Collaborative Response to Emerging Critical RCE Vulnerabilities in Exposed Edge Devices

Piotr Kijewski, @piotrkijewski

piotr@shadowserver.org

September 24th, 2025
VB2025, Berlin

SHADOWSERVER.ORG

Introduction

What is the Shadowserver Foundation & what does it do?

The Shadowserver Foundation - Since 2004...

The Shadowserver Foundation - Since 2004...

US: 501c3 nonprofit organization

NL: “Stichting” w/ public benefit status

TLP CLEAR

The Shadowserver Foundation - Since 2004...

US: 501c3 nonprofit organization

NL: “Stichting” w/ public benefit status

SHADOWSERVER

Mission: make the Internet more secure for all

TLP CLEAR

The Shadowserver Foundation - Since 2004...

US: 501c3 nonprofit organization

NL: “Stichting” w/ public benefit status

Mission: make the Internet more secure for all

Share information with network defenders at **no cost** to mitigate vulnerabilities, detect malicious activity and counter emerging threats

SHADOWSERVER

The Shadowserver Foundation - Since 2004...

US: 501c3 nonprofit organization

NL: “Stichting” w/ public benefit status

We serve and partner with:

- National Computer Security Incident Response Teams (nCSIRTs)
- Network owners across all sectors of all types and sizes
- Law Enforcement
- Security researchers

Mission: make the Internet more secure for all

Share information with network defenders at **no cost** to mitigate vulnerabilities, detect malicious activity and counter emerging threats

TLP CLEAR

The Shadowserver Foundation - Since 2004...

US: 501c3 nonprofit organization

NL: “Stichting” w/ public benefit status

We serve and partner with:

- National Computer Security Incident Response Teams (nCSIRTs)
- Network owners across all sectors of all types and sizes
- Law Enforcement
- Security researchers

5 Primary Services:

- Attack Surface Monitoring & Victim Notification Services
- Large Scale (Internet-wide) Early Warning
- Law Enforcement investigations & operations support
- Cybersecurity Capacity Building
- Funded Public Benefit Projects

SHADOWSERVER

Mission: make the Internet more secure for all

Share information with network defenders at **no cost** to mitigate vulnerabilities, detect malicious activity and counter emerging threats

TLP CLEAR

The Shadowserver Foundation - Since 2004...

US: 501c3 nonprofit organization

NL: “Stichting” w/ public benefit status

We serve and partner with:

- National Computer Security Incident Response Teams (nCSIRTs)
- Network owners across all sectors of all types and sizes
- Law Enforcement
- Security researchers

<u>Funded by:</u>

- Grants
- Donations
- Sponsorships
- At cost project work
- Alliance partnerships

SHADOWSERVER

<u>Mission</u>: make the Internet more secure for all

Share information with network defenders at **no cost** to mitigate vulnerabilities, detect malicious activity and counter emerging threats

Who does the Shadowserver Foundation Serve?

TLP CLEAR

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries
covering 175 countries & territories

SHADOWSERVER

TLP CLEAR

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries covering 175 countries & territories

Sectoral CERTs and ISACs

SHADOWSERVER

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries covering 175 countries & territories

Sectoral CERTs and ISACs

Regional, State, City, Local Government CERTs

TLP CLEAR

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries covering 175 countries & territories

Sectoral CERTs and ISACs

Regional, State, City, Local Government CERTs

Hospitals & Healthcare Sector

SHADOWSERVER

TLP CLEAR

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries covering 175 countries & territories

Sectoral CERTs and ISACs

Regional, State, City, Local Government CERTs

Hospitals & Healthcare Sector

Universities and Local School Districts

SHADOWSERVER

TLP CLEAR

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries covering 175 countries & territories

Sectoral CERTs and ISACs

Regional, State, City, Local Government CERTs

Hospitals & Healthcare Sector

Universities and Local School Districts

NGOs, underserved regions

SHADOWSERVER

TLP CLEAR

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries covering 175 countries & territories

Critical infrastructure including water, power, utility companies

Sectoral CERTs and ISACs

Regional, State, City, Local Government CERTs

Hospitals & Healthcare Sector

Universities and Local School Districts

NGOs, underserved regions

SHADOWSERVER

TLP CLEAR

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries covering 175 countries & territories

Sectoral CERTs and ISACs

Regional, State, City, Local Government CERTs

Hospitals & Healthcare Sector

Universities and Local School Districts

NGOs, underserved regions

Critical infrastructure including water, power, utility companies

Internet Service Providers, Hosting & Content Providers

SHADOWSERVER

TLP CLEAR

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries covering 175 countries & territories

Sectoral CERTs and ISACs

Regional, State, City, Local Government CERTs

Hospitals & Healthcare Sector

Universities and Local School Districts

NGOs, underserved regions

Critical infrastructure including water, power, utility companies

Internet Service Providers, Hosting & Content Providers

Airline, Defence, Maritime, Space Industries

SHADOWSERVER

TLP CLEAR

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries covering 175 countries & territories

Sectoral CERTs and ISACs

Regional, State, City, Local Government CERTs

Hospitals & Healthcare Sector

Universities and Local School Districts

NGOs, underserved regions

Critical infrastructure including water, power, utility companies

Internet Service Providers, Hosting & Content Providers

Airline, Defence, Maritime, Space Industries

Retail, Hospitality, Packaging

SHADOWSERVER

TLP CLEAR

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries covering 175 countries & territories

Sectoral CERTs and ISACs

Regional, State, City, Local Government CERTs

Hospitals & Healthcare Sector

Universities and Local School Districts

NGOs, underserved regions

Critical infrastructure including water, power, utility companies

Internet Service Providers, Hosting & Content Providers

Airline, Defence, Maritime, Space Industries

Retail, Hospitality, Packaging

Manufacturing, Mining

SHADOWSERVER

TLP CLEAR

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries covering 175 countries & territories

Sectoral CERTs and ISACs

Regional, State, City, Local Government CERTs

Hospitals & Healthcare Sector

Universities and Local School Districts

NGOs, underserved regions

Critical infrastructure including water, power, utility companies

Internet Service Providers, Hosting & Content Providers

Airline, Defence, Maritime, Space Industries

Retail, Hospitality, Packaging

Manufacturing, Mining

Grocery stores, Food suppliers

SHADOWSERVER

TLP CLEAR

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries covering 175 countries & territories

Sectoral CERTs and ISACs

Regional, State, City, Local Government CERTs

Hospitals & Healthcare Sector

Universities and Local School Districts

NGOs, underserved regions

Critical infrastructure including water, power, utility companies

Internet Service Providers, Hosting & Content Providers

Airline, Defence, Maritime, Space Industries

Retail, Hospitality, Packaging

Manufacturing, Mining

Grocery stores, Food suppliers

Small Businesses to Fortune 500 companies

SHADOWSERVER

TLP CLEAR

Who does the Shadowserver Foundation Serve?

201 National CSIRT teams from 135 countries covering 175 countries & territories

Critical infrastructure including water, power, utility companies

Sectoral CERTs and ISACs

Internet Service Providers, Hosting & Content Providers

Regional, State, City, Local Government CERTs

Airline, Defence, Maritime, Space Industries

Hospitals & Healthcare Sector

Retail, Hospitality, Packaging

Universities and Local School Districts

Manufacturing, Mining

NGOs, underserved regions

Grocery stores, Food suppliers

Law Enforcement Organizations

Small Businesses to Fortune 500 companies

SHADOWSE

TLP CLEAR

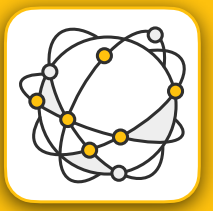
What does The Shadowserver Foundation do?

- **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 ~3.2 Billion IPv6 addresses many times a day looking for different types of vulnerable, potentially 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

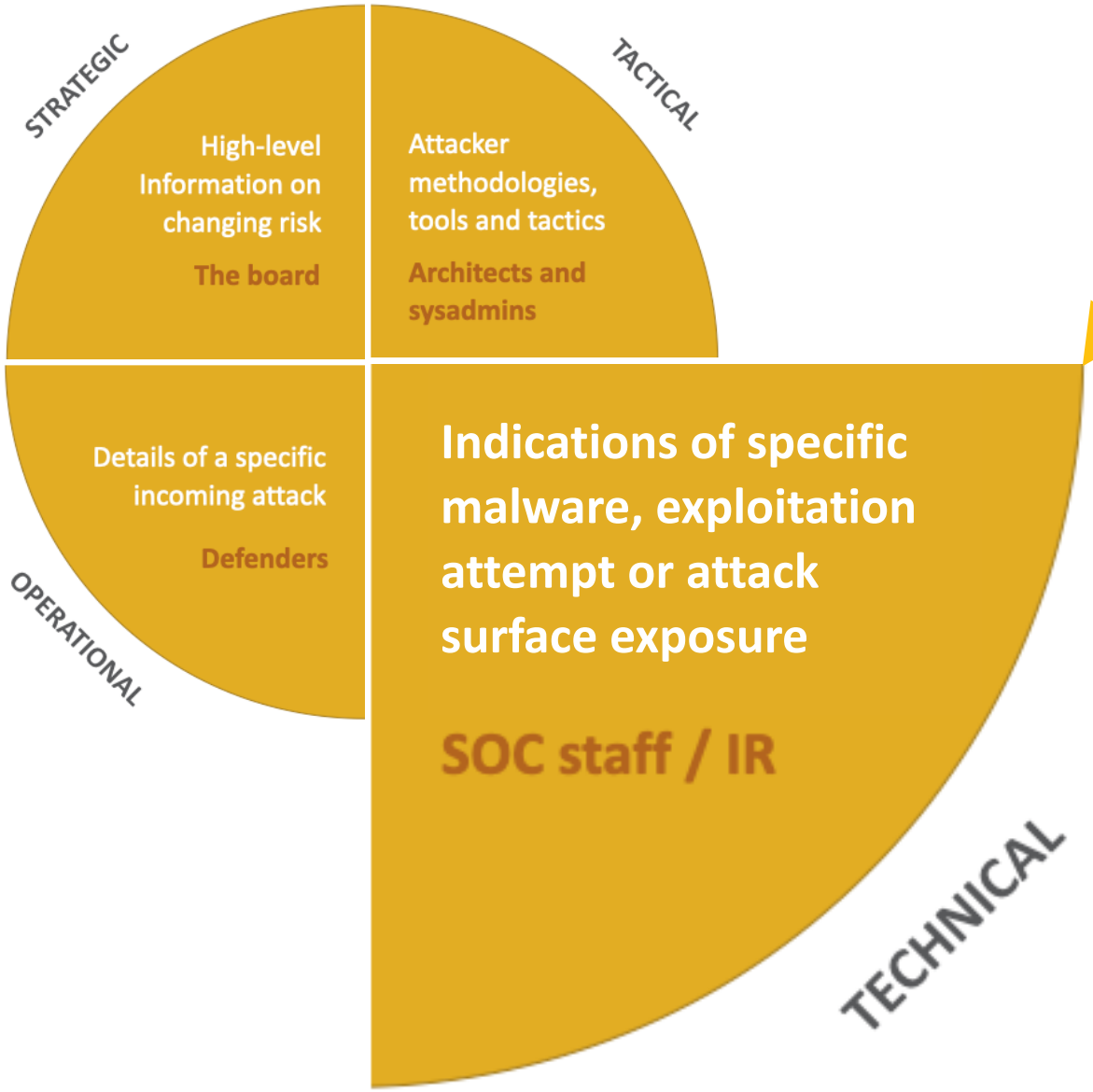
Our Sharing Model: Who Gets The Data?

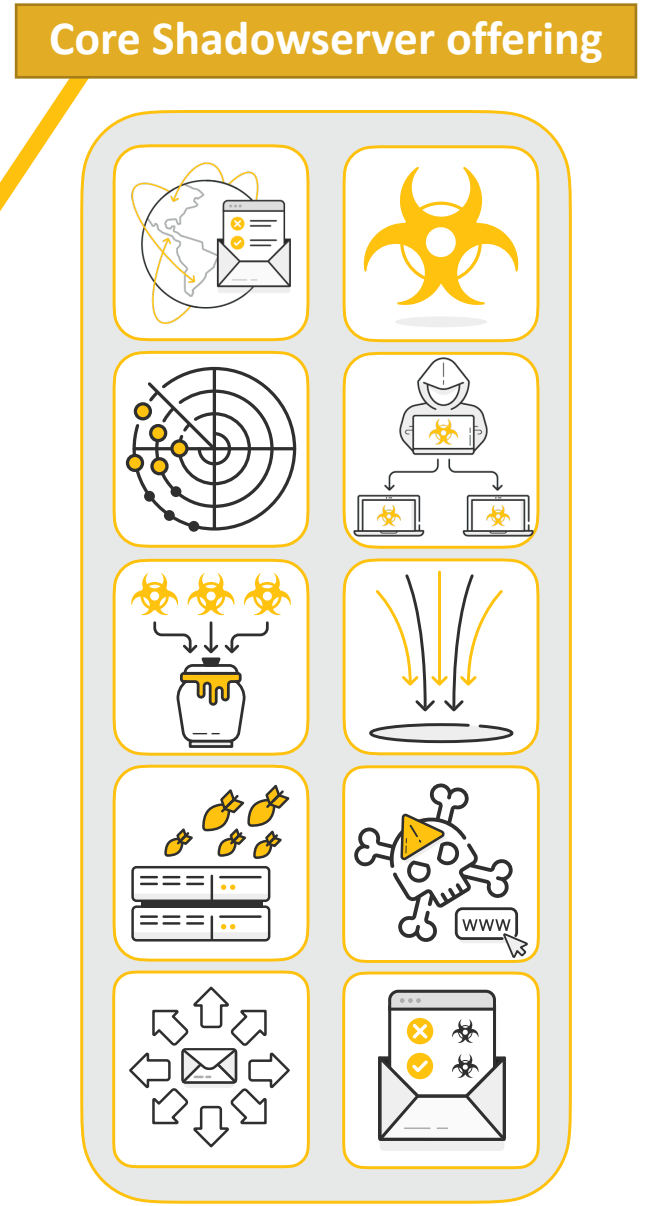
	National CSIRTs	Network Owners	Law Enforcement
Who?			
What Data?	Sliced Geographically (no cost)	Sliced by defined IP Address Space / ASN / CIDR /Domains (no cost, regardless of size)	Limited to specific investigation needs, intel only (no cost)
MSSP Model?	nCSIRT can delegate all/ part to 3rd parties for processing, we will accommodate (no cost)	Network Owner can delegate all/part to 3rd parties for processing, we will accommodate (no cost)	

(MSSP model must be at end user request)

MSSP = Managed Security Service Provider

TLP
CLEAR


STRATEGIC
High-level Information on changing risk
The board
TACTICAL
Attacker methodologies, tools and tactics
Architects and sysadmins
OPERATIONAL
Details of a specific incoming attack
Defenders
Indications of specific malware, exploitation attempt or attack surface exposure
SOC staff / IR
TECHNICAL


Core Shadowserver offering
www

TLP CLEAR

Free Daily Remediation Reports - National CSIRTs and Network Owners

Network Reporting

Every day, Shadowserver sends custom remediation reports to more than **9000 vetted subscribers**, including over **201 national CSIRTs in 175 countries** and territories. 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

Free Daily Remediation Reports - National CSIRTs and Network Owners

Network Reporting

Every day, Shadowserver sends custom remediation reports to more than **9000 vetted subscribers**, including over **201 national CSIRTs in 175 countries** and t
detailed, targeted, r

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
					Sandbox URL	Synful Scan
					Sandbox Connection	Vulnerable ISAKMP
					Sandbox IRC	Accessible Cisco Smart Install
					Sandbox SMTP	Accessible FTP/RDP

1 BILLION events shared EACH DAY!

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

The Bad Actor's Network Visibility

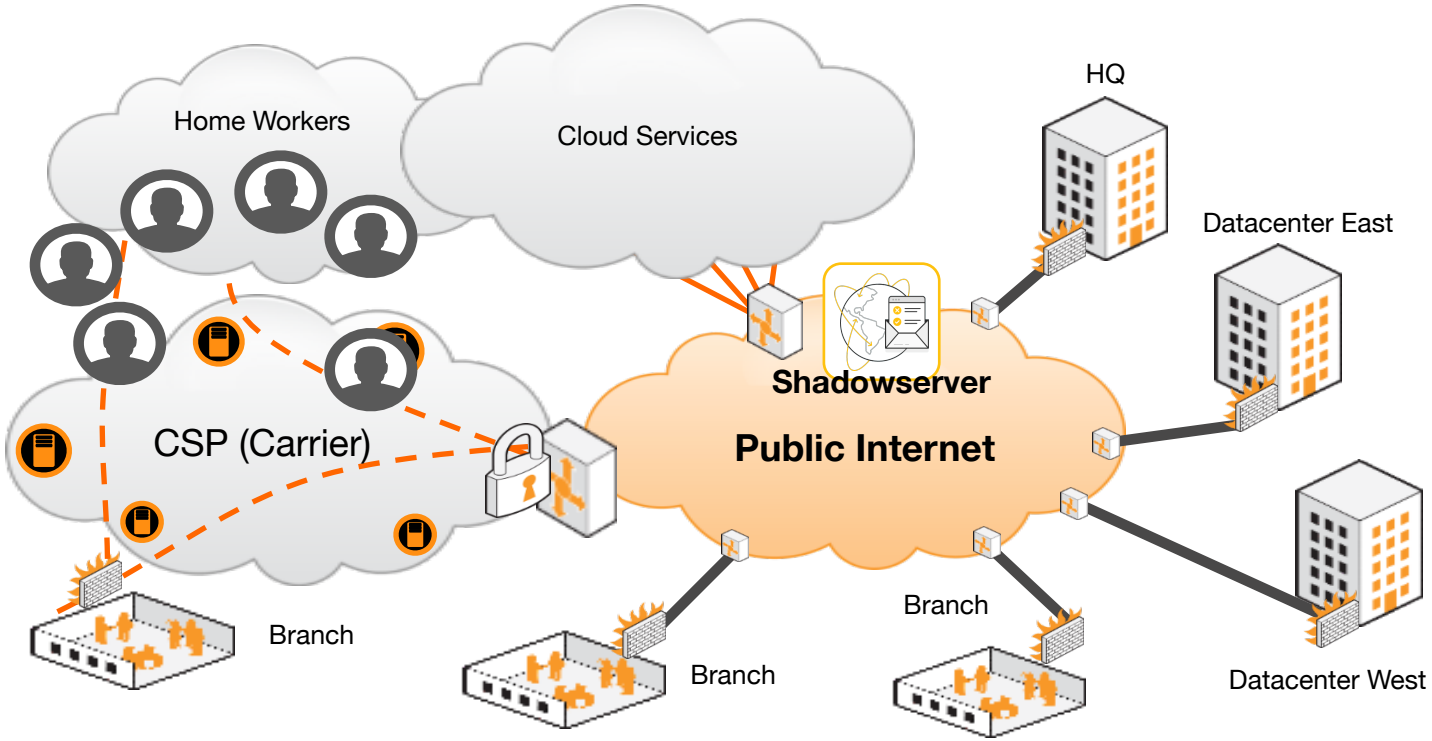
What can others see when looking into your network from the outside?

What is your organization's risk?

If you are using cloud services that dynamically change IPs you can submit these changes automatically

Shadowserver's daily Network Reporting is tuned by:

- ASNs for the organization
- CIDR Blocks (including IPv6)
- Delegated IP Blocks (Cloud)
- Domains (including entire TLDs)
- Geo-location (for National CSIRTs)



SHADOWSERVER

TLP CLEAR

Subscribing to the Free Daily Network Reports

Subscribe to Reports

Your information

Your name

Your organization

Your role within the organization

Your email address

Your phone number

Your PGP key (for an encrypted reply)

Your network

List the **ASNs or CIDRs** for the network space that you control (ASNs are preferred, but only if you control the complete ASN). Do not list the entire ASN of your ISP unless you are that ISP - list just the ranges the ISP allocated to you.
You can also list **domain name space** under your control. If you are not aware which IP ranges (CIDRs) to list, ask your network administrator. Note you can also report **IPv6** ranges as well!
If you're a National CSIRT, simply list the country you represent.
We recommend requesting an **API** key to access our reports via the **API**, otherwise by default you will receive reports via e-mail which does not scale to larger networks.
Please also consider signing up to our **public mailing list** where we make service announcements.

Report Recipient(s)

Enter the email(s) where reports should be sent. Use a comma to separate multiple email addresses.

Your references

Enter the name and contact information for one or more individuals in your organization, ideally someone listed on the whois for your network space. This will help us verify your identity.

How did you hear about us?

— Select one

Please specify/Other

If you selected a 'please specify' or 'other' option in the How you heard about us question.

View our **privacy policy** for details on use and storage of your personal data.

Submit My Request

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/

TLP CLEAR

Shadowserver's 2020+ Data Center

- California
- Caged & secure
- 68 Server Racks (16 Dark)
- 1078 physical servers, 14.2 petabytes storage
- 1751 worker VMs
- 2127 CPUs with 30,812 CPU cores and 142.6 TB RAM
- 4 x 10GB Internet uplinks
- Full backup power, 323kWh capacity
- $30-40M total infrastructure = mid sized enterprise

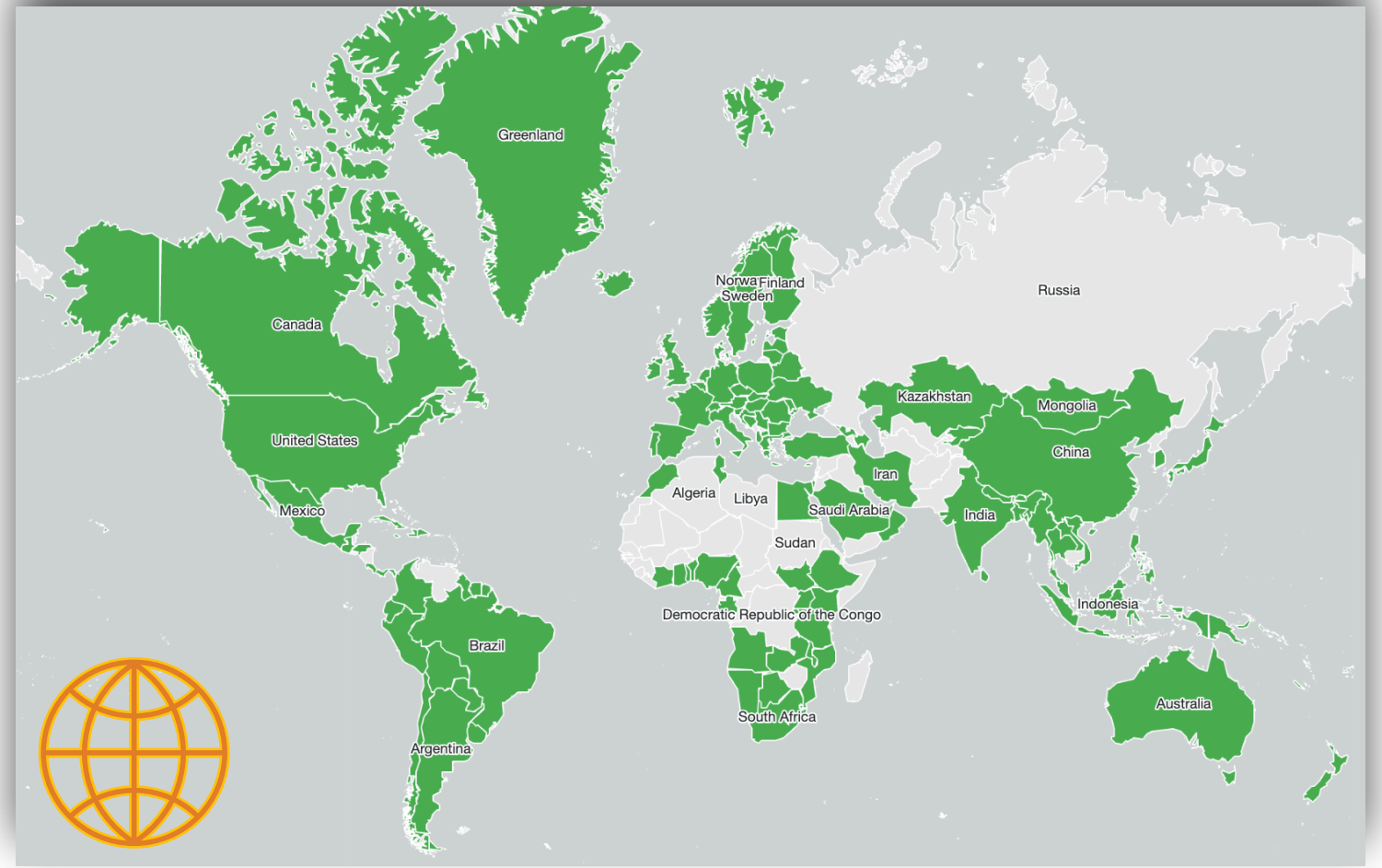
May 2023

SHADOWSERVER

https://www.shadowserver.org/news/the-data-center-move-all-the-gory-details-and-extras/

TLP CLEAR

“Global Plumbing” - nCSIRT Coverage



201 nCSIRTs
(175 Countries)

+

9000+ Network Owners (Direct)

+ many more (Indirect)

Every Day
Free!

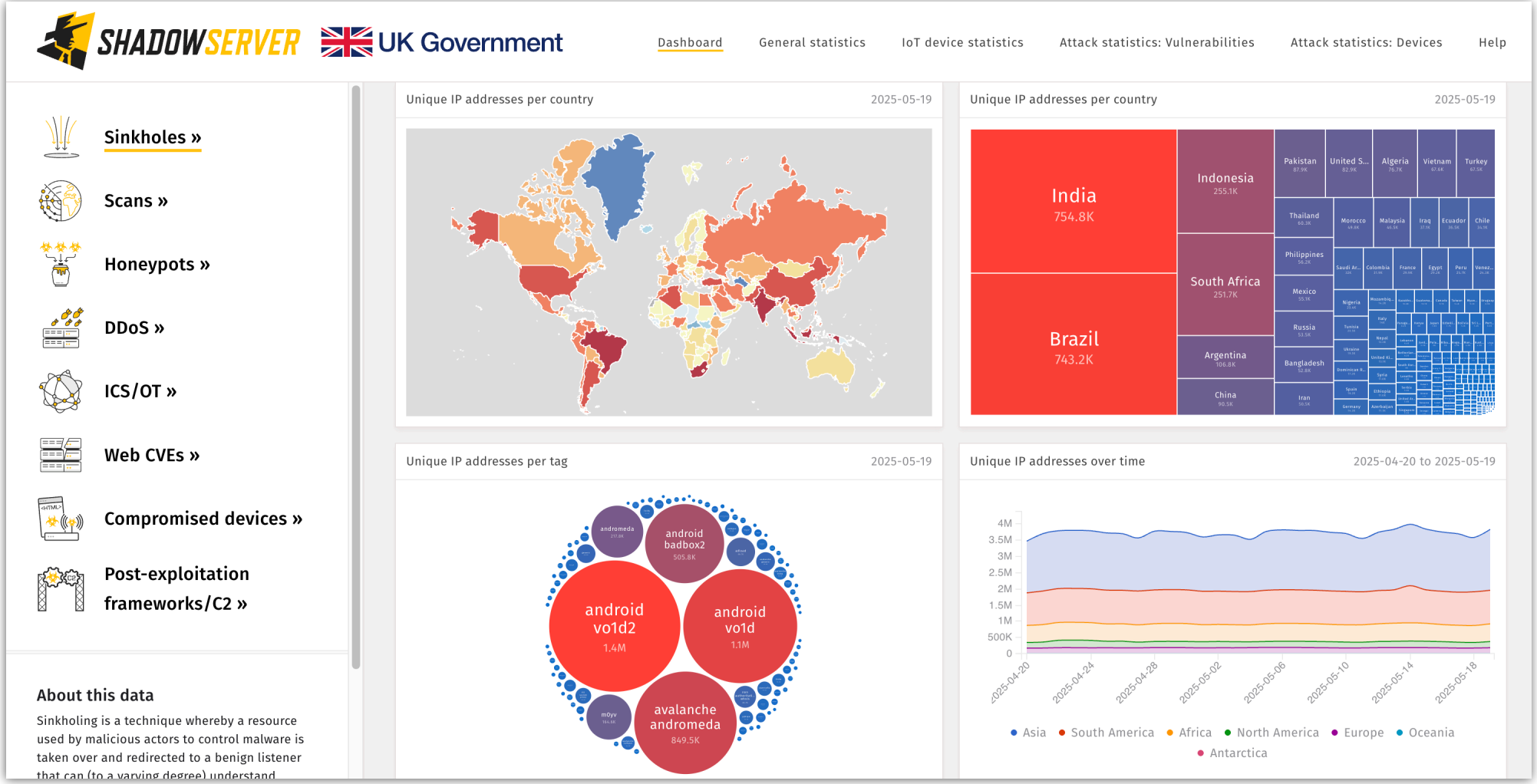
SHADOWSERVER

Shadowserver ASN Coverage By Continent (Sep 2025)

Europe	**69%**
North America	76%
Oceania	73%
Africa	47%
South America	41%
Asia	30%

TLP CLEAR

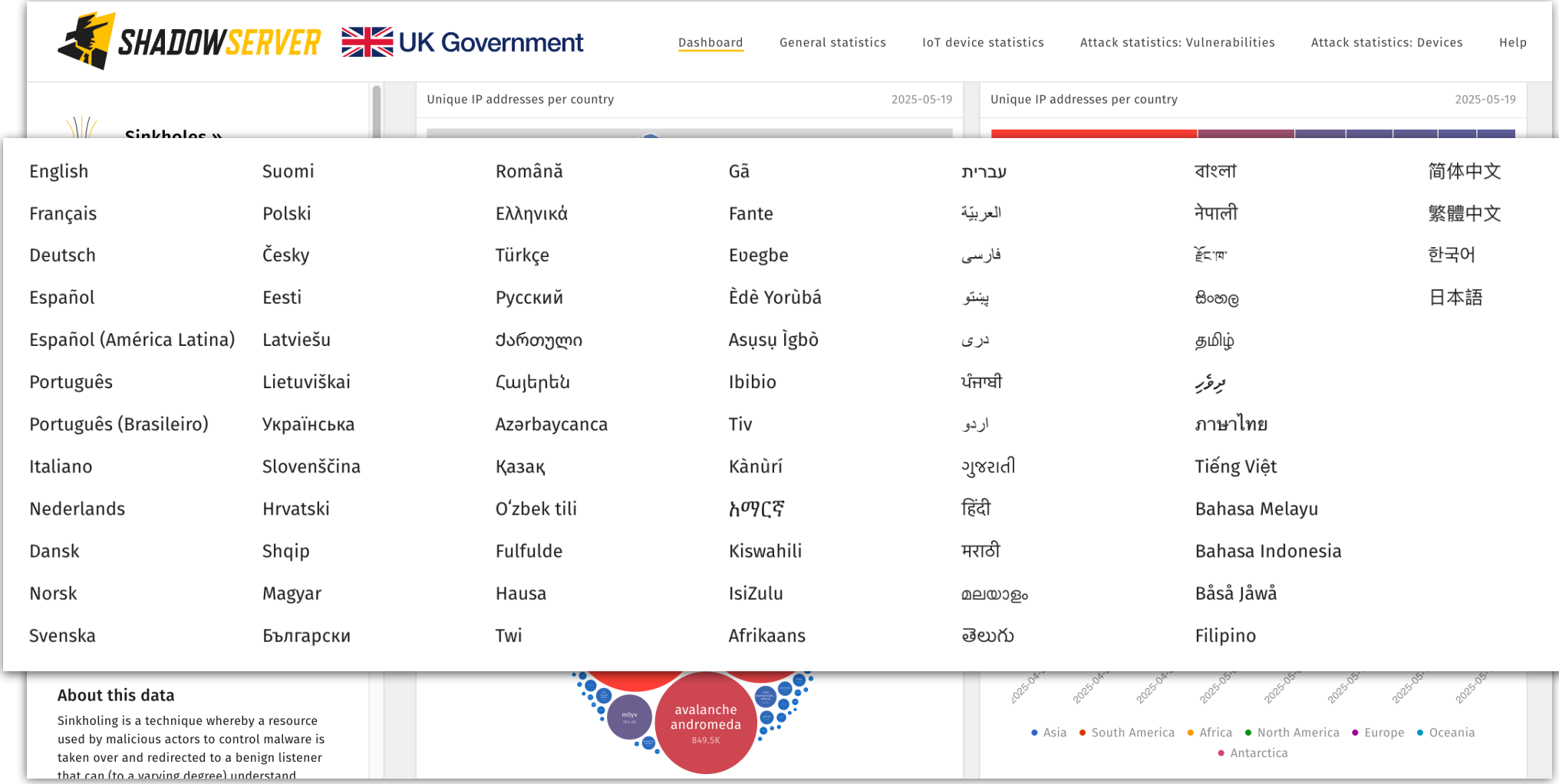
Shadowserver Public Dashboard



SHADOWSERVER

https://dashboard.shadowserver.org

Shadowserver Public Dashboard



SHADOWSERVER

https://dashboard.shadowserver.org

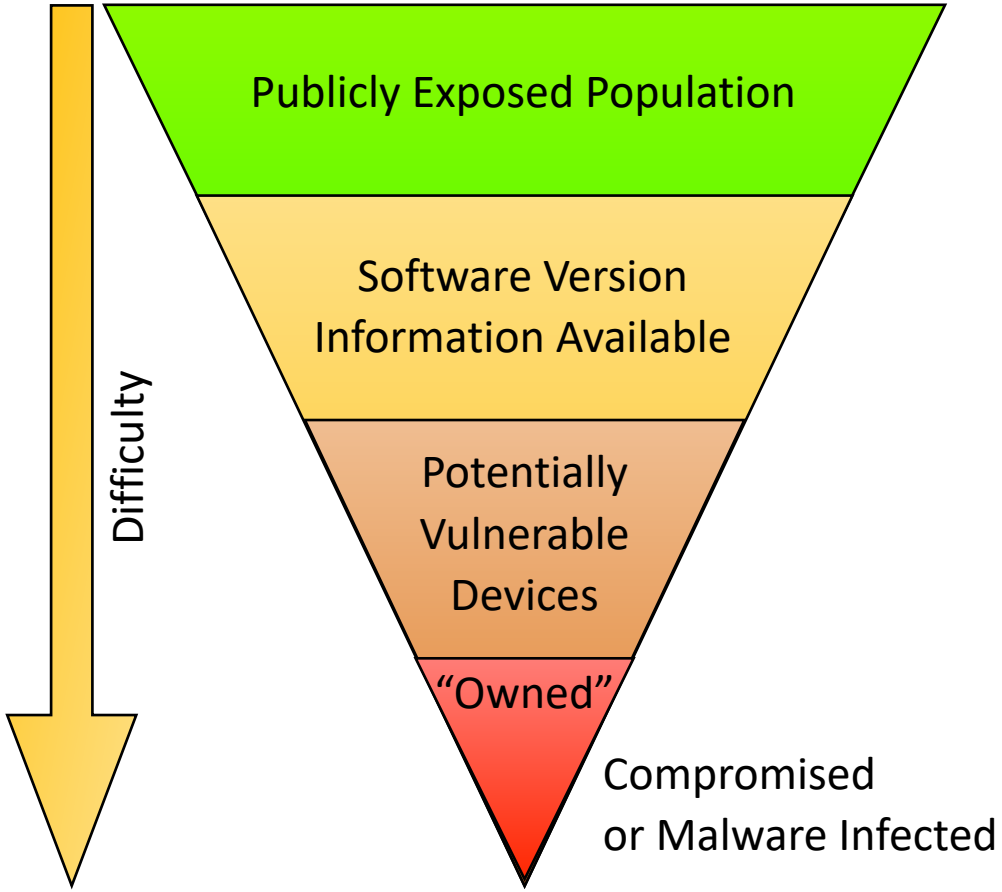
Internet-wide scanning

Fingerprinting all things

Shadowserver's Internet-wide Scanning

Critical to understand which devices are exposed to public Internet:
Attack Surface Management (ASM)

- Generic scans across hundreds protocols/ports, results used for identifying specific type, vendor & product
- Targeted vulnerability scans for most critical Remote Code Execution (RCE) in exposed assets
- Target compromised device scans (if possible)
- Key Points:
  - 24-hour cycle
  - Data only shared with network owner*



TLP CLEAR

New RCE vulnerability scans

- Alert/details typically from the public domain (vendor advisory, industry article, Twitter/X …)
  - Sometimes from closed sources
- Key ethical/legal consideration: can we identify vulnerable instances without exploitation?
  - What are the red lines? How intrusive can a scan be?
  - Can we obtain version information to understand if they have been patched?
- Remotely identifying versions can be challenging (vendors try to make it difficult …)
  - Often needs to be inferred indirectly (example: looking at Last-Modified responses for specific resource queries to identify dates vs date of patch)
- Results dependent on initial target selection
- Speed of implementation of vulnerability scans may vary
  - Can be hours or days, depending on protocol complexity
  - Important to have examples of known patched vs known unpatched systems
- Mitigations often difficult to detect remotely - which may effectively lead to False Positives or False Negatives

SHADOWSERVER

TLP CLEAR

New RCE vulnerability scans

- What are the red lines?
  - Avoid directory traversals
  - Avoid POST data where possible
  - Avoid any actions that can obtain sensitive information that is not needed
  - Avoid WRITE actions on APIs
  - Avoid anything that requires LOGINS at all costs. NO CREDENTIAL USE
- How intrusive can a scan be?
  - Try not to muddy the waters for DFIR teams
  - Try not to generate an absurd amount of logs
  - Kind of like hiking “Take nothing but pictures, leave nothing but footprints”

SHADOWSERVER

Collaboration

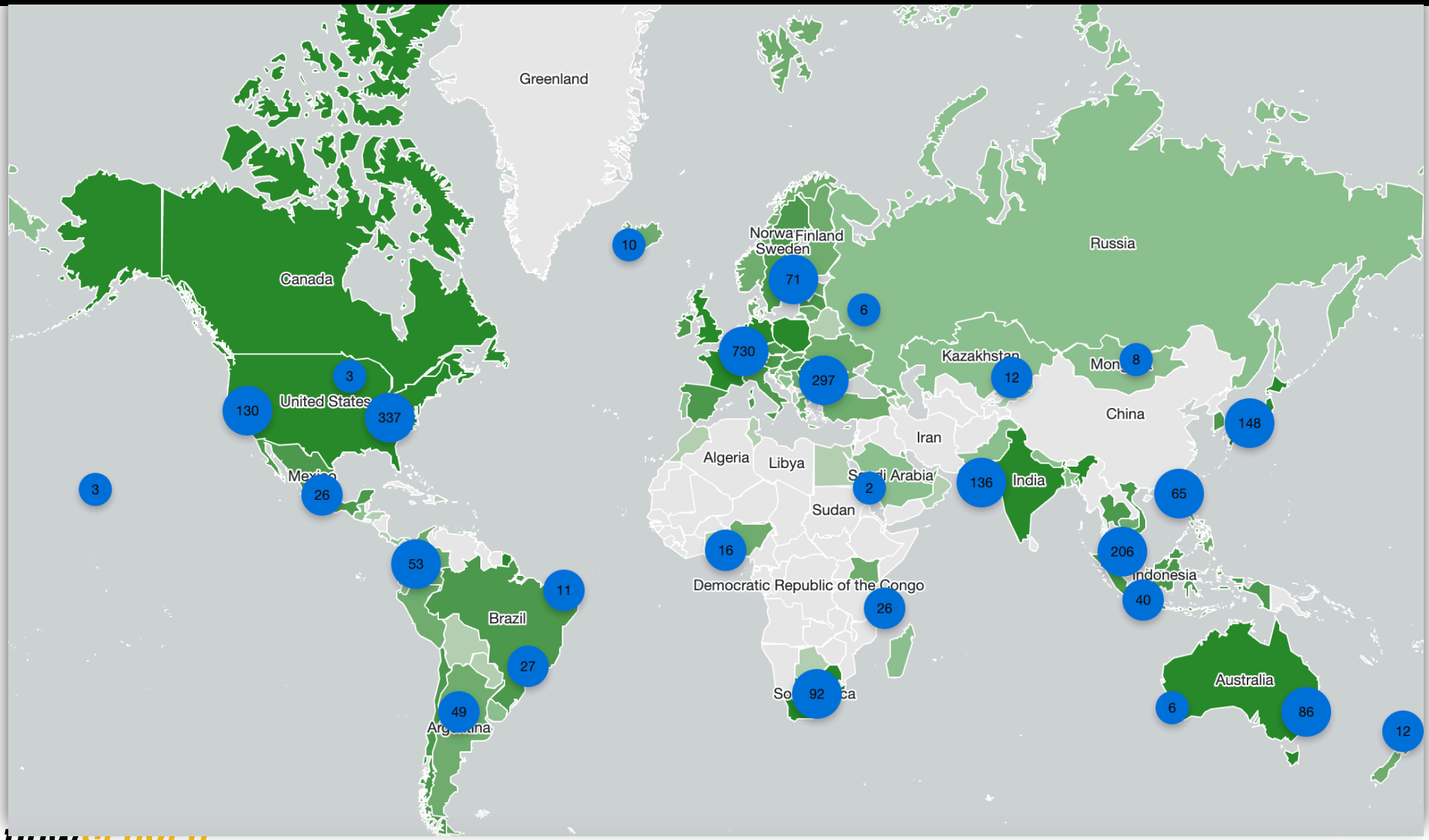
- Are there any scans you would like to see us implement?
- Device fingerprinting suggestions? (including remote version identification)
- Any RCE vulnerabilities we should scan for (without actual exploitation)? How?
- Are there any remote webshells/ implant/backdoor scans we should implement? How?
- Happy to collaborate on the above for any emerging RCE vulnerability …

Tracking vulnerability exploitation in the wild

Using honeypots

TLP CLEAR

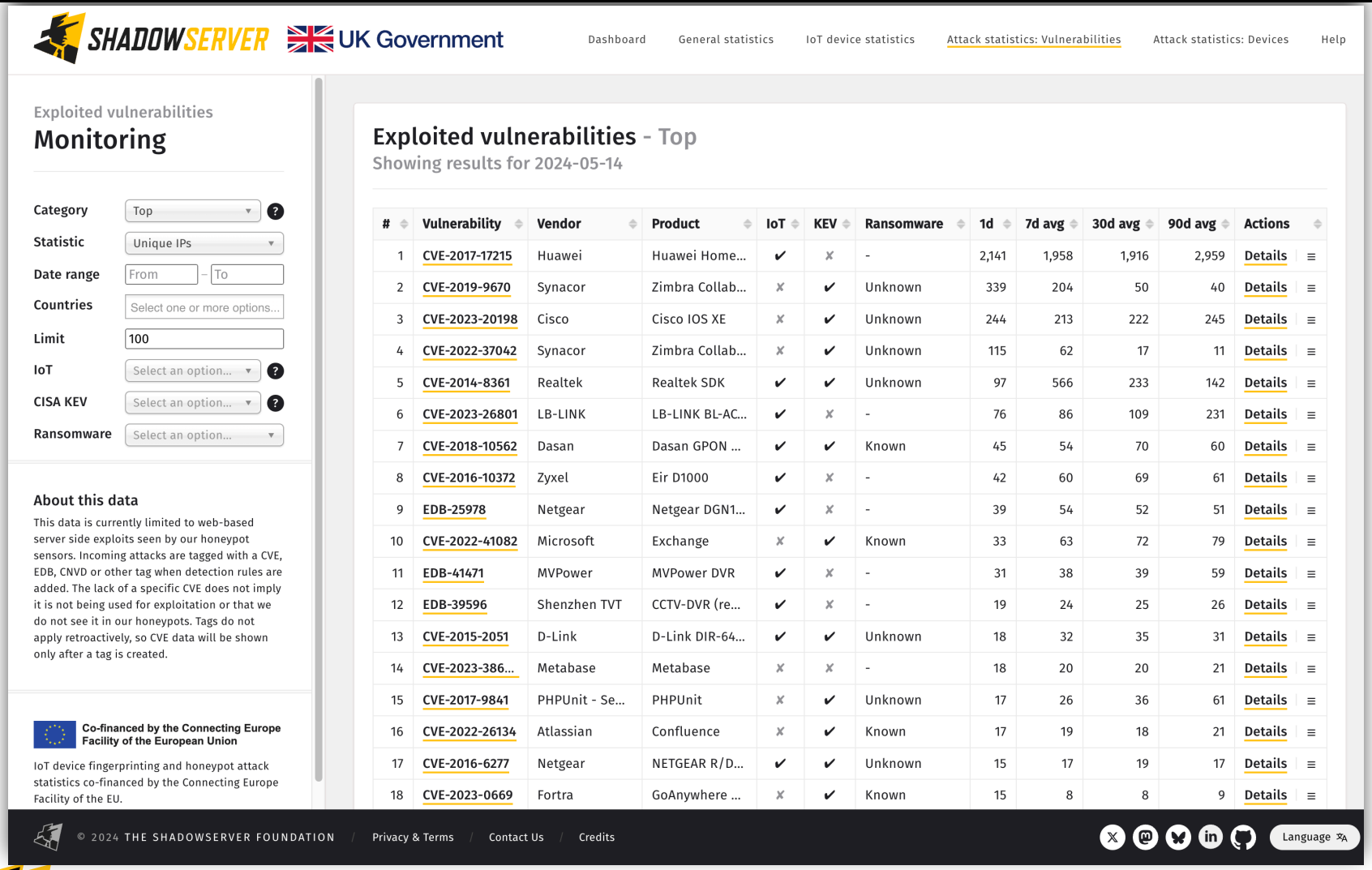
Honeypot sensor network - World (Sep 2025)



SHADOWSERVER

TLP CLEAR

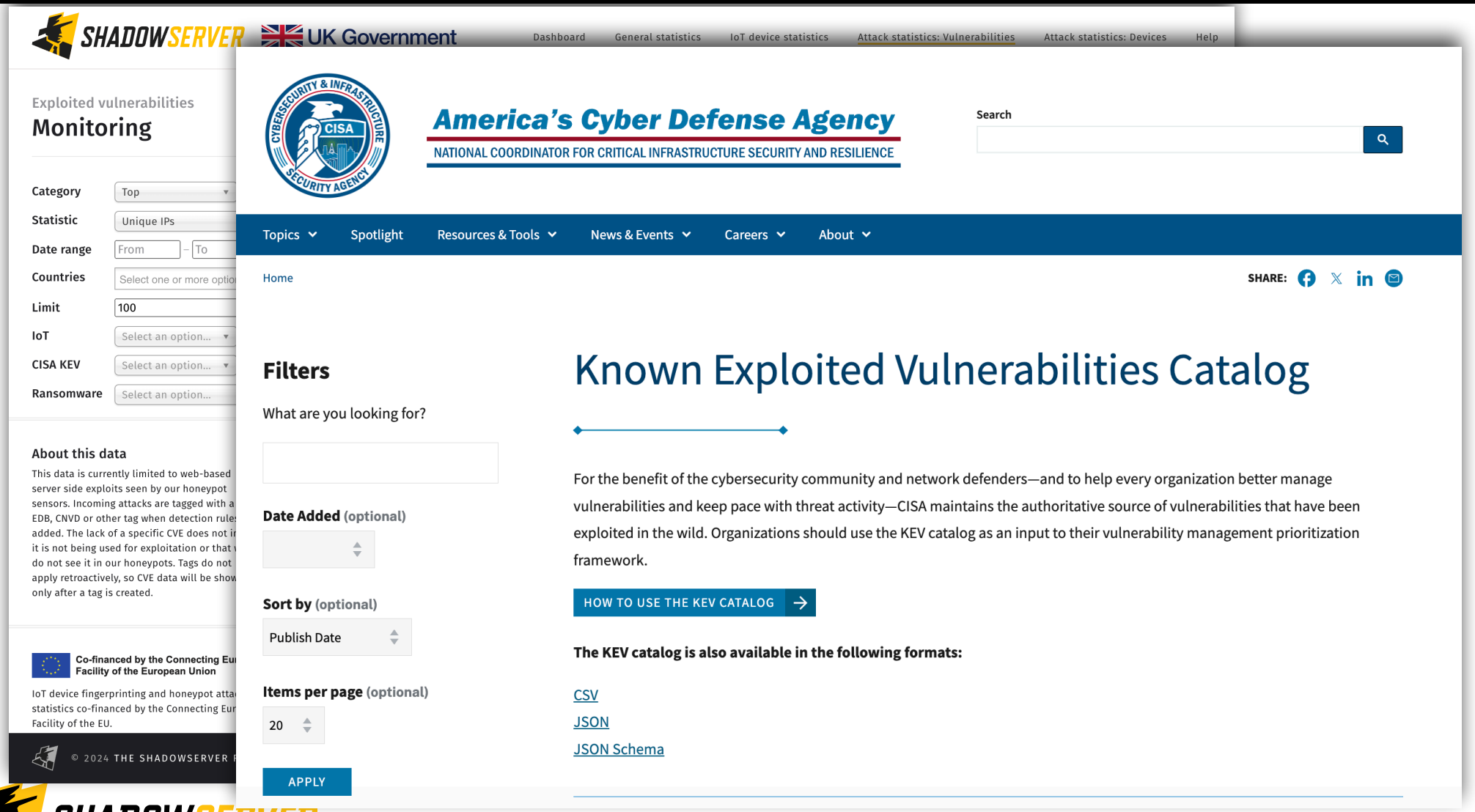
Exploitation tracking (by CVE or similar)



SHADOWSERVER

TLP CLEAR

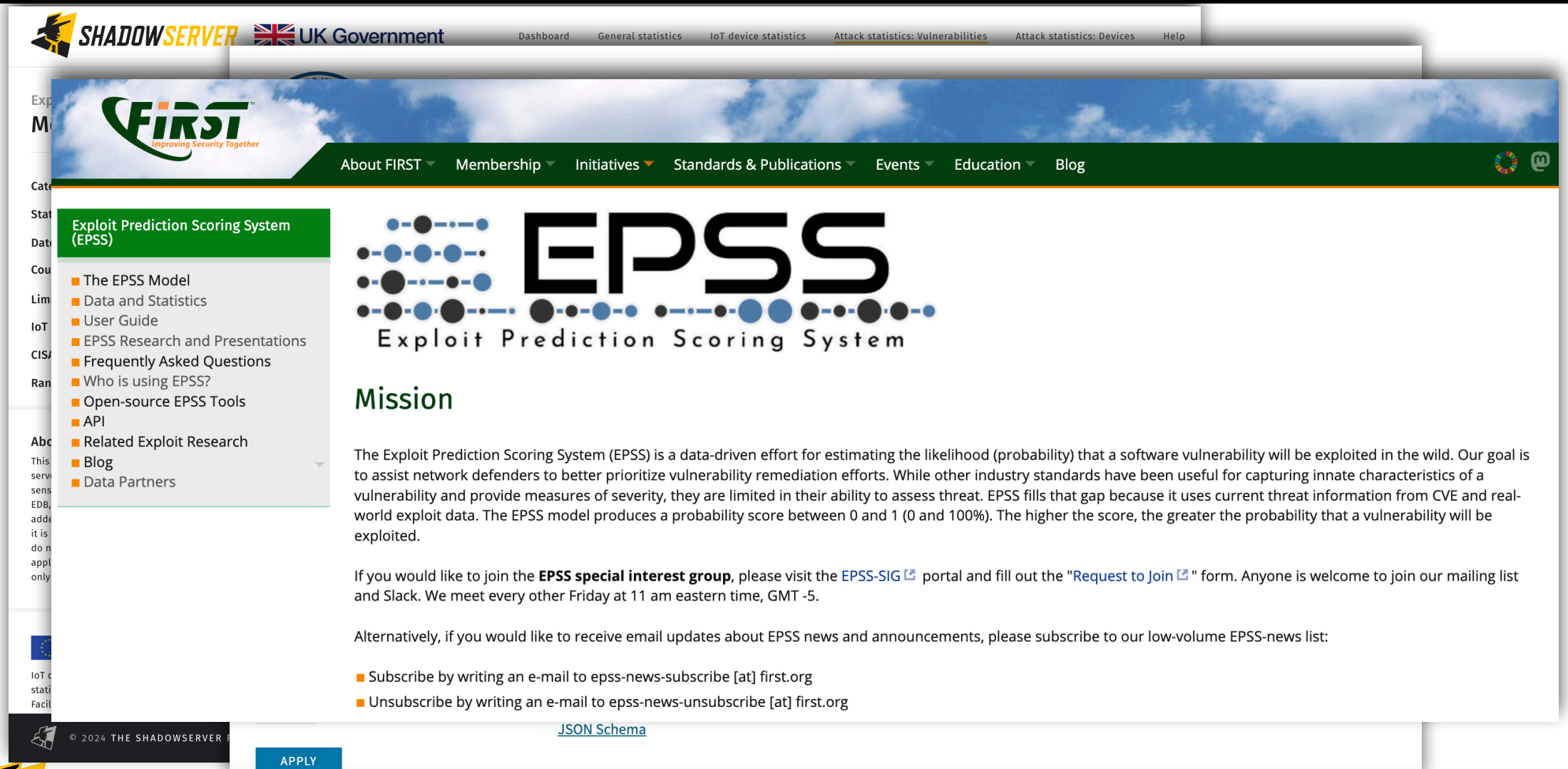
Exploitation tracking (by CVE or similar)



SHADOWSERVER

TLP CLEAR

Exploitation tracking (by CVE or similar)



SHADOWSERVER

TLP CLEAR

Earliest Reporter of Exploitation in the Wild

Response to latest incidents involving RCE CVEs

- Early detection and response to multiple prominent RCE CVE exploitation in the wild, examples:
  - Citrix NetScaler (CVE-2023-3519, …)
  - Cisco IOS XE (CVE-2023-20198, …)
  - Fortinet Fortigate (CVE-2024-23113, …)
  - Ivanti Connect Secure (CVE-2025-22467, …)
  - Palo Alto PAN-OS (CVE-2024-0012, …)
  - SharePoint (CVE-2025-49706 & CVE-2025-53770 et al)
- Working with Alliance partners & incident responder communities on the ground to understand vulnerable populations, compromised assets

Case studies

Collaborative Response to Emerging Critical RCE Vulnerabilities in Exposed Assets

Citrix NetScaler

CVE-2023-3519 (Summer 2023)

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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

TLP CLEAR

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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

- 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 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.

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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 (mid-2023)

TLP CLEAR

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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)

TLP CLEAR

Citrix NetS 2023)

July 19th: CISA Adds Citrix Net

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

July 20th: Shadowserver share TTP report)

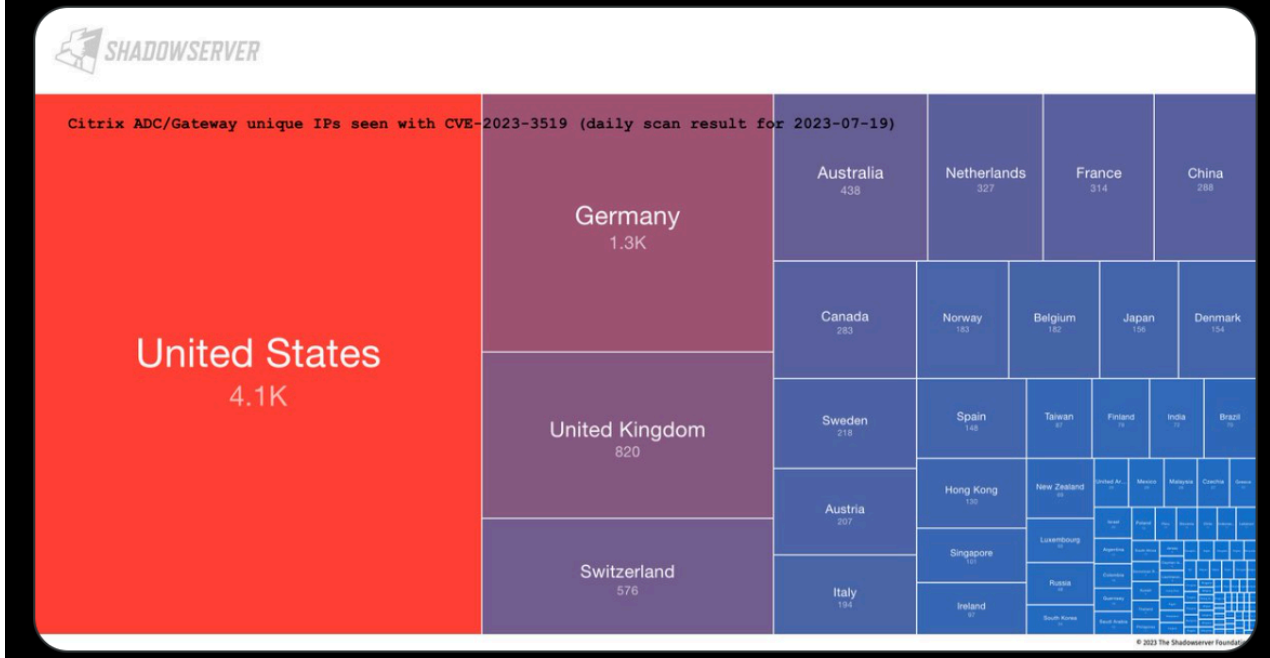
The Shadowserver Foundation
@Shadowserver

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

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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)

TLP CLEAR

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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 (mid-2023)

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 (mid-2023)

July 19th: CISA Adds Citrix Net

July 19th: Shadowserver devel

July 20th: Shadowserver share

July 20th: CISA Advisory on CV

July 21st: Shadowserver impro

ml body content)

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 (mid-2023)

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 (mid-2023)

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 (mid-2023)

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: Shadowserver Citrix gateway honeypot profile added

SHADOWSERVER

Citrix NetScaler: CVE-2023-3519 (mid-2023)

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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

TLP CLEAR

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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

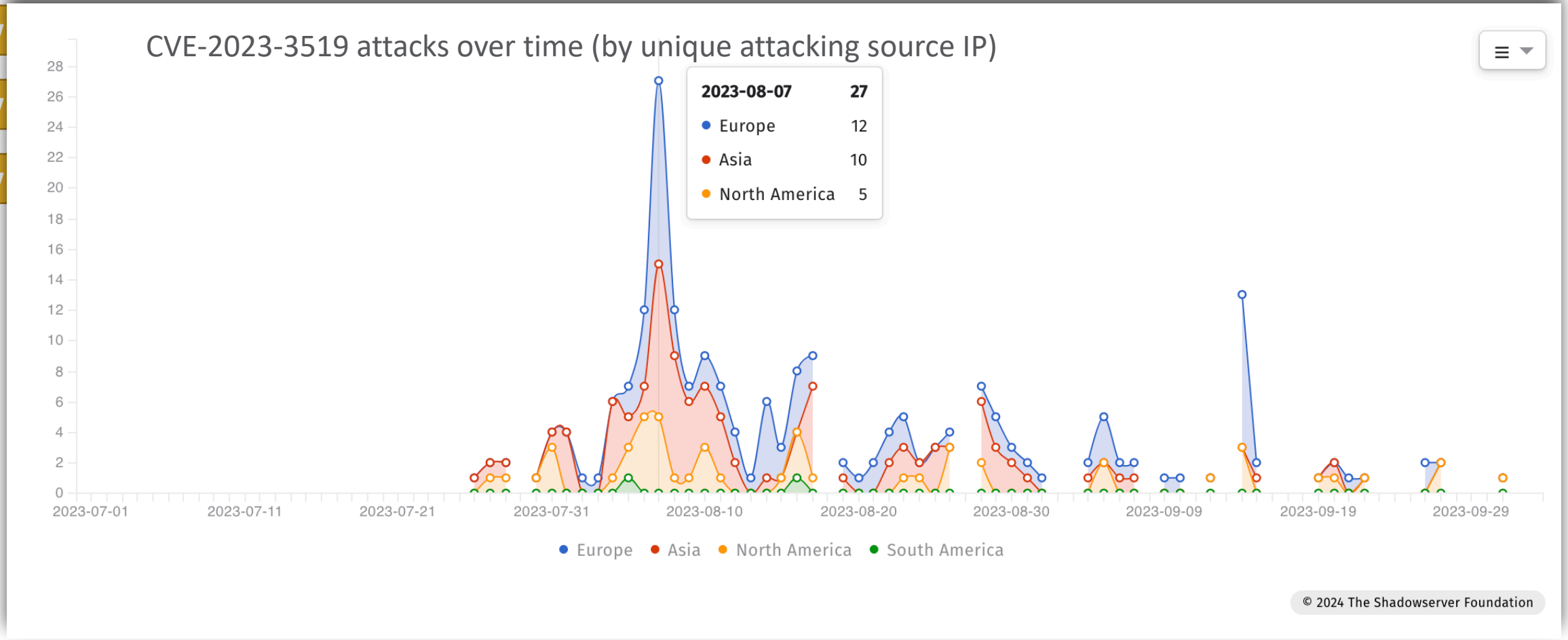
TLP CLEAR

Citrix NetScaler: CVE-2023-3519 (mid-2023)

July

July

July



SHADOWSERVER

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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

TLP CLEAR

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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

Citrix NetScaler: CVE-2023-3519 (mid-2023)

July 24th: CVE-2024-3519 PoC pub

July 24th: First Exploitation attemp by Shadowserver

July 26th: First CVE-2024-3519 tag

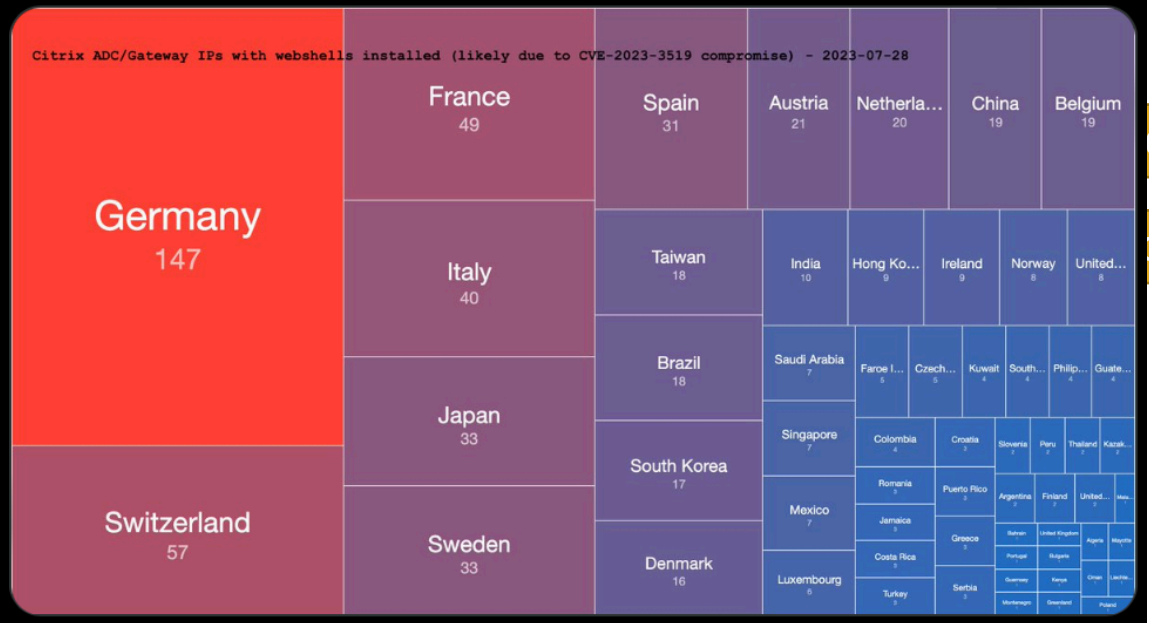
July 27th: Trusted partner reaches d on compromised instances

July 28th: First full scan for websh 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 (mid-2023)

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 (mid-2023)

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 (mid-2023)

July 24th: CVE-2024-3519 PoC pub

July 24th: First Exploitation attemp

July 26th: First CVE-2024-3519 tag

July 27th: Trusted partner reaches

July 28th: First full scan for websh

Aug 7th: We publish a technical bl

by Shadowserver

d on compromised instances

d

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 (mid-2023)

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

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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

TLP CLEAR

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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 (mid-2023)

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

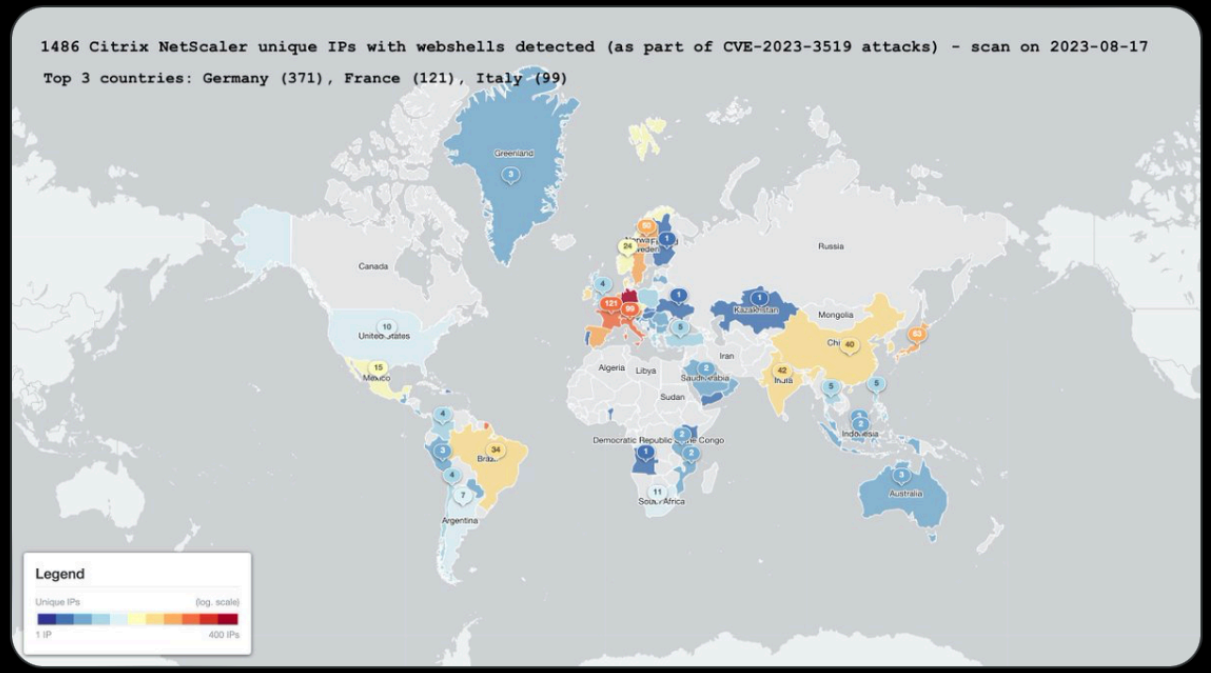
n compromised instances

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 (mid-2023)

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

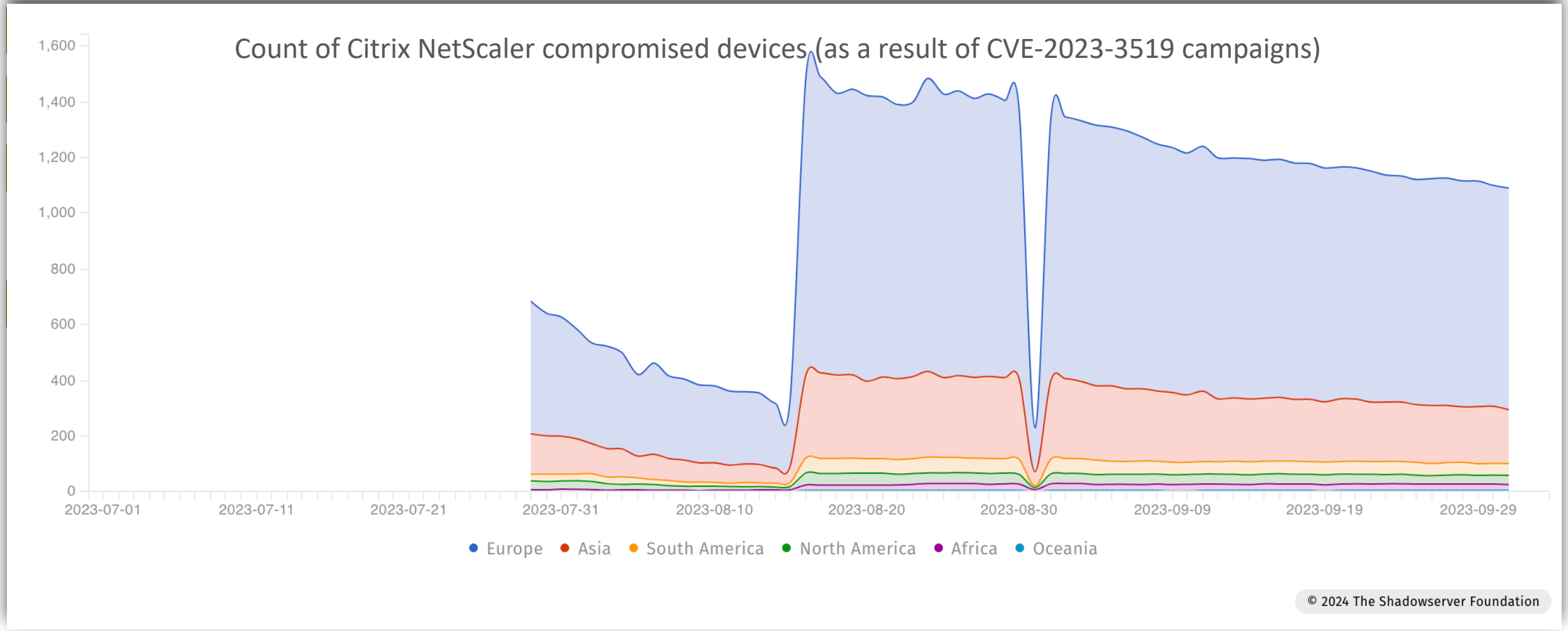
Aug 13th: Mandiant update their blogs/tooling to include Shadowserver contribution

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

SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519 (mid-2023)



SHADOWSERVER

TLP CLEAR

Citrix NetScaler: CVE-2023-3519 (mid-2023)

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 (mid-2023)

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

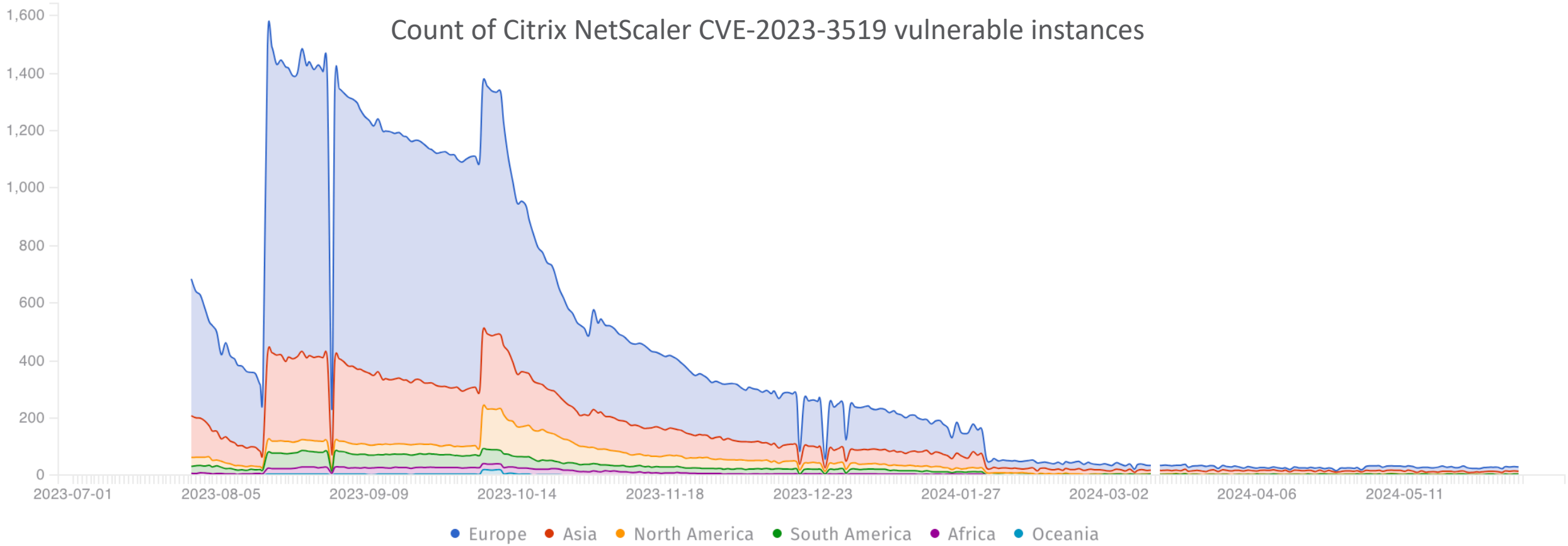
Aug 18th: Share further reports on compromised devices based on Fox-IT/DIVD NL collaboration

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 (mid-2023)



SHADOWSERVER

Cisco IOS XE

BadCandy implants (Autumn 2023 - ongoing)

Cisco IOS XE BadCandy (2023 -)

Cisco IOS XE BadCandy (2023 -)

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

TLP CLEAR

Cisco IOS XE BadCandy (2023 -)

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

Cisco IOS XE BadCandy (2023 -)

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

Cisco IOS XE BadCandy (2023 -)

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

TLP CLEAR

Cisco IOS XE

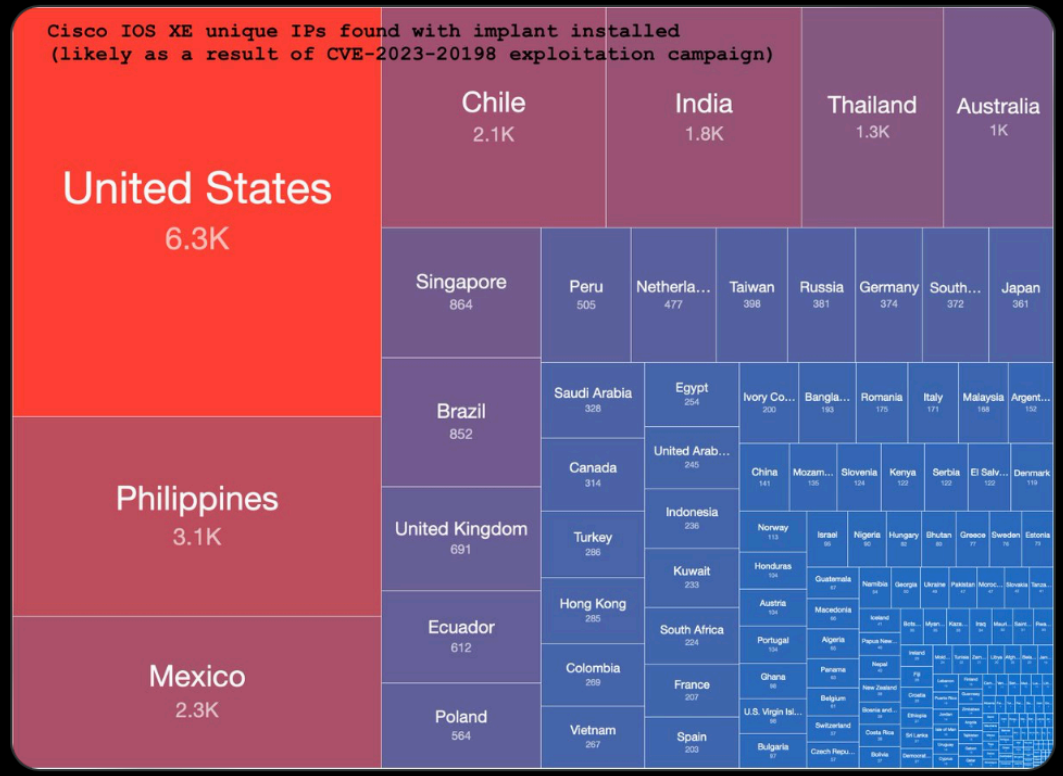
Oct 16th: Cisco Talos publication on … bilities. Scan implemented

Oct 17th: Shadowserver conducts fi…

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

SHADOWSERVER

Cisco IOS XE BadCandy (2023 -)

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

Cisco IOS XE BadCandy (2023 -)

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 for Cisco IOS XE

TLP CLEAR

Cisco IOS XE BadCandy (2023 -)

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 for Cisco IOS XE

Oct 19th: First implant scans immediately detected after rollout

SHADOWSERVER

Cisco IOS XE BadCandy (2023 -)

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 for Cisco IOS XE

Oct 19th: First implant scans immediately detected after rollout

Oct 22nd: Implant updated by attackers

TLP CLEAR

Cisco IOS XE BadCandy (2023 -)

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 for Cisco IOS XE

Oct 19th: First implant scans immediately detected after rollout

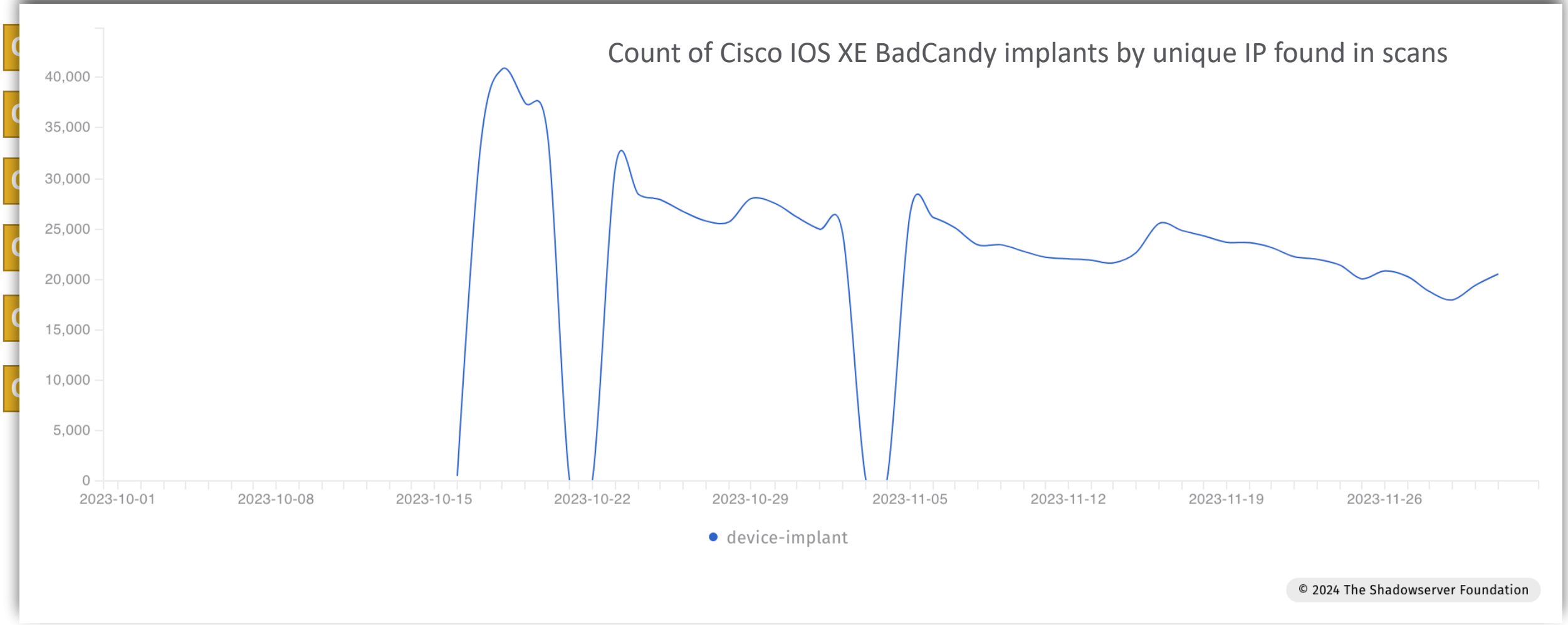
Oct 22nd: Implant updated by attackers

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

SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy (2023 -)



SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy (2023 -)

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 for Cisco IOS XE

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 (2023 -)

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 for Cisco IOS XE

Oct 19th: First implant scans immediately detected after rollout

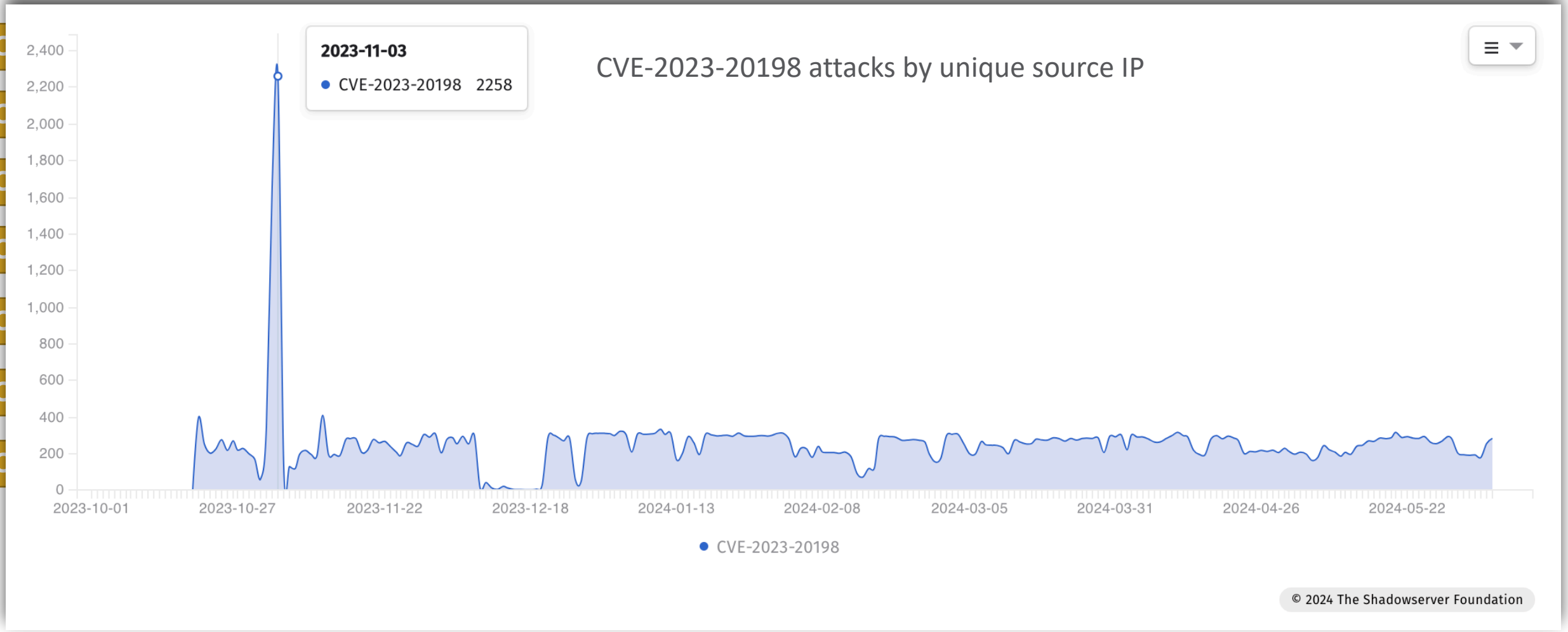
Oct 22nd: Implant updated by attackers

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

Cisco IOS XE BadCandy (2023 -)



TLP CLEAR

Cisco IOS XE BadCandy (2023 -)

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 for Cisco IOS XE

Oct 19th: First implant scans immediately detected after rollout

Oct 22nd: Implant updated by attackers

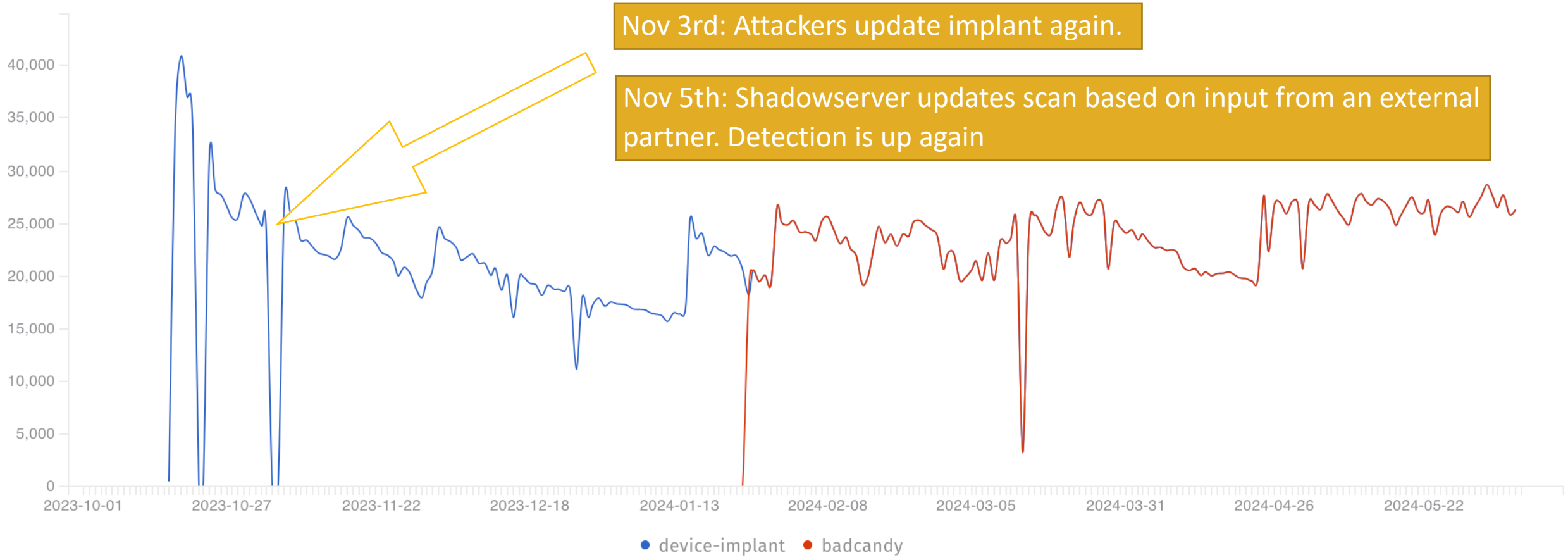
Oct 23rd: Cisco updates advisory with new implant details. Shadowserver scans updated

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

SHADOWSERVER

TLP CLEAR

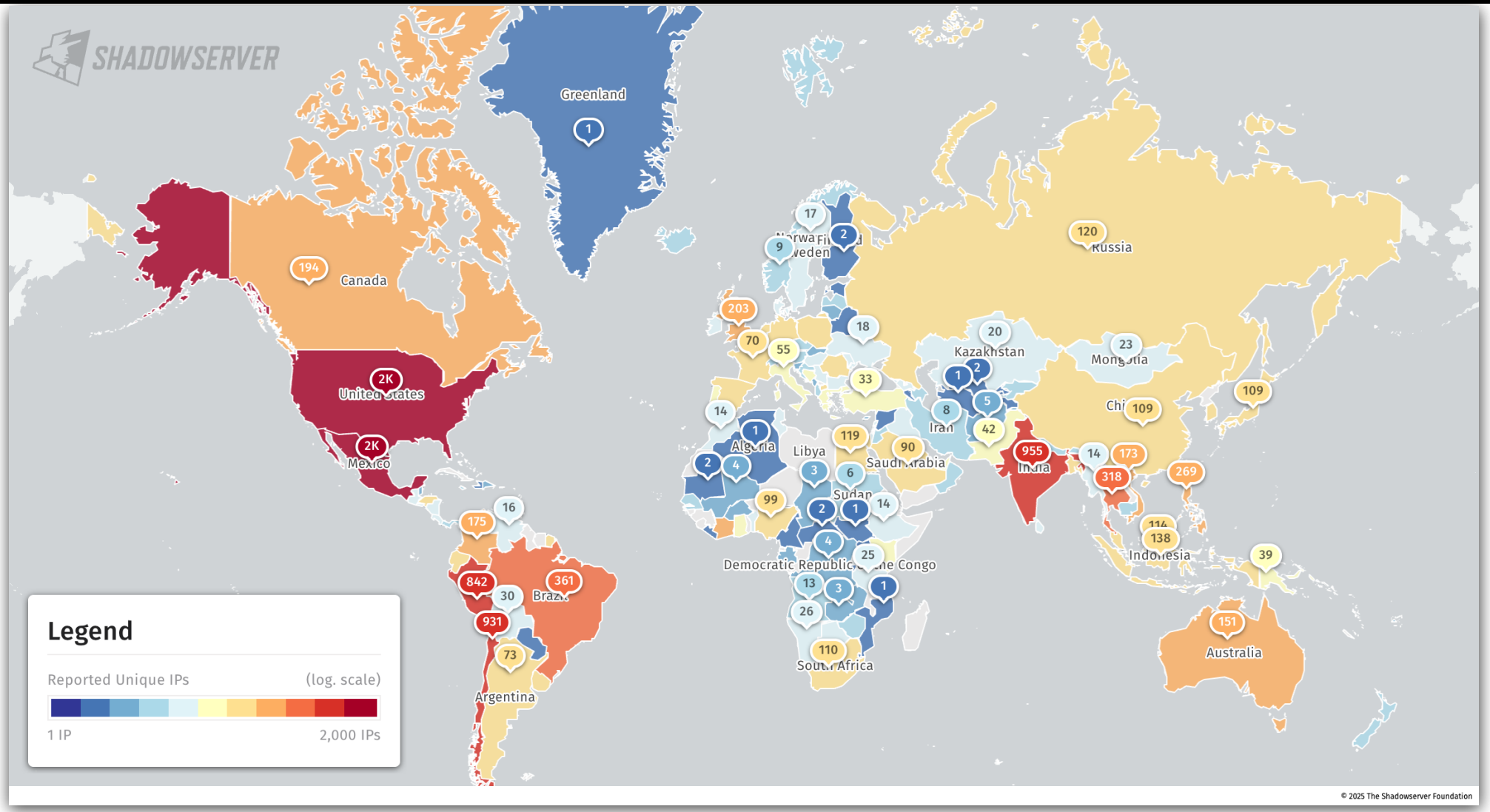
Cisco IOS XE BadCandy (2023 -)



SHADOWSERVER

TLP CLEAR

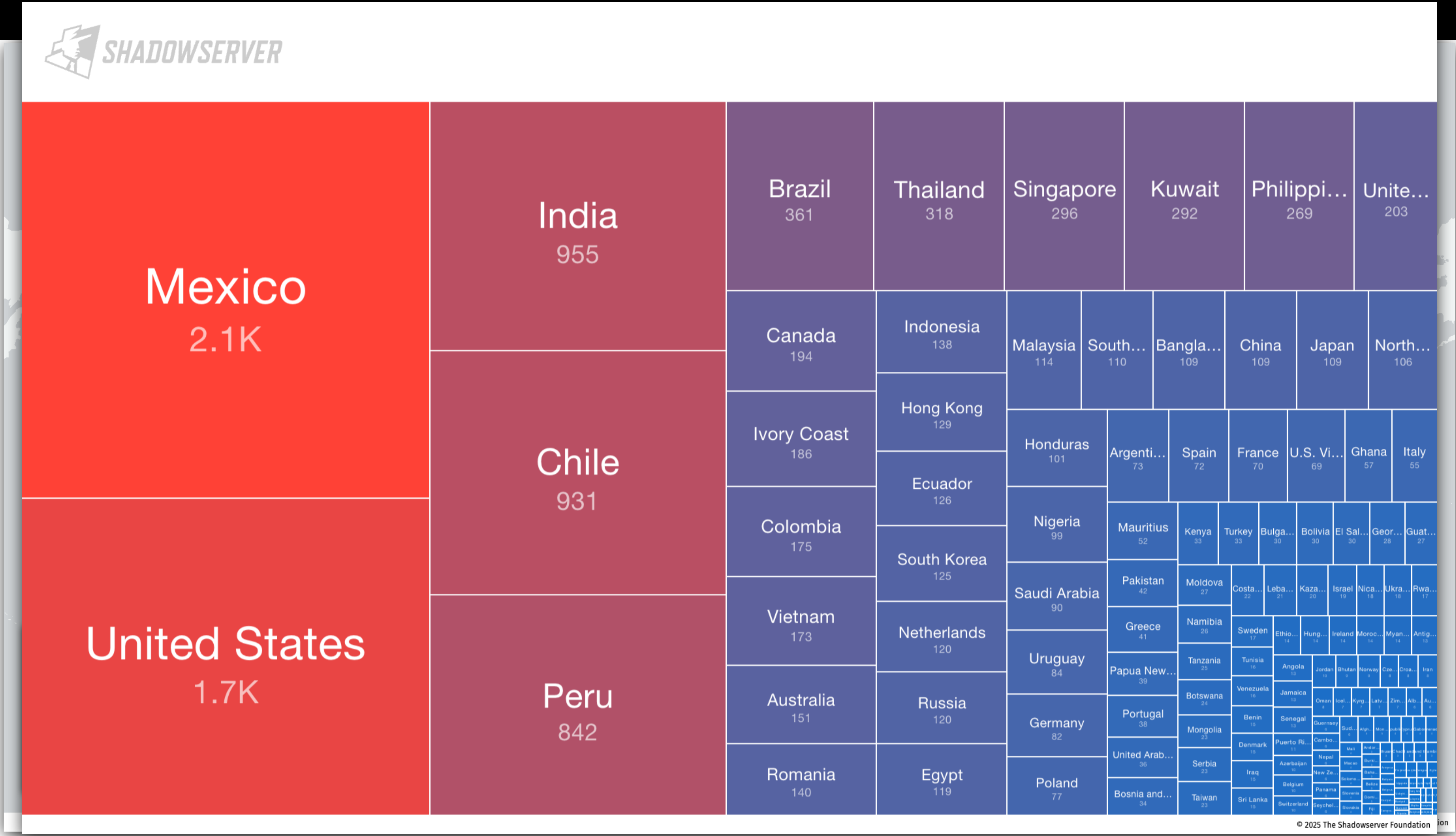
Cisco IOS XE BadCandy - 2025-09-22 - Still ongoing!



SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy - 2025-09-22 - Still ongoing!



SHADOWSERVER

Palo Alto PAN-OS

CVE-2024-0012 (Autumn 2024)

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

November 8th: Tipped off that exposed PAN-OS management interfaces may be vulnerable to a 0-day

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

November 8th: Tipped off that exposed PAN-OS management interfaces may be vulnerable to a 0-day

November 8th: Detections added and device id rules generated. Palo Alto issues initial advisory about potential 0day

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

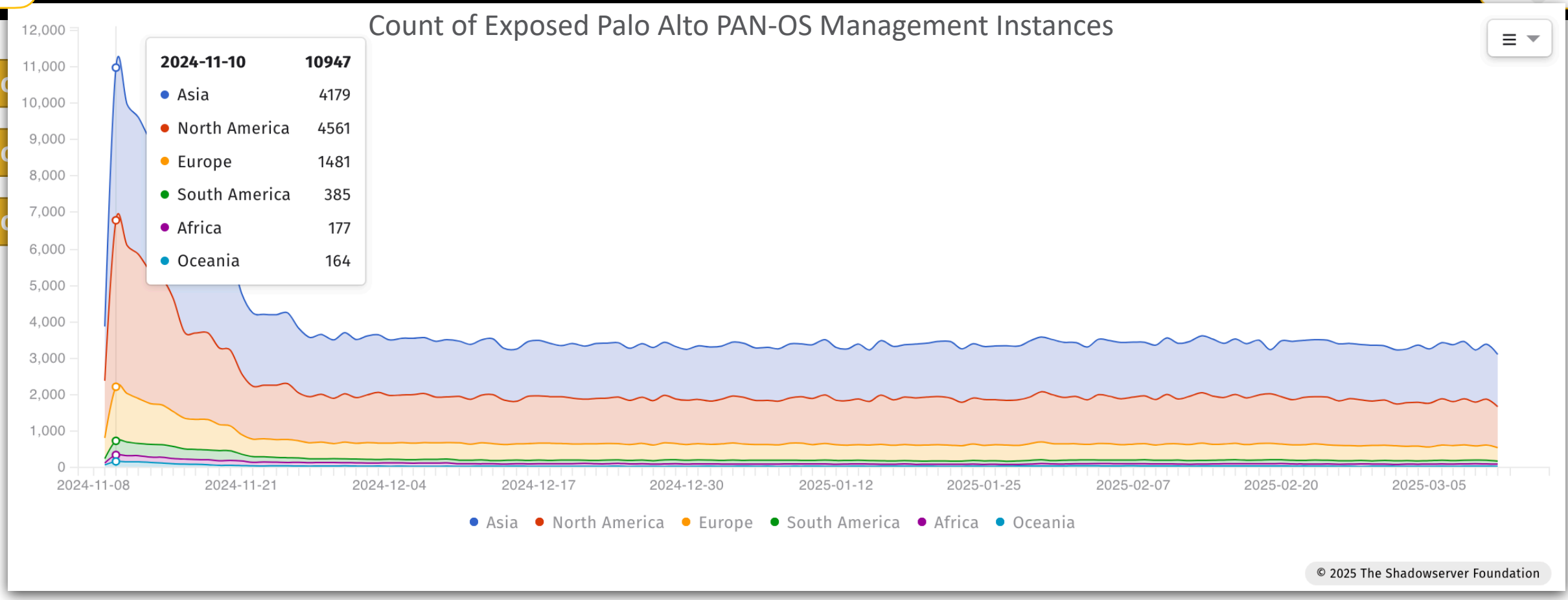
November 8th: Tipped off that exposed PAN-OS management interfaces may be vulnerable to a 0-day

November 8th: Detections added and device id rules generated. Palo Alto issues initial advisory about potential 0day

November 10th: Data on exposed interfaces goes out to report recipients

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012 (2024 -)



SHADOWSERVER

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

November 8th: Tipped off that exposed PAN-OS management interfaces may be vulnerable to a 0-day

November 8th: Detections added and device id rules generated. Palo Alto issues initial advisory about potential 0day

November 10th: Data on exposed interfaces goes out to report recipients

November 14th: Palo Alto issues updated notice that there is a vulnerability

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

Palo Alto Networks Security Advisories / PAN-SA-2024-0015

PAN-SA-2024-0015 Critical Security Bulletin: Ensure Access to Management Interface is Secured

Urgency HIGHEST

Severity 9.3 · CRITICAL

Exploit Maturity **ATTACKED**	Response Effort **MODERATE**	Recovery **USER**	Value Density **CONCENTRATED**
Attack Vector **NETWORK**	Attack Complexity **LOW**	Attack Requirements **NONE**	Automatable **YES**
User Interaction **NONE**	Product Confidentiality **HIGH**	Product Integrity **HIGH**	Product Availability **HIGH**
Privileges Required **NONE**	Subsequent Confidentiality **LOW**	Subsequent Integrity **LOW**	Subsequent Availability **LOW**

JSON

Published **2024-11-08**

Updated **2024-11-14**

Reference

Discovered **externally**

Description

Palo Alto Networks has observed threat activity exploiting an unauthenticated remote command execution vulnerability against a limited number of firewall management interfaces which are exposed to the Internet. We are actively investigating this activity.

SHADOWSERVER

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

November 8th: Tipped off that exposed PAN-OS management interfaces may be vulnerable to a 0-day

November 8th: Detections added and device id rules generated. Palo Alto issues initial advisory about potential 0day

November 10th: Data on exposed interfaces goes out to report recipients

November 14th: Palo Alto issues updated notice that there is a vulnerability

November 18th: CVE-2024-0012 assigned and added to the CISA KEV

SHADOWSERVER

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

PALO ALTO NETWORKS | PAN-OS

CVE-2024-0012

Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability: *Palo Alto Networks PAN-OS contains an authentication bypass vulnerability in the web-based management interface for several PAN-OS products, including firewalls and VPN concentrators.*

Related CWE: CWE-306

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. Additionally, management interface for affected devices should not be exposed to untrusted networks, including the internet.

- **Date Added:** 2024-11-18
- **Due Date:** 2024-12-09

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

November 8th: Tipped off that exposed PAN-OS management interfaces may be vulnerable to a 0-day

November 8th: Detections added and device id rules generated. Palo Alto issues initial advisory about potential 0day

November 10th: Data on exposed interfaces goes out to report recipients

November 14th: Palo Alto issues updated notice that there is a vulnerability

November 18th: CVE-2024-0012 assigned and added to the CISA KEV

November 19th: POC code released AND first exploit attempts using CVE-2024-0012 seen in our honeypots

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

palo-alto-panos-cve-2024-0012 / palo-alto-vpn-CVE-2024-0012-check-wt.yaml

h888t Create palo-alto-vpn-CVE-2024-0012-check-wt.yaml 83341cf

Code Blame 38 lines (31 loc) · 1.05 KB

```yaml
id: palo-alto-vpn-CVE-2024-0012-check-wt

info:
  name: Palo Alto PAN-OS Authentication Bypass in the Management Web Interface CVE-2024-0012
  author: watchTowr
  severity: critical
  description: An authentication bypass in Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to
  tags: palo-alto
  metadata:
    max-request: 4

http:
  - method: GET
    path:
      - "{{BaseURL}}/php/utils/CmsGetDeviceSoftwareVersion.php/.js.map"
```

SHADOWSERVER

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

November 8th: Tipped off that exposed PAN-OS management interfaces may be vulnerable to a 0-day

November 8th: Detections added and device id rules generated. Palo Alto issues initial advisory about potential 0day

November 10th: Data on exposed interfaces goes out to report recipients

November 14th: Palo Alto issues updated notice that there is a vulnerability

November 18th: CVE-2024-0012 assigned and added to the CISA KEV

November 19th: POC code released AND first exploit attempts using CVE-2024-0012 seen in our honeypots

November 19th: Method to determine vulnerability found and first scans performed

SHADOWSERVER

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

November 8th: Tipped off that exposed PAN-OS management interfaces may be vulnerable to a 0-day

November 8th: Detections added and device id rules generated. Palo Alto issues initial advisory about potential 0day

November 10th: Data on exposed interfaces goes out to report recipients

November 14th: Palo Alto issues updated notice that there is a vulnerability

November 18th: CVE-2024-0012 assigned and added to the CISA KEV

November 19th: POC code released AND first exploit attempts using CVE-2024-0012 seen in our honeypots

November 19th: Method to determine vulnerability found and first scans performed

November 20th: Partner shares artifacts left behind after exploit and scanning for those commences

SHADOWSERVER

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

November 21st: Begin mining the honeypots for potential artifacts and then scanning known PAN-OS instances in as close to realtime as possible

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

November 21st: Begin mining the honeypots for potential artifacts and then scanning known PAN-OS instances in as close to realtime as possible

```
GET /unauth/9.txt


<config version="9.1.0">
  <mgt-config>
    <users>
      <entry name="admin">
          <phash>XXXXXXXXXXXX</phash>
        <permissions>
          <role-based>
            <superuser>yes</superuser>
          </role-based>
        </permissions>
      </entry>
    </users>
    <password-complexity>
      <enabled>yes</enabled>
      <minimum-length>8</minimum-length>
    </password-complexity>
  </mgt-config>
  <shared>
    <application/>
    <application-group/>
    <service/>
    <service-group/>
    <botnet>
      <configuration>
        <http>
          <dynamic-dns>
            <enabled>yes</enabled>
```

SHADOWSERVER

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

November 21st: Begin mining the honeypots for potential artifacts and then scanning known PAN-OS instances in as close to realtime as possible

```
GET /unauth/9.txt


<config version="9.1.0">
  <mgt-config>
    <users>
      <entry name="admin">
          <phash>XXXXXXXXXXXX</phash>
        <permissions>
          <role-based>
            <superuser>yes</superuser>
          </role-based>
        </permissions>
      </entry>
    </users>
    <password-complexity>
      <enabled>yes</enabled>
      <minimum-length>8</minimum-length>
    </password-complexity>
  </mgt-config>
  <shared>
    <application/>
    <application-group/>
    <service/>
    <service-group/>
    <botnet>
      <configuration>
        <http>
          <dynamic-dns>
            <enabled>yes</enabled>
```

```
root:$X$XXXXXXXX$XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:19585:0:99999:7:::
bin:*:18808:0:99999:7:::
daemon:*:18808:0:99999:7:::
adm:*:18808:0:99999:7:::
lp:*:18808:0:99999:7:::
sync:*:18808:0:99999:7:::
shutdown:*:18808:0:99999:7:::
halt:*:18808:0:99999:7:::
mail:*:18808:0:99999:7:::
operator:*:18808:0:99999:7:::
games:*:18808:0:99999:7:::
ftp:*:18808:0:99999:7:::
nobody:*:18808:0:99999:7:::
apache:!!:19515::::::
vcsa:!!:19515::::::
nginx:!!:19515::::::
ntp:!!:19515::::::
rpc:!!:19515:0:99999:7:::
rpcuser:!!:19515::::::
tcpdump:!!:19515::::::
sshd:!!:19515::::::
dhcpd:!!:19515::::::
named:!!:19515::::::
nslcd:!!:19515::::::
redis:!!:19515::::::
nfast:!!:19515:0:99999:7:::
ha-ssh-private-account:!!:19515:0:99999:7:::
admin:$X$XXXXXXXX$XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:19585:0:99999:7:::
panorama:!!:19515:0:99999:7:::
```

SHADOWSERVER

Palo Alto PAN-OS CVE-2024-0012 (2024 -)

November 21st: Begin mining the honeypots for potential artifacts and then scanning known PAN-OS instances in as close to realtime as possible

November 22nd - onward: Notify nCIRTs / LE / affected groups of artifacts of compromise.

```
<config version="9.1.0">
  <mgt-config>
    <users>
      <entry name="admin">
          <phash>XXXXXXXXXXXX</phash>
        <permissions>
          <role-based>
            <superuser>yes</superuser>
          </role-based>
        </permissions>
      </entry>
    </users>
    <password-complexity>
      <enabled>yes</enabled>
      <minimum-length>8</minimum-length>
    </password-complexity>
  </mgt-config>
  <shared>
    <application/>
    <application-group/>
    <service/>
    <service-group/>
    <botnet>
      <configuration>
        <http>
          <dynamic-dns>
            <enabled>yes</enabled>
```

```
XXXXXXXXXXXXXXXXXX:19585:0:99999:7:::
daemon:*:18808:0:99999:7:::
adm:*:18808:0:99999:7:::
lp:*:18808:0:99999:7:::
sync:*:18808:0:99999:7:::
shutdown:*:18808:0:99999:7:::
halt:*:18808:0:99999:7:::
mail:*:18808:0:99999:7:::
operator:*:18808:0:99999:7:::
games:*:18808:0:99999:7:::
ftp:*:18808:0:99999:7:::
nobody:*:18808:0:99999:7:::
apache:!!:19515::::::
vcsa:!!:19515::::::
nginx:!!:19515::::::
ntp:!!:19515::::::
rpc:!!:19515:0:99999:7:::
rpcuser:!!:19515::::::
tcpdump:!!:19515::::::
sshd:!!:19515::::::
dhcpd:!!:19515::::::
named:!!:19515::::::
nslcd:!!:19515::::::
redis:!!:19515::::::
nfast:!!:19515:0:99999:7:::
ha-ssh-private-account:!!:19515:0:99999:7:::
admin:$X$XXXXXXXX$XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:19585:0:99999:7:::
panorama:!!:19515:0:99999:7:::
```

SHADOWSERVER

Microsoft SharePoint

Not just edge devices - CVE-2025-49706/CVE-2025-49704 & CVE-2025-53770/CVE-2025-53771 (Summer 2025 - Current)

SharePoint - CVE-2025-49706, CVE-2025-53770

19th July: EYE Security alerts on mass SharePoint compromise incidents (possible 0-day)

SharePoint - CVE-2025-49706, CVE-2025-53770

19th July: EYE Security alerts on mass SharePoint compromise incidents (possible 0-day)

20th July: EYE Security & watchTowr reach out to Shadowserver to help alert victims, inform on webshell paths

SharePoint - CVE-2025-49706, CVE-2025-53770

19th July: EYE Security alerts on mass SharePoint compromise incidents (possible 0-day)

20th July: EYE Security & watchTowr reach out to Shadowserver to help alert victims, inform on webshell paths

20th July: Shadowserver immediately starts manual notifications of victims to National CSIRTs via our Alliance Mattermost & other contacts

SharePoint - CVE-2025-49706, CVE-2025-53770

19th July: EYE Security alerts on mass SharePoint compromise incidents (possible 0-day)

20th July: EYE Security & watchTowr reach out to Shadowserver to help alert victims, inform on webshell paths

20th July: Shadowserver immediately starts manual notifications of victims to National CSIRTs via our Alliance Mattermost & other contacts

20th July: First automated reporting scan implementations from Shadowserver on vulnerable/compromised hosts - automated notifications start 21st July

SharePoint - CVE-2025-49706, CVE-2025-53770

19th July: EYE Security alerts on mass SharePoint compromise incidents (possible 0-day)

20th July: EYE Security & watchTowr reach out to Shadowserver to help alert victims, inform on webshell paths

20th July: Shadowserver immediately starts manual notifications of victims to National CSIRTs via our Alliance Mattermost & other contacts

20th July: First automated reporting scan implementations from Shadowserver on vulnerable/compromised hosts - automated notifications start 21st July

21st July: Data on new victims thanks to DIVD.NL - immediate manual notifications from Shadowserver

SharePoint - CVE-2025-49706, CVE-2025-53770

19th July: EYE Security alerts on mass SharePoint compromise incidents (possible 0-day)

20th July: EYE Security & watchTowr reach out to Shadowserver to help alert victims, inform on webshell paths

20th July: Shadowserver immediately starts manual notifications of victims to National CSIRTs via our Alliance Mattermost & other contacts

20th July: First automated reporting scan implementations from Shadowserver on vulnerable/compromised hosts - automated notifications start 21st July

21st July: Data on new victims thanks to DIVD.NL - immediate manual notifications from Shadowserver

24th July: LeakIX share vulnerability data based on their scans, which Shadowserver immediately shares out

SharePoint - CVE-2025-49706, CVE-2025-53770

19th July: EYE Security alerts on mass SharePoint compromise incidents (possible 0-day)

20th July: EYE Security & watchTowr reach out to Shadowserver to help alert victims, inform on webshell paths

20th July: Shadowserver immediately starts manual notifications of victims to National CSIRTs via our Alliance Mattermost & other contacts

20th July: First automated reporting scan implementations from Shadowserver on vulnerable/compromised hosts - automated notifications start 21st July

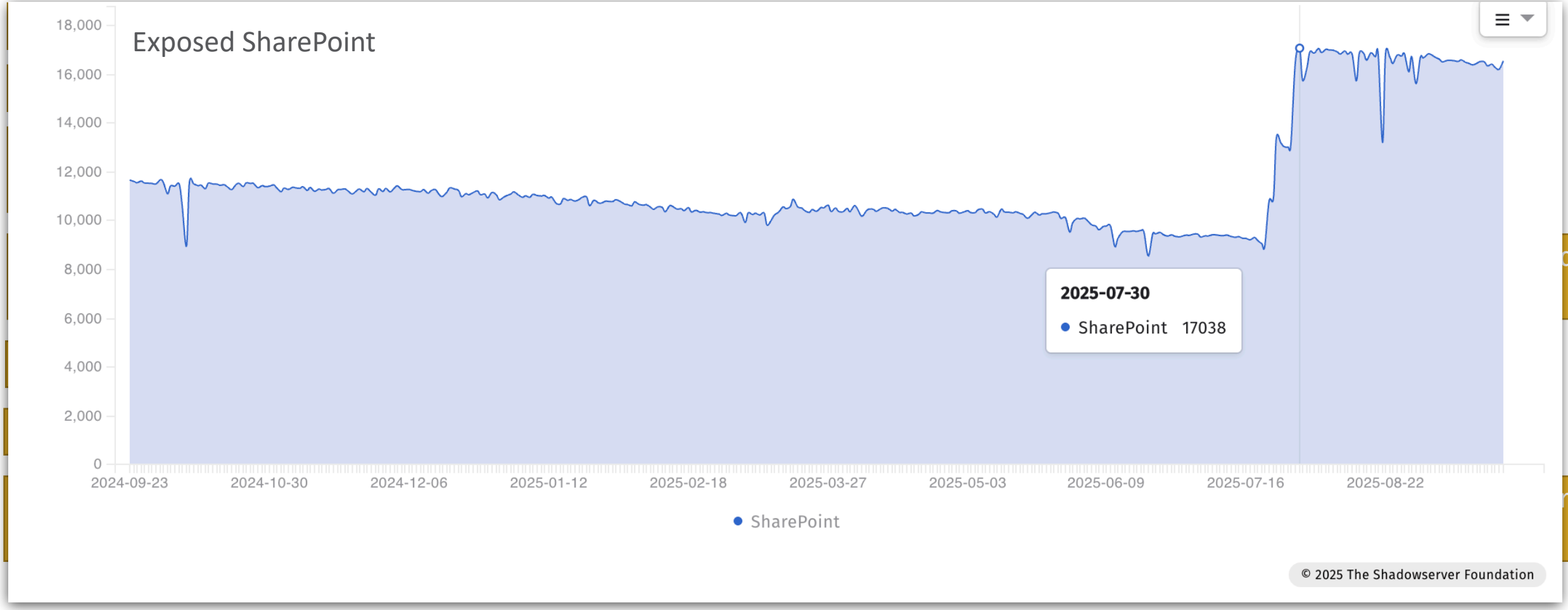
21st July: Data on new victims thanks to DIVD.NL - immediate manual notifications from Shadowserver

24th July: LeakIX share vulnerability data based on their scans, which Shadowserver immediately shares out

31st July: Additional insights in collaboration with Validin and CERT-BUND: 1) access to vhost data improves our scans 2) better version detection for vulnerability scans

TLP CLEAR

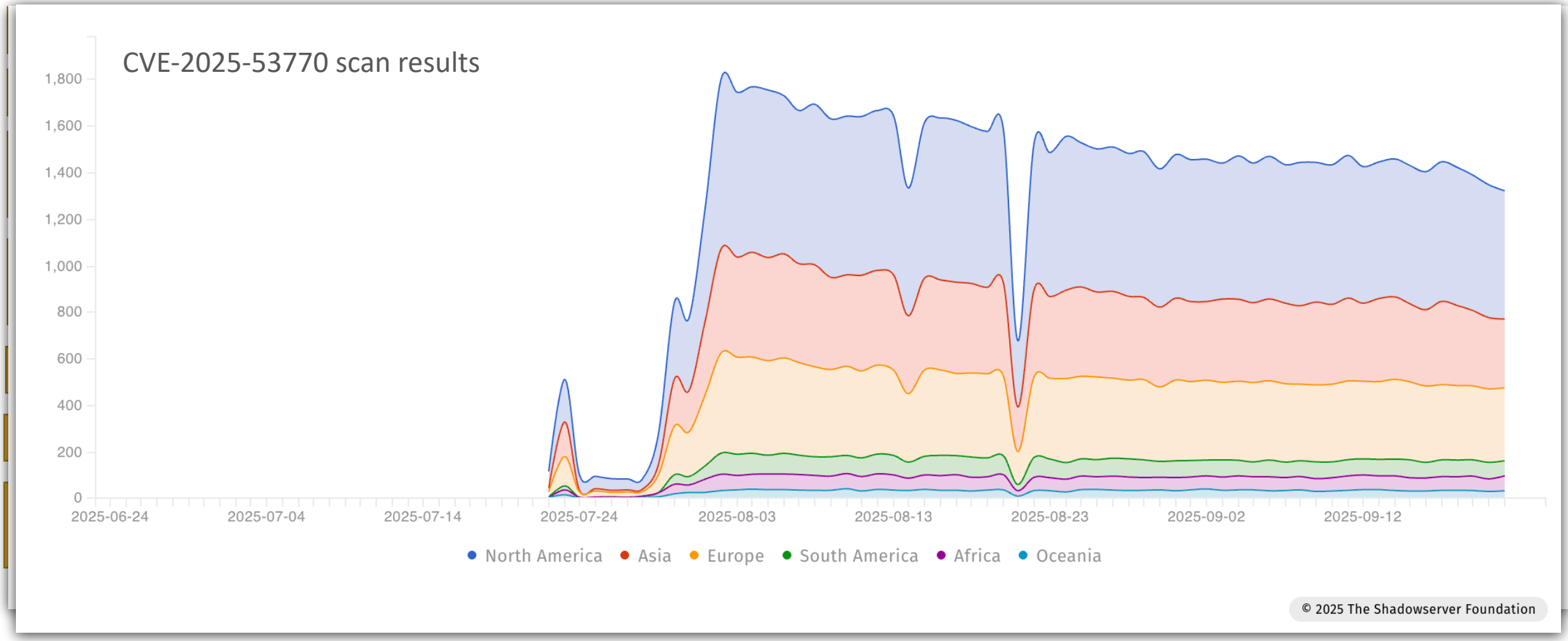
SharePoint - CVE-2025-49706, CVE-2025-53770



SHADOWSERVER

TLP CLEAR

SharePoint - CVE-2025-49706, CVE-2025-53770



SHADOWSERVER

Call to action!

Taking collaboration to the next level

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 & industry actions,** enabling new insights
- **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!
- Best results are achieved thanks to **collaboration** - we are happy to work with industry partners/vendors on scanning & detection of emerging threats so we can carry out our joint mission of achieving a more secure Internet

SHADOWSERVER

Thank You!

SHADOWSERVER

Lighting the way to a more secure Internet

@shadowserver, @piotrkijewski

@shadowserver.bsky.social

@shadowserver@infosec.exchange

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

contact@shadowserver.org

SHADOWSERVER.ORG