVE-2023-3519



SHADOWSERVER

TLP CLEAR

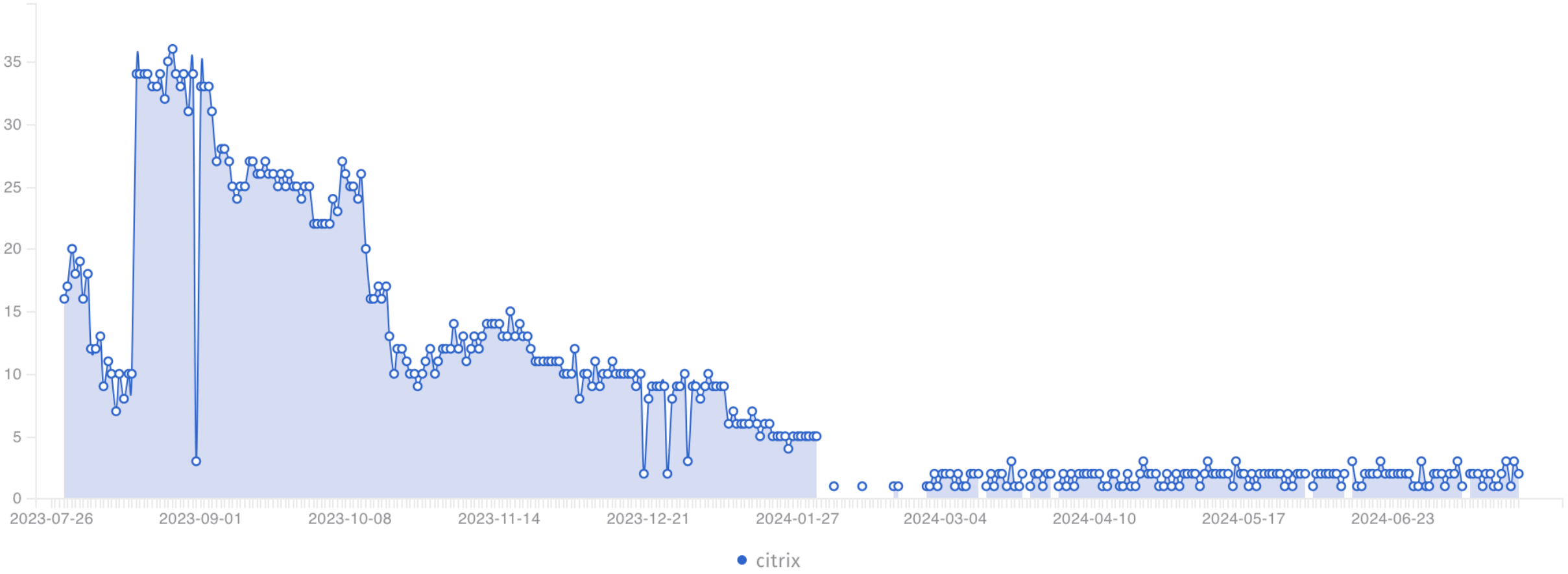
Citrix NetScaler CVE-2023-3519 Vulnerable - Brazil



SHADOWSERVER

TLP CLEAR

Citrix NetScaler CVE-2023-3519 Compromised - Brazil



SHADOWSERVER

Compromises

(Critical compromised assets tracked by Shadowserver)

Cisco IOS XE BadCandy

TLP CLEAR

Cisco IOS XE BadCandy

Oct 16th: Cisco Talos publication on active exploitation of Cisco IOS XE Web Interface vulnerabilities. Scan implemented

SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy

Oct 16th: Cisco Talos publicati plemented

Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerabilities

By Cisco Talos

MONDAY, OCTOBER 16, 2023 11:05

THREAT ADVISORY

Updates

Nov. 02: Identified a third version of the BadCandy implant. Added expected response from the new version of the implant against one of the HTTP requests used to check for infected device.

Nov. 1: Observed increase in exploitation attempts since the publication of the proofs-of-concept (POCs) of the exploits involved. Named the Lua-based web shell "BadCandy."

Oct. 23: Identified an updated version of the implant. Provided new curl command to check for infected devices. Fixes for CVE-2023-20198 and CVE-2023-20273 started to roll out on Oct. 22.

Oct. 20: Identified an additional vulnerability (CVE-2023-20273) that is exploited to deploy the implant. Fixes for both CVE-2023-20198 and CVE-2023-20273 are estimated to be available on Oct. 22. The CVE-2021-1435 that had previously been mentioned is no longer assessed to be associated with this activity.

Oct. 19: Added additional attacker IP and username, defense evasion observations, and new Snort rules. Also added new information regarding our assessment that the activity is being carried out by the same actor.

SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy

Oct 16th: Cisco Talos publication on active exploitation of Cisco IOS XE Web Interface vulnerabilities. Scan implemented

SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy

Oct 16th: Cisco Talos publication on active exploitation of Cisco IOS XE Web Interface vulnerabilities. Scan implemented

Oct 17th: Shadowserver conducts first full daily scan for compromised devices

SHADOWSERVER

TLP CLEAR

Cisco IOS X

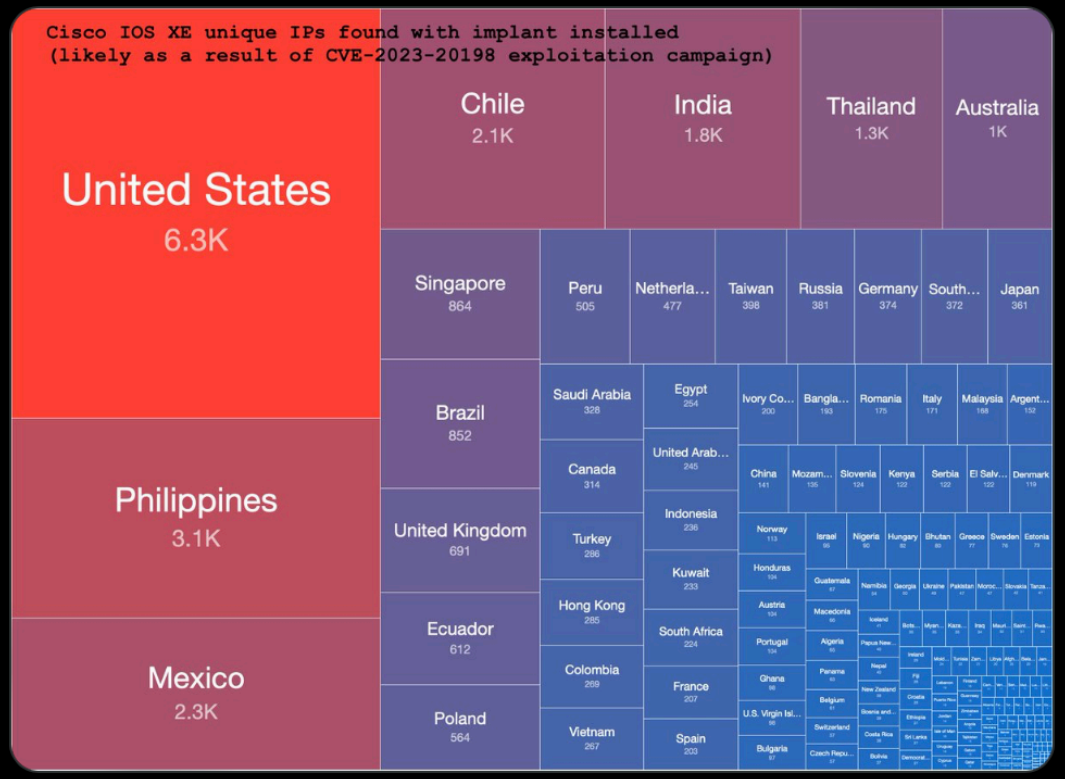
Oct 16th: Cisco Talos publicatio … ulnerabilities. Scan implemented

Oct 17th: Shadowserver condu

The Shadowserver Foundation
@Shadowserver

Cisco CVE-2023-20198 exploitation activity: We see over 32.8K Cisco IOS XE IPs compromised with implants based on the check published by Cisco in blog.talosintelligence.com/active-exploit...

IP data on implants shared out daily in: shadowserver.org/what-we-do/net... tagged 'device-implant'.



5:27 AM · Oct 18, 2023 · **91.1K** Views

View post engagements

3 121 175 48

SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy

Oct 16th: Cisco Talos publication on active exploitation of Cisco IOS XE Web Interface vulnerabilities. Scan implemented

Oct 17th: Shadowserver conducts first full daily scan for compromised devices

SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy

Oct 16th: Cisco Talos publication on active exploitation of Cisco IOS XE Web Interface vulnerabilities. Scan implemented

Oct 17th: Shadowserver conducts first full daily scan for compromised devices

Oct 19th: Shadowserver rolls out honeypot profile

SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy

Oct 16th: Cisco Talos publication on active exploitation of Cisco IOS XE Web Interface vulnerabilities. Scan implemented

Oct 17th: Shadowserver conducts first full daily scan for compromised devices

Oct 19th: Shadowserver rolls out honeypot profile

Oct 19th: First implant scans immediately detected after rollout

SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy

Oct 16th: Cisco Talos publication on active exploitation of Cisco IOS XE Web Interface vulnerabilities. Scan implemented

Oct 17th: Shadowserver conducts first full daily scan for compromised devices

Oct 19th: Shadowserver rolls out honeypot profile

Oct 19th: First implant scans immediately detected after rollout

Oct 22nd: Implant updated by attackers

SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy

Oct 16th: Cisco Talos publication on active exploitation of Cisco IOS XE Web Interface vulnerabilities. Scan implemented

Oct 17th: Shadowserver conducts first full daily scan for compromised devices

Oct 19th: Shadowserver rolls out honeypot profile

Oct 19th: First implant scans immediately detected after rollout

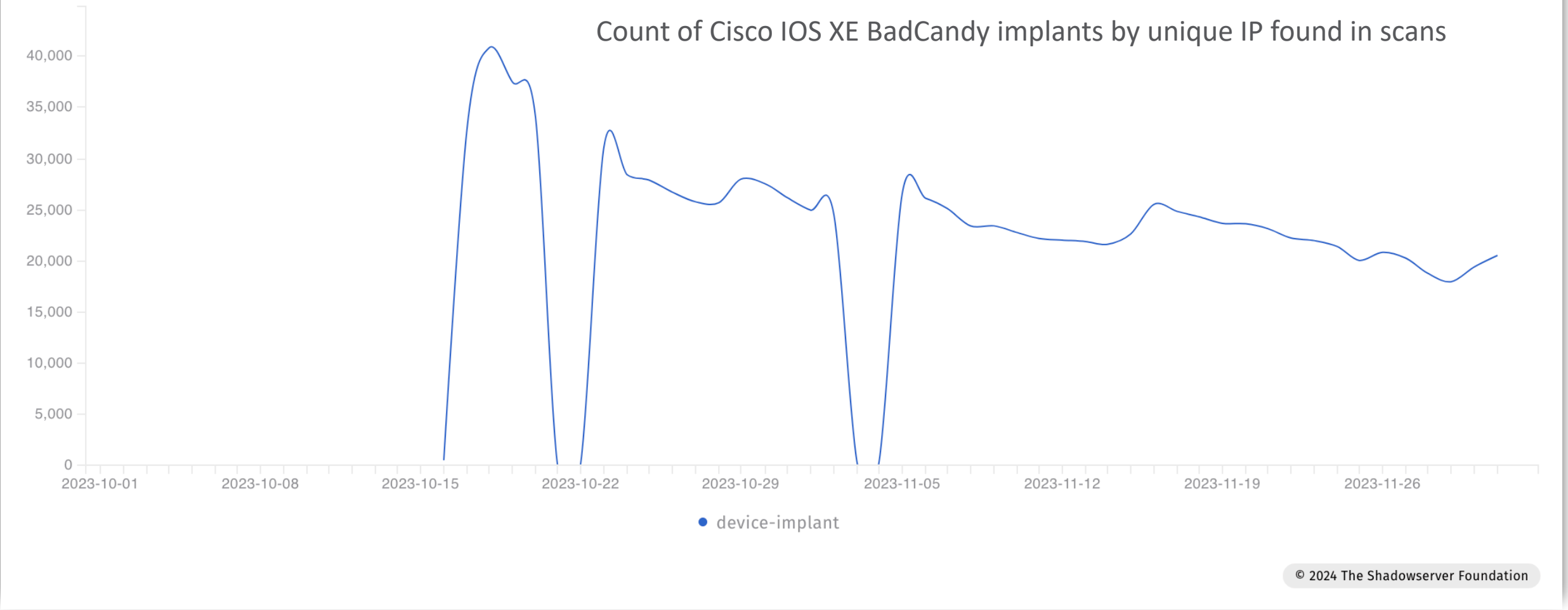
Oct 22nd: Implant updated by attackers

Oct 23rd: Cisco updates advisory with new implant details. Shadowserver scans updated

SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy



SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy

Oct 16th: Cisco Talos publication on active exploitation of Cisco IOS XE Web Interface vulnerabilities. Scan implemented

Oct 17th: Shadowserver conducts first full daily scan for compromised devices

Oct 19th: Shadowserver rolls out honeypot profile

Oct 19th: First implant scans immediately detected after rollout

Oct 22nd: Implant updated by attackers

Oct 23rd: Cisco updates advisory with new implant details. Shadowserver scans updated

SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy

Oct 16th: Cisco Talos publication on active exploitation of Cisco IOS XE Web Interface vulnerabilities. Scan implemented

Oct 17th: Shadowserver conducts first full daily scan for compromised devices

Oct 19th: Shadowserver rolls out honeypot profile

Oct 19th: First implant scans immediately detected after rollout

Oct 22nd: Implant updated by attackers

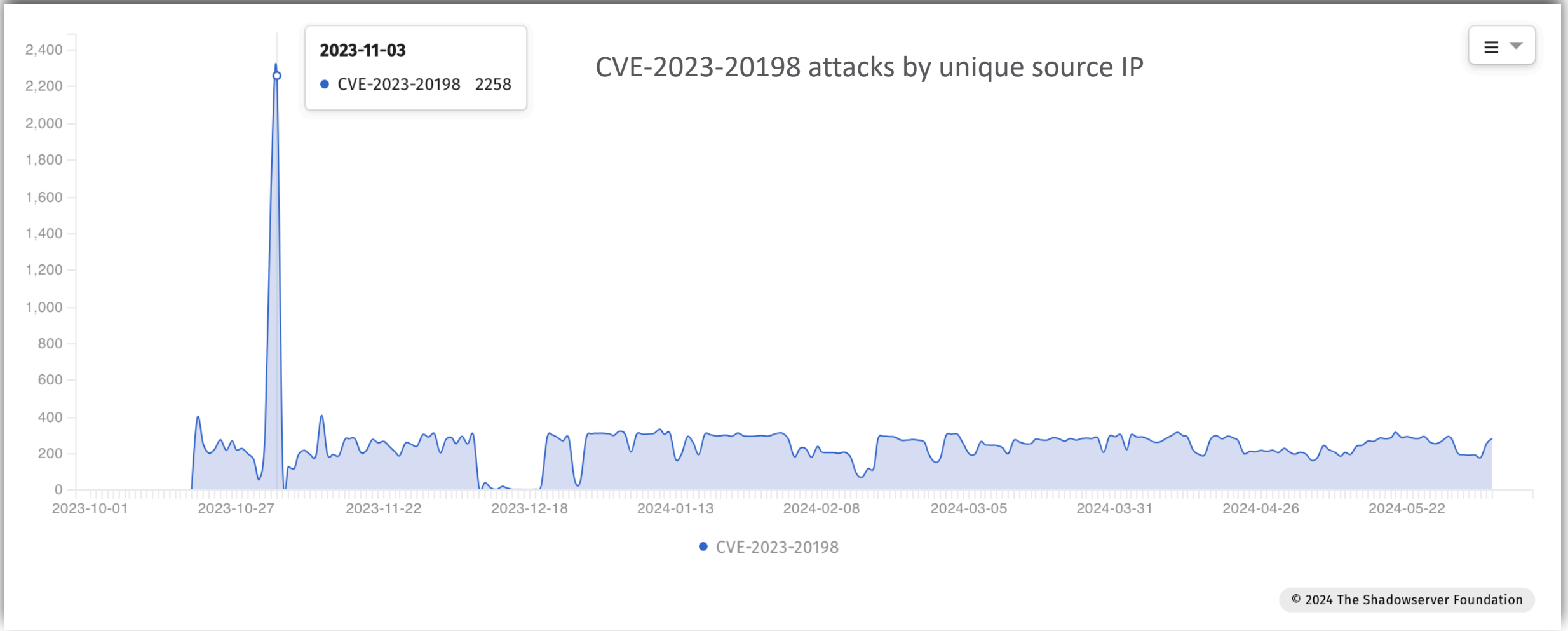
Oct 23rd: Cisco updates advisory with new implant details. Shadowserver scans updated

Oct 30th/31st:PoC exploit code published for CVE-2023-20198 and CVE-2023-20273

SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy



SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy

Oct 16th: Cisco Talos publication on active exploitation of Cisco IOS XE Web Interface vulnerabilities. Scan implemented

Oct 17th: Shadowserver conducts first full daily scan for compromised devices

Oct 19th: Shadowserver rolls out honeypot profile

Oct 19th: First implant scans immediately detected after rollout

Oct 22nd: Implant updated by attackers

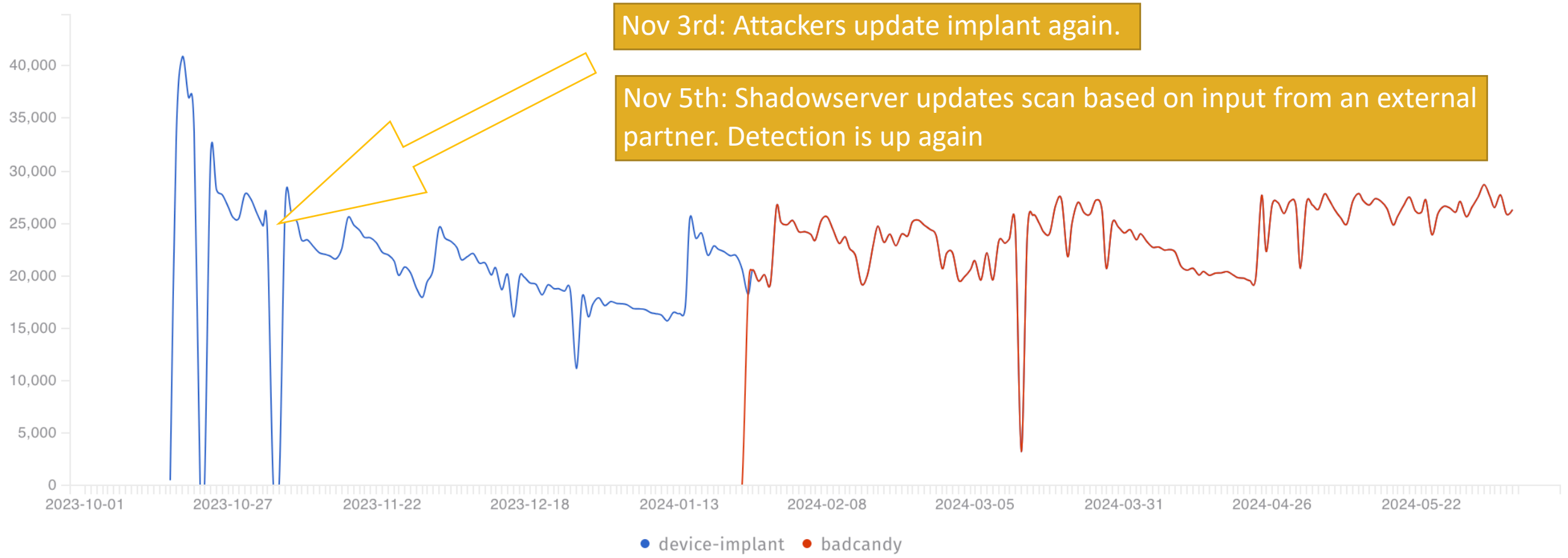
Oct 23rd: Cisco updates advisory with new implant details. Shadowserver scans updated

Oct 30th/31st:PoC exploit code published for CVE-2023-20198 and CVE-2023-20273

SHADOWSERVER

TLP CLEAR

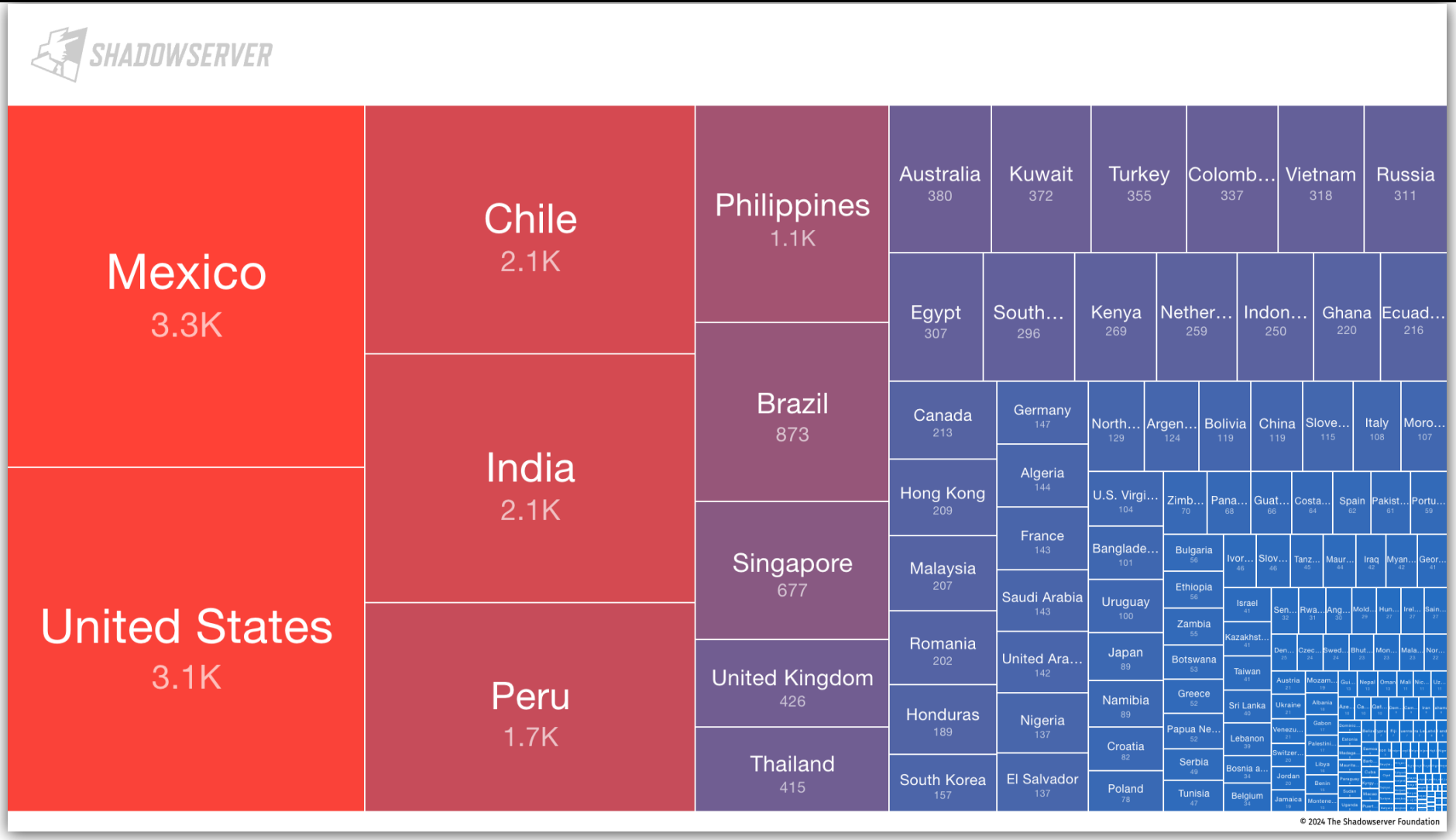
Cisco IOS XE BadCandy



SHADOWSERVER

TLP CLEAR

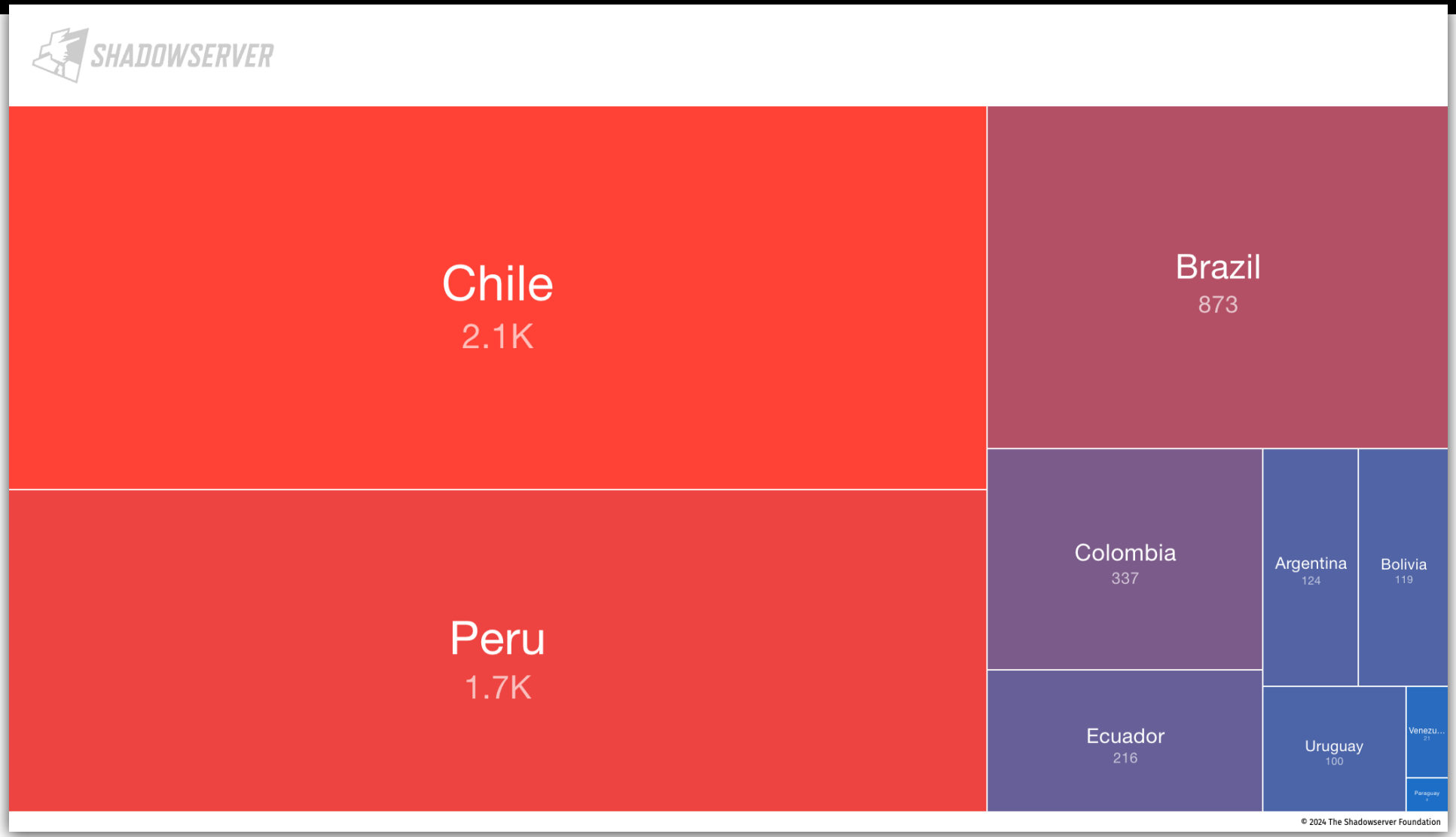
Cisco IOS XE BadCandy - World (2024-07-24)



SHADOWSERVER

TLP CLEAR

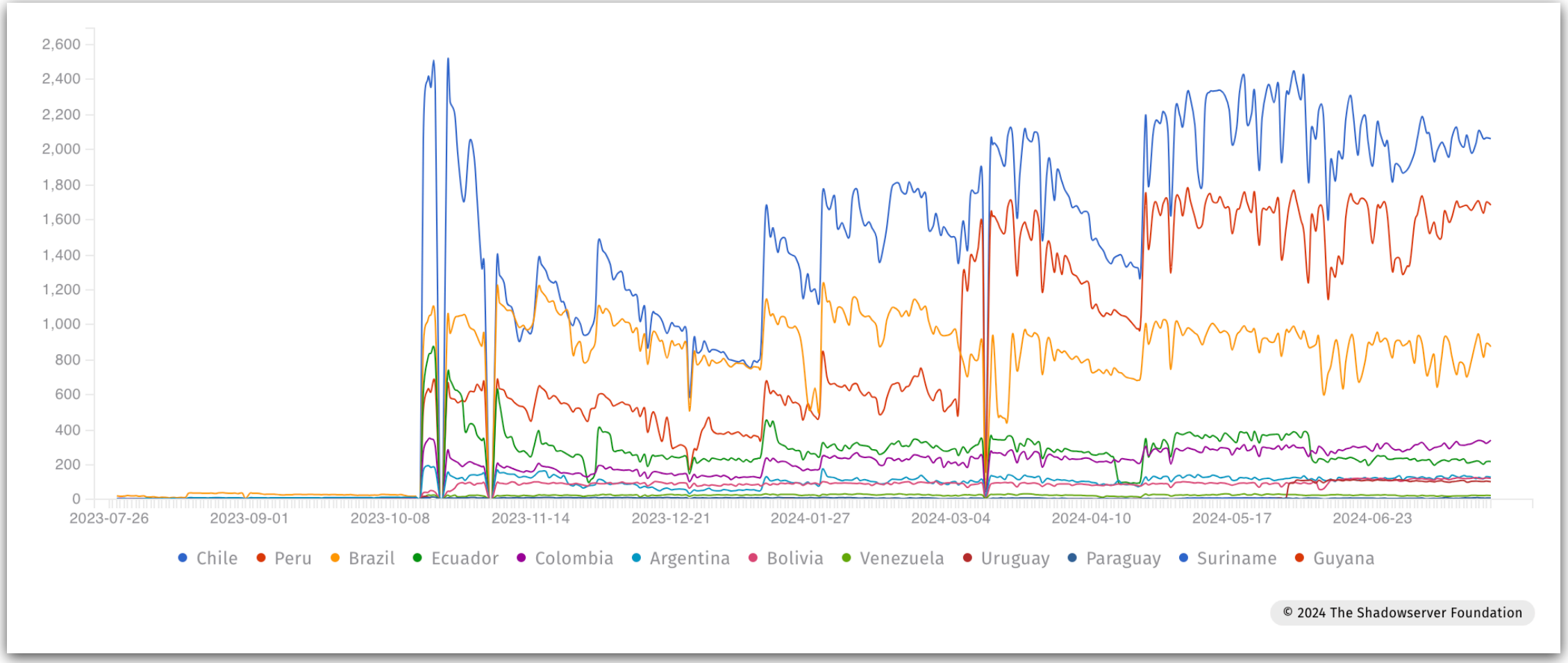
Cisco IOS XE BadCandy - South America (2024-07-24)



SHADOWSERVER

TLP CLEAR

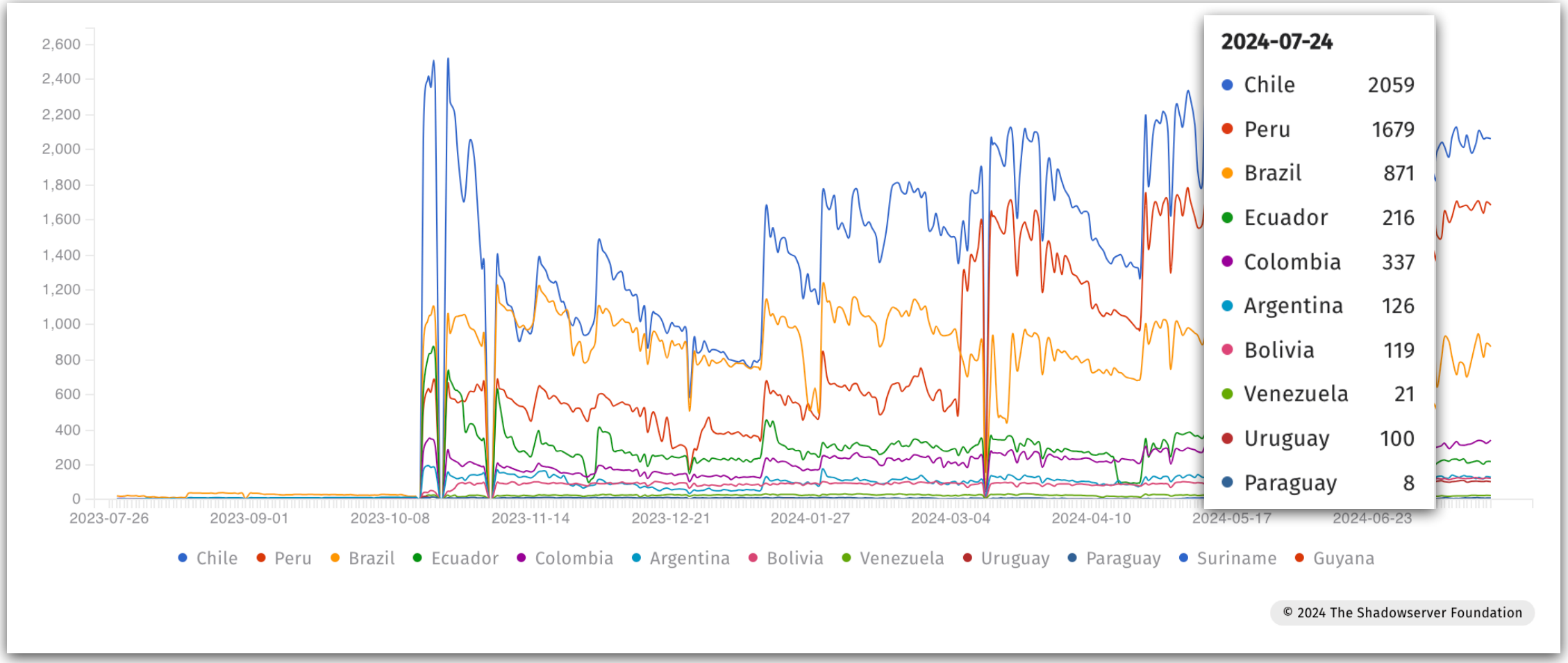
Compromised Devices (Citrix, Ivanti, Cisco IOS XE …) - South America



SHADOWSERVER

TLP CLEAR

Compromised Devices (Citrix, Ivanti, Cisco IOS XE …) - South America



SHADOWSERVER

TLP CLEAR

Compromised Devices (Citrix, Ivanti, Cisco IOS XE …) - Brazil

SHADOWSERVER

Malware sinkholes

Infected System Observations

TLP CLEAR

Qakbot Botnet Disruption (2023-08-24)

An official website of the United States government. Here's how you know

MORE > NEWS > STORIES

FBI

Search FBI

NEWS

Stories | News Blog | Videos | Podcasts | Press Releases | Speeches | Testimony | Photos | Apps

August 29, 2023

Twitter Facebook Email

FBI, Partners Dismantle Qakbot Infrastructure in Multinational Cyber Takedown

Operation marks one of the largest-ever U.S.-led enforcement actions against a botnet

SHADOWSERVER

Src: FBI, DoJ

TLP CLEAR

Qakbot Botnet Disruption (2023-08-24)

An official website of the United States government. Here's how you know

MORE > NEWS > STORIES

FBI

NEWS

Stories | News Blog | Videos | Podcasts | Press Releases | Speeches | Testimony | Photos | Apps

August 29, 2023

Twitter

FBI, Partners Dismantle Qakbot Infrastructure in Mu
Cyber Takedown

Operation marks one of the largest-ever U.S.-led enforcement acti

Qakbot Malware Disrupted in International Cyber Takedown

Tuesday, August 29, 2023

Share

For Immediate Release

U.S. Attorney's Office, Central District of California

Qakbot Malware Infected More Than 700,000 Victim Computers, Facilitated Ransomware Deployments, and Caused Hundreds of Millions of Dollars in Damage

LOS ANGELES – The Justice Department today announced a multinational operation involving actions in the United States, France, Germany, the Netherlands, the United Kingdom, Romania, and Latvia to disrupt the botnet and malware known as Qakbot and take down its infrastructure.

The Qakbot malicious code is being deleted from victim computers, preventing it from doing any more harm. The Department also announced the seizure of more than $8.6 million in cryptocurrency in illicit profits.

The action represents the largest U.S.-led financial and technical disruption of a botnet infrastructure leveraged by cybercriminals to commit ransomware, financial fraud, and other cyber-enabled criminal activity.

"Cybercriminals who rely on malware like Qakbot to steal private data from innocent victims have been reminded today that they do not operate outside the bounds of the law," said Attorney General Merrick B. Garland. "Together with our international partners, the Justice Department has hacked Qakbot's infrastructure, launched an aggressive campaign to uninstall the malware from victim computers in the United States and around the world, and seized $8.6 million in extorted funds."

TOP

SHADOWSERVER

Src: FBI, DoJ

TLP CLEAR

Qakbot Botnet Disruption (2023-08-24)

An official website of the United States government. Here's how you know

MORE > NEWS > STORIES

FBI

NEWS

Stories News Blog

August 29, 2023

FBI, Partne
Cyber Take
Operation ma

FBI Director Ch

Home > News & Insights > Qakbot Botnet Disruption

Qakbot Botnet Disruption

AUGUST 29, 2023

On Tuesday 29th August 2023, the **US Department of Justice (DoJ)** and **US Federal Bureau of Investigations (FBI)** – along with law enforcement partners in France, Germany, **the Netherlands**, and the **United Kingdom** – announced a disruption action against the very long running **Qakbot** botnet.

Qakbot (also known as QBot, Pinkslipbot, Quakbot and Oakbot) has been active since around 2007, having initially been developed as information stealer and banking trojan malware, before later becoming primarily a distribution network for other malware/ransomware. See **Malpedia's timeline** for more information about its lengthy evolution, and **CISA's advisory** for Indicators of Compromise (IOCs) and mitigation information.

In recent years, Qakbot has been used as an initial infection vector by many ransomware groups including Conti, ProLock, Egregor, REvil, MegaCortex, and Black Basta. This has likely enabled significant financial losses globally.

Recent Articles

Qakbot Historical Bot Infections Special Report

SEPTEMBER 8, 2023

On Tuesday 29th August 2023, the US DoJ and FBI, together with other global law enforcement partners, announced a disruption... **Read more »**

Technical Summary of Observed Citrix CVE-2023-3519 Incidents

AUGUST 7, 2023

The Shadowserver Foundation and trusted partners have observed three different malicious campaigns that have exploited... **Read more »**

Qakbot Malware Disrupted in International Cyber

ral District of California

Ransomware

ons in the United States, France,
lware known as Qakbot and take

more harm. The Department also

ture leveraged by

been reminded today that they
r with our international partner
uninstall the malware from
nds."

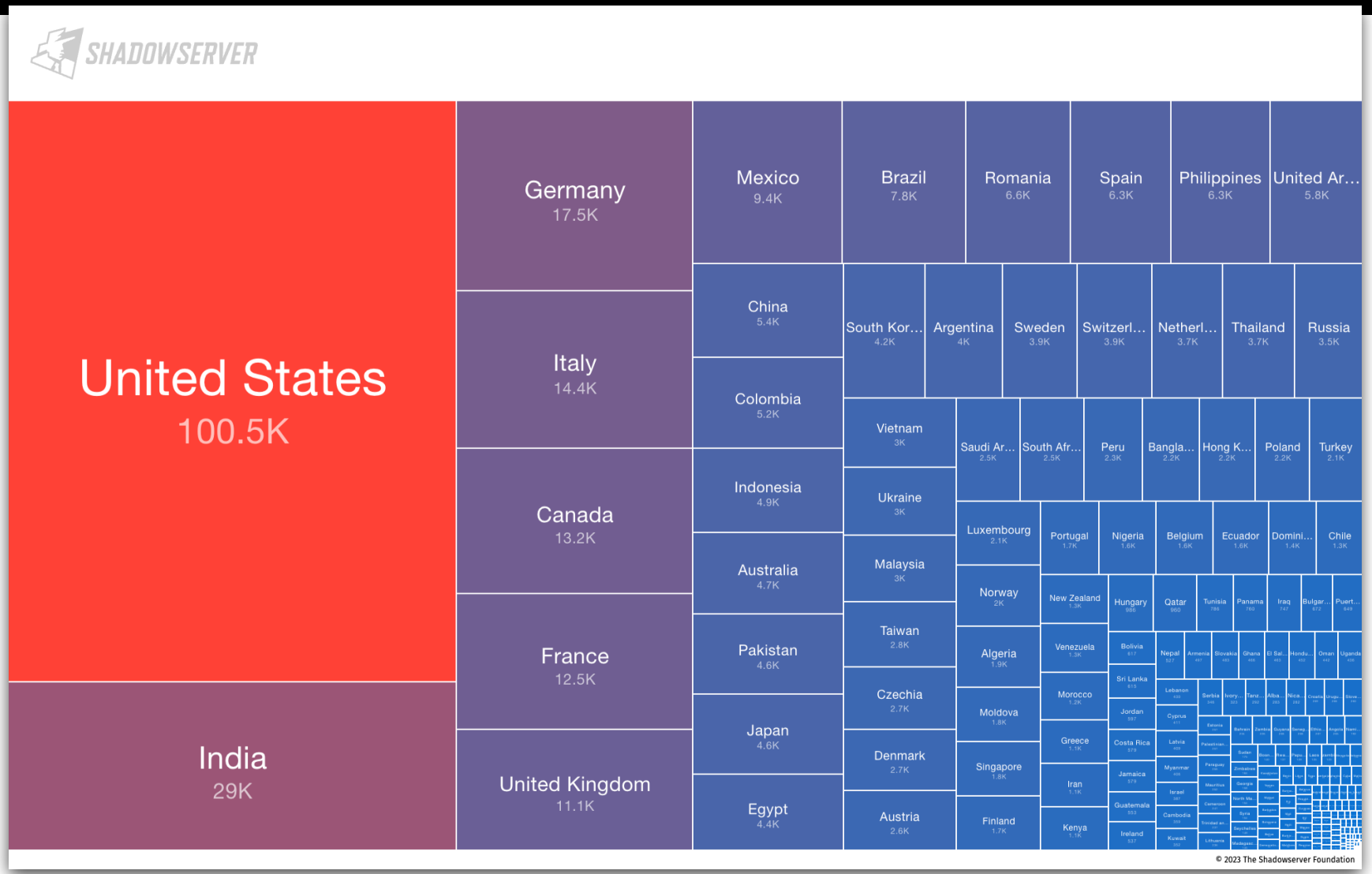
TOP

SHADOWSERVER

Src: FBI, DoJ

TLP CLEAR

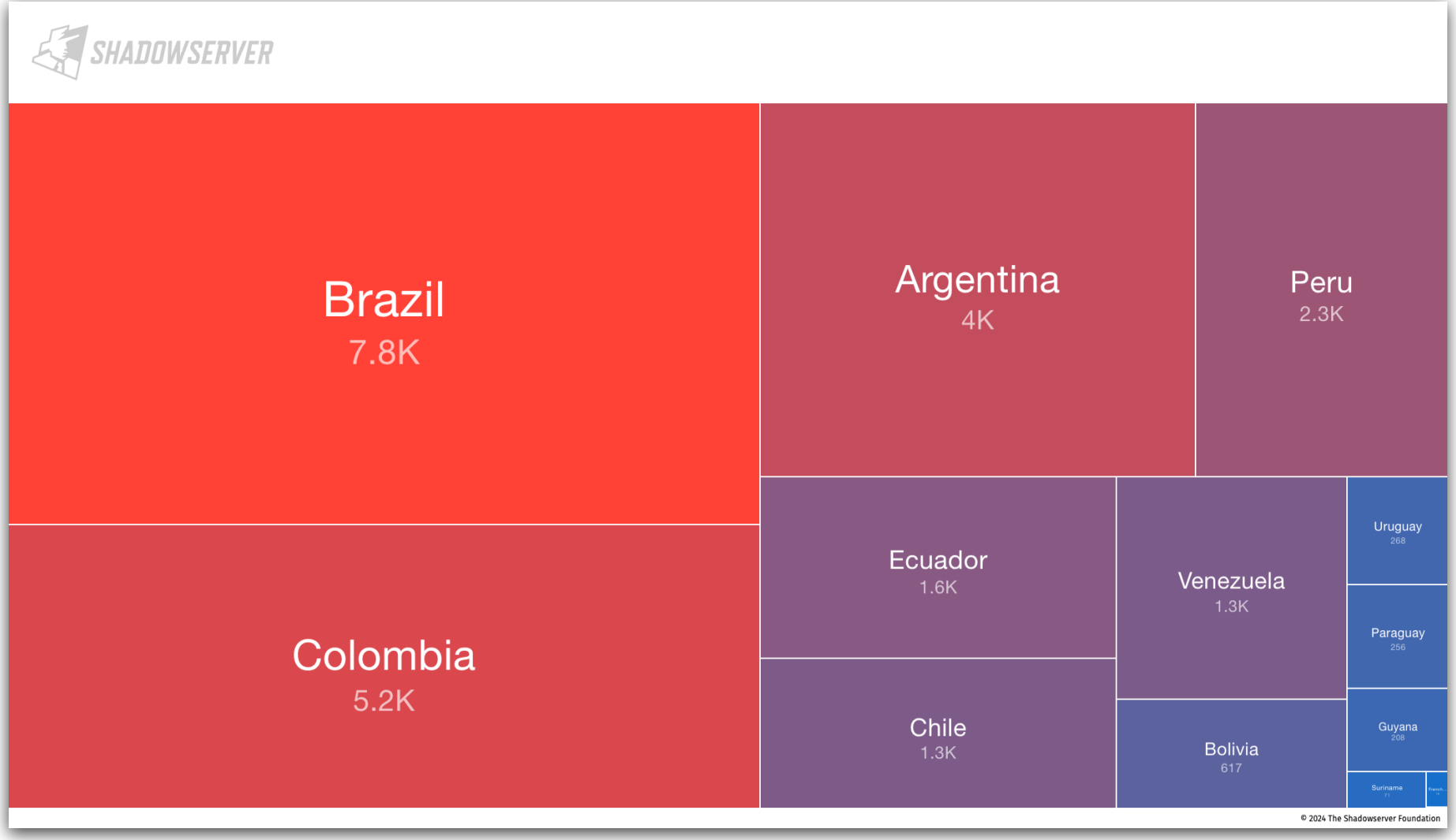
Qakbot Botnet Disruption, World (2023-08-24)



SHADOWSERVER

TLP CLEAR

Qakbot Botnet Disruption, South America (2023-08-24)



SHADOWSERVER

TLP CLEAR

Moobot Disruption

Office of Public Affairs
U.S. Department of Justice

Our Offices | Find Help | Contact Us

Search

About | News | Documents | Internships | FOIA | Contact | Information for Journalists

Justice.gov > Office of Public Affairs > News > Press Releases > Justice Department Conducts Court-Authorized Disruption of Botnet Controlled By The Russian Federation's Main Intelligence Directorate of The General Staff (GRU)

News

- All News
- Blogs
- Photo Galleries
- Podcasts
- Press Releases
- Speeches
- Videos

PRESS RELEASE

Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU)

Thursday, February 15, 2024

Share

For Immediate Release
Office of Public Affairs

Note: *Following the publication of this press release, the FBI and international partners issued a joint multinational cybersecurity advisory on Russian cyber actors' use of compromised routers to*

Home > News > Security > FBI disrupts Russian Moobot botnet infecting Ubiquiti routers

FBI disrupts Russian Moobot botnet infecting Ubiquiti routers

By Sergiu Gatlan | February 15, 2024 | 01:00 PM | 3

The FBI took down a botnet of small office/home office (SOHO) routers used by Russia's Main Intelligence Directorate of the General Staff (GRU) to proxy malicious traffic and to target the United States and its allies in spearphishing and credential theft attacks.

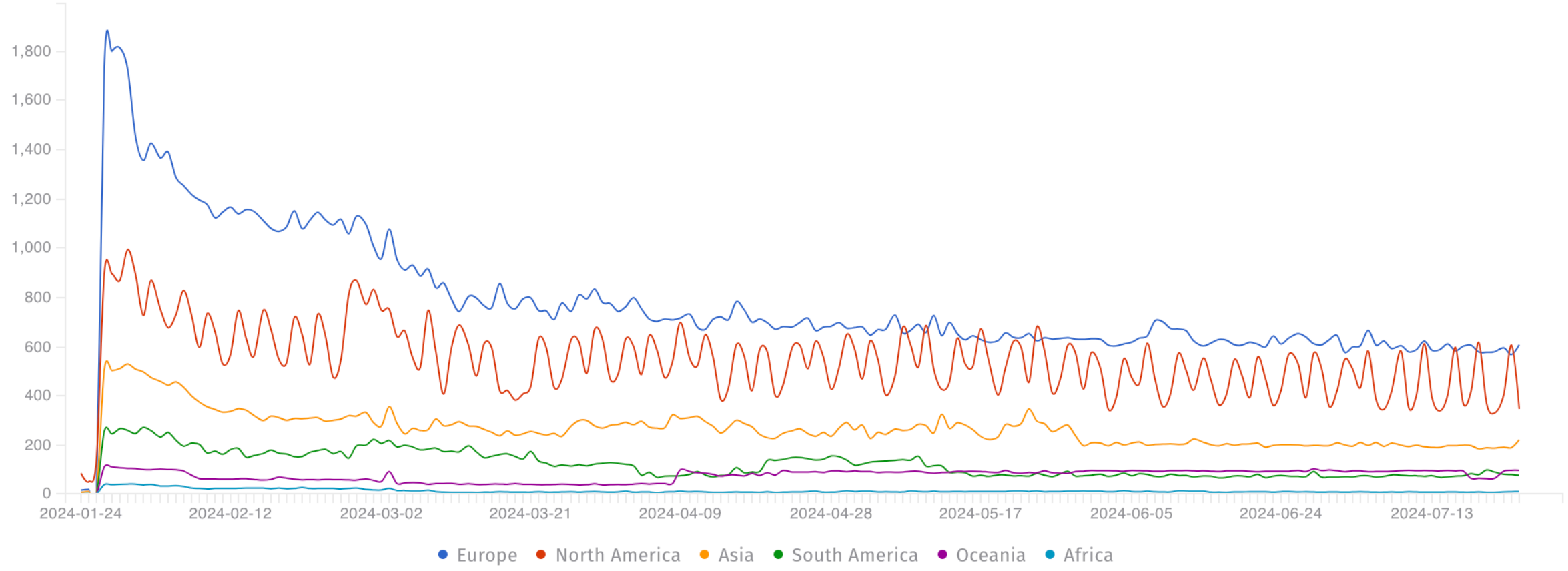
This network of hundreds of Ubiquiti Edge OS routers infected with Moobot malware was controlled by GRU Military Unit 26165, also tracked as APT28, Fancy Bear, and Sednit.

The Russian hackers' targets include U.S. and foreign governments, military entities, and security and corporate organizations.

SHADOWSERVER

TLP CLEAR

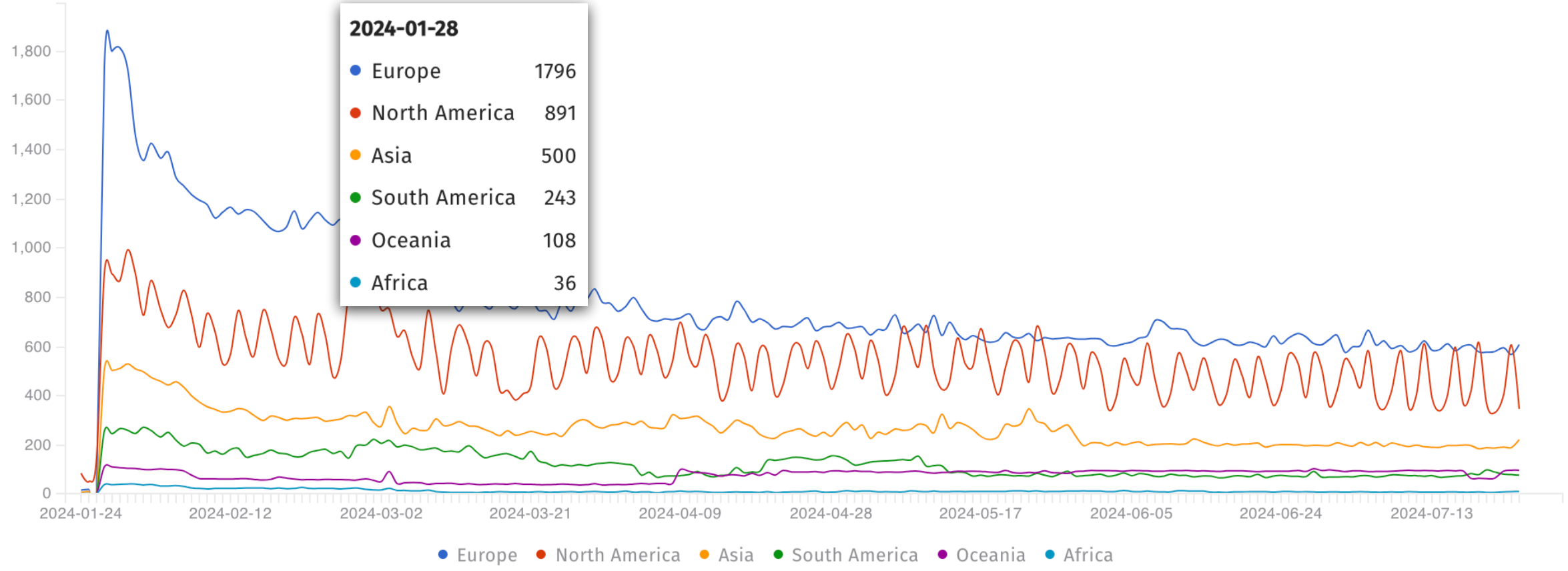
Moobot Disruption



SHADOWSERVER

TLP CLEAR

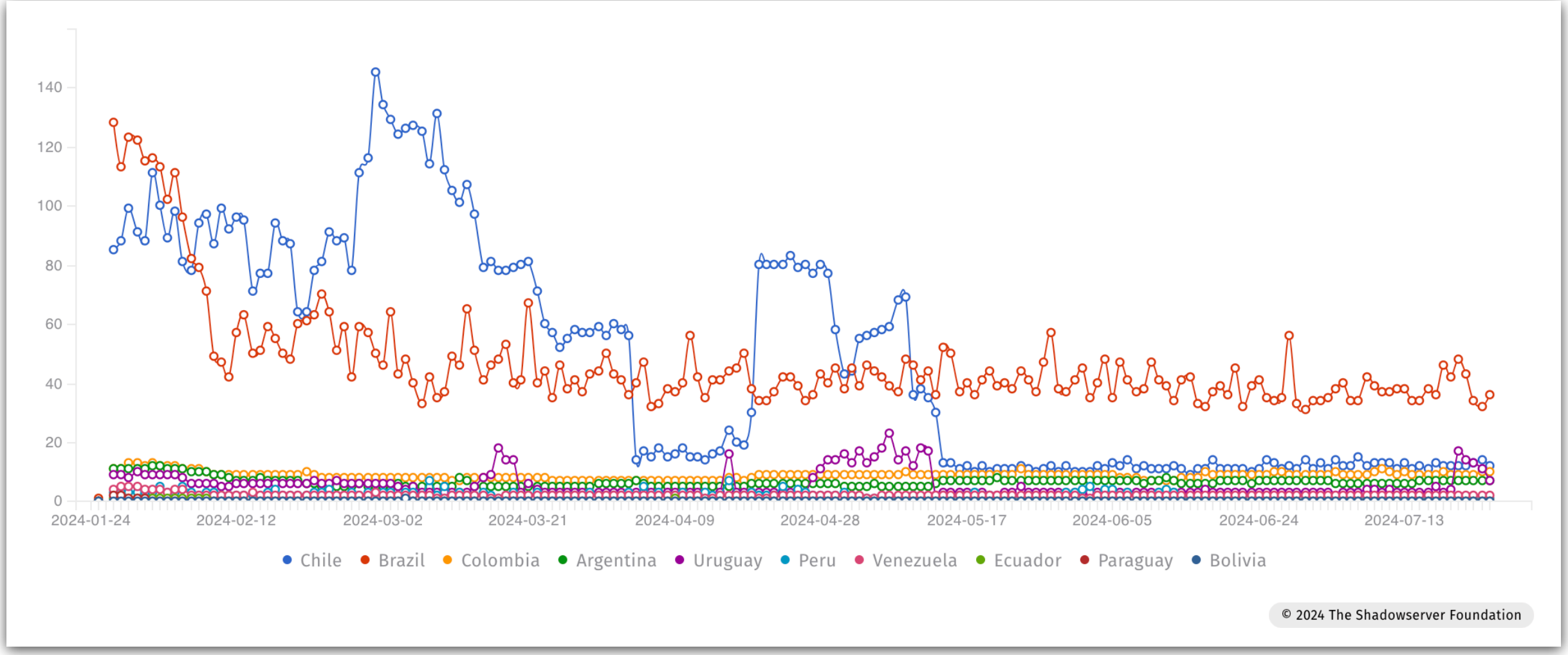
Moobot Disruption



SHADOWSERVER

TLP CLEAR

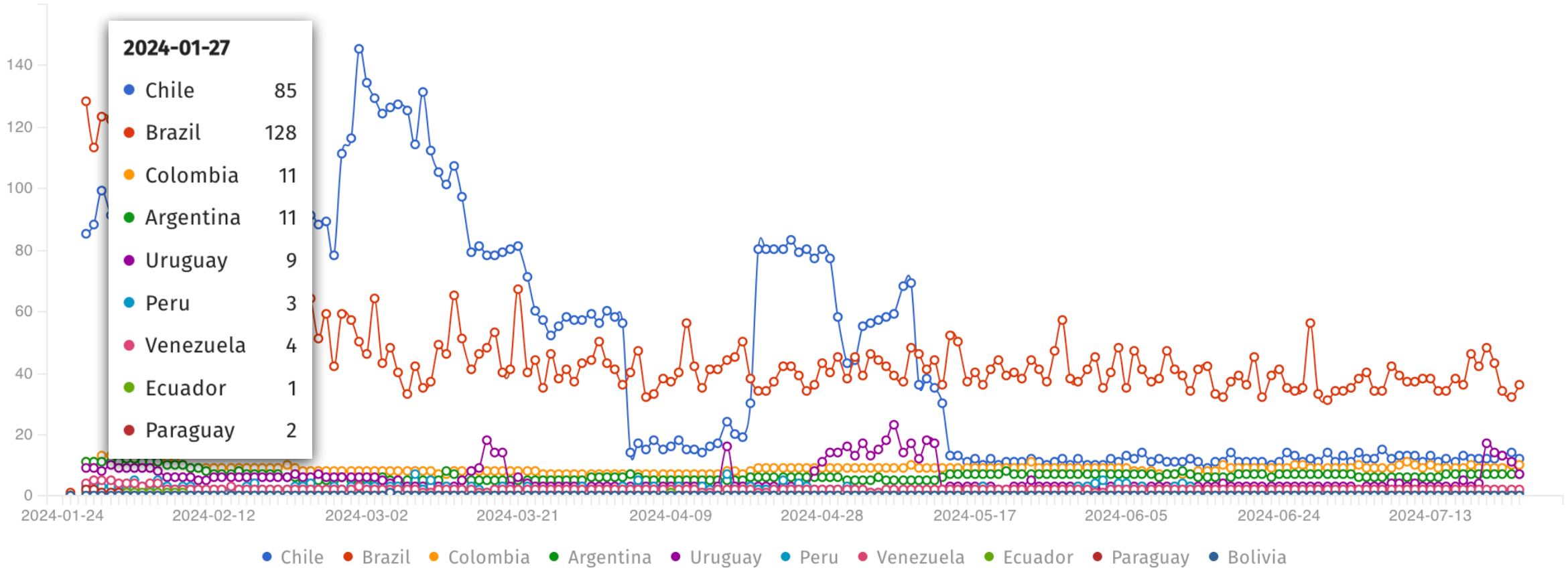
Moobot Disruption



SHADOWSERVER

TLP CLEAR

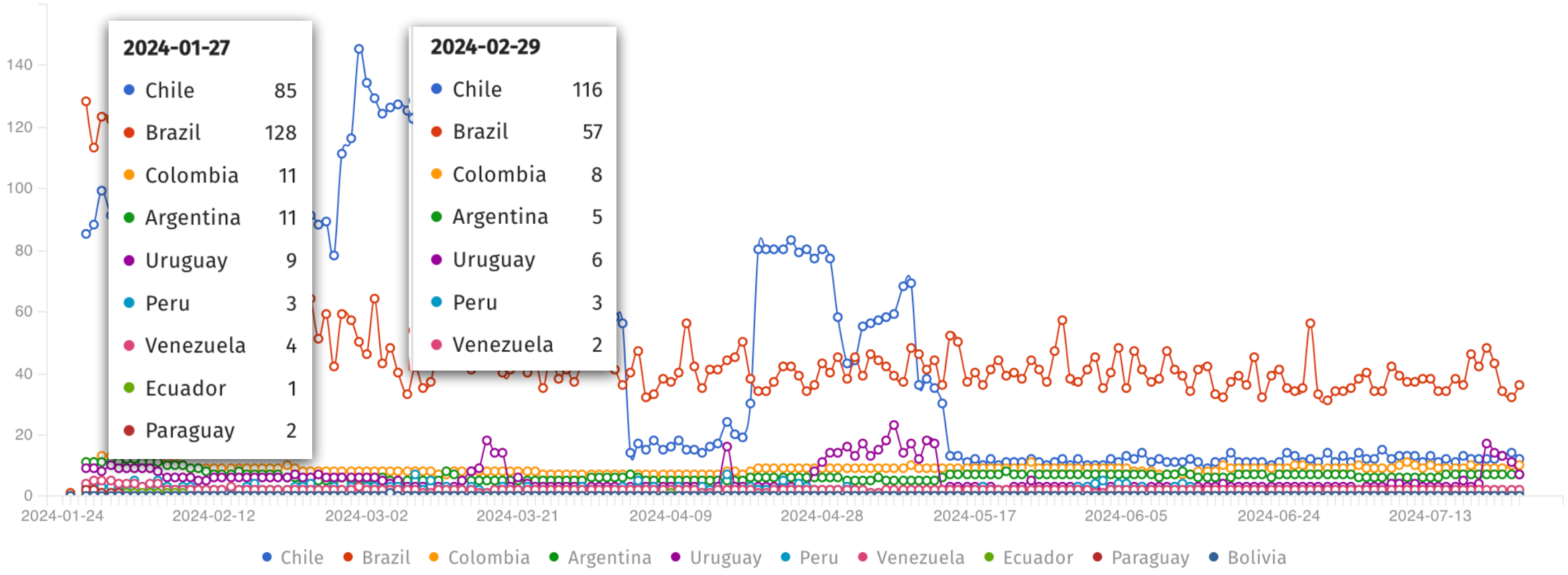
Moobot Disruption



SHADOWSERVER

TLP CLEAR

Moobot Disruption



SHADOWSERVER

TLP CLEAR

911 Socks 5 Proxy Botnet Takedown

Office of Public Affairs
U.S. Department of Justice

Our Offices | Find Help | Contact Us

Search

About | News | Documents | Internships | FOIA | Contact | Information for Journalists

Justice.gov > Office of Public Affairs > News > Press Releases > 911 S5 Botnet Dismantled and Its Administrator Arrested In Coordinated International Operation

News

- All News
- Blogs
- Photo Galleries
- Podcasts
- Press Releases
- Speeches
- Videos

PRESS RELEASE

911 S5 Botnet Dismantled and Its Administrator Arrested in Coordinated International Operation

Wednesday, May 29, 2024

Share

For Immediate Release

Office of Public Affairs

Botnet Infected Over 19M IP Addresses to Enable Billions of Dollars in Pandemic and Unemployment Fraud, and Access to Child Exploitation Materials

of the United States government. Here's how you know

WHAT WE INVESTIGATE > CYBER CRIME

FBI

Search

What We Investigate

Terrorism | Counterintelligence | Cyber Crime | Public Corruption | Civil Rights | Organized Crime | White-Collar Crime | Violent Crime | More

News | Most Wanted | FBI Guidance to Victims of Cyber Incidents on SEC Reporting Requirements | Business and Industry Partners

How to Identify and Remove VPN Applications That Contain 911 S5 Back Doors

The FBI, the Defense Criminal Investigative Service, and the Department of Commerce's Office of Export Enforcement have published a public service announcement (the "PSA") for individuals and businesses to better understand and guard against the 911 S5 residential proxy service and botnet. The PSA is available at ic3.gov/Media/Y2024/PSA240529.

As explained in the PSA, 911 S5 began operating in May 2014 and was taken offline by the administrator in July 2022 before reconstituting as Cloudrouter in October 2023. 911 S5 was likely the largest residential proxy service and botnet with over 19 million compromised IP addresses in over 190 countries and confirmed victim losses in the billions of dollars.

Free, illegitimate VPN applications that were created to connect to the 911 S5 service are: MaskVPN, DewVPN, PaladinVPN, ProxyGate, ShieldVPN, and ShineVPN.

Unaware of the proxy backdoor, once users downloaded these VPN applications, they unknowingly became a victim of the 911 S5 botnet. The proxy backdoor enabled 911 S5 users to re-route their devices through victims' devices, allowing criminals to carry out crimes such as bomb threats, financial fraud, identity theft, child exploitation, and initial access brokering. By using a proxy backdoor, criminals made nefarious activity appear as though it was coming from the victims' devices.

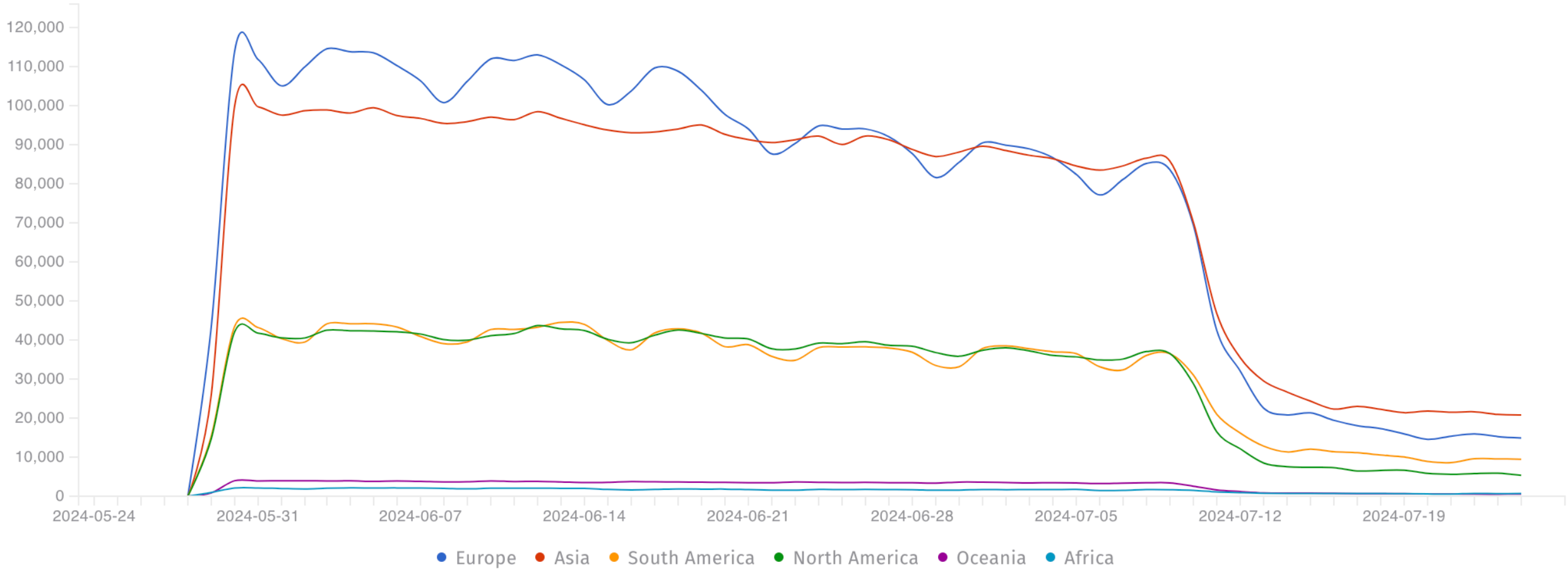
The below information is intended to help identify and remove 911 S5's VPN applications from devices or machines.

Before electing to use this information, users may want to consult with legal counsel and cybersecurity professionals, potentially including an incident response firm if they deem necessary, to explore all options and assist with any remediation efforts to avoid further harm by malicious software applications or botnets. The FBI makes no warranties or representations regarding the efficacy of this information.

SHADOWSERVER

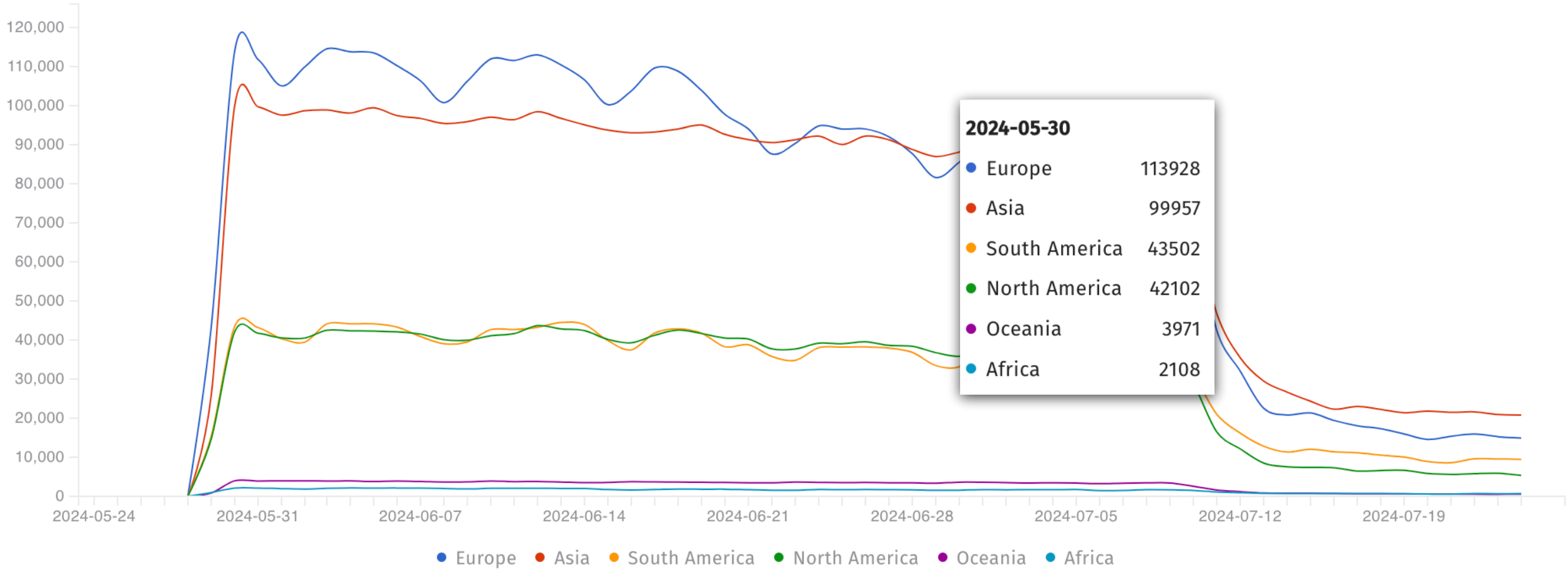
TLP CLEAR

911 Socks 5 Proxy Botnet Takedown



TLP CLEAR

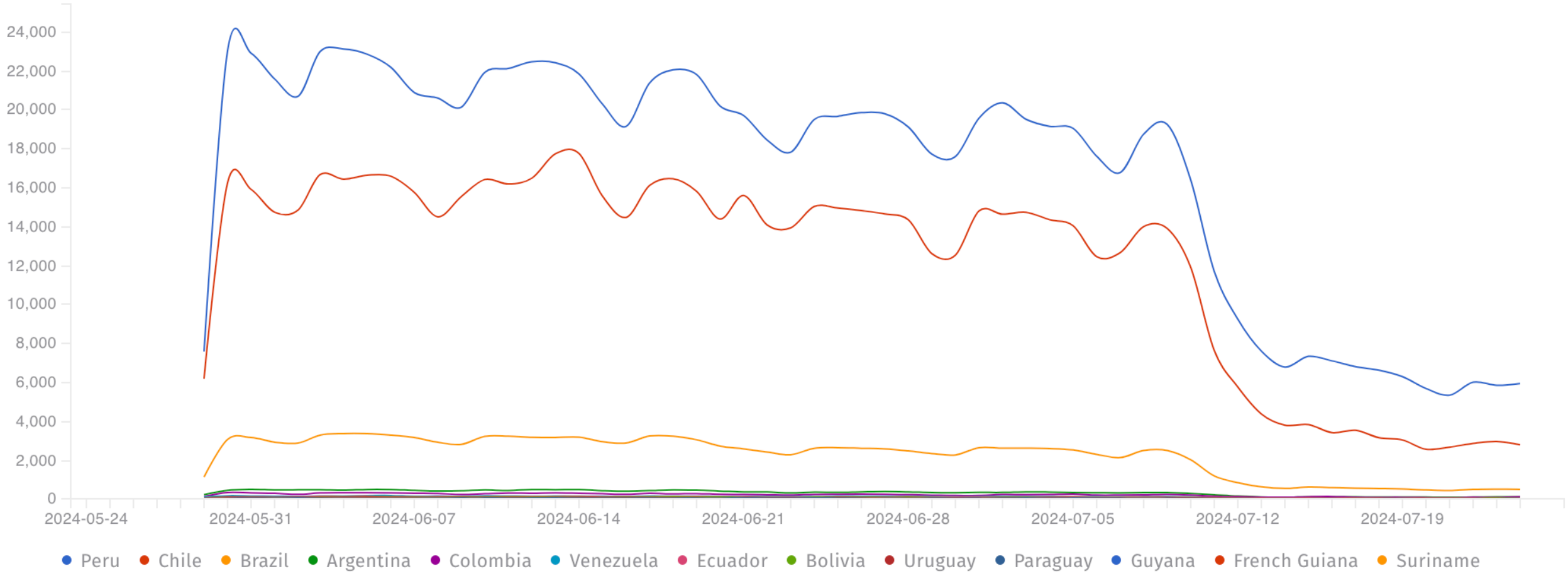
911 Socks 5 Proxy Botnet Takedown



SHADOWSERVER

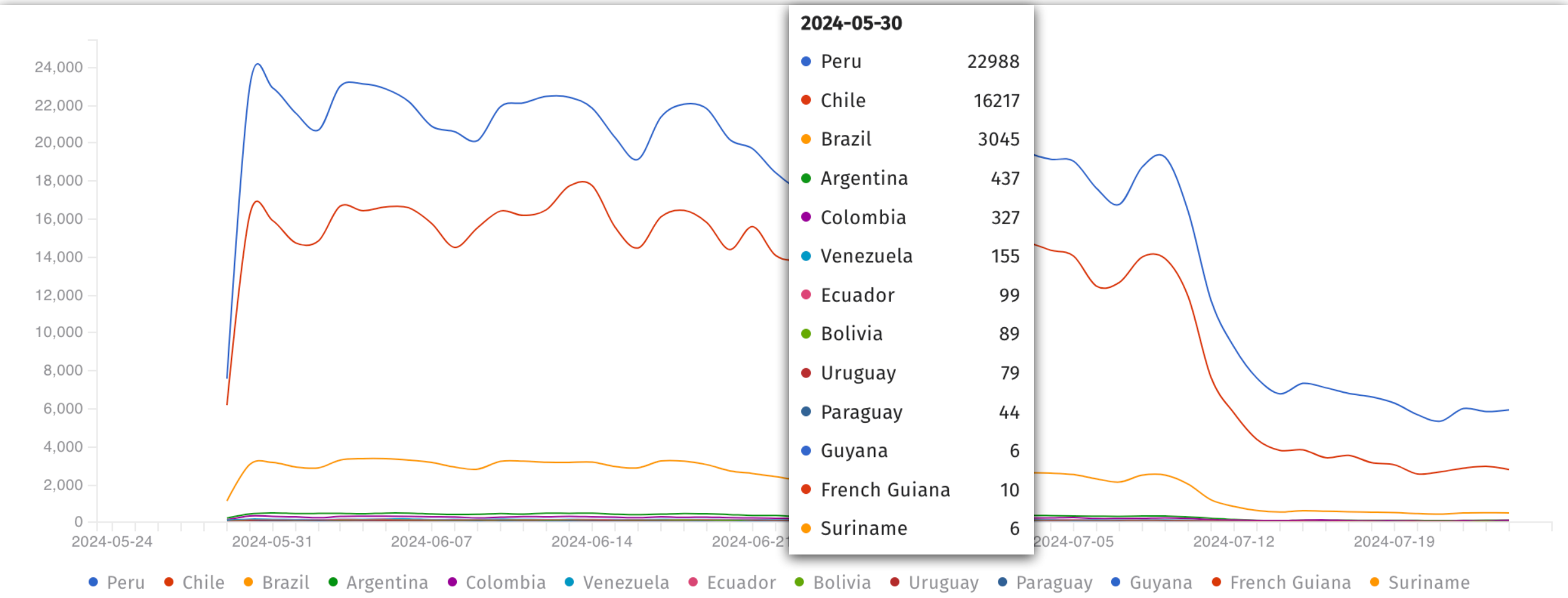
TLP CLEAR

911 Socks 5 Proxy Botnet Takedown



TLP CLEAR

911 Socks 5 Proxy Botnet Takedown



2024-05-30	
Peru	22988
Chile	16217
Brazil	3045
Argentina	437
Colombia	327
Venezuela	155
Ecuador	99
Bolivia	89
Uruguay	79
Paraguay	44
Guyana	6
French Guiana	10
Suriname	6

TLP CLEAR

Operation Endgame

Largest ever operation against botnets hits dropper malware ecosystem

International operation shut down droppers including IcedID, SystemBC, Pikabot, Smokeloader and Bumblebee leading to four arrests and takedown of over 100 servers worldwide

Part of the EMPACT Cycle

Between 27 and 29 May 2024 Operation Endgame, coordinated from Europol's headquarters, targeted droppers including, IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee and Trickbot. The actions focused on disrupting criminal services through arresting High Value Targets, taking down the criminal infrastructures and freezing illegal proceeds. This approach had a global impact on the dropper ecosystem. The malware, whose infrastructure was taken down during the action days, facilitated attacks with ransomware and other malicious software. Following the action days, eight fugitives linked to these criminal activities, wanted by Germany, will be added to Europe's Most Wanted list on 30 May 2024. The individuals are wanted for their involvement in serious cybercrime activities.

This is the largest ever operation against botnets, which play a major role in the deployment of ransomware. The operation, initiated and led by France, Germany and the Netherlands was also supported by Eurojust and involved Denmark, the United Kingdom and the United States. In addition, Armenia, Bulgaria, Lithuania, Portugal, Romania, Switzerland and Ukraine also supported the operation with different actions, such as arrests, interviewing suspects, searches, and seizures or takedowns of servers and domains. The operation was also supported by a number of private partners at national and international level including Bitdefender, Cryptolaemus, Sekoia, Shadowserver, Team Cymru, Prodaft, Proofpoint, NFIR, Computest, Northwave, Fox-IT, HaveIBeenPwned, Spamhaus, DIVD, abuse.ch and Zscaler.

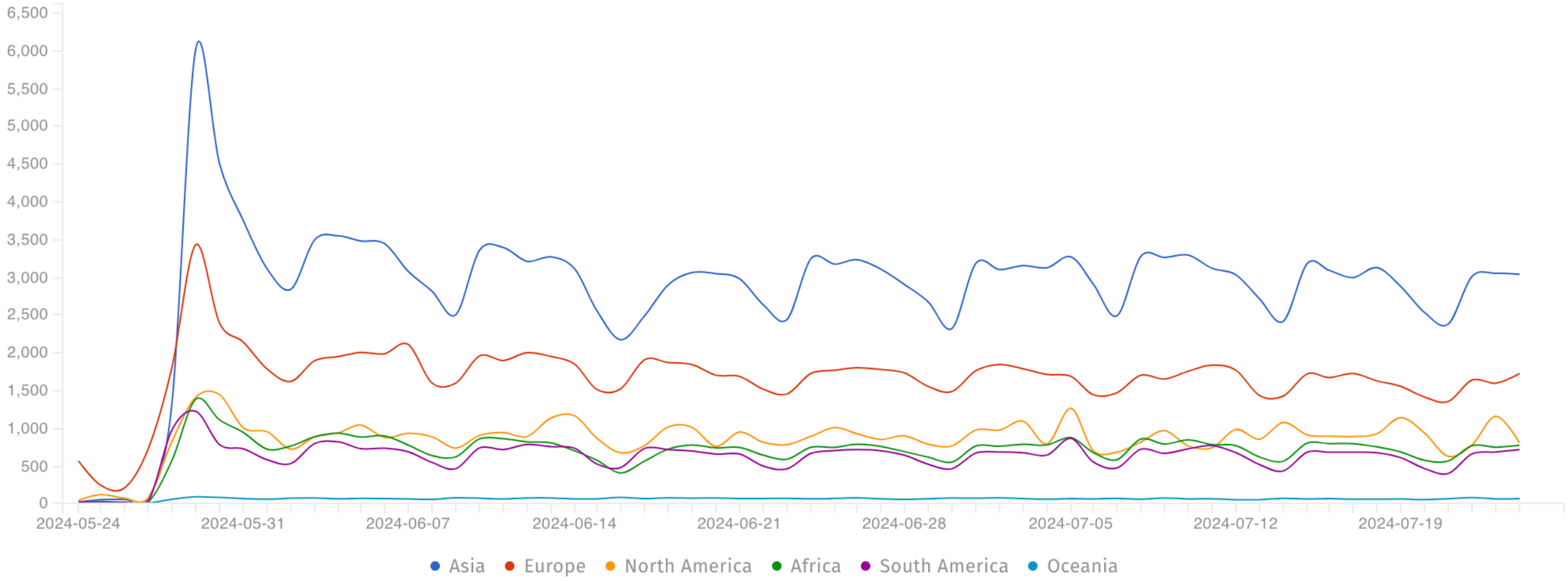
The coordinated actions led to:

- 4 arrests (1 in Armenia and 3 in Ukraine)
- 16 location searches (1 in Armenia, 1 in the Netherlands, 3 in Portugal and 11 in Ukraine)
- Over 100 servers taken down or disrupted in Bulgaria, Canada, Germany, Lithuania, the Netherlands, Romania, Switzerland, the United Kingdom, the United States and Ukraine
- Over 2 000 domains under the control of law enforcement

Furthermore, it has been discovered through the investigations so far that one of the main suspects has earned at least EUR 69 million in cryptocurrency by renting out criminal infrastructure sites to deploy ransomware. The suspect's transactions are constantly being monitored and legal permission to seize these assets upon future actions has already been obtained.

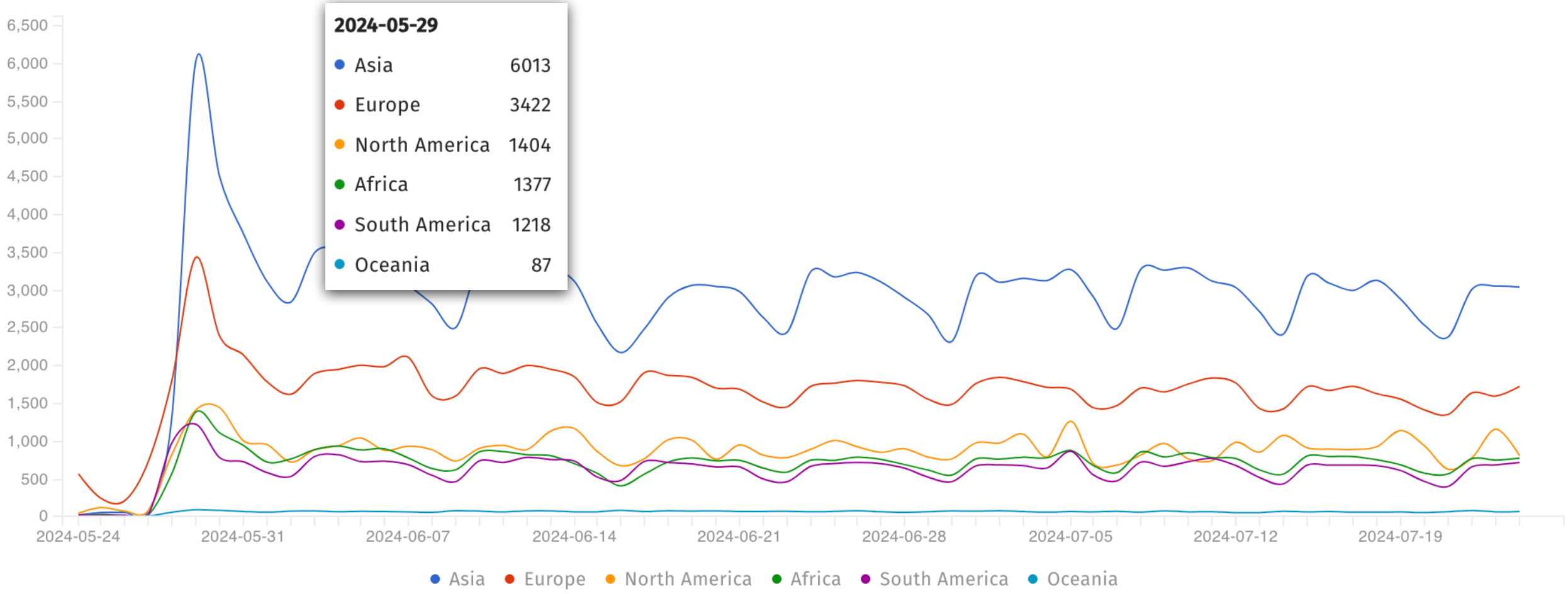
TLP CLEAR

Operation Endgame



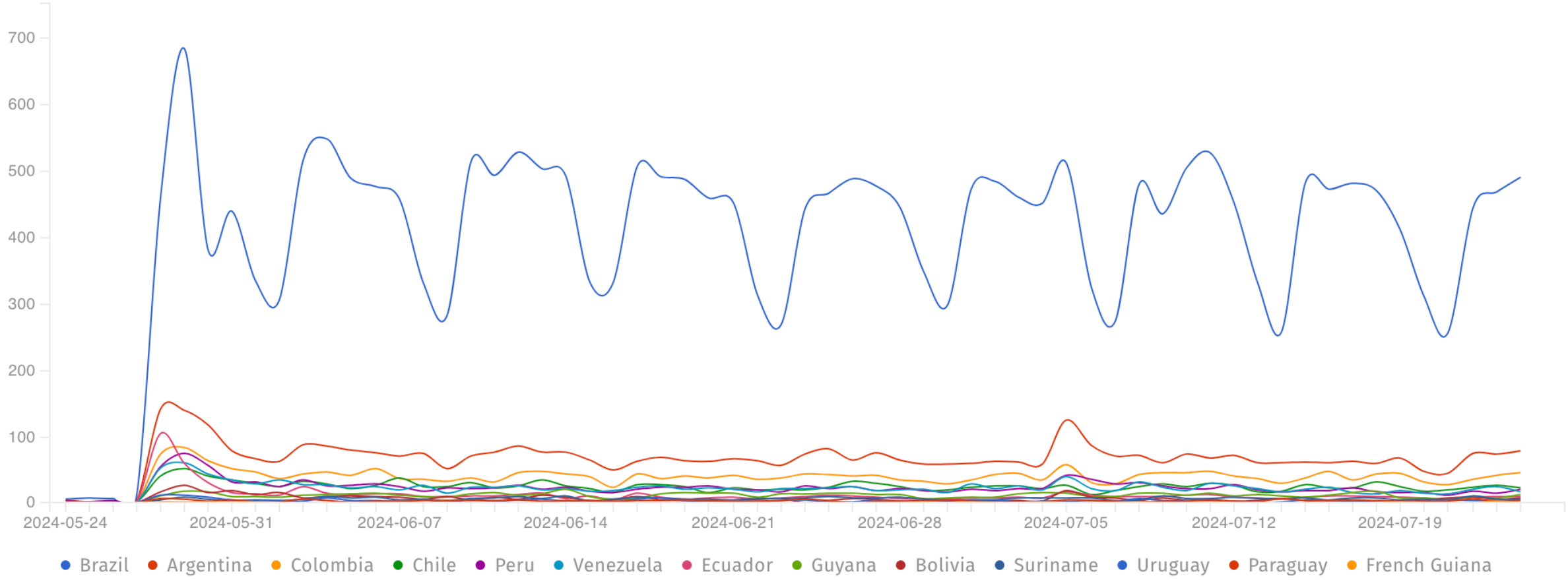
TLP CLEAR

Operation Endgame



TLP CLEAR

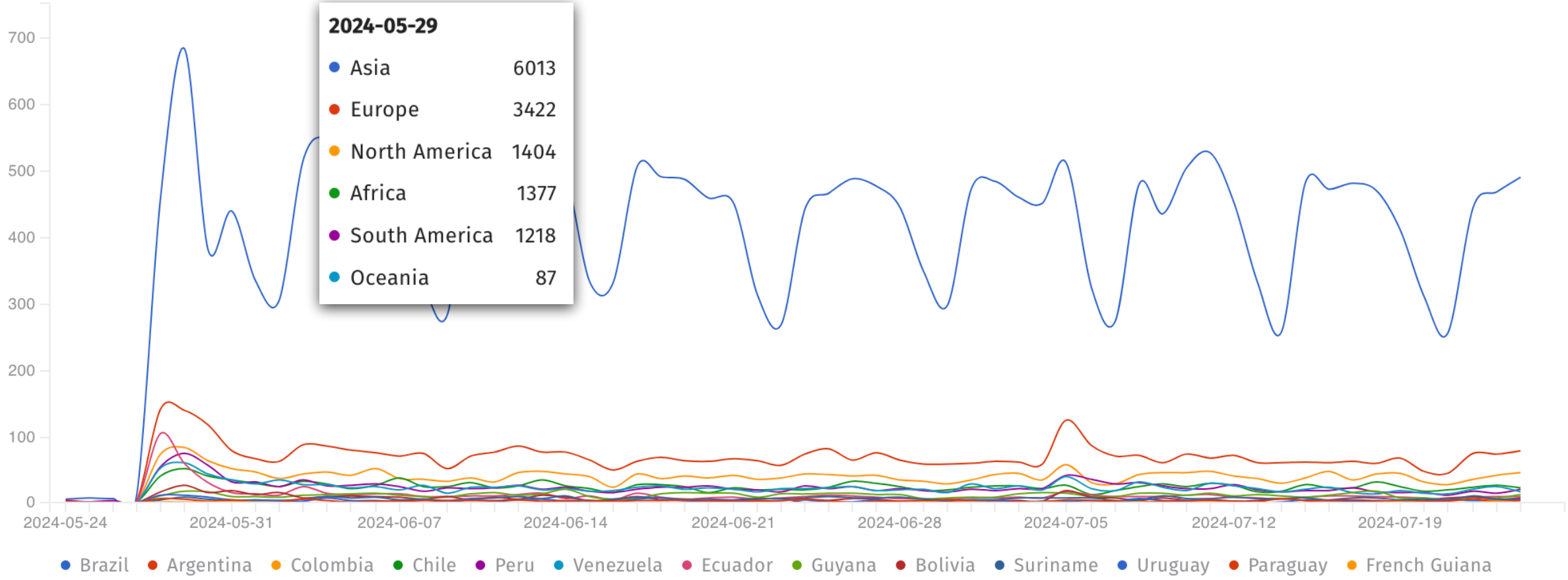
Operation Endgame



SHADOWSERVER

TLP CLEAR

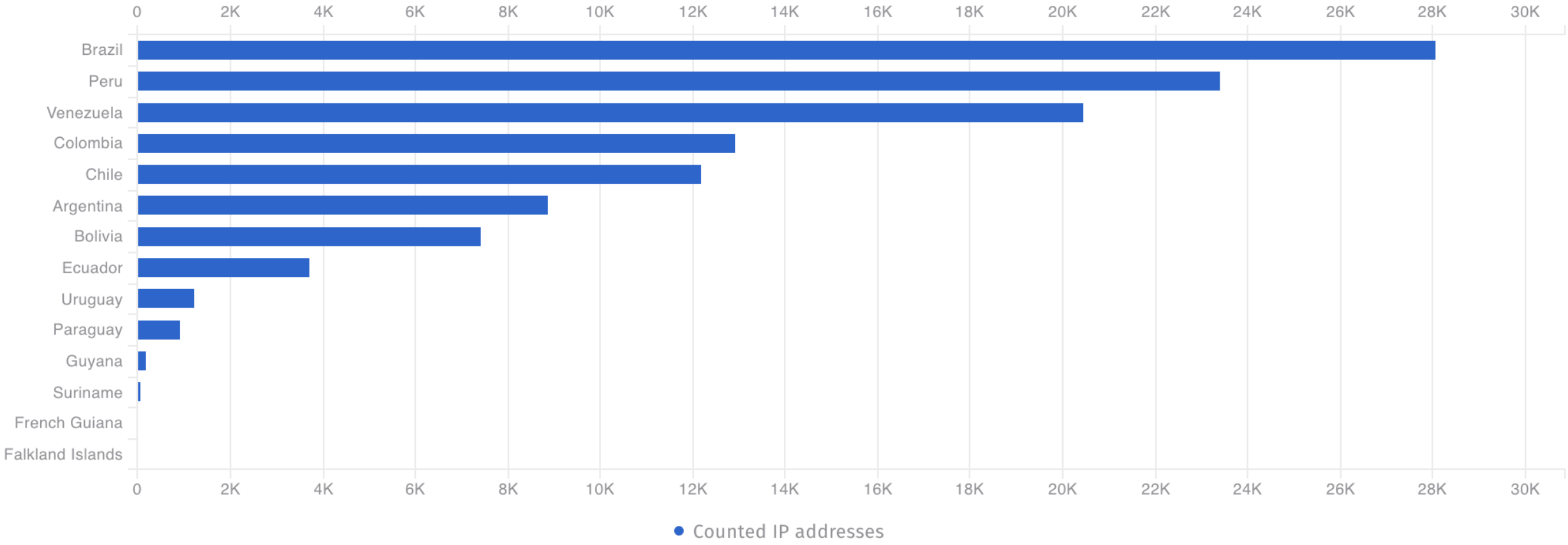
Operation Endgame



SHADOWSERVER

TLP CLEAR

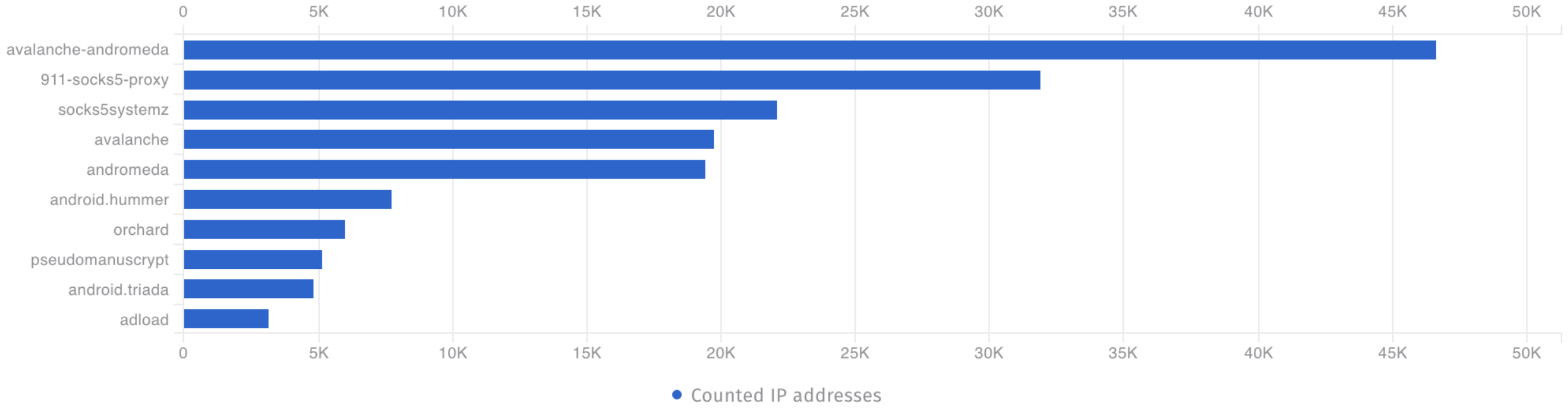
Top 10 Sinkhole Infections by Country - South America (Last 3 Months)



SHADOWSERVER

TLP CLEAR

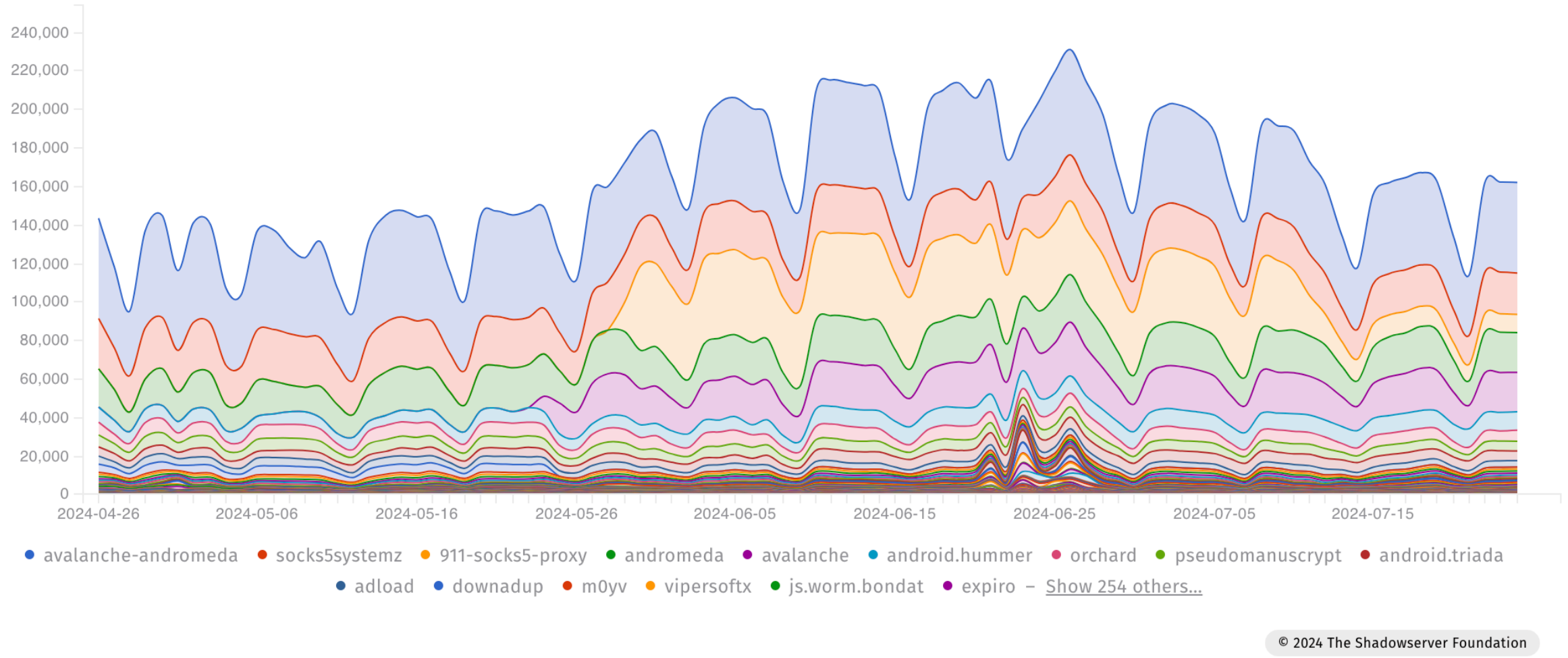
Top 10 Sinkhole Infections by Type - South America (Last 3 Months)



SHADOWSERVER

TLP CLEAR

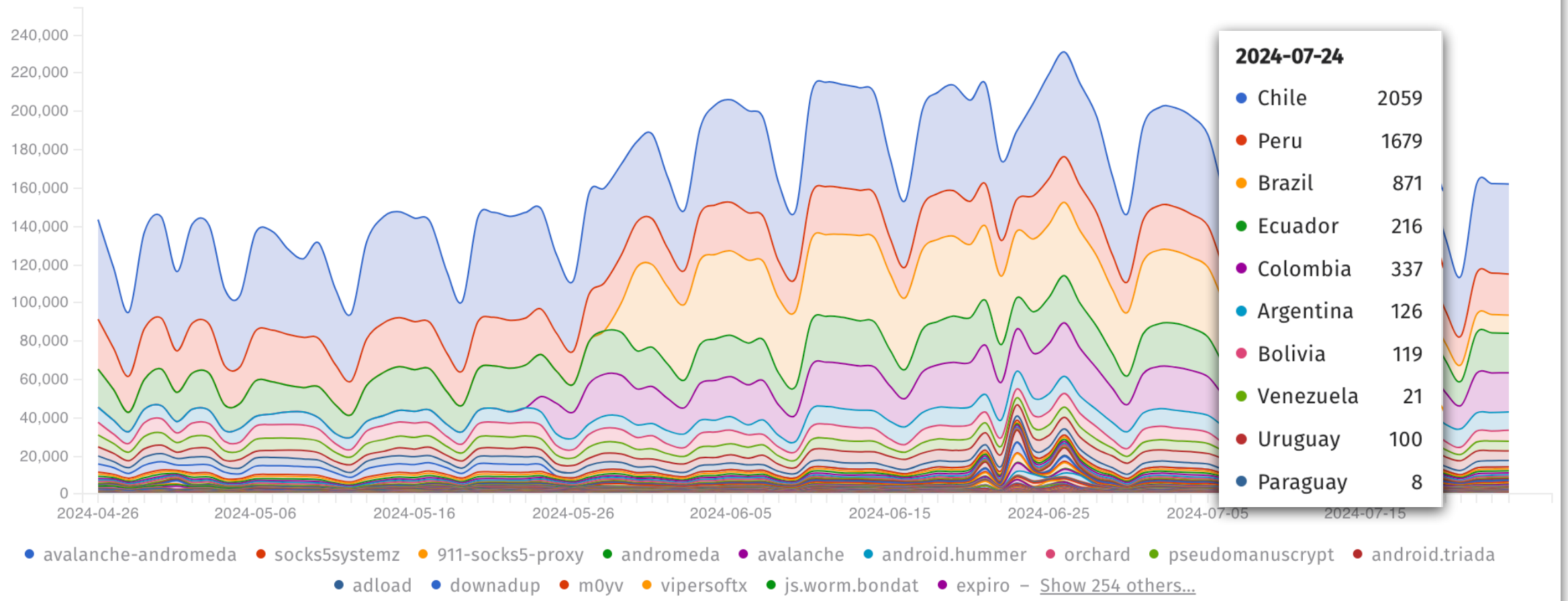
Top Infections in South America over time



SHADOWSERVER

TLP CLEAR

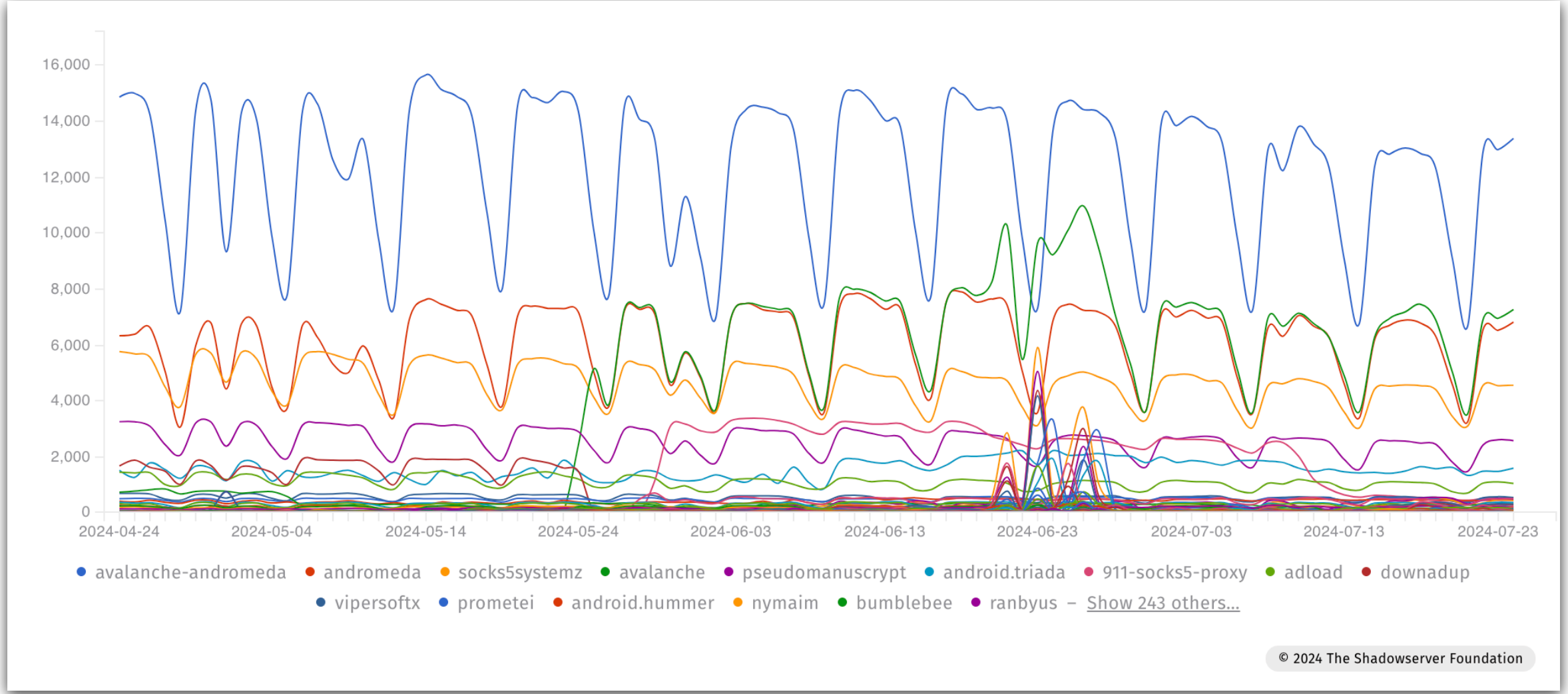
Top Infections in South America over time



SHADOWSERVER

TLP CLEAR

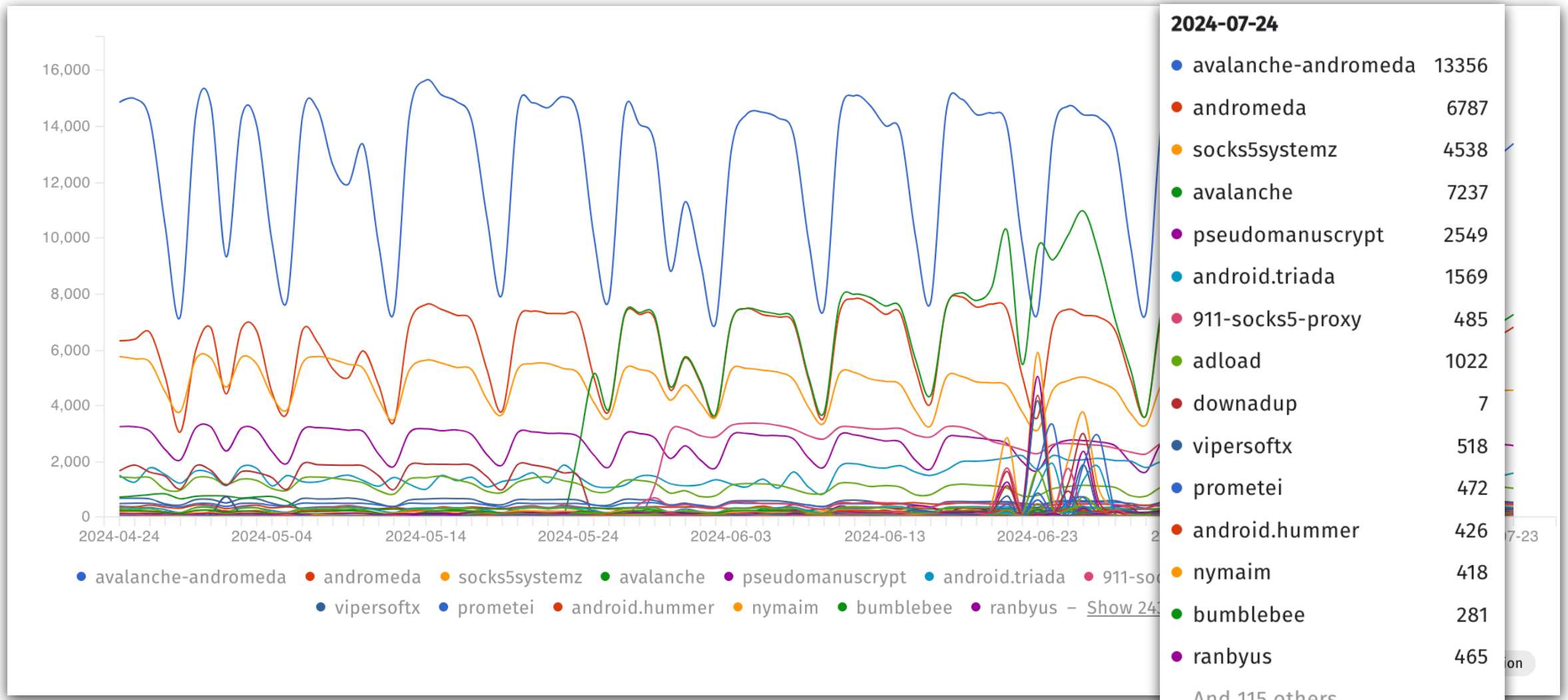
Top Infections in Brazil over time



SHADOWSERVER

TLP CLEAR

Top Infections in Brazil over time



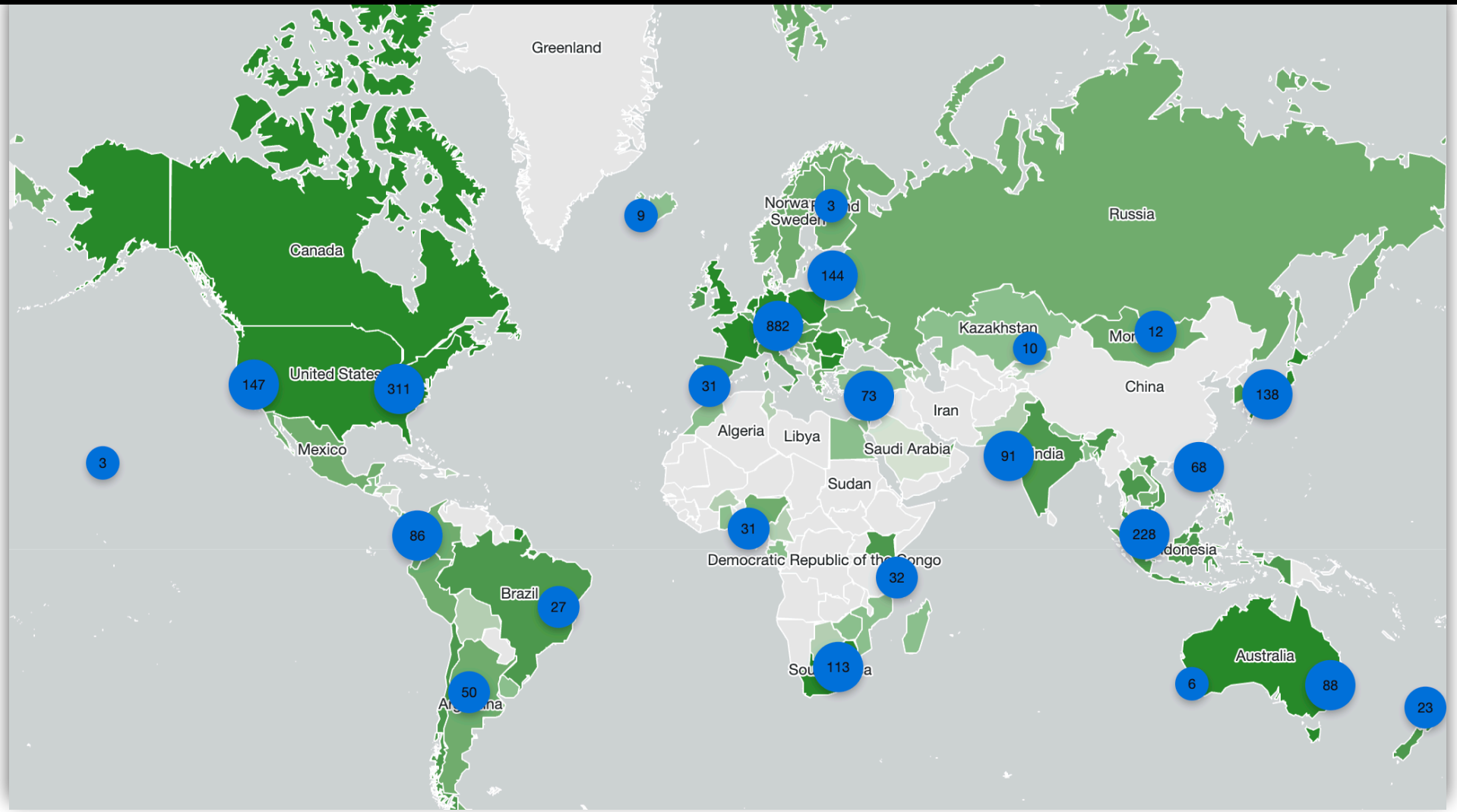
SHADOWSERVER

Attacking Devices

What Attacks Are Seen Coming from/to Brazil?

TLP CLEAR

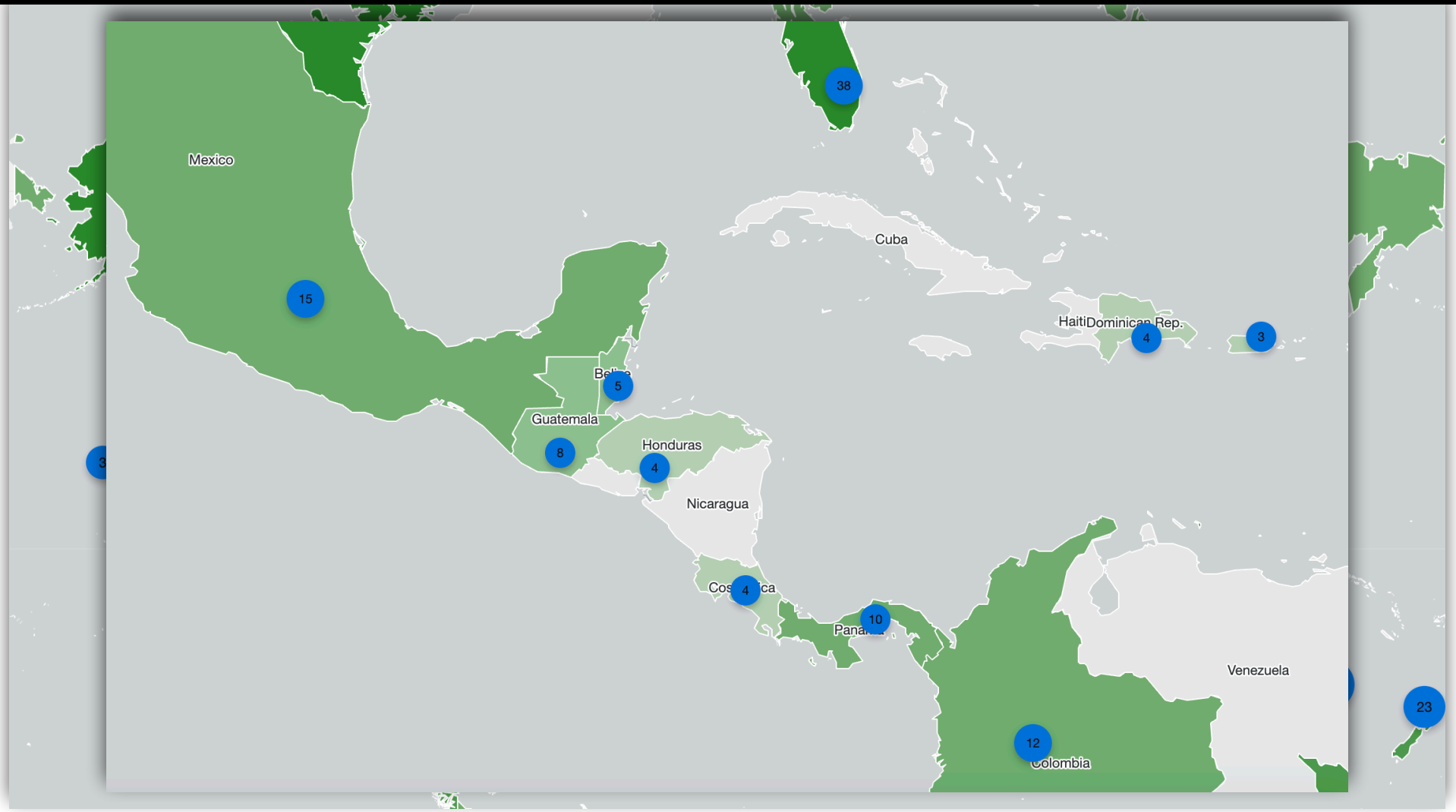
Honeypot sensor network - World & South America (July 2024)



SHADOWSERVER

TLP CLEAR

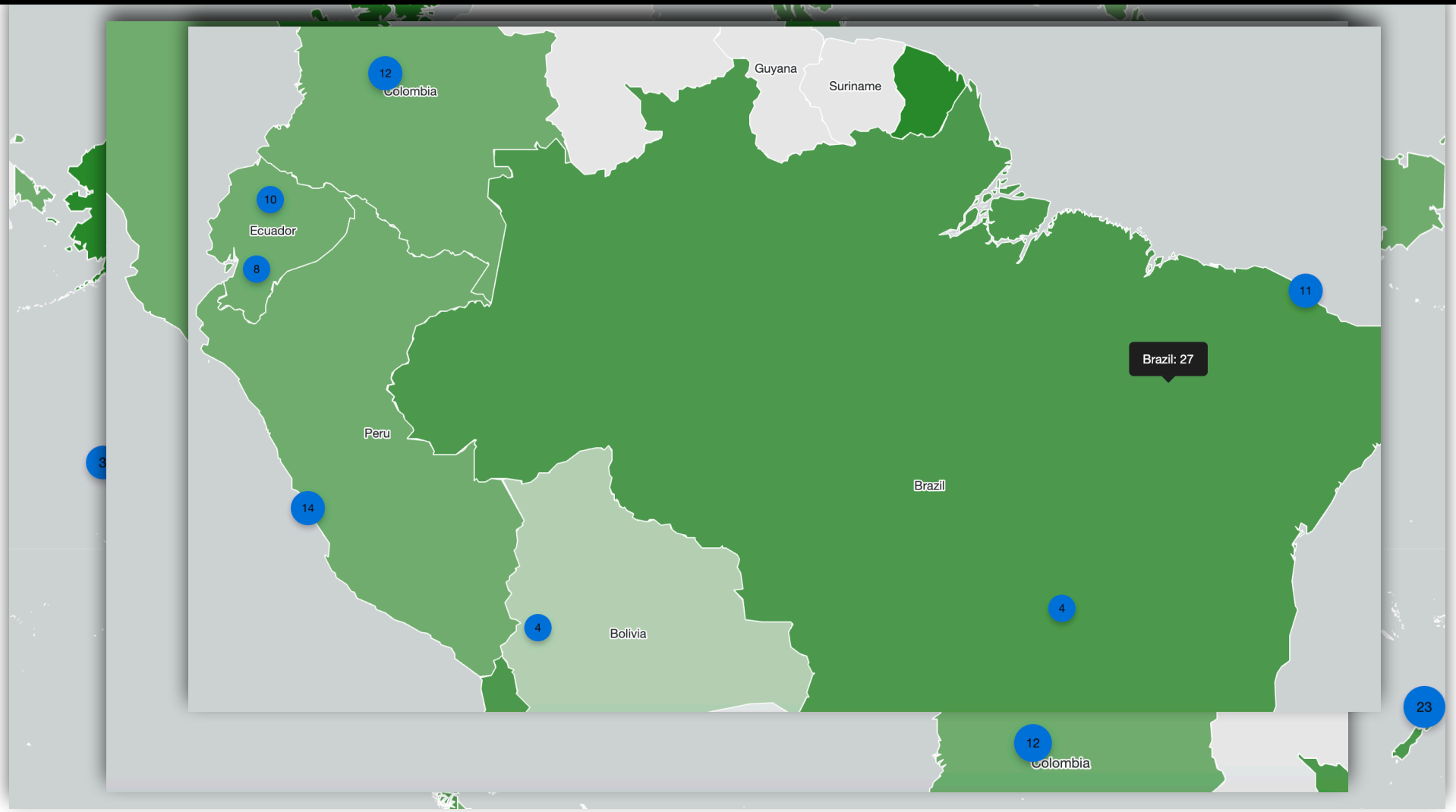
Honeypot sensor network - World & South America (July 2024)



SHADOWSERVER

TLP CLEAR

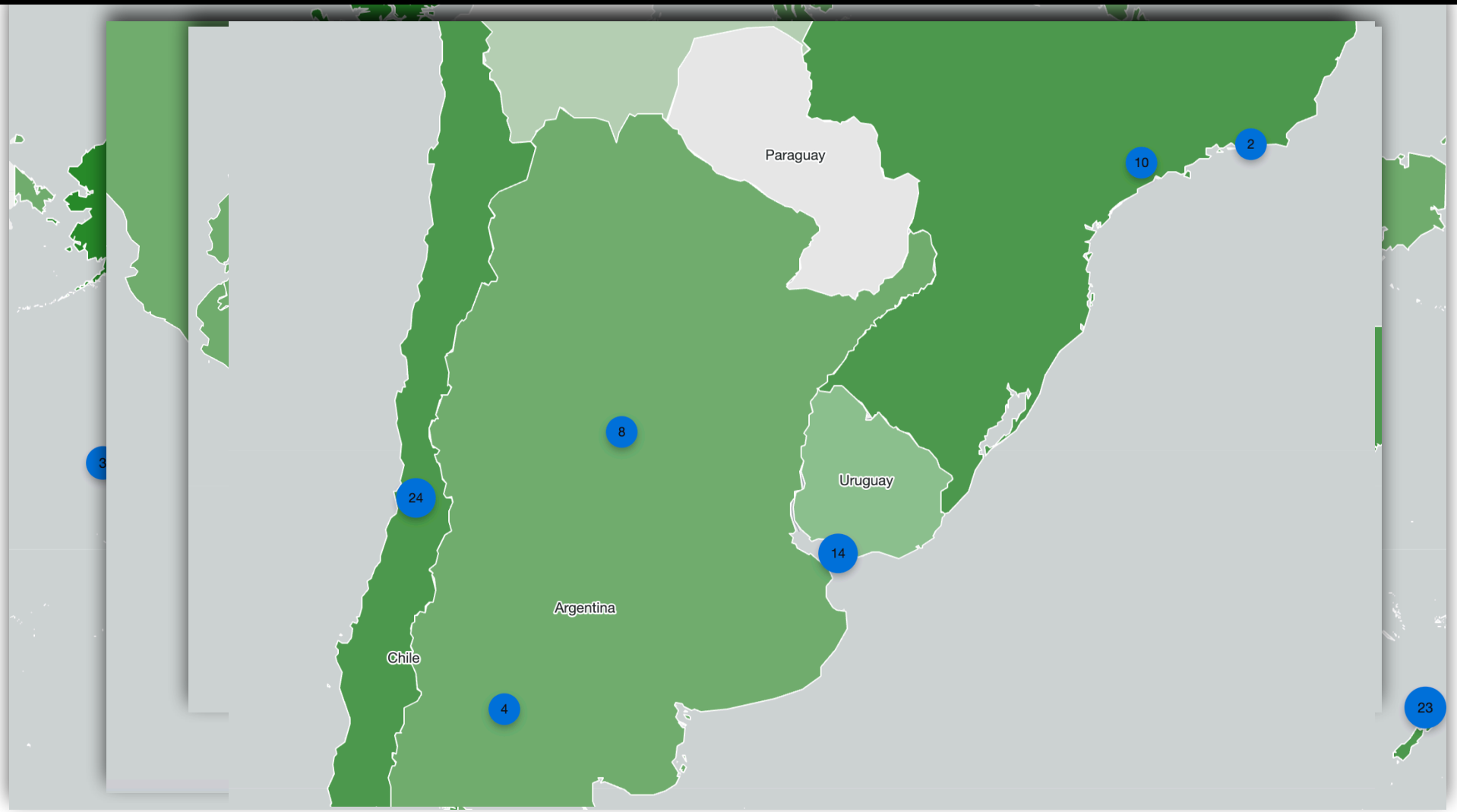
Honeypot sensor network - World & South America (July 2024)



SHADOWSERVER

TLP CLEAR

Honeypot sensor network - World & South America (July 2024)



SHADOWSERVER

TLP CLEAR

Exploitation tracking (by CVE or similar)

SHADOWSERVER UK Government

Dashboard | General statistics | IoT device statistics | Attack statistics: Vulnerabilities | Attack statistics: Devices | Help

Exploited vulnerabilities

Monitoring

Category: Top
Statistic: Unique IPs
Date range: From – To
Countries: Select one or more options...
Limit: 100
IoT: Select an option...
CISA KEV: Select an option...
Ransomware: Select an option...

About this data

This data is currently limited to web-based server side exploits seen by our honeypot sensors. Incoming attacks are tagged with a CVE, EDB, CNVD or other tag when detection rules are added. The lack of a specific CVE does not imply it is not being used for exploitation or that we do not see it in our honeypots. Tags do not apply retroactively, so CVE data will be shown only after a tag is created.

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

IoT device fingerprinting and honeypot attack statistics co-financed by the Connecting Europe Facility of the EU.

Exploited vulnerabilities - Top

Showing results for 2024-05-14

#	Vulnerability	Vendor	Product	IoT	KEV	Ransomware	1d	7d avg	30d avg	90d avg	Actions
1	CVE-2017-17215	Huawei	Huawei Home...	✔	✘	-	2,141	1,958	1,916	2,959	Details
2	CVE-2019-9670	Synacor	Zimbra Collab...	✘	✔	Unknown	339	204	50	40	Details
3	CVE-2023-20198	Cisco	Cisco IOS XE	✘	✔	Unknown	244	213	222	245	Details
4	CVE-2022-37042	Synacor	Zimbra Collab...	✘	✔	Unknown	115	62	17	11	Details
5	CVE-2014-8361	Realtek	Realtek SDK	✔	✔	Unknown	97	566	233	142	Details
6	CVE-2023-26801	LB-LINK	LB-LINK BL-AC...	✔	✘	-	76	86	109	231	Details
7	CVE-2018-10562	Dasan	Dasan GPON ...	✔	✔	Known	45	54	70	60	Details
8	CVE-2016-10372	Zyxel	Eir D1000	✔	✘	-	42	60	69	61	Details
9	EDB-25978	Netgear	Netgear DGN1...	✔	✘	-	39	54	52	51	Details
10	CVE-2022-41082	Microsoft	Exchange	✘	✔	Known	33	63	72	79	Details
11	EDB-41471	MVPower	MVPower DVR	✔	✘	-	31	38	39	59	Details
12	EDB-39596	Shenzhen TVT	CCTV-DVR (re...	✔	✘	-	19	24	25	26	Details
13	CVE-2015-2051	D-Link	D-Link DIR-64...	✔	✔	Unknown	18	32	35	31	Details
14	CVE-2023-386...	Metabase	Metabase	✘	✘	-	18	20	20	21	Details
15	CVE-2017-9841	PHPUnit - Se...	PHPUnit	✘	✔	Unknown	17	26	36	61	Details
16	CVE-2022-26134	Atlassian	Confluence	✘	✔	Known	17	19	18	21	Details
17	CVE-2016-6277	Netgear	NETGEAR R/D...	✔	✔	Unknown	15	17	19	17	Details
18	CVE-2023-0669	Fortra	GoAnywhere ...	✘	✔	Known	15	8	8	9	Details

© 2024 THE SHADOWSERVER FOUNDATION / Privacy & Terms / Contact Us / Credits

Language

SHADOWSERVER

TLP CLEAR

Exploitation tracking (by CVE or similar)

SHADOWSERVER

Exploited vulnerabilities

Monitoring

Category: Top
Statistic: Unique IPs
Date range: From – To
Countries: Select one or more optio
Limit: 100
IoT: Select an option...
CISA KEV: Select an option...
Ransomware: Select an option...

About this data

This data is currently limited to web-based server side exploits seen by our honeypot sensors. Incoming attacks are tagged with a EDB, CNVD or other tag when detection rules added. The lack of a specific CVE does not i it is not being used for exploitation or that do not see it in our honeypots. Tags do not apply retroactively, so CVE data will be show only after a tag is created.

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

IoT device fingerprinting and honeypot atta statistics co-financed by the Connecting Eur Facility of the EU.

© 2024 THE SHADOWSERVER F

UK Government

Dashboard | General statistics | IoT device statistics | Attack statistics: Vulnerabilities | Attack statistics: Devices | Help

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home

SHARE:

Filters

What are you looking for?

Date Added (optional)

Sort by (optional)

Publish Date

Items per page (optional)

20

APPLY

Known Exploited Vulnerabilities Catalog

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.

HOW TO USE THE KEV CATALOG

The KEV catalog is also available in the following formats:

CSV
JSON
JSON Schema

SHADOWSERVER

TLP CLEAR

Exploitation tracking (by CVE or similar)

SHADOWSERVER UK Government

Dashboard | General statistics | IoT device statistics | Attack statistics: Vulnerabilities | Attack statistics: Devices | Help

FIRST Improving Security Together

About FIRST | Membership | Initiatives | Standards & Publications | Events | Education | Blog

Exploit Prediction Scoring System (EPSS)

- The EPSS Model
- Data and Statistics
- User Guide
- EPSS Research and Presentations
- Frequently Asked Questions
- Who is using EPSS?
- Open-source EPSS Tools
- API
- Related Exploit Research
- Blog
- Data Partners

EPSS

Exploit Prediction Scoring System

Mission

The Exploit Prediction Scoring System (EPSS) is a data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild. Our goal is to assist network defenders to better prioritize vulnerability remediation efforts. While other industry standards have been useful for capturing innate characteristics of a vulnerability and provide measures of severity, they are limited in their ability to assess threat. EPSS fills that gap because it uses current threat information from CVE and real-world exploit data. The EPSS model produces a probability score between 0 and 1 (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited.

If you would like to join the **EPSS special interest group**, please visit the EPSS-SIG portal and fill out the "Request to Join" form. Anyone is welcome to join our mailing list and Slack. We meet every other Friday at 11 am eastern time, GMT -5.

Alternatively, if you would like to receive email updates about EPSS news and announcements, please subscribe to our low-volume EPSS-news list:

- Subscribe by writing an e-mail to epss-news-subscribe [at] first.org
- Unsubscribe by writing an e-mail to epss-news-unsubscribe [at] first.org

© 2024 THE SHADOWSERVER

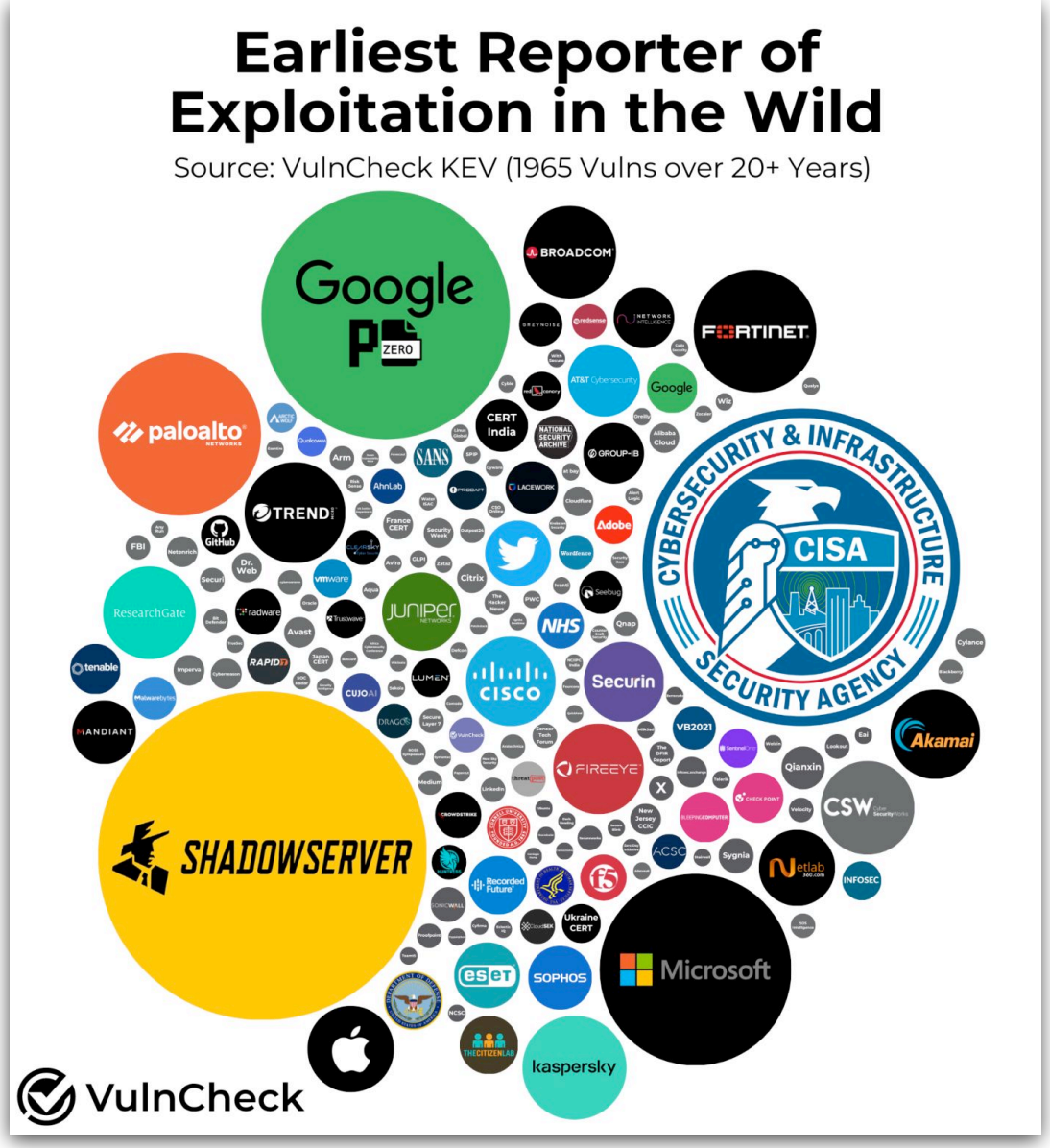
JSON Schema

APPLY

SHADOWSERVER

TLP CLEAR

Earliest Reporter of Exploitation in the Wild



SHADOWSERVER

TLP CLEAR

Most Exploited Vulnerabilities - from BR (Daily Breakdown)

SHADOWSERVER UK Government

Dashboard | General statistics | IoT device statistics | Attack statistics: Vulnerabilities | Attack statistics: Devices | Help

Exploited vulnerabilities

Monitoring

Category: Top
Statistic: Unique IPs
Date range: From – 2024-07-24
Countries: Brazil (BR)
Limit: 100
IoT: Select an option...
CISA KEV: Select an option...
Ransomware: Select an option...

About this data

This data is currently limited to web-based server side exploits seen by our honeypot sensors. Incoming attacks are tagged with a CVE, EDB, CNVD or other tag when detection rules are added. The lack of a specific CVE does not imply it is not being used for exploitation or that we do not see it in our honeypots. Tags do not apply retroactively, so CVE data will be shown only after a tag is created.

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

IoT device fingerprinting and honeypot attack statistics co-financed by the Connecting Europe Facility of the EU.

Exploited vulnerabilities - Top

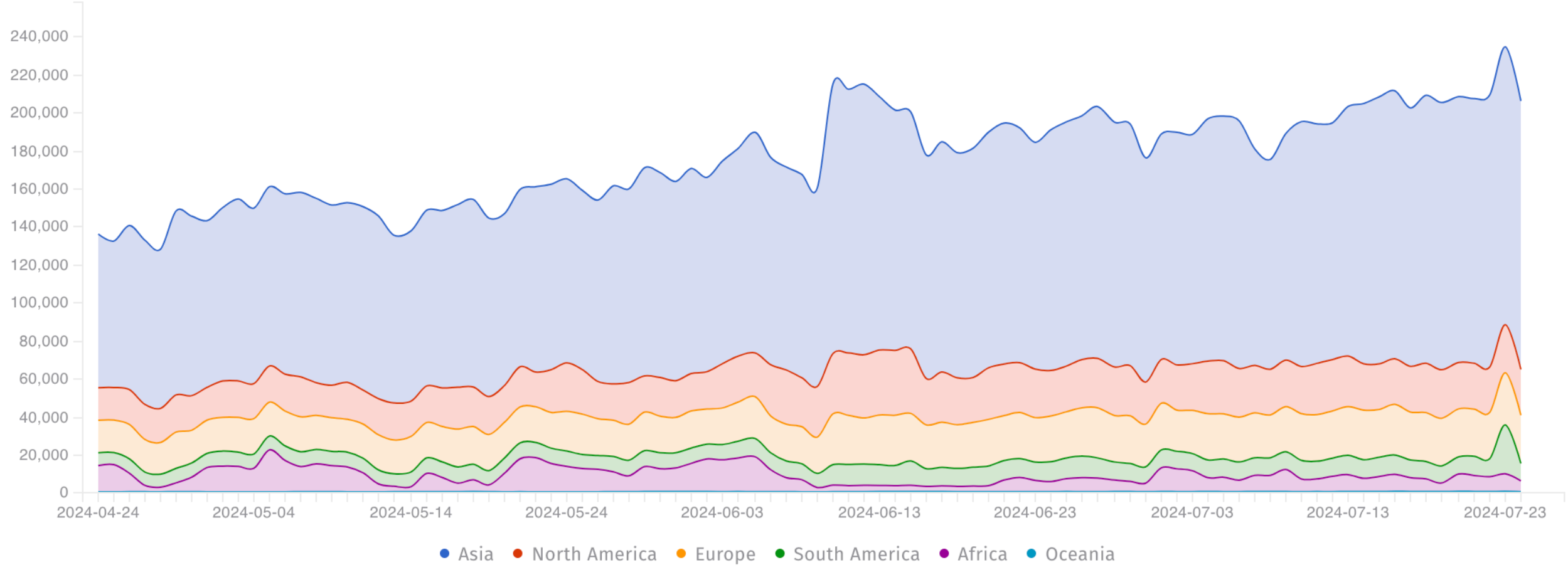
Showing results for 2024-07-24

#	Vulnerability	Vendor	Product	IoT	KEV	Ransomware	1d	7d avg	30d avg	90d avg	Actions
1	CVE-2017-17215	Huawei	Huawei Home...	✓	✗	-	523	423	297	217	Details
2	CVE-2023-20198	Cisco	Cisco IOS XE	✗	✓	Unknown	16	19	14	13	Details
3	CVE-2018-10562	Dasan	Dasan GPON ...	✓	✓	Known	2	1	2	2	Details
4	CVE-2020-16846	SaltStack	Salt	✗	✓	Unknown	2	1	1	1	Details
5	CVE-2017-9841	PHPUnit - Seb...	PHPUnit	✗	✓	Unknown	1	2	3	2	Details
6	CNVD-2018-24...	TopThink	ThinkPHP5	✗	✗	-	1	2	2	2	Details
7	CVE-2023-26801	LB-LINK	LB-LINK BL-AC...	✓	✗	-	1	2	2	2	Details
8	CVE-2016-10372	Zyxel	Eir D1000	✓	✗	-	1	2	2	1	Details
9	EDB-25978	Netgear	Netgear DGN1...	✓	✗	-	1	1	2	2	Details
10	CVE-2014-8361	Realtek	Realtek SDK	✓	✓	Unknown	1	1	1	2	Details
11	EDB-41471	MVPower	MVPower DVR	✓	✗	-	1	1	3	3	Details
12	CVE-2023-3608	Ruijie Networks	Ruijie BCR810W	✓	✗	-	1	1	1	1	Details
13	CVE-2021-3129	Laravel	Ignition	✗	✓	Known	0	2	2	1	Details
14	CVE-2021-42013	Apache	Apache HTTP ...	✗	✓	Known	0	2	2	2	Details
15	CVE-2017-18368	Zyxel/Billion	ZyXEL P660HN...	✓	✓	Unknown	0	1	1	1	Details
16	EDB-39596	Shenzhen TVT	CCTV-DVR (reb...	✓	✗	-	0	1	1	1	Details
17	EDB-45025	Apache	Hadoop (YAR...	✗	✗	-	0	1	1	1	Details
18	CVE-2016-6277	Netgear	NETGEAR R/D ...	✓	✓	Unknown	0	1	1	1	Details

SHADOWSERVER

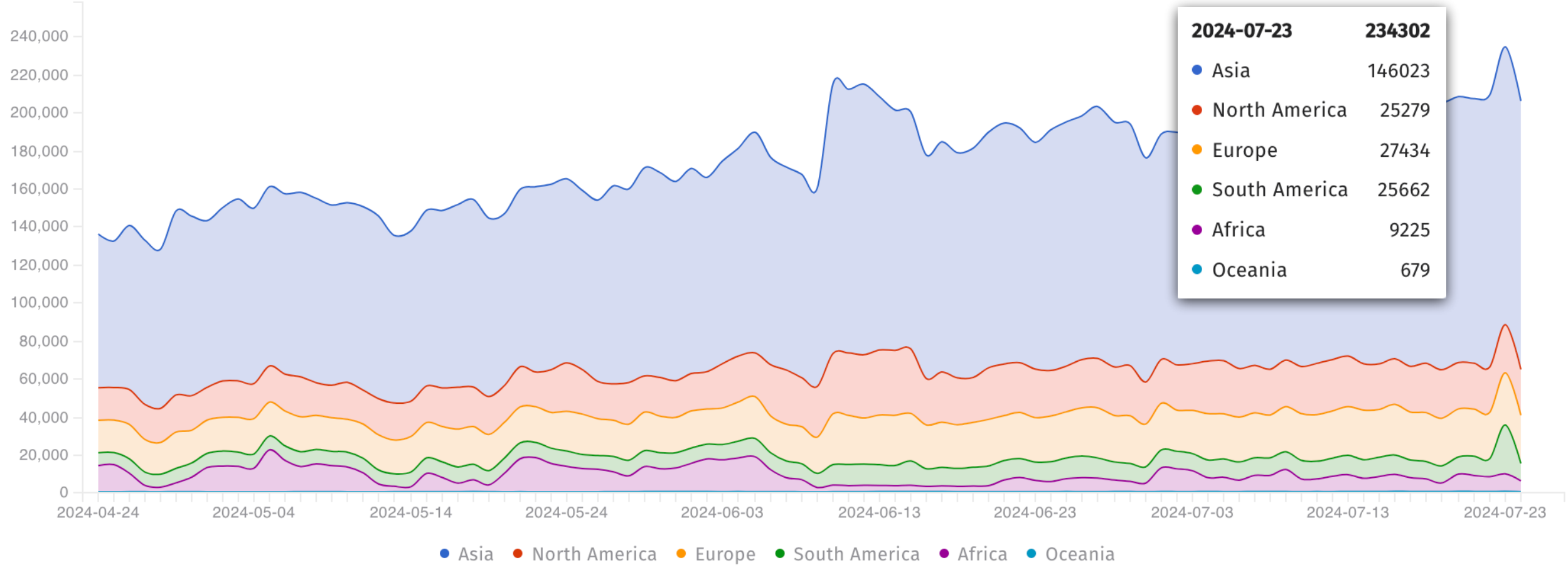
TLP CLEAR

Attacking Devices - Source by Continent



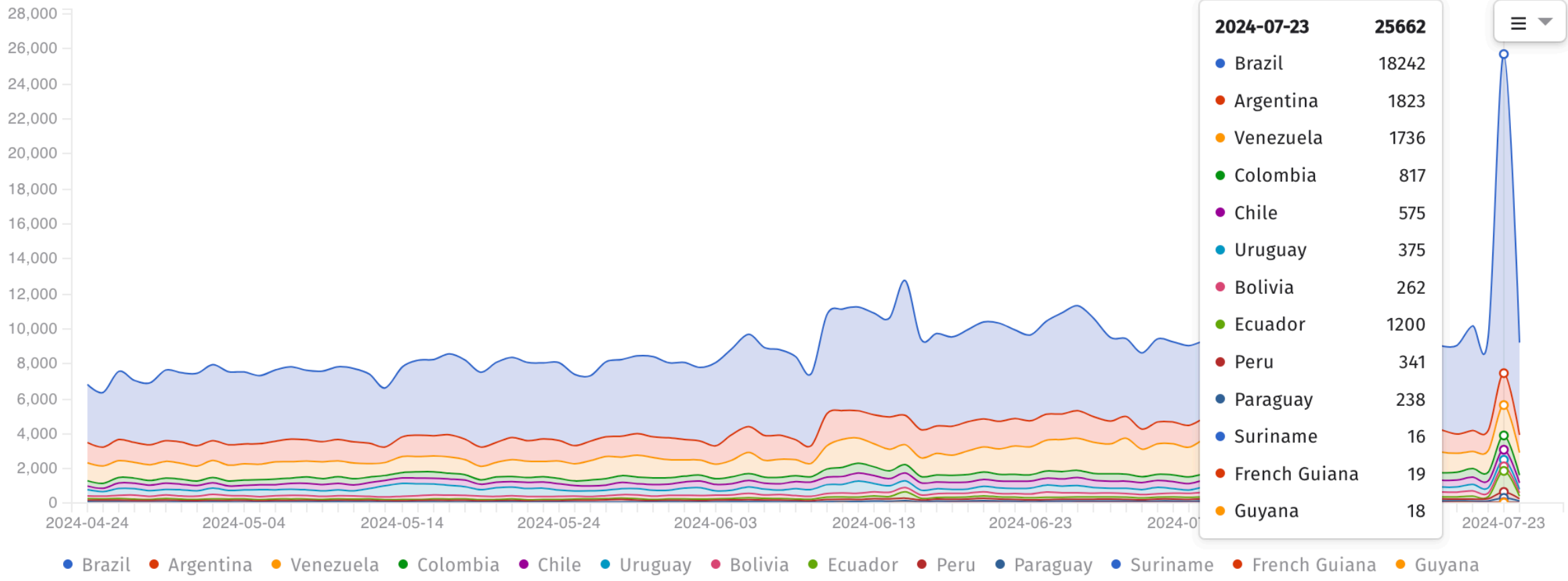
TLP CLEAR

Attacking Devices - Source by Continent



TLP CLEAR

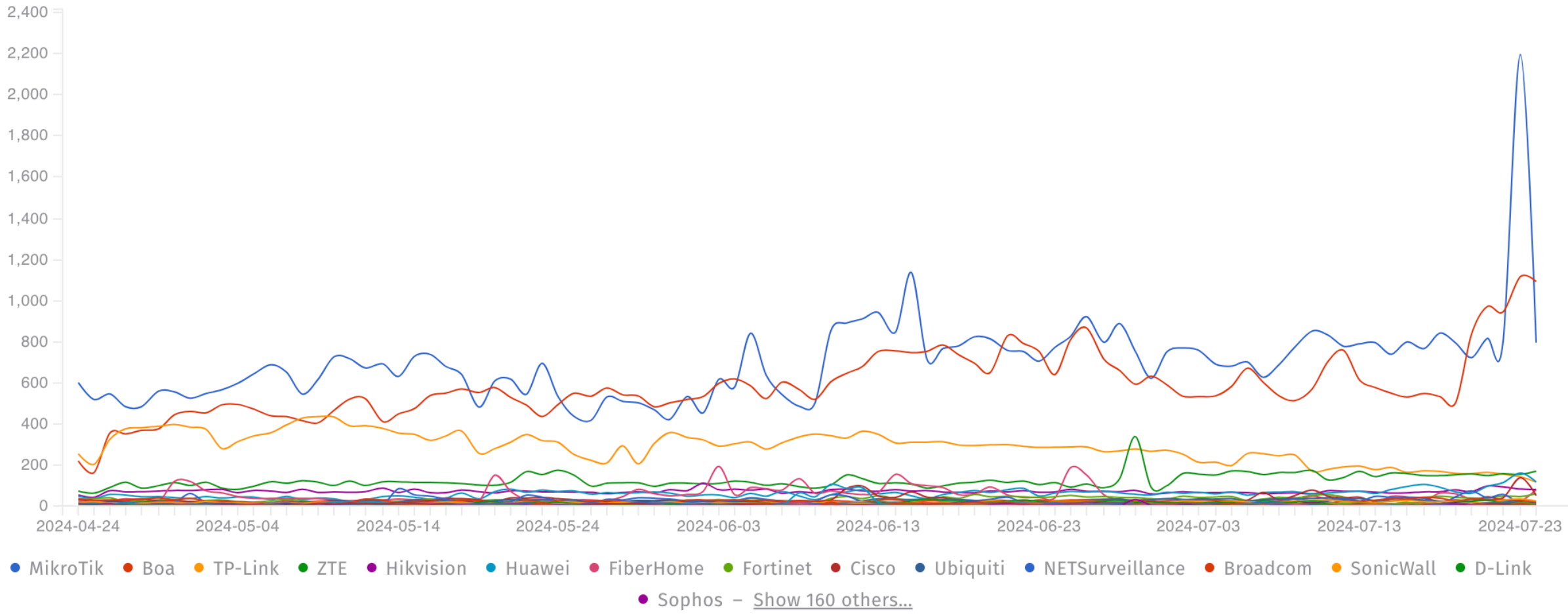
Attacking Devices - Source by Country (South America)



SHADOWSERVER

TLP CLEAR

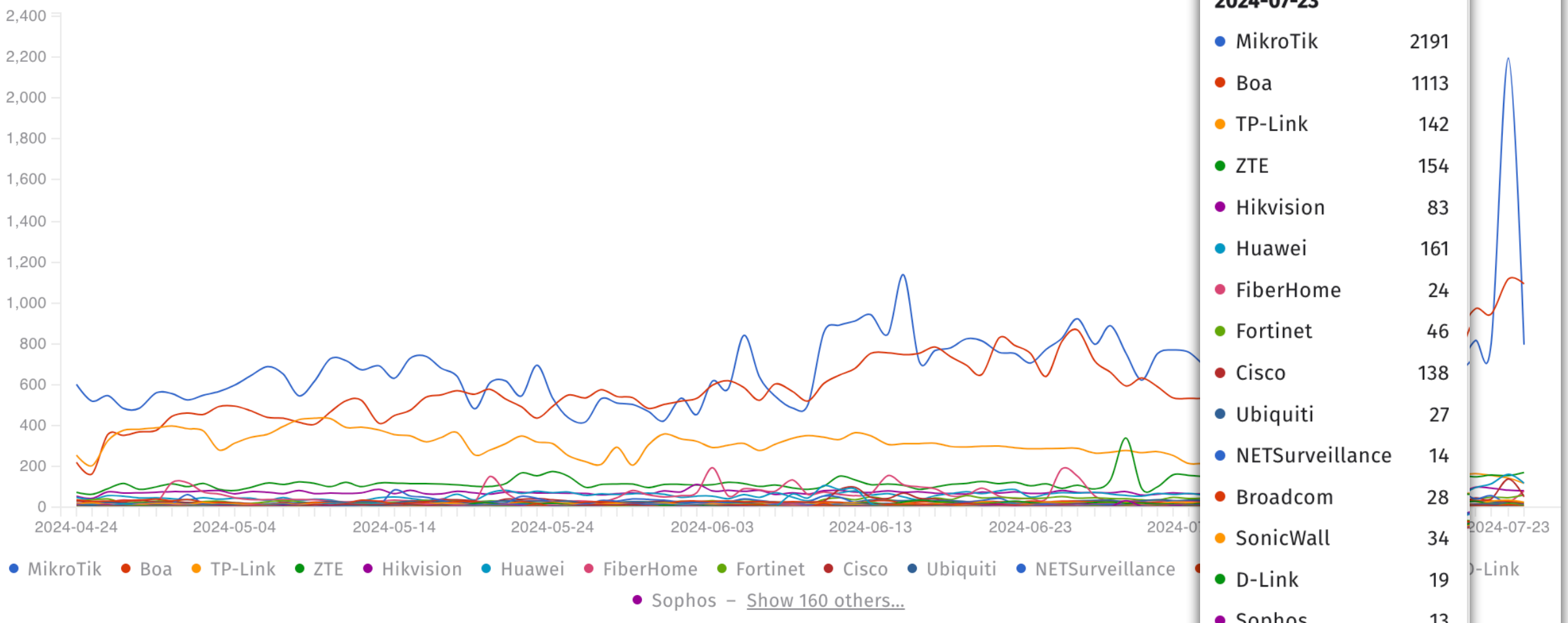
Attacking Devices by Vendor - South America



SHADOWSERVER

TLP CLEAR

Attacking Devices by Vendor - South America

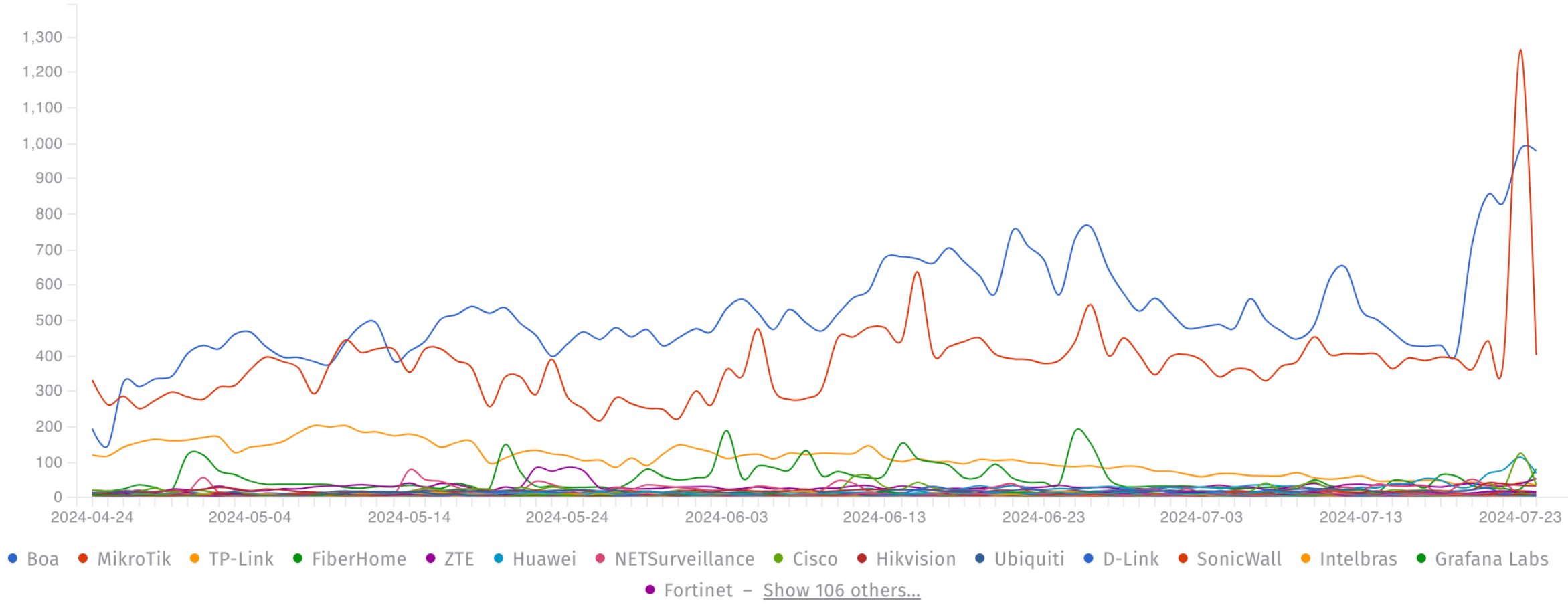


2024-07-23	
MikroTik	2191
Boa	1113
TP-Link	142
ZTE	154
Hikvision	83
Huawei	161
FiberHome	24
Fortinet	46
Cisco	138
Ubiquiti	27
NETSurveillance	14
Broadcom	28
SonicWall	34
D-Link	19
Sophos	13
And 66 others...	

SHADOWSERVER

TLP CLEAR

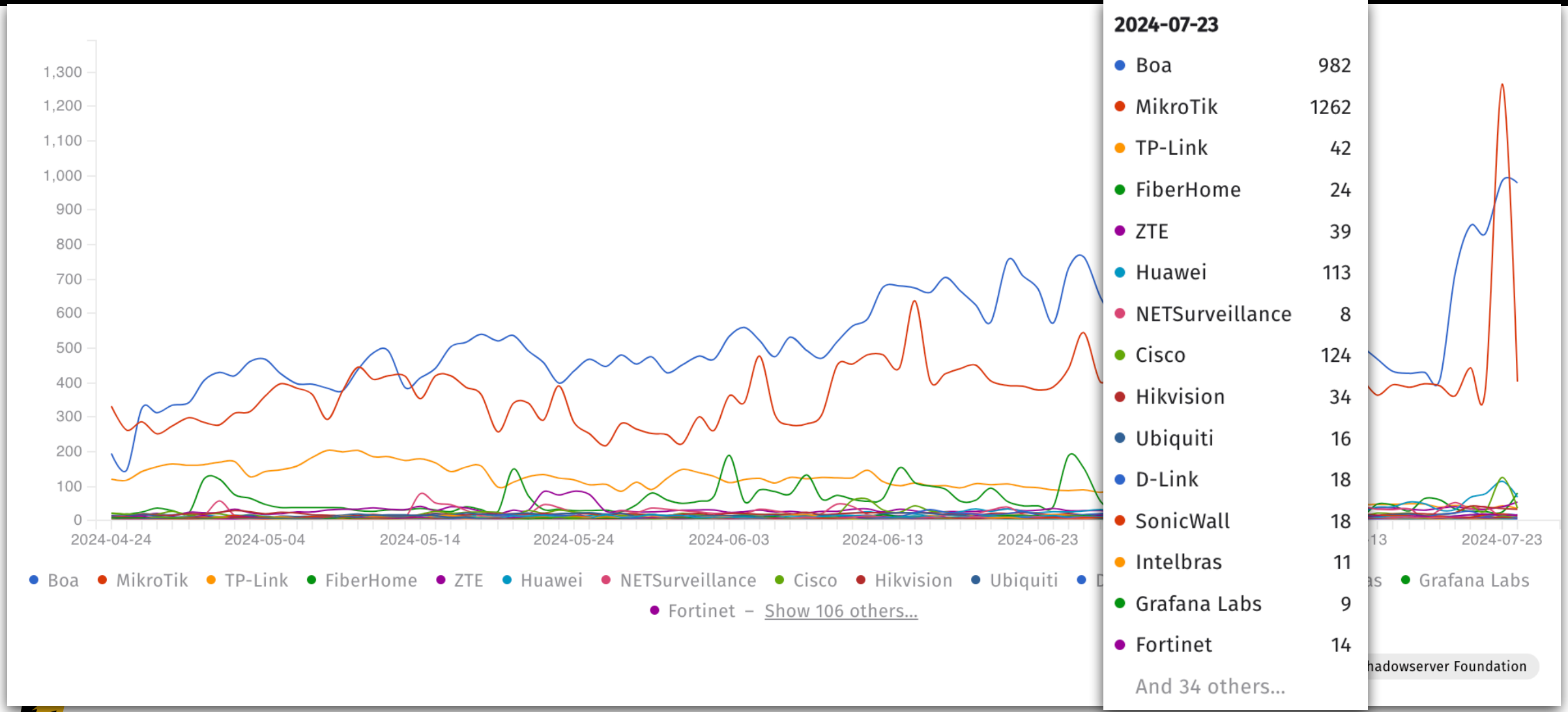
Attacking Devices by Vendor - Brazil



SHADOWSERVER

TLP CLEAR

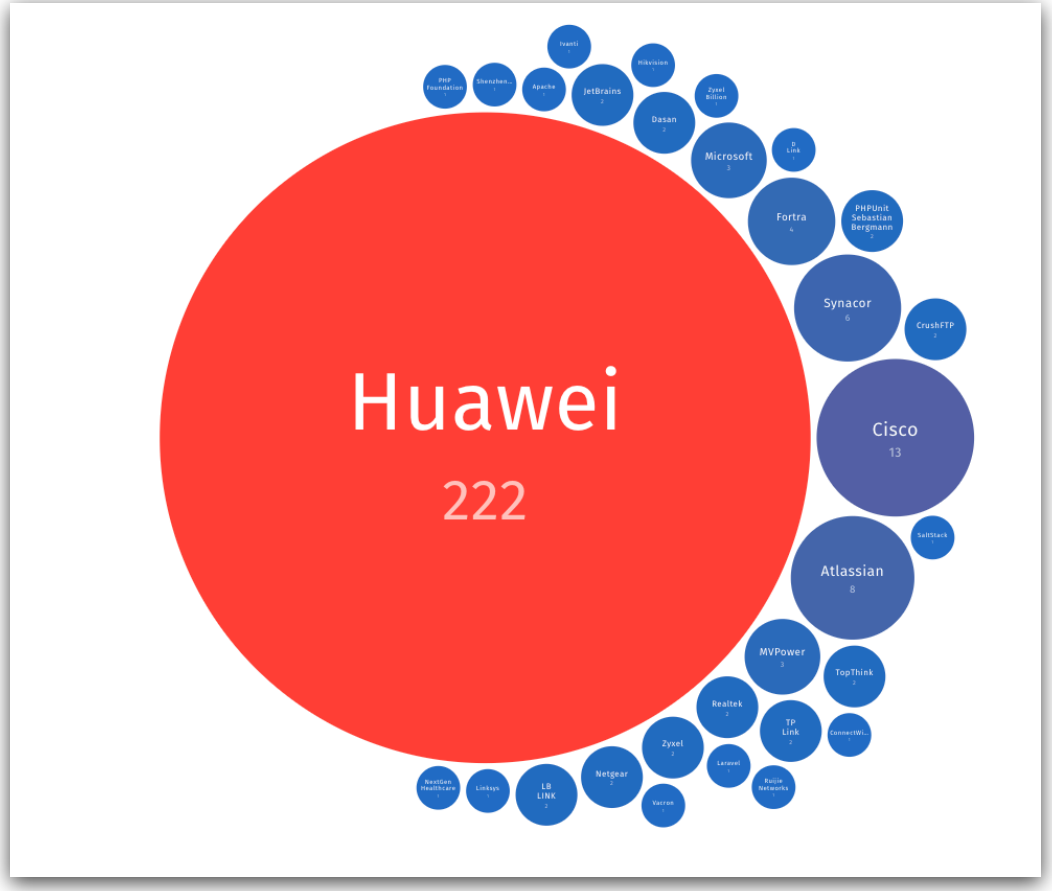
Attacking Devices by Vendor - Brazil

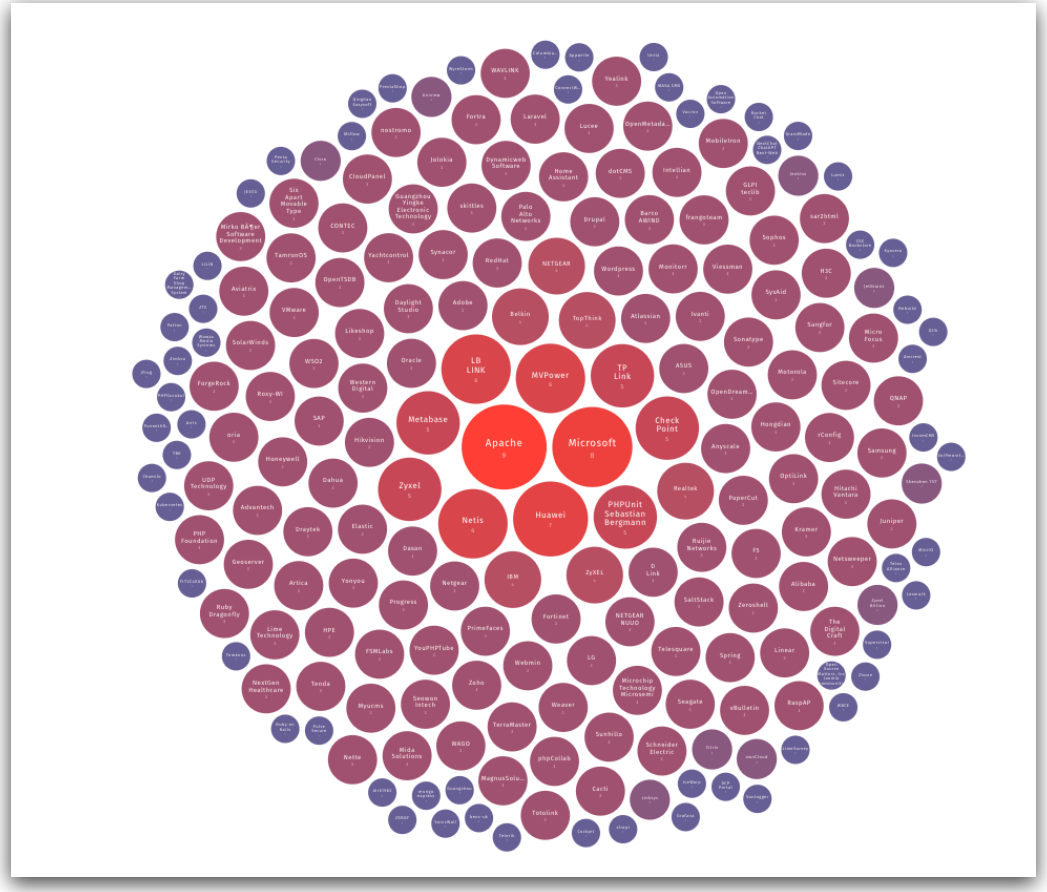


SHADOWSERVER

TLP
CLEAR

Vendor Most Targeted by Exploits (from/to BR)





SHADOWSERVER Attacks from BR

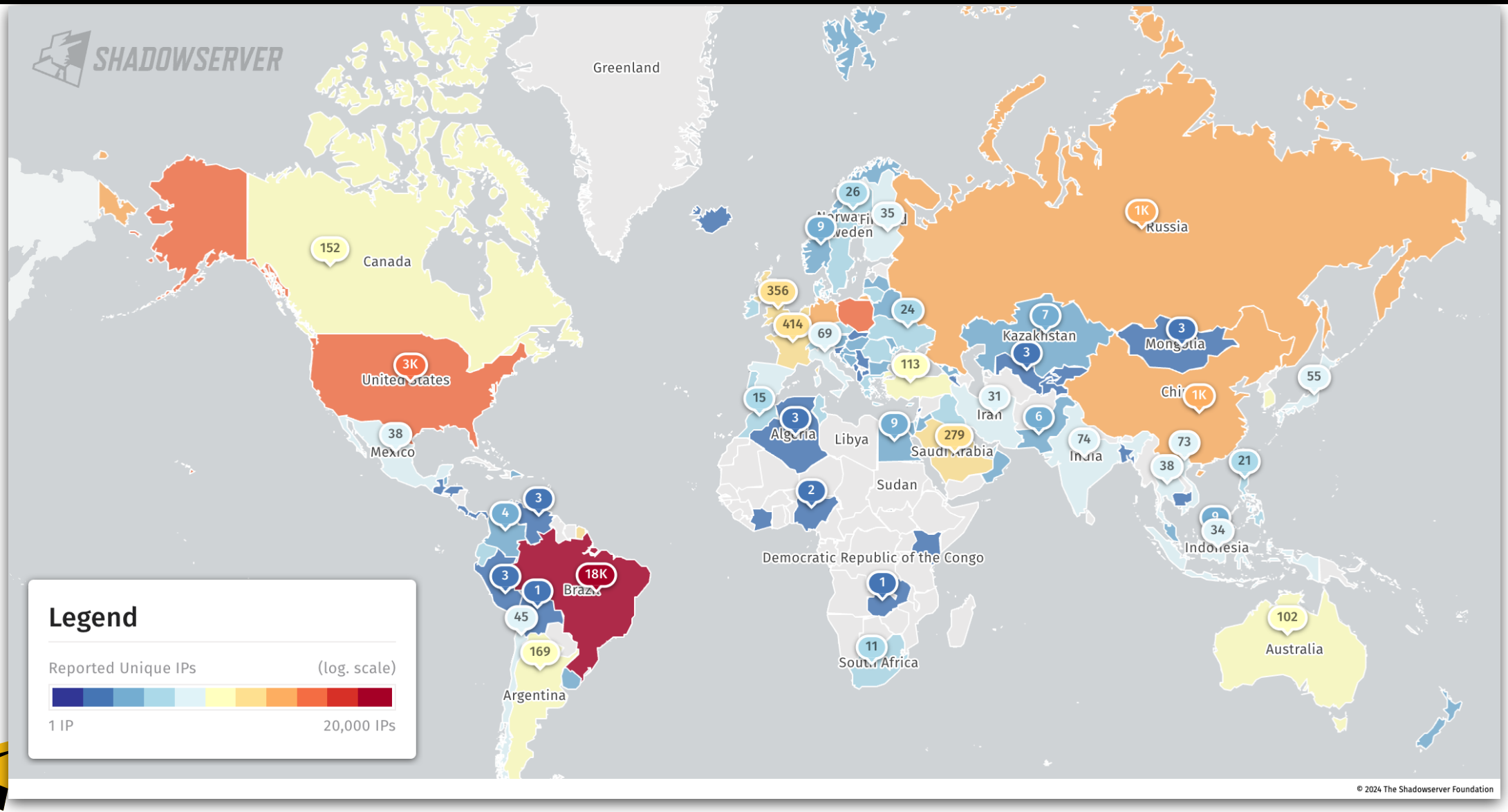
Attacks against BR sensors

DDoS Attacks

Amplification Attacks - As seen by honeypot sensors

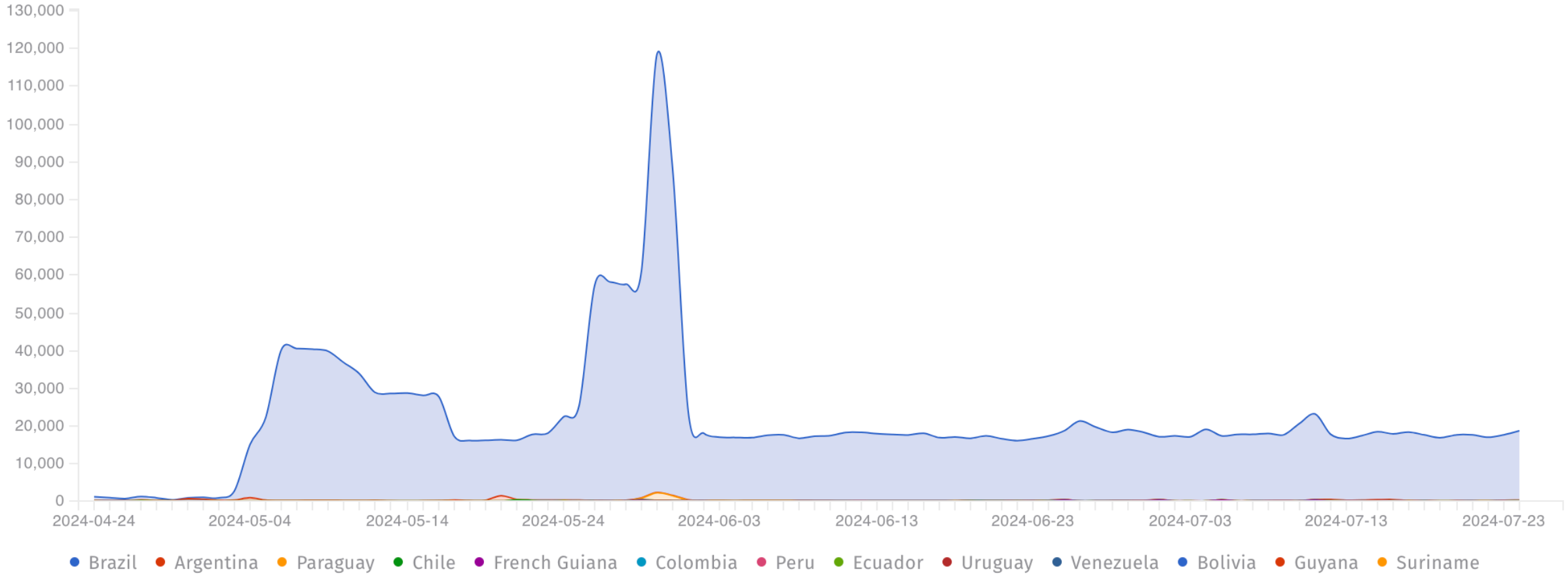
TLP CLEAR

Amp DDoS Attacks by Unique Targets - 2024-07-24



TLP CLEAR

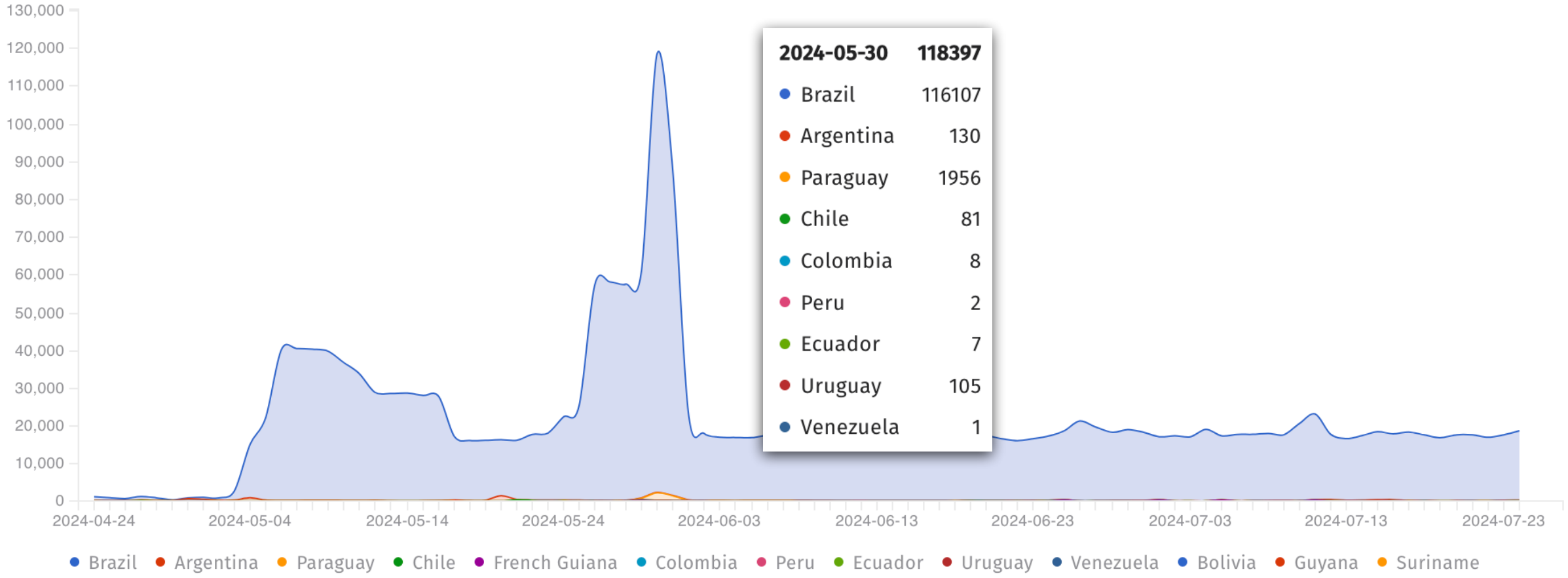
Amp DDoS Attacks by Unique Targets (South America)



SHADOWSERVER

TLP CLEAR

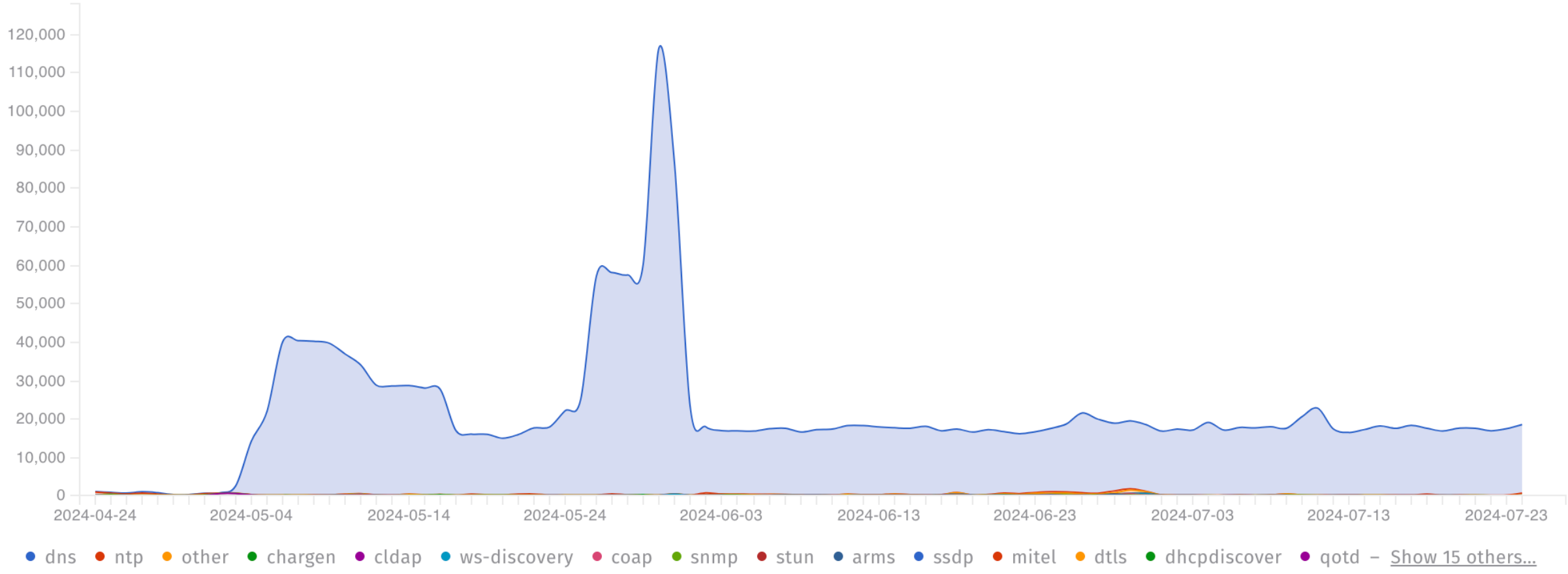
Amp DDoS Attacks by Unique Targets (South America)



SHADOWSERVER

TLP CLEAR

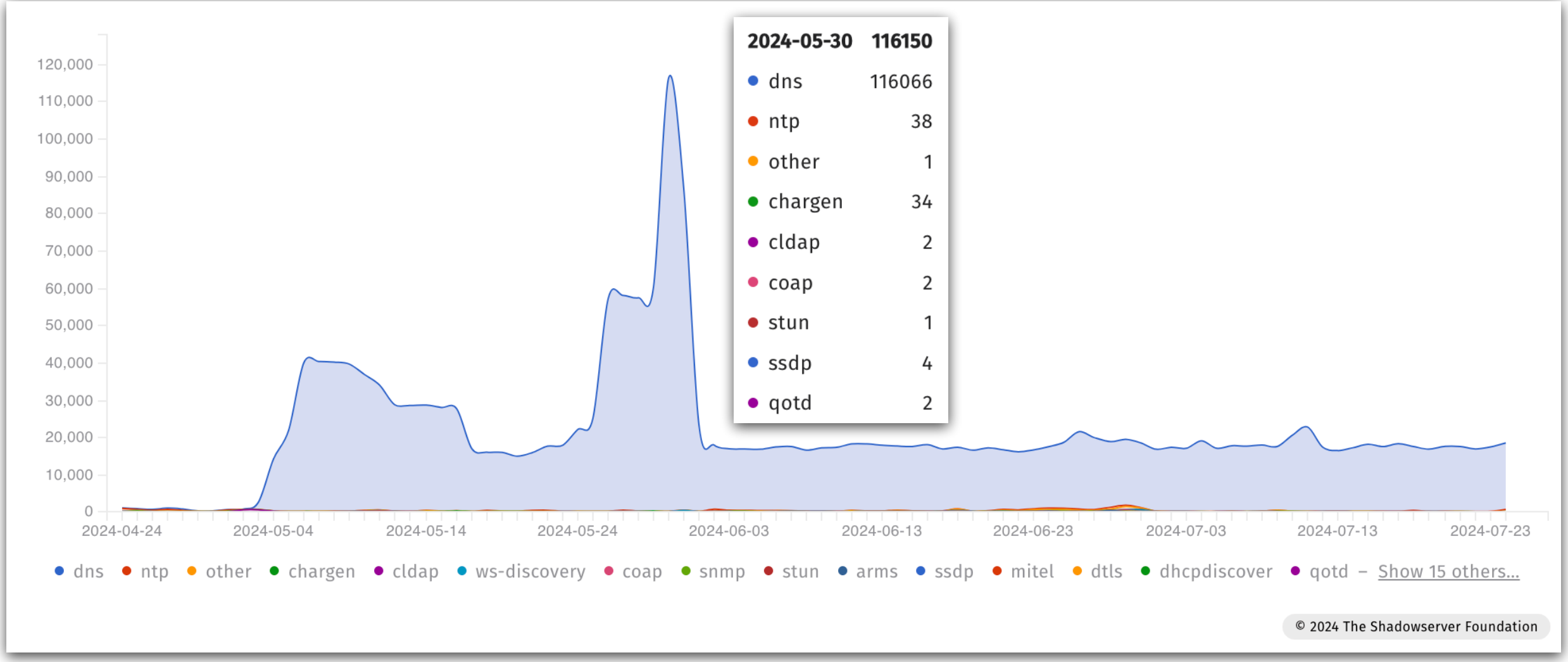
DDoS Attacks - Amplification type (Brazil)



SHADOWSERVER

TLP CLEAR

DDoS Attacks - Amplification type (Brazil)



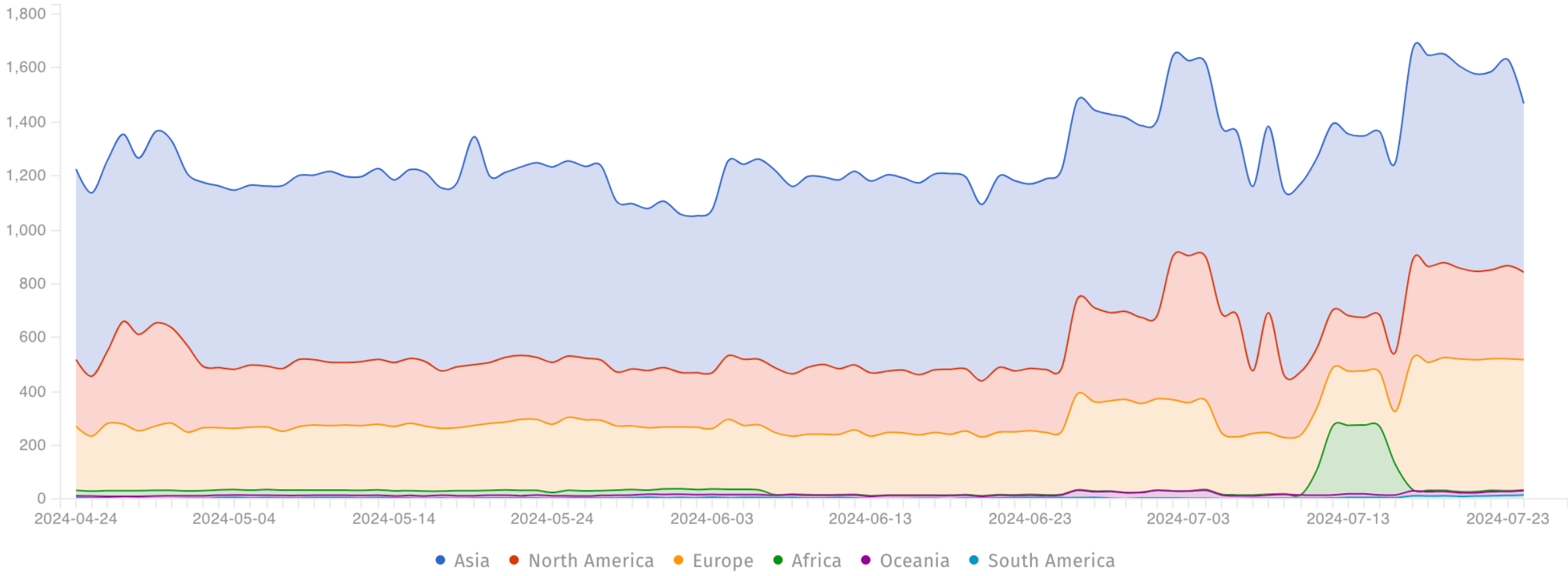
SHADOWSERVER

Post Exploitation Frameworks/C2

As seen in scans

TLP CLEAR

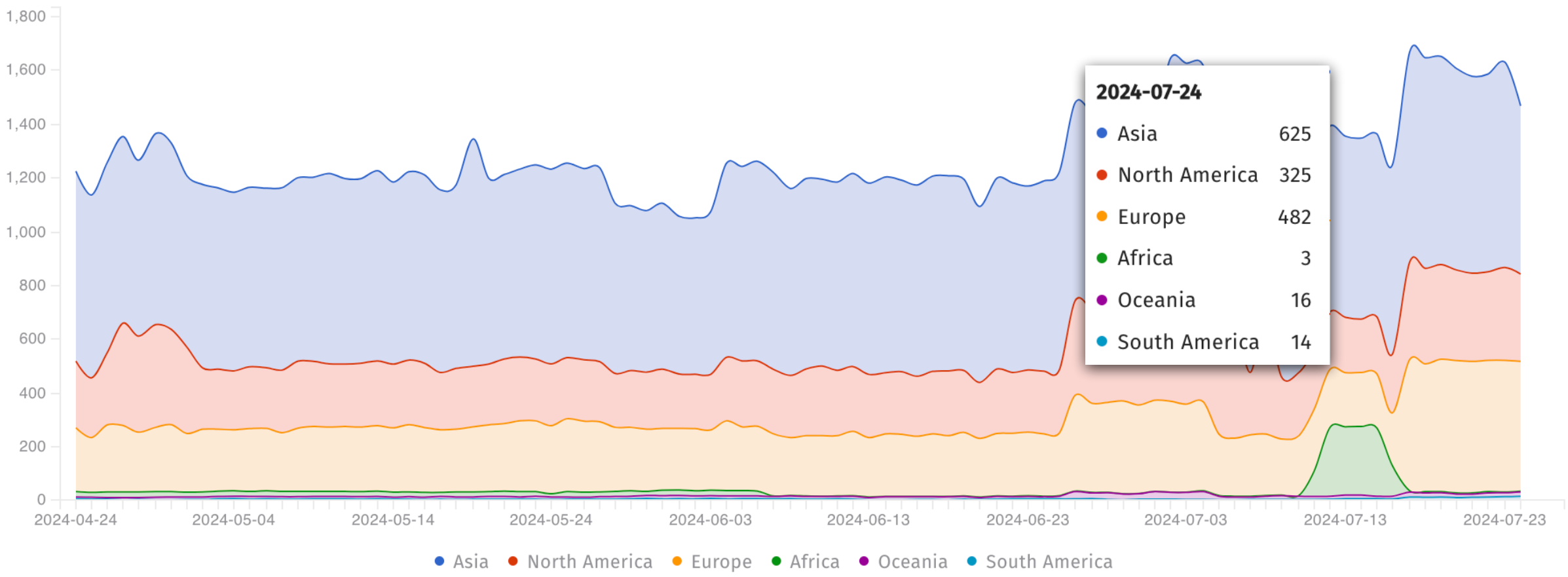
Post-Exploitation Frameworks - World



SHADOWSERVER

TLP CLEAR

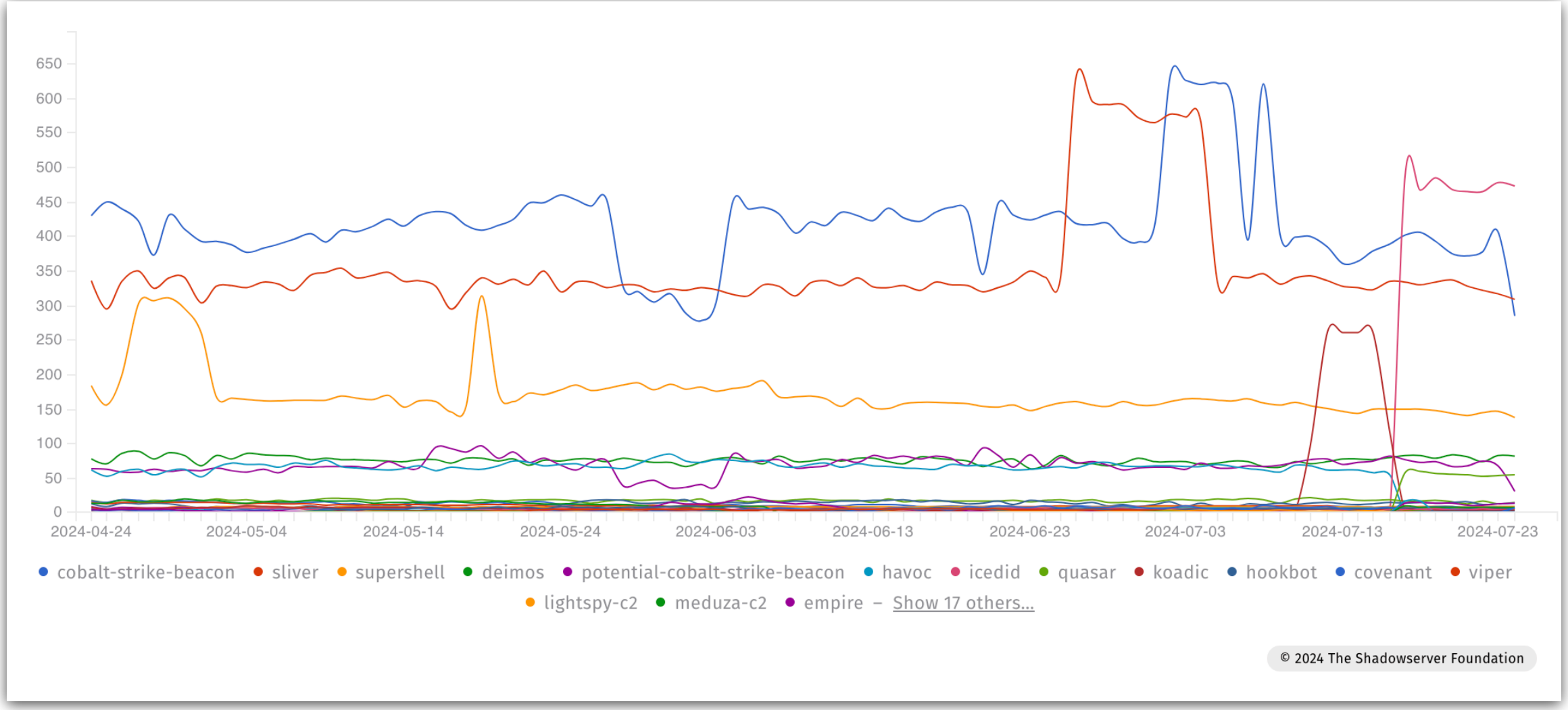
Post-Exploitation Frameworks - World



SHADOWSERVER

TLP CLEAR

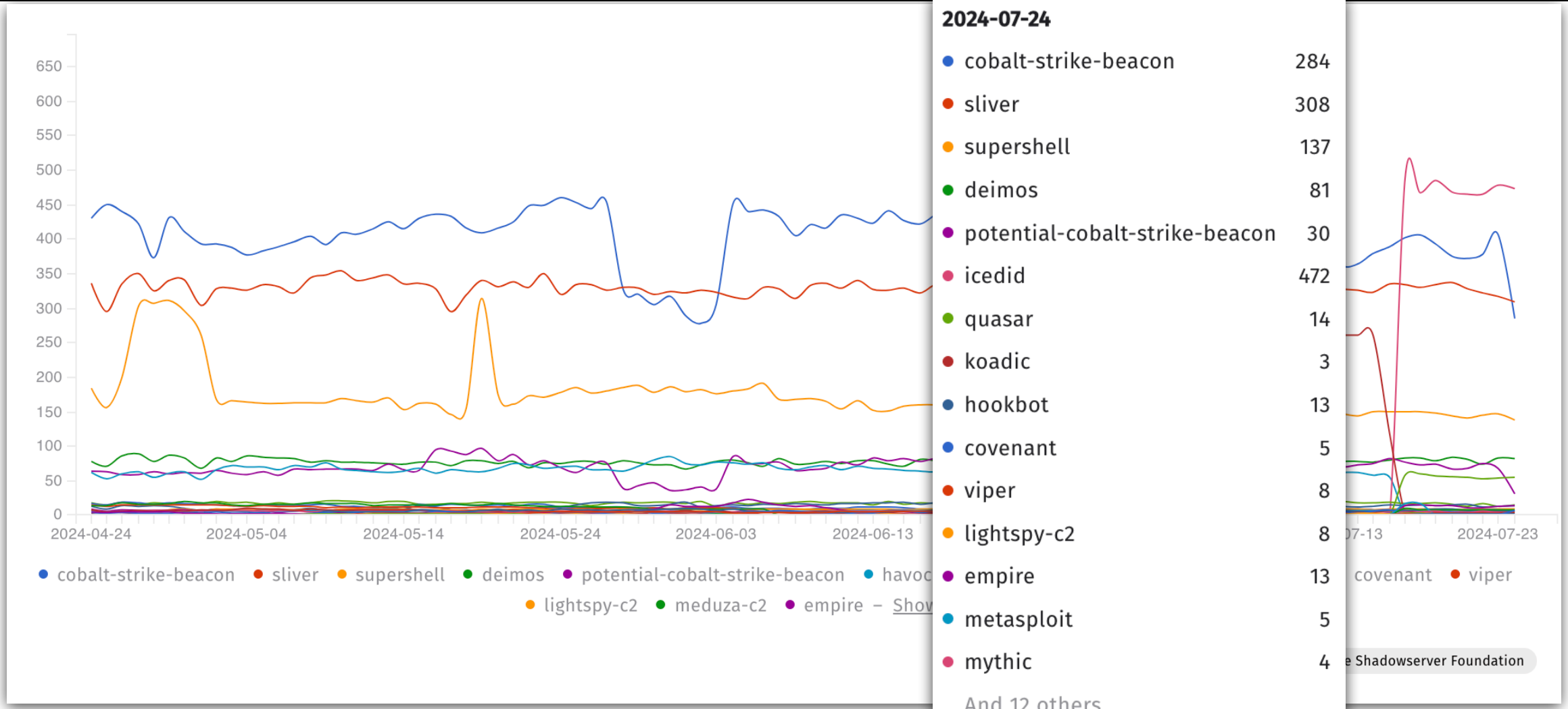
Post-Exploitation Frameworks by Type (World)



SHADOWSERVER

TLP CLEAR

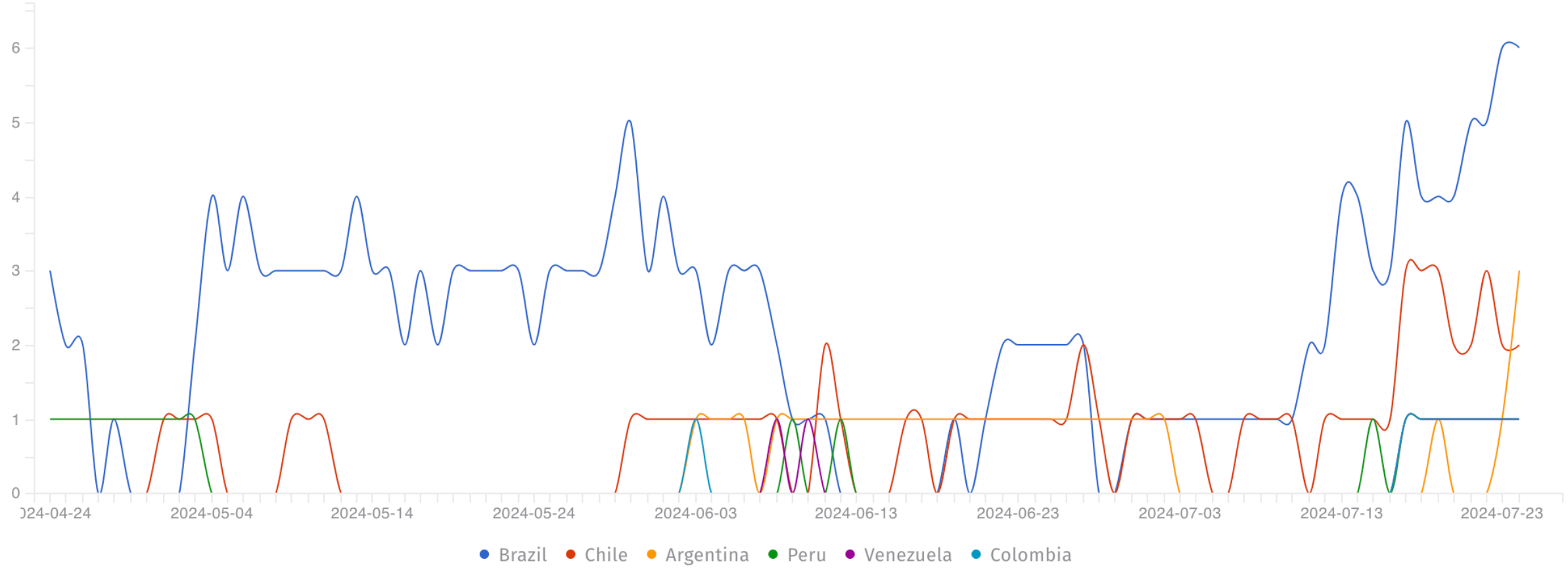
Post-Exploitation Frameworks by Type (World)



SHADOWSERVER

TLP CLEAR

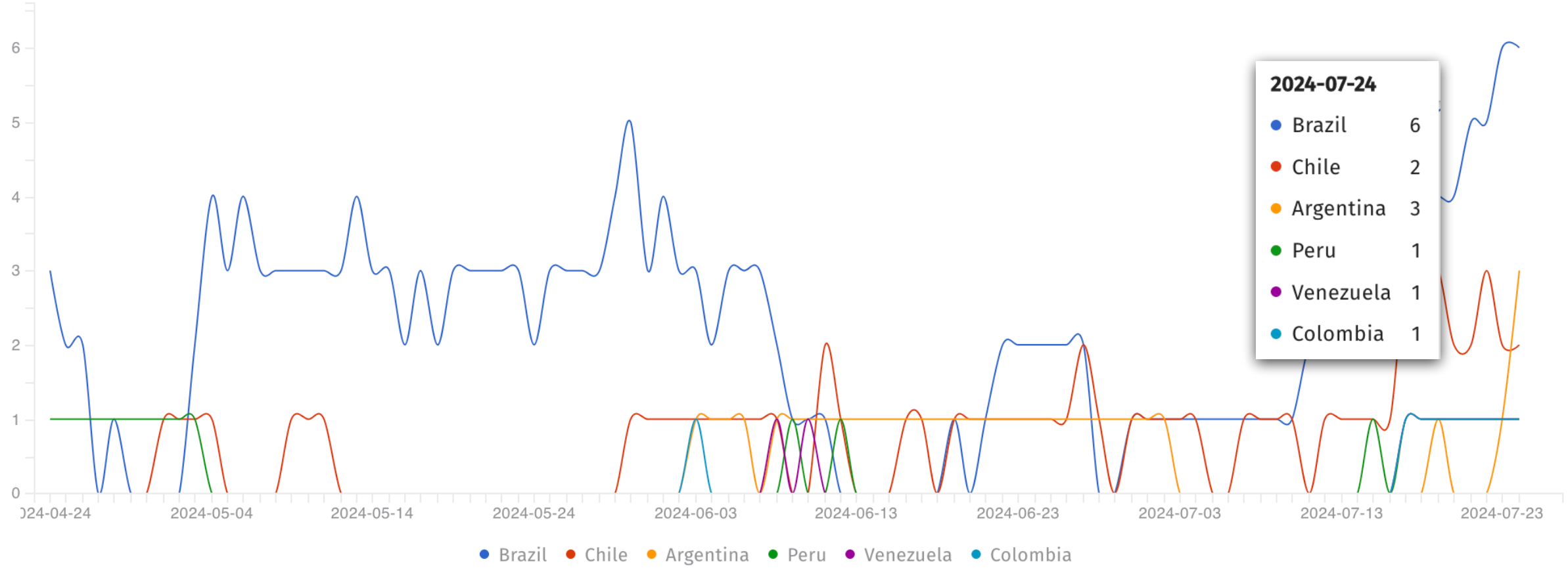
Post-Exploitation Frameworks (South America)



SHADOWSERVER

TLP CLEAR

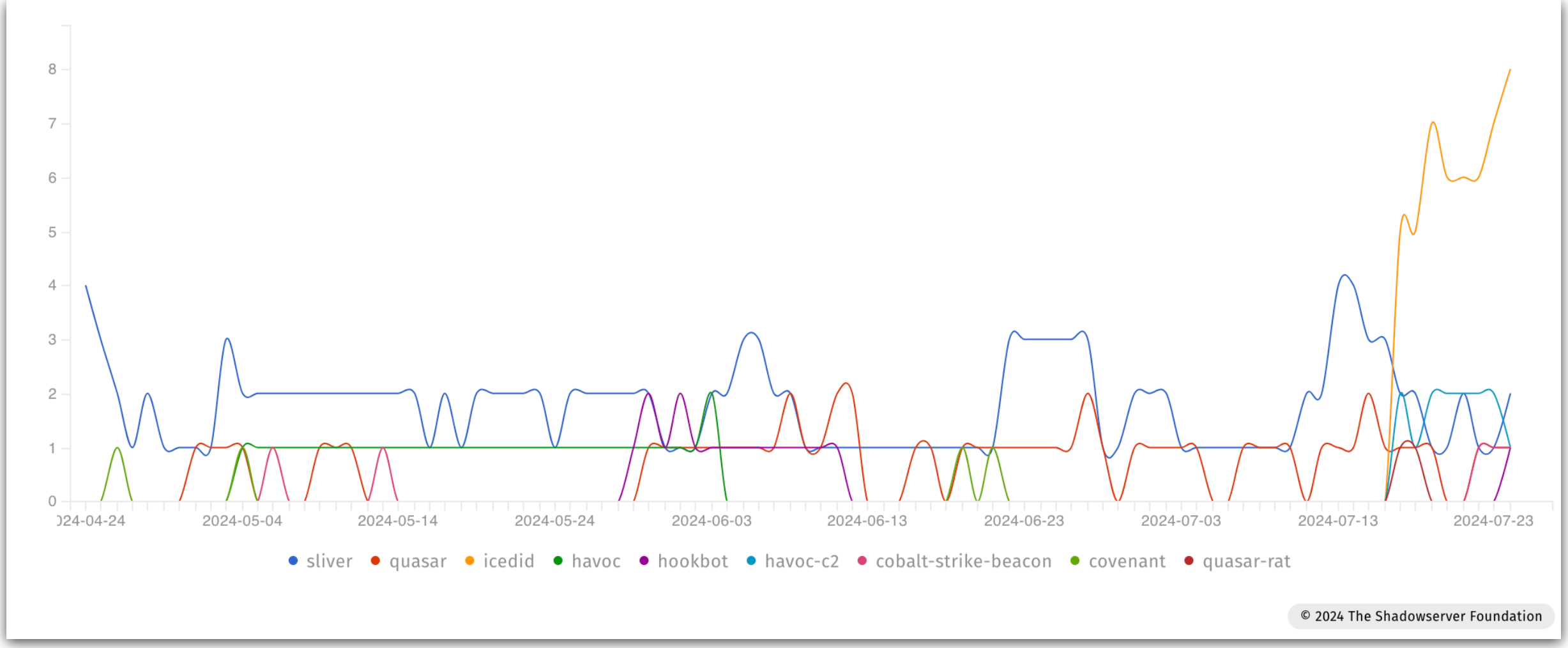
Post-Exploitation Frameworks (South America)



SHADOWSERVER

TLP CLEAR

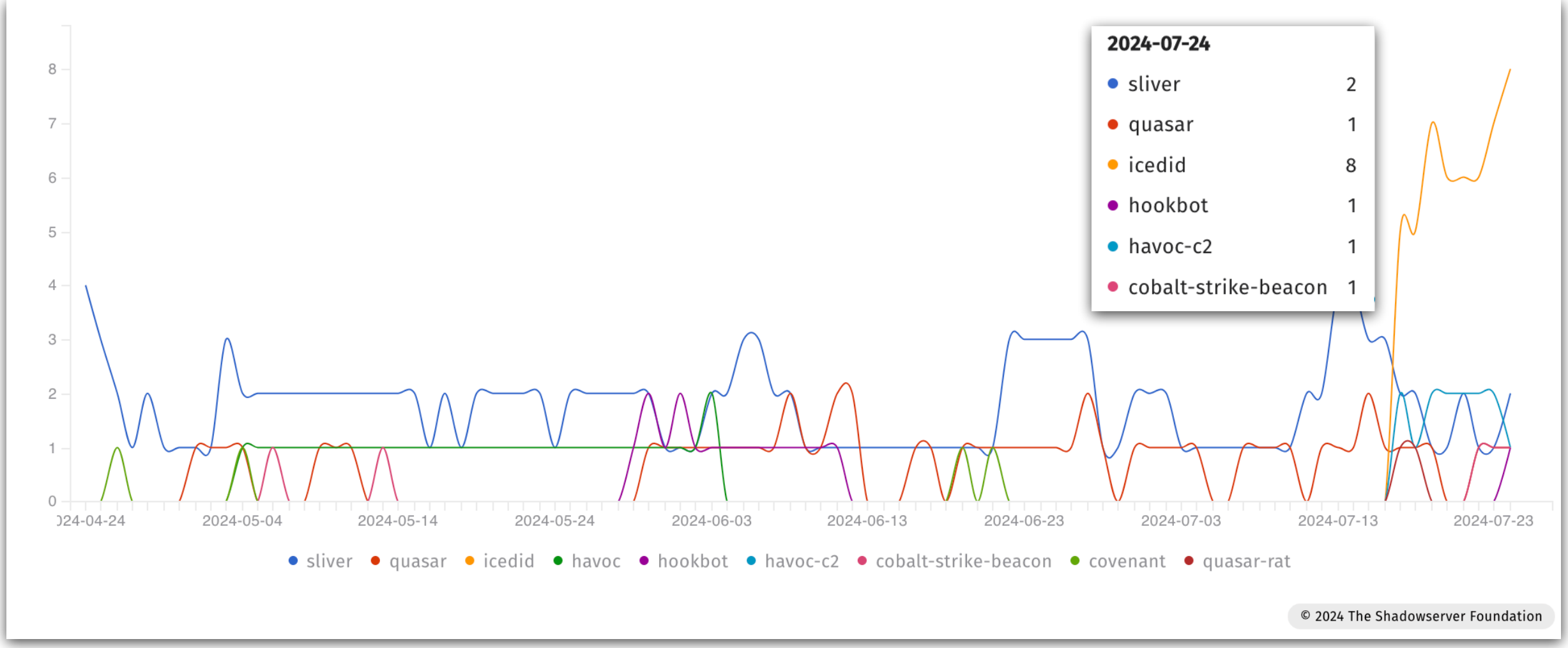
Post-Exploitation Frameworks by Type (South America)



SHADOWSERVER

TLP CLEAR

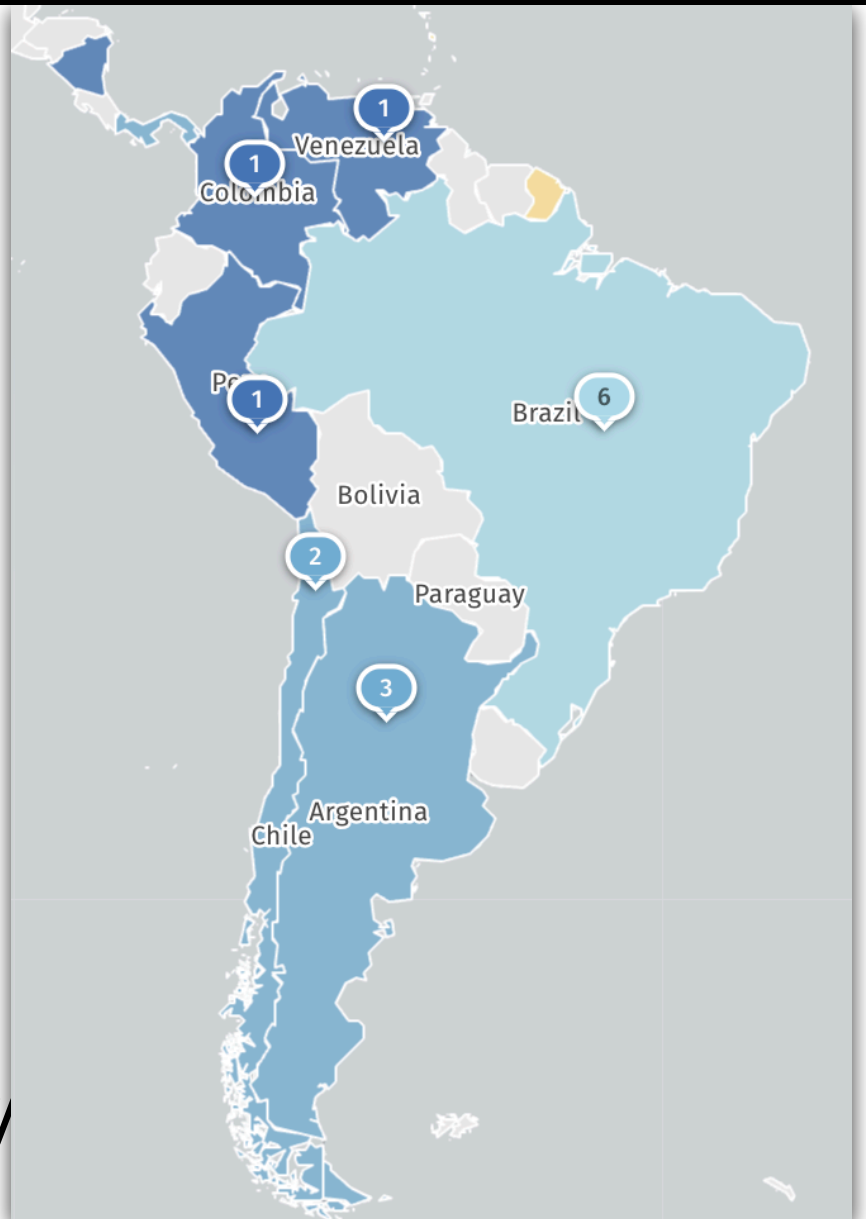
Post-Exploitation Frameworks by Type (South America)

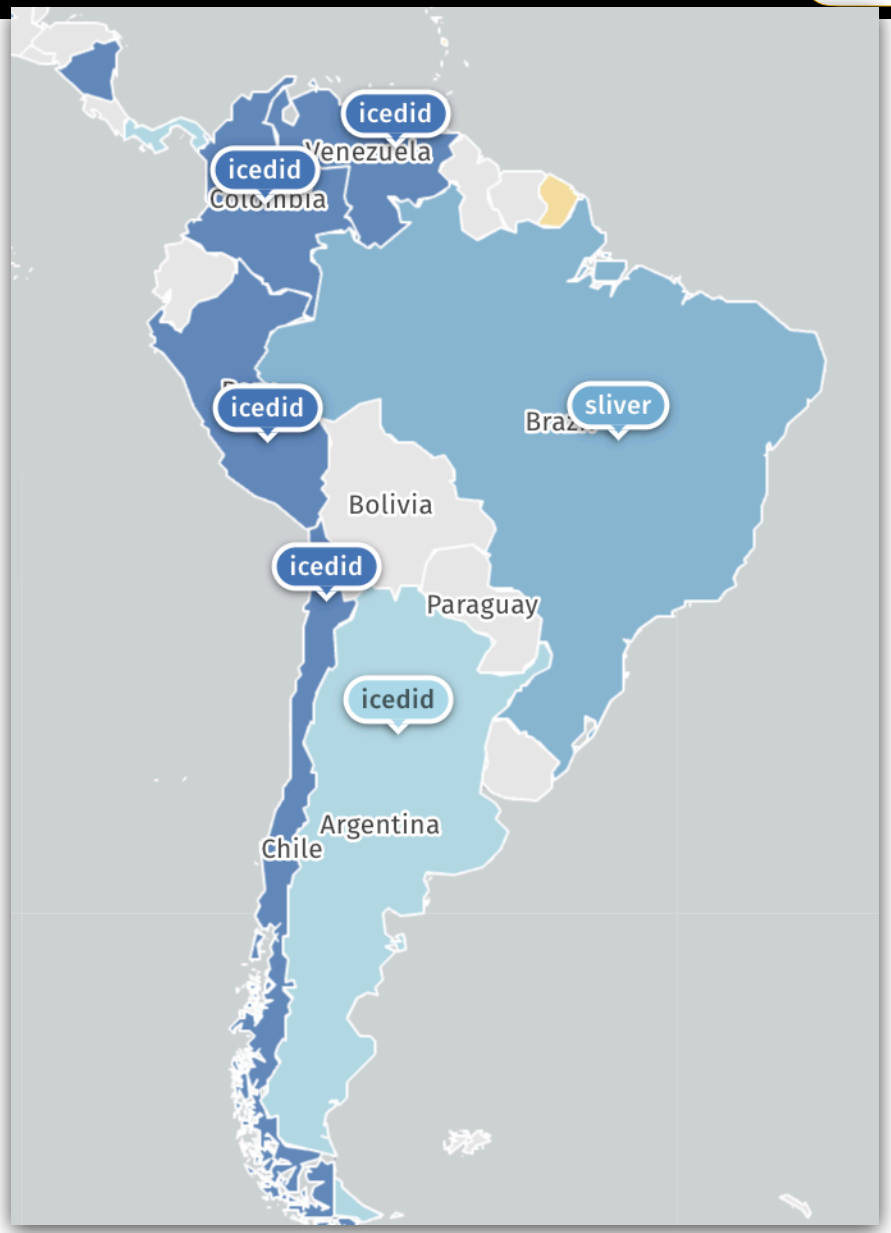


SHADOWSERVER

TLP CLEAR

Post-Exploitation Frameworks (South America - 2024-07-24)

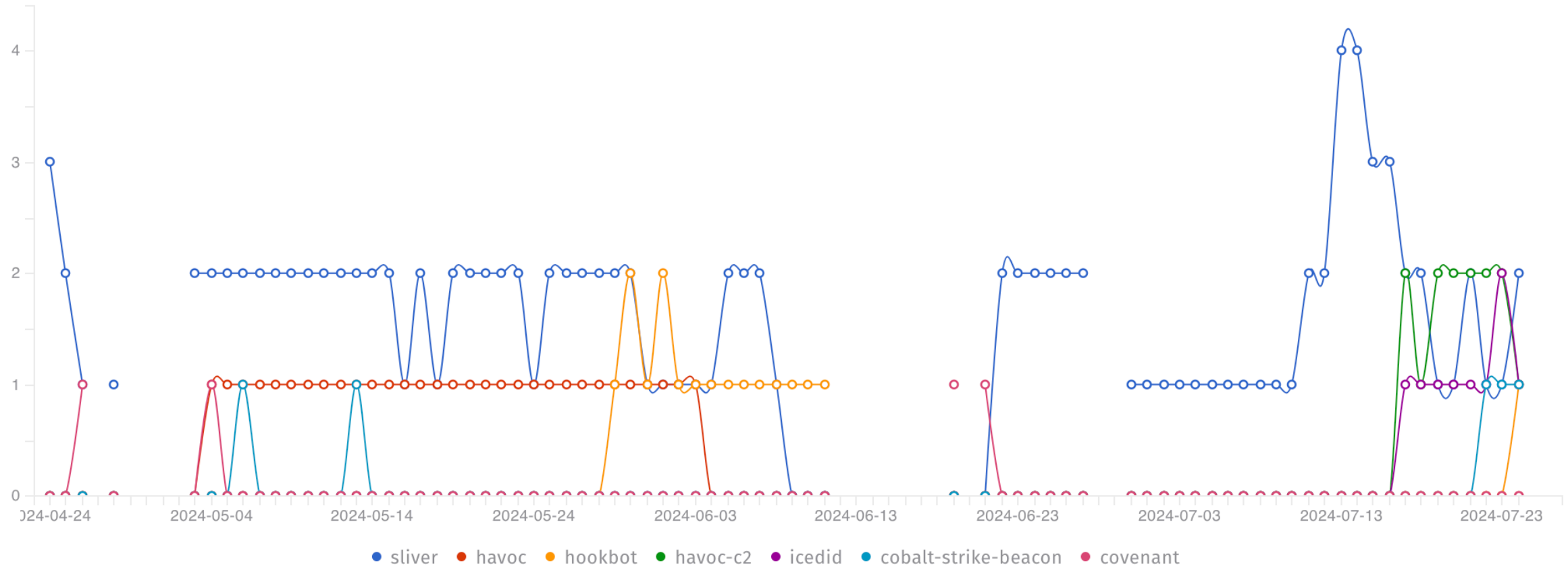




SHADOW

TLP CLEAR

Post-Exploitation Frameworks - Brazil



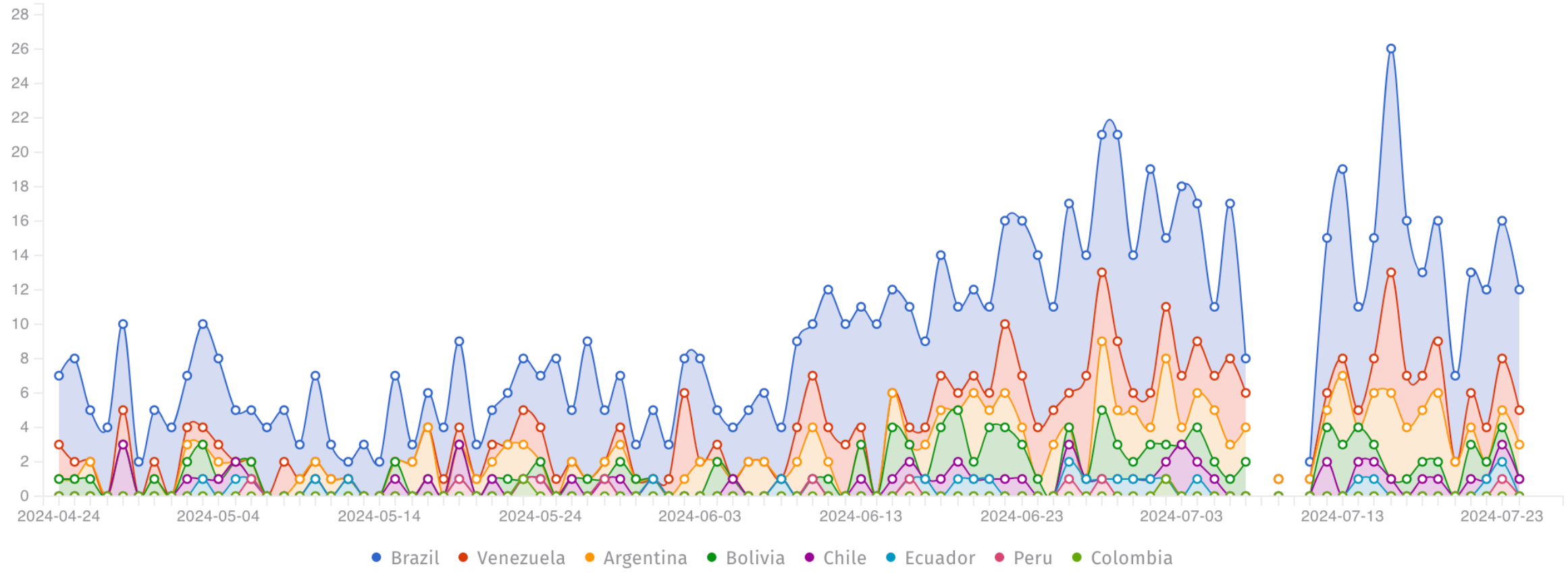
SHADOWSERVER

Malware URLs

Callbacks, C2s, Spreaders - a View from Honeypot sensors

TLP CLEAR

Malware URLs (Callbacks, C2s, Spreaders)



SHADOWSERVER

Last comments …

with a Summary

TLP CLEAR

Better Insights? Host a Honeypot Sensor …

- VM Sensor node spec
  - Ubuntu 22.04 LTS
  - 1 GB RAM
  - 30 GB disk
  - Preferably 4 publicly routable IPv4 (single NIC, no NAT, no network filtering) - but 2 is perfectly good too!
  - 1 Mbit/s uplink

SHADOWSERVER

Better Insights? Host a Honeypot Sensor …

- VM Sensor node spec
  - Ubuntu 22.04 LTS
  - 1 GB RAM
  - 30 GB disk
  - Preferably 4 publicly routable IPv4 (single NIC, no NAT, no network filtering) - but 2 is perfectly good too!
  - 1 Mbit/s uplink

TLP CLEAR

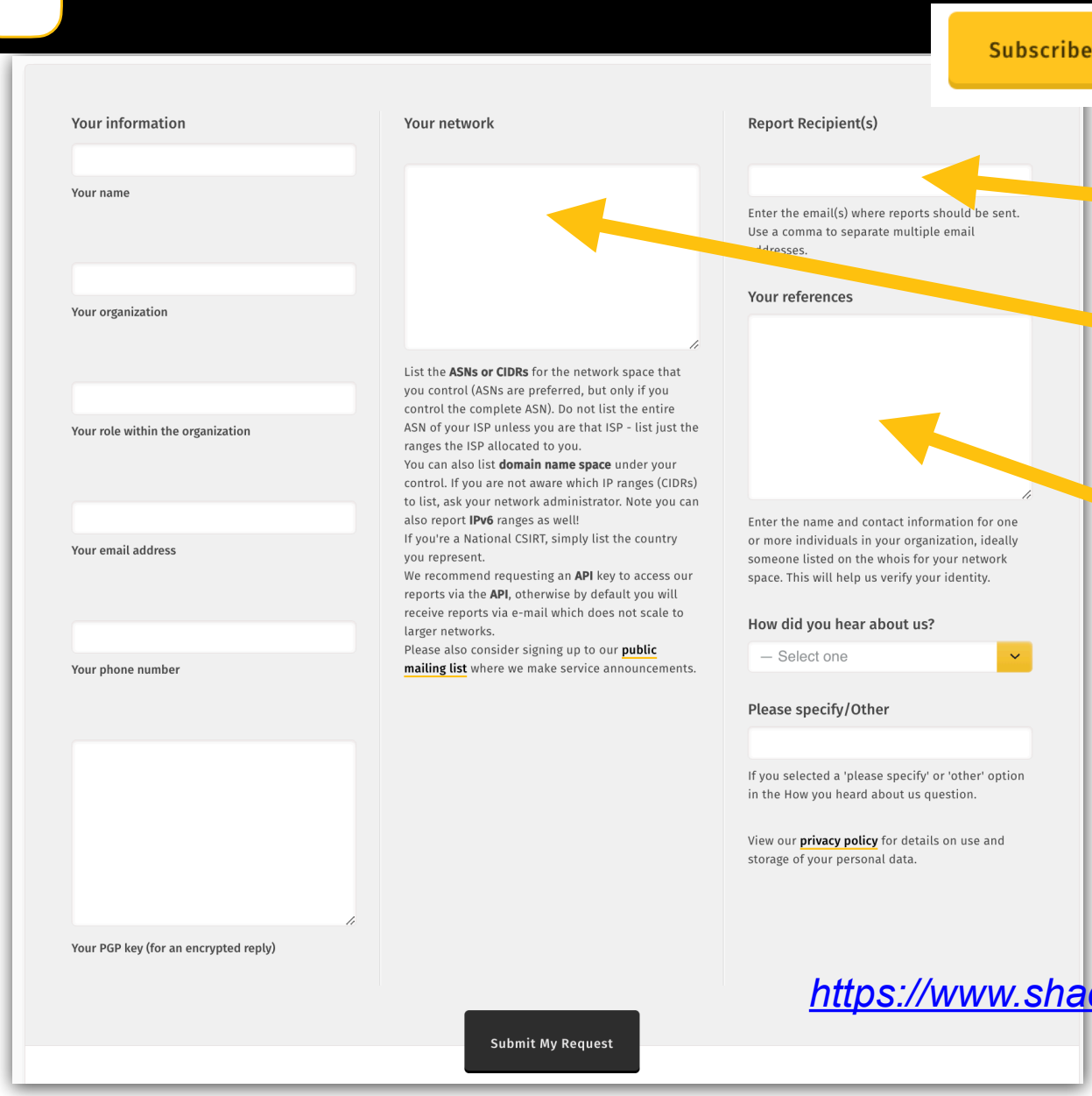
Takeaways

- There are free services available that can help the community understand new attacks/vulnerabilities as they emerge, serving as early warning
- These free services can help you understand your exposed assets (external attack surface) as well as identify potential compromised systems, for effective triage & victim notification
- The combination of Internet-wide scanning plus a global honeypot sensor network that can be quickly updated with new threat signatures enables rapid measurement and reporting of emerging threats
- Emerging or established threats can be disrupted by globally coordinated LEA actions, enabling new insights
- All the above helps to develop a “big picture” of the state of security/cyber-resilience of the Internet - such as the one presented in this talk
- Everyone benefits through improved sharing - subscribe to our free services, provide feedback & help us defend better against future threats. The more we receive local insights the more effective we can be!
- If your receive a report from Shadowserver please act!

SHADOWSERVER

TLP CLEAR

Subscribing to the Free Daily Network Reports



Email address where reports or download links will be sent

Network details, domains

Ask for an API key

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

Thank You!

SHADOWSERVER

Lighting the way to a more secure Internet

@shadowserver, @piotrkijewski

@shadowserver@infosec.exchange

https://www.linkedin.com/company/the-shadowserver-foundation/

contact@shadowserver.org

SHADOWSERVER.ORG