SHADOWSERVER

Collaborative Response to Emerging Critical RCE Vulnerabilities in Exposed Assets

Piotr Kijewski, @piotrkijewski

piotr@shadowserver.org

September 10th, 2025
APNIC 60/FIRST Technical Colloquium, Da Nang, Vietnam

SHADOWSERVER.ORG

TLP CLEAR

# whoami

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

SHADOWSERVER

Introduction

What is the Shadowserver Foundation & what does it do?

TLP
CLEAR

The Shadowserver Foundation - Since 2004…

SHADOWSERVER

TLP CLEAR

The Shadowserver Foundation - Since 2004…

US: 501c3 nonprofit organization

NL: “Stichting” w/ public benefit status

SHADOWSERVER

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

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

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

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

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

Who does the Shadowserver Foundation Serve?

SHADOWSERVER

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

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

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

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

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

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

Critical infrastructure including water, power, utility companies

Sectoral CERTs and ISACs

Internet Service Providers, Hosting & Content Providers

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

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

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

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

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

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

Law Enforcement Organizations

Small Businesses to Fortune 500 companies

SHADOWS

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

TLP CLEAR

Our Sharing Model: Who Gets The Data?

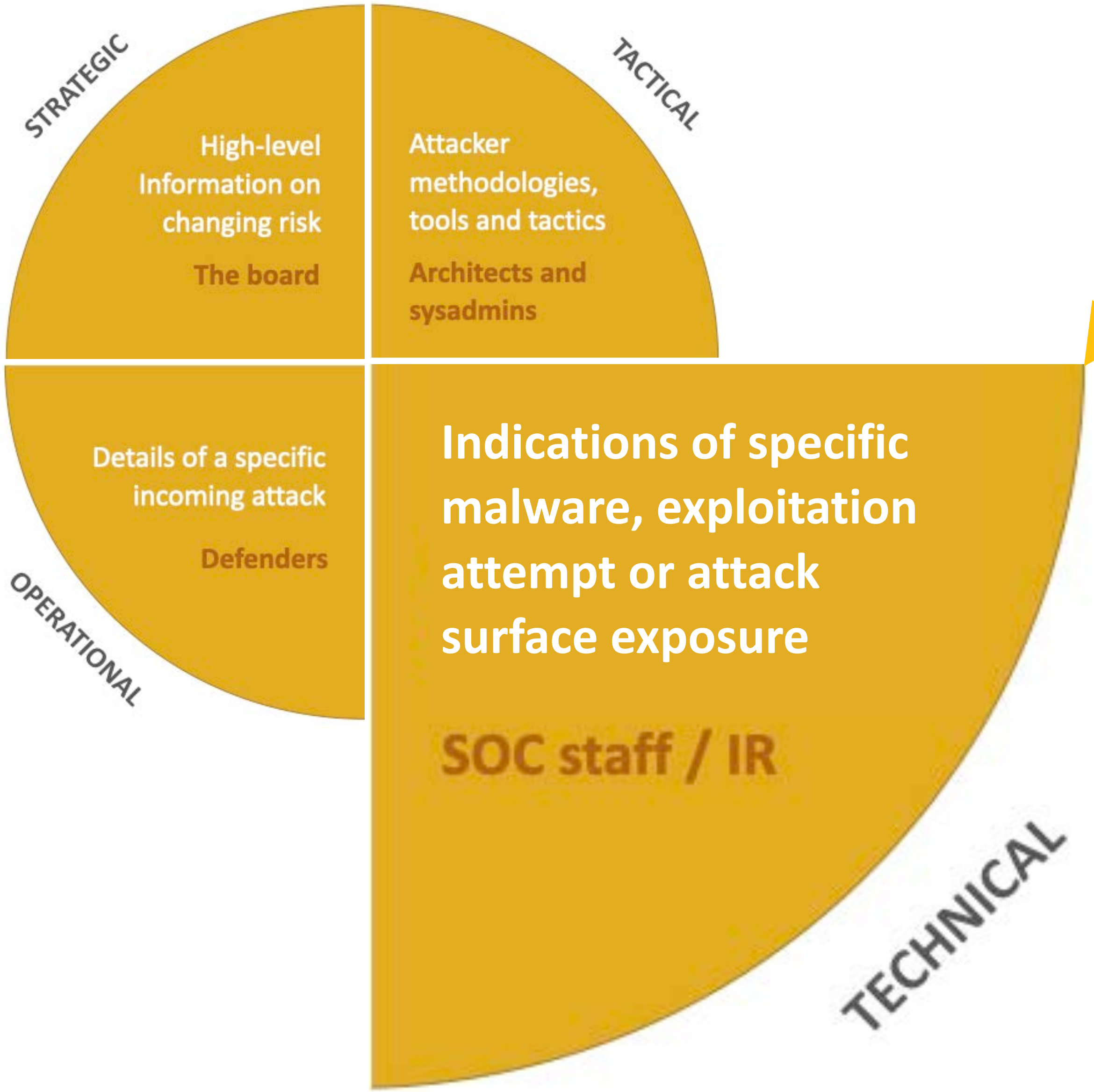
Who?	National CSIRTs	Network Owners	Law Enforcement
What Data?	Sliced Geographically (no cost)	Sliced by defined IP Address Space / ASN / CIDR /Domains (no cost, regardless of size)	Limited to specific investigation needs, intel only (no cost)
MSSP Model?	nCSIRT can delegate all/ part to 3rd parties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

SHADOWSERVER

MSSP = Managed Security Service Provider

TLP
CLEAR



High-level Information on changing risk

The board

Attacker methodologies, tools and tactics

Architects and sysadmins

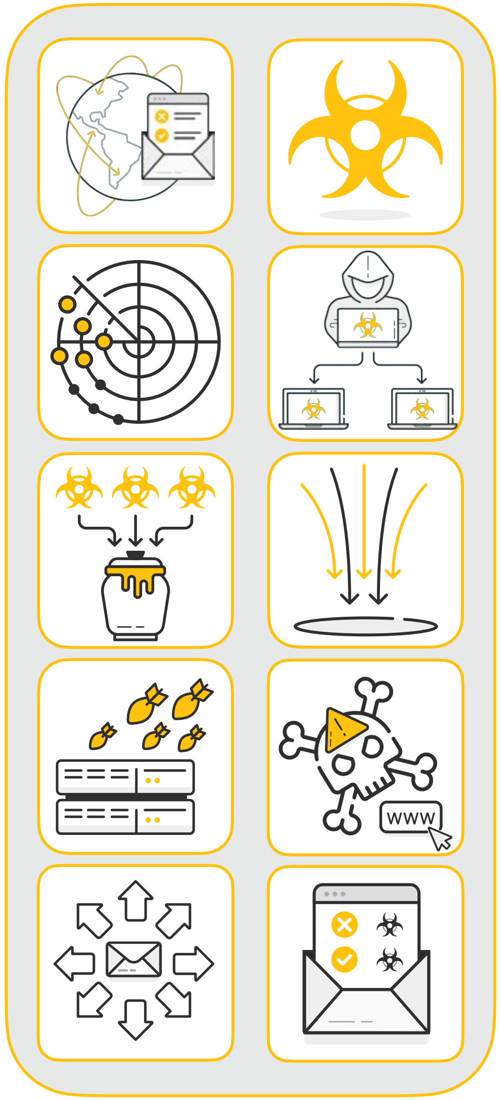
Details of a specific incoming attack

Defenders

Indications of specific malware, exploitation attempt or attack surface exposure

SOC staff / IR

Core Shadowserver offering

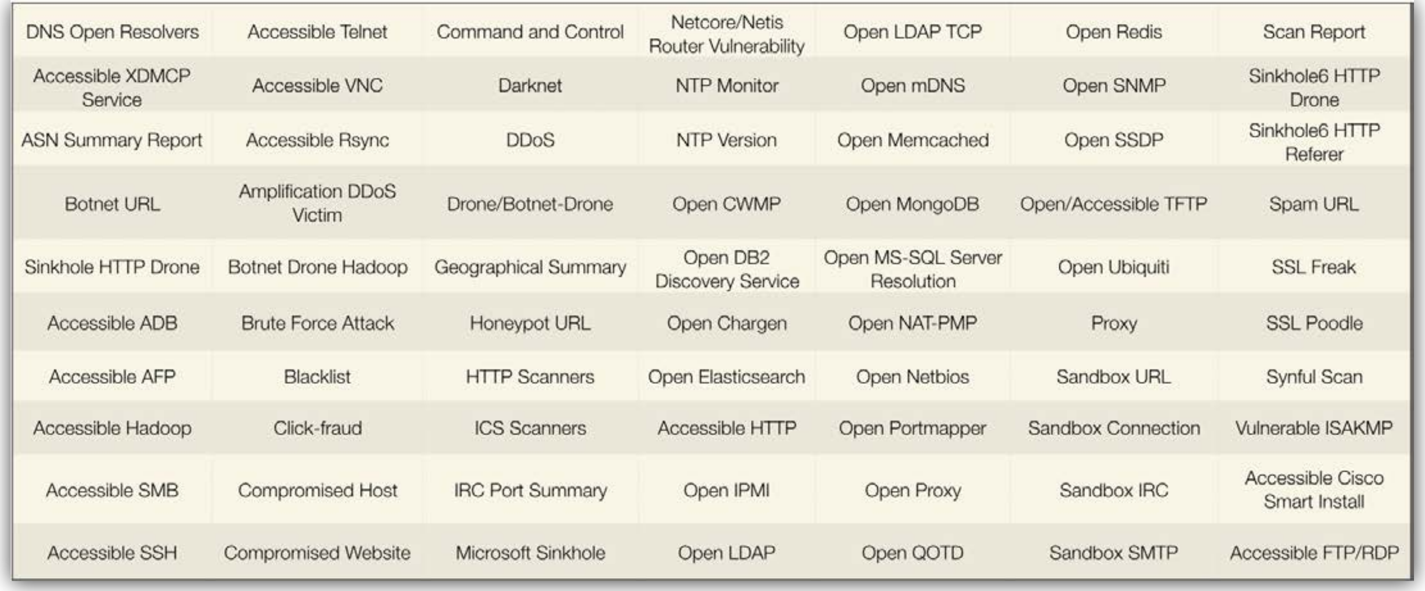


TLP CLEAR

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 …

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

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

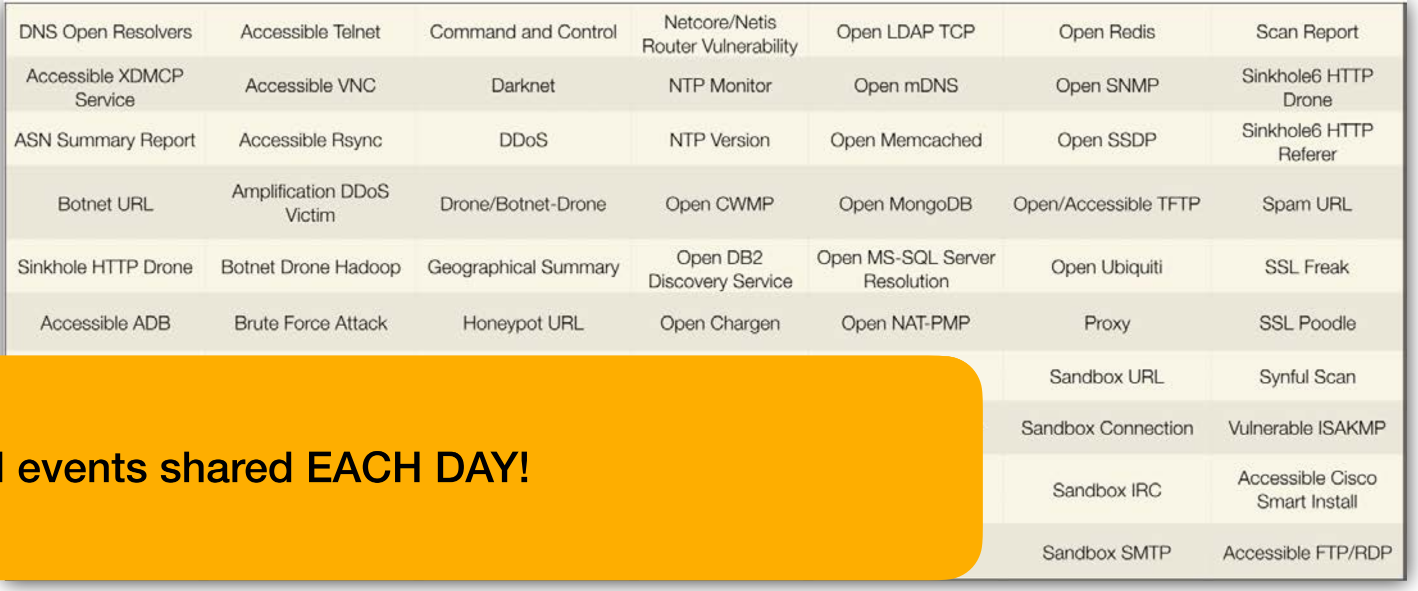
TLP CLEAR

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/

Shadowserver's 2020+ Data Center

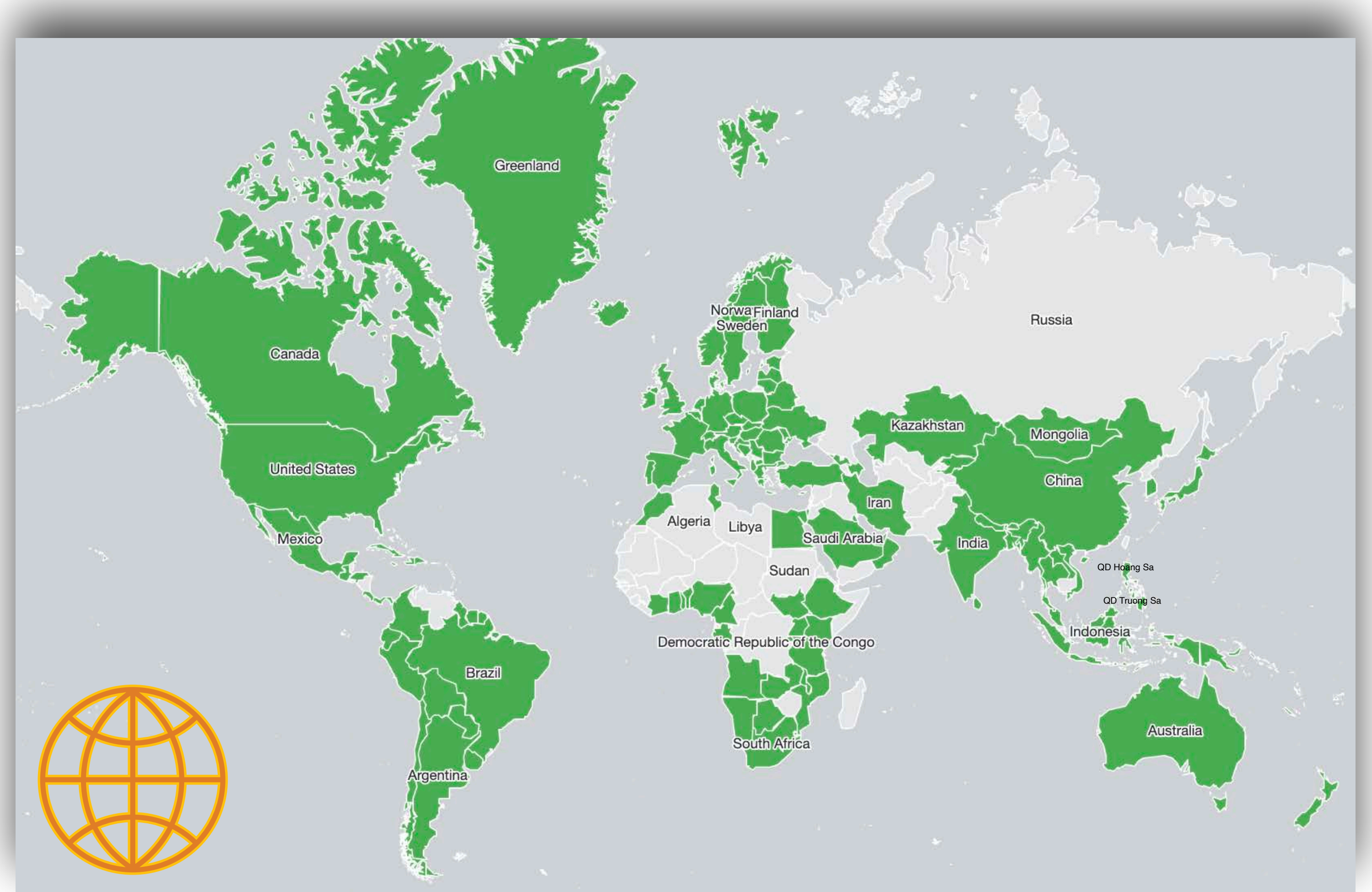
- California
- Caged & secure
- 68 Server Racks (16 Dark)
- 1078 physical servers, 14.2 petabytes storage
- 1751 worker VMs
- 2127 CPUs with 30,812 CPU cores and 142.6 TB RAM
- 4 x 10GB Internet uplinks
- Full backup power, 323kWh capacity
- $30-40M total infrastructure = mid sized enterprise

May 2023

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!

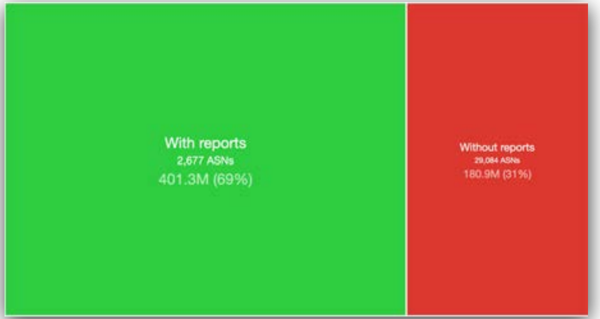
SHADOWSERVER

TLP CLEAR

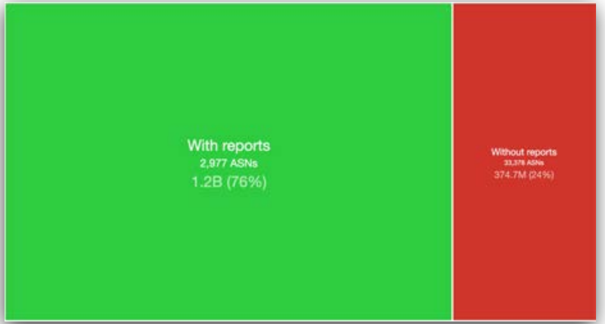
Shadowserver ASN Coverage By Continent (Sep 2025)

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

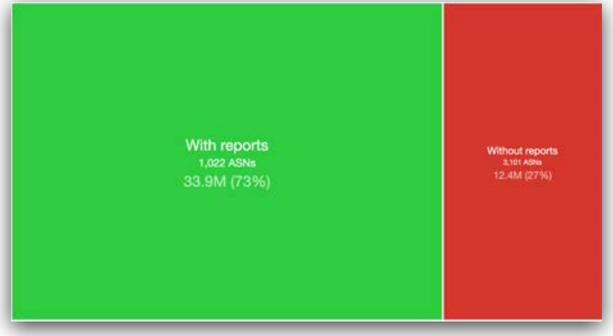
Europe

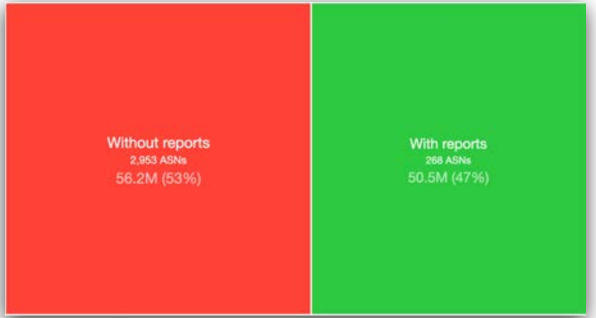


North America

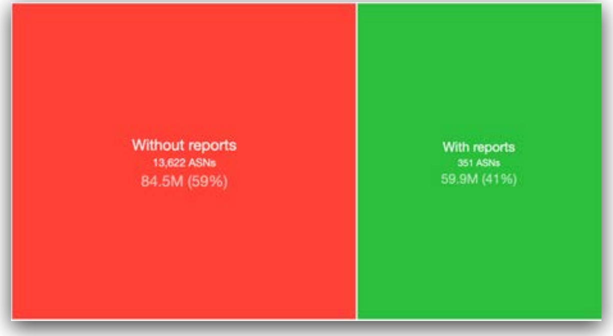


Oceania

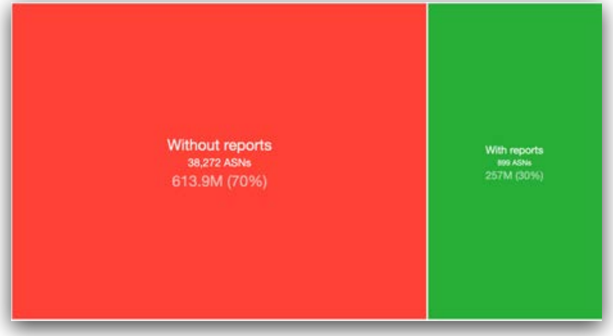




Africa



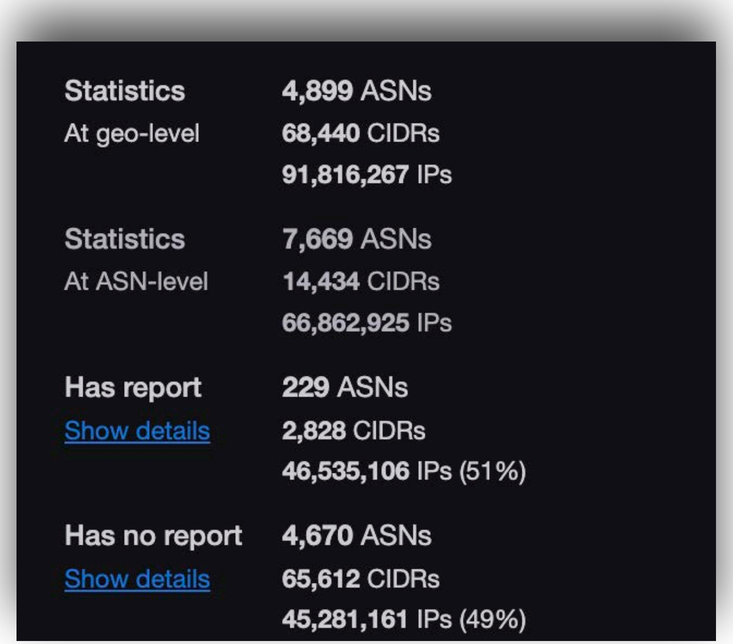
South America



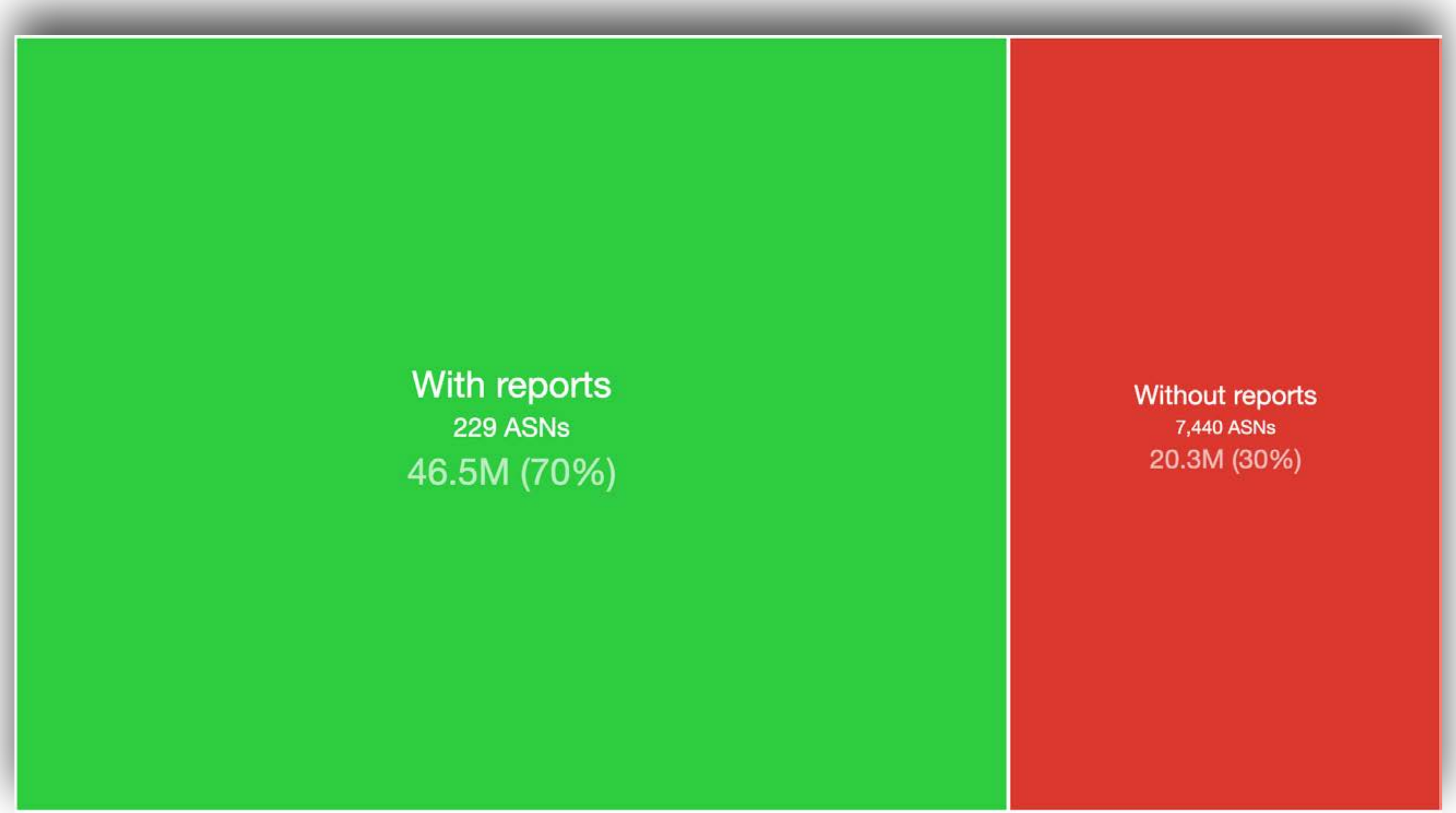
Asia

TLP
CLEAR

ASEAN ASN Owners Subscribed to Daily Reports - Sep 2025



Statistics At geo-level	**4,899** ASNs **68,440** CIDRs **91,816,267** IPs
Statistics At ASN-level	**7,669** ASNs **14,434** CIDRs **66,862,925** IPs
Has report Show details	**229** ASNs **2,828** CIDRs **46,535,106** IPs (51%)
Has no report Show details	**4,670** ASNs **65,612** CIDRs **45,281,161** IPs (49%)

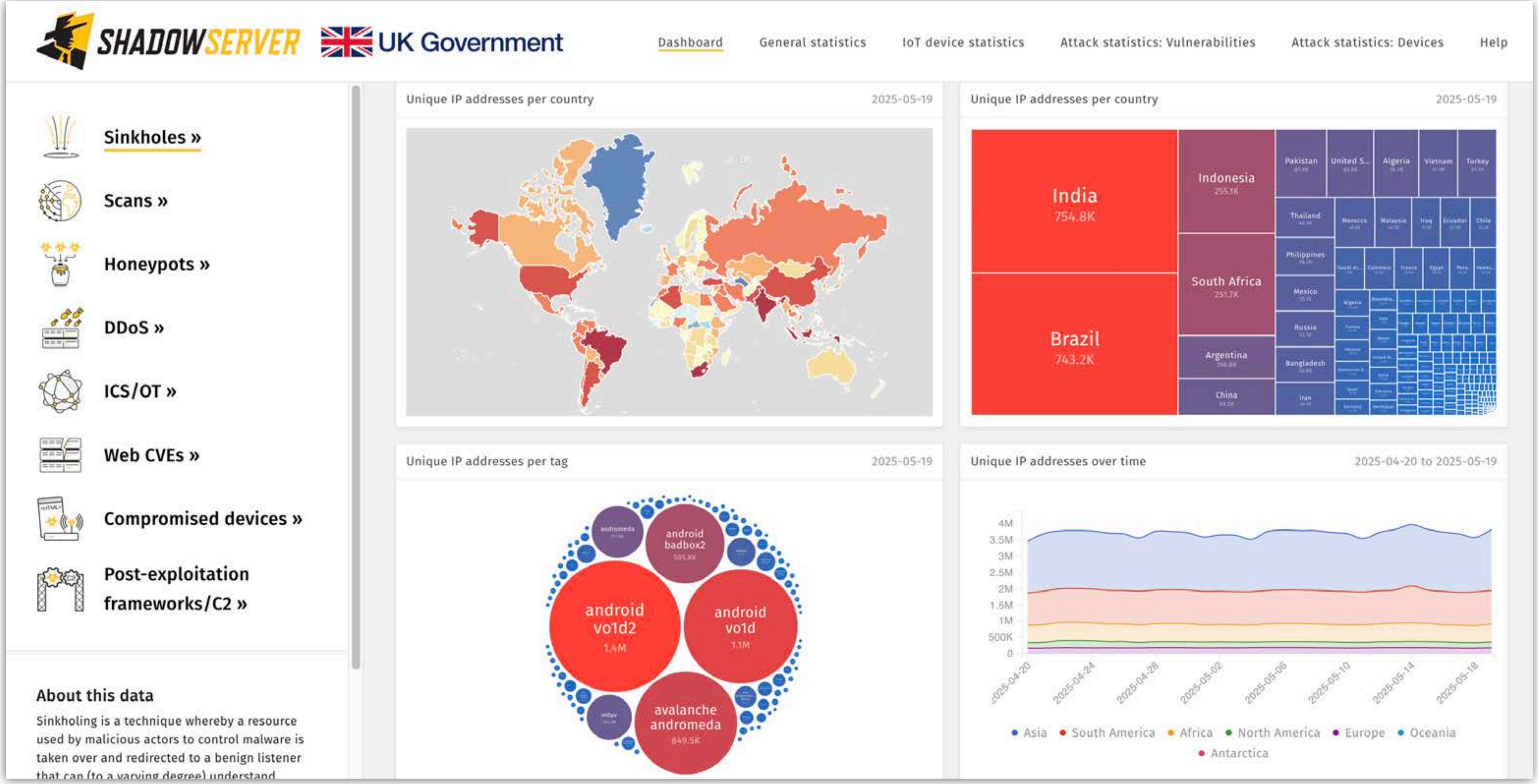


SHADOWSERVER

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

TLP CLEAR

Shadowserver Public Dashboard



SHADOWSERVER | UK Government

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

- Sinkholes »
- Scans »
- Honeypots »
- DDoS »
- ICS/OT »
- Web CVEs »
- Compromised devices »
- Post-exploitation frameworks/C2 »

About this data

Sinkholing is a technique whereby a resource used by malicious actors to control malware is taken over and redirected to a benign listener that can (to a varying degree) understand

Unique IP addresses per country 2025-05-19

Unique IP addresses per country 2025-05-19

Unique IP addresses per tag 2025-05-19

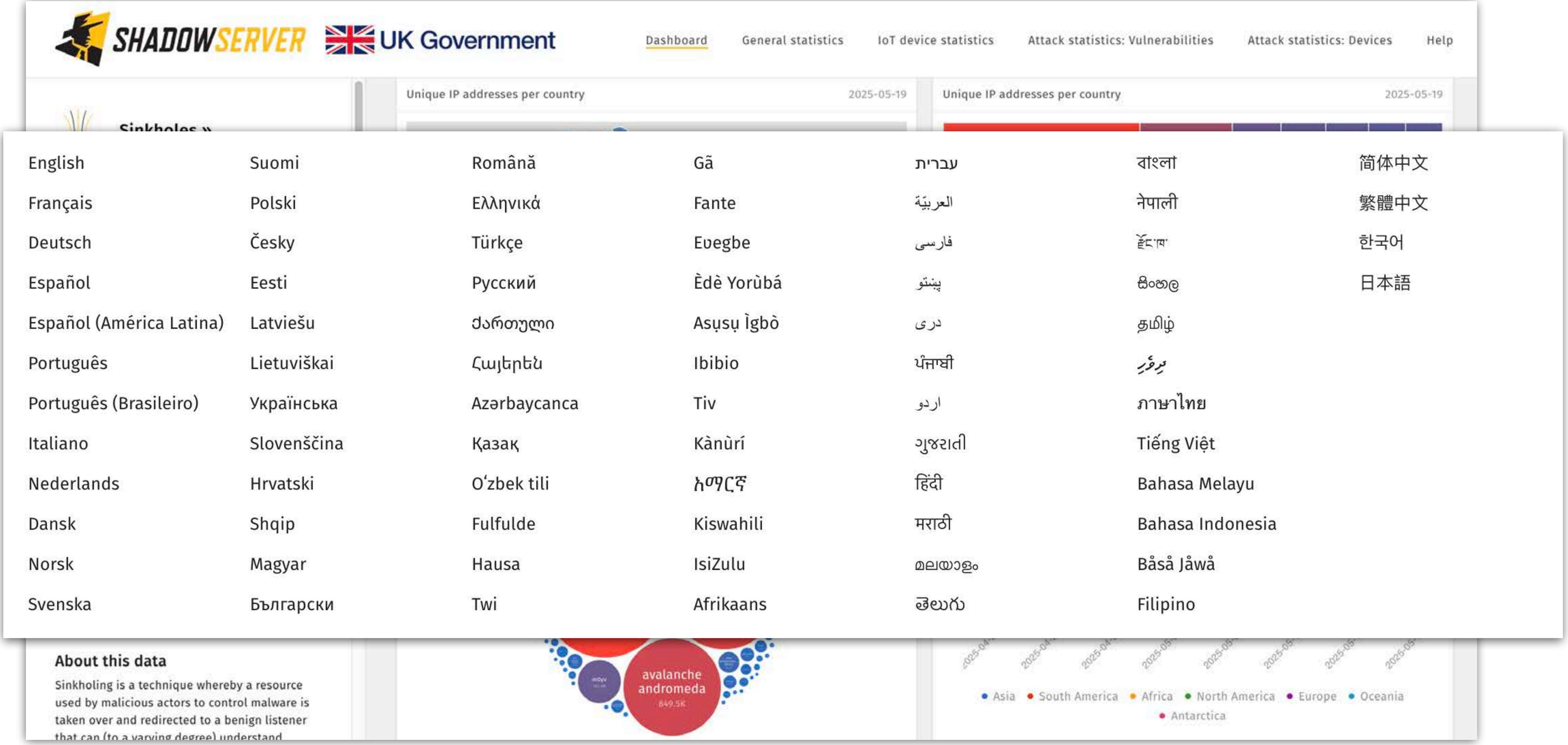
Unique IP addresses over time 2025-04-20 to 2025-05-19

SHADOWSERVER

https://dashboard.shadowserver.org

TLP CLEAR

Shadowserver Public Dashboard



SHADOWSERVER UK Government

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

Unique IP addresses per country 2025-05-19

Unique IP addresses per country 2025-05-19

Sinkholes »

English
Français
Deutsch
Español
Español (América Latina)
Português
Português (Brasileiro)
Italiano
Nederlands
Dansk
Norsk
Svenska

Suomi
Polski
Česky
Eesti
Latviešu
Lietuviškai
Українська
Slovenščina
Hrvatski
Shqip
Magyar
Български

Română
Ελληνικά
Türkçe
Русский
ქართული
Հայերեն
Azərbaycanca
Қазақ
O‘zbek tili
Fulfulde
Hausa
Twi

Gã
Fante
Eʋegbe
Èdè Yorùbá
Asụsụ Ìgbò
Ibibio
Tiv
Kànùrí
አማርኛ
Kiswahili
IsiZulu
Afrikaans

עברית
العربيّة
فارسی
پښتو
دری
ਪੰਜਾਬੀ
اردو
ગુજરાતી
हिंदी
मराठी
മലയാളം
తెలుగు

বাংলা
नेपाली
རྫོང་ཁ
සිංහල
தமிழ்
ދިވެހި
ภาษาไทย
Tiếng Việt
Bahasa Melayu
Bahasa Indonesia
Båså Jåwå
Filipino

简体中文
繁體中文
한국어
日本語

About this data

Sinkholing is a technique whereby a resource used by malicious actors to control malware is taken over and redirected to a benign listener that can (to a varying degree) understand

SHADOWSERVER

https://dashboard.shadowserver.org

Internet-wide scanning

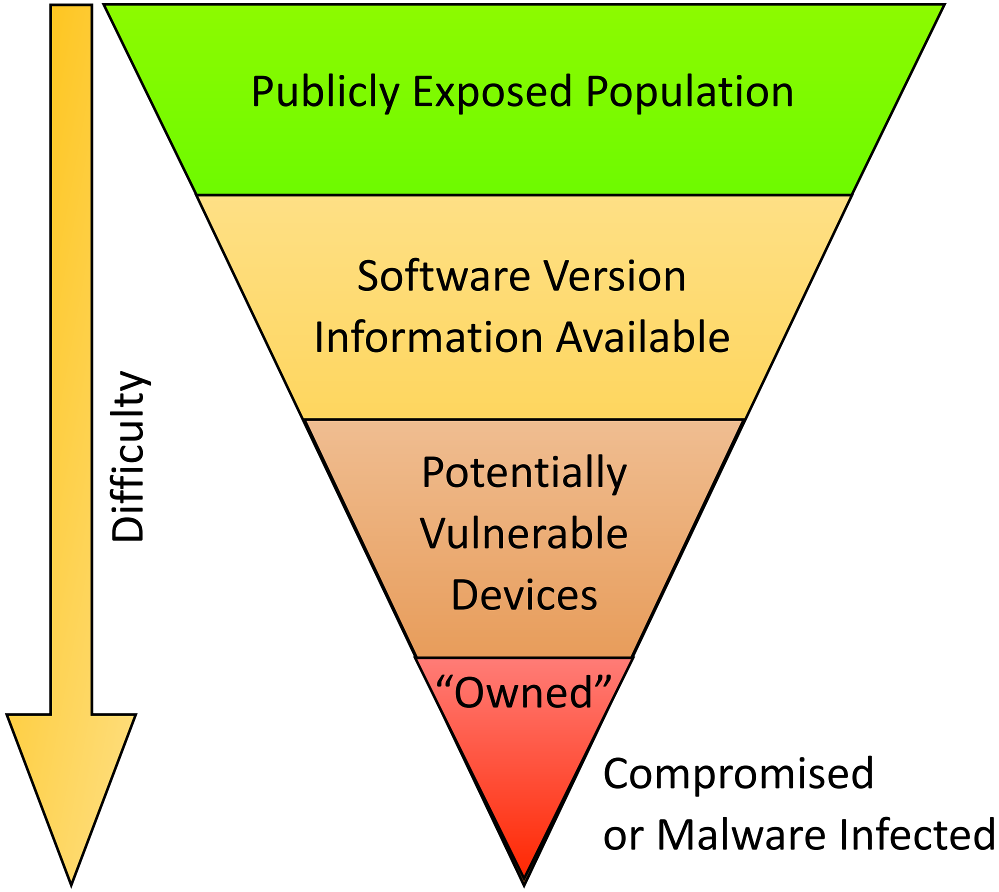
Fingerprinting all things

TLP CLEAR

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*


Difficulty
Publicly Exposed Population
Software Version Information Available
Potentially Vulnerable Devices
"Owned"
Compromised or Malware Infected

SHADOWSERVER

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

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”

TLP CLEAR

Collaboration

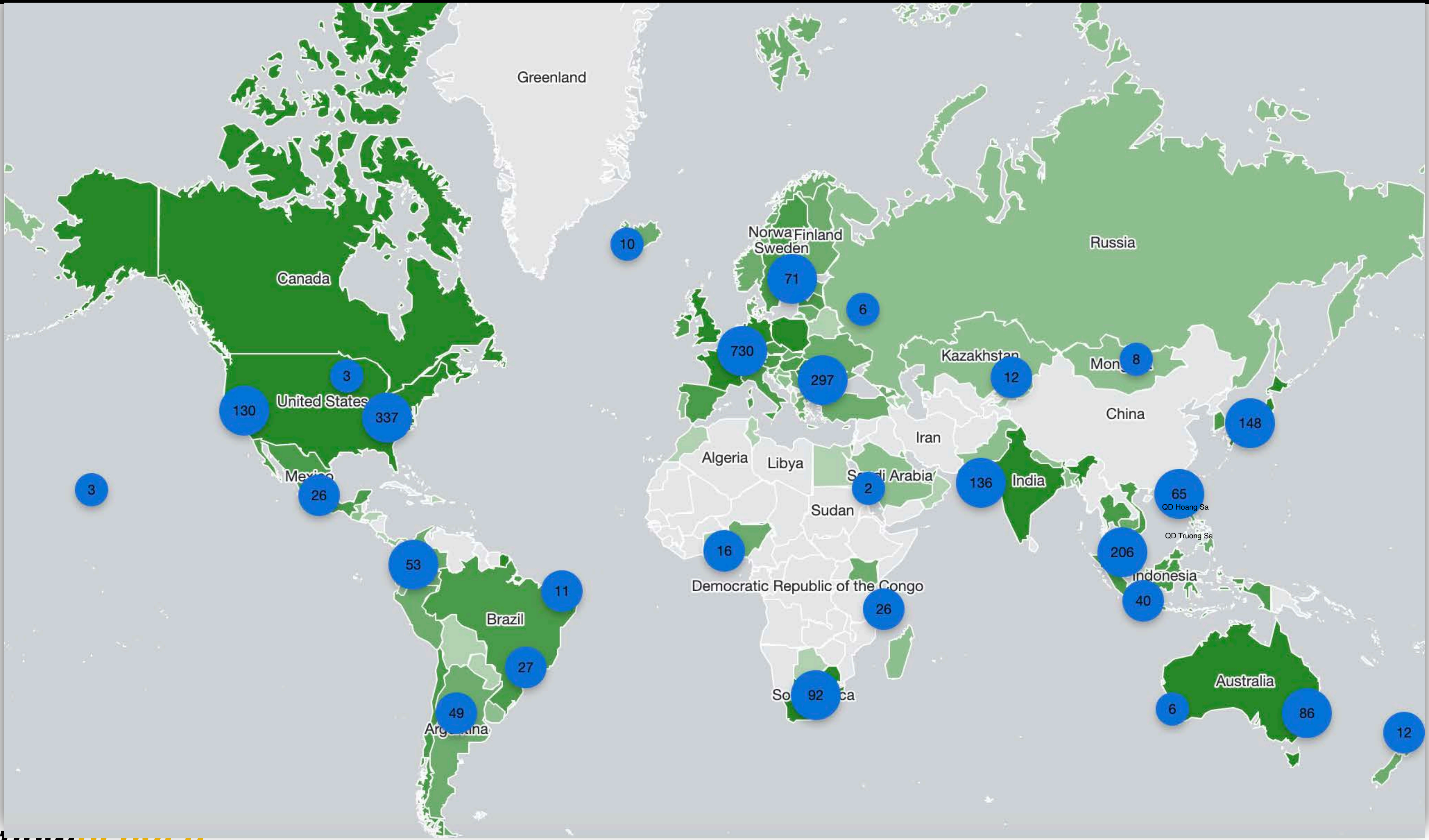
- Are there any scans you would like to see us implement?
- Device fingerprinting suggestions? (including remote version identification)
- Any RCE vulnerabilities we should scan for (without actual exploitation)? How?
- Are there any remote webshells/ implant/backdoor scans we should implement? How?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

SHADOWSERVER

Tracking vulnerability exploitation in the wild

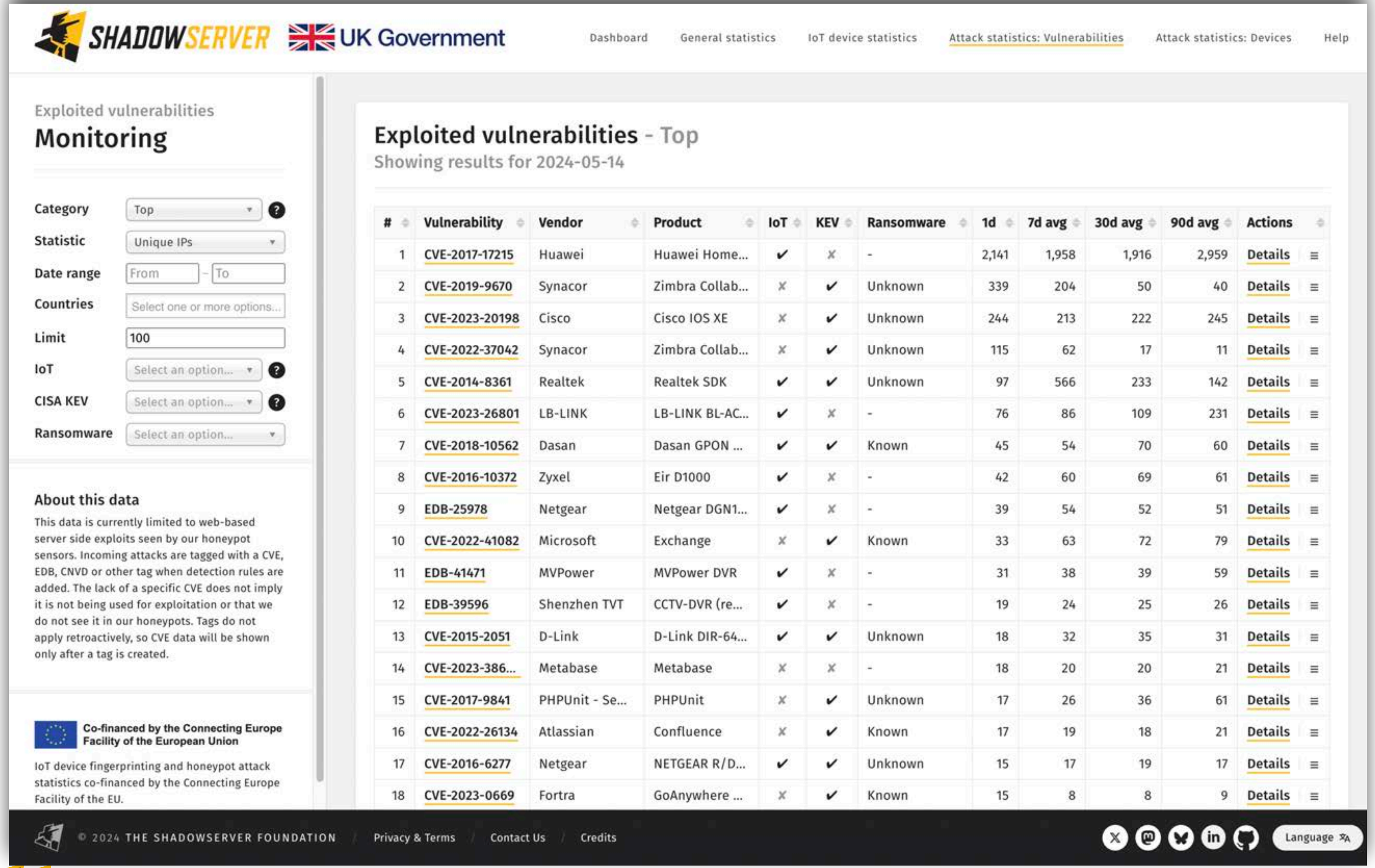
Using honeypots

Honeypot sensor network - World & ASEAN (Sep 2025)



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

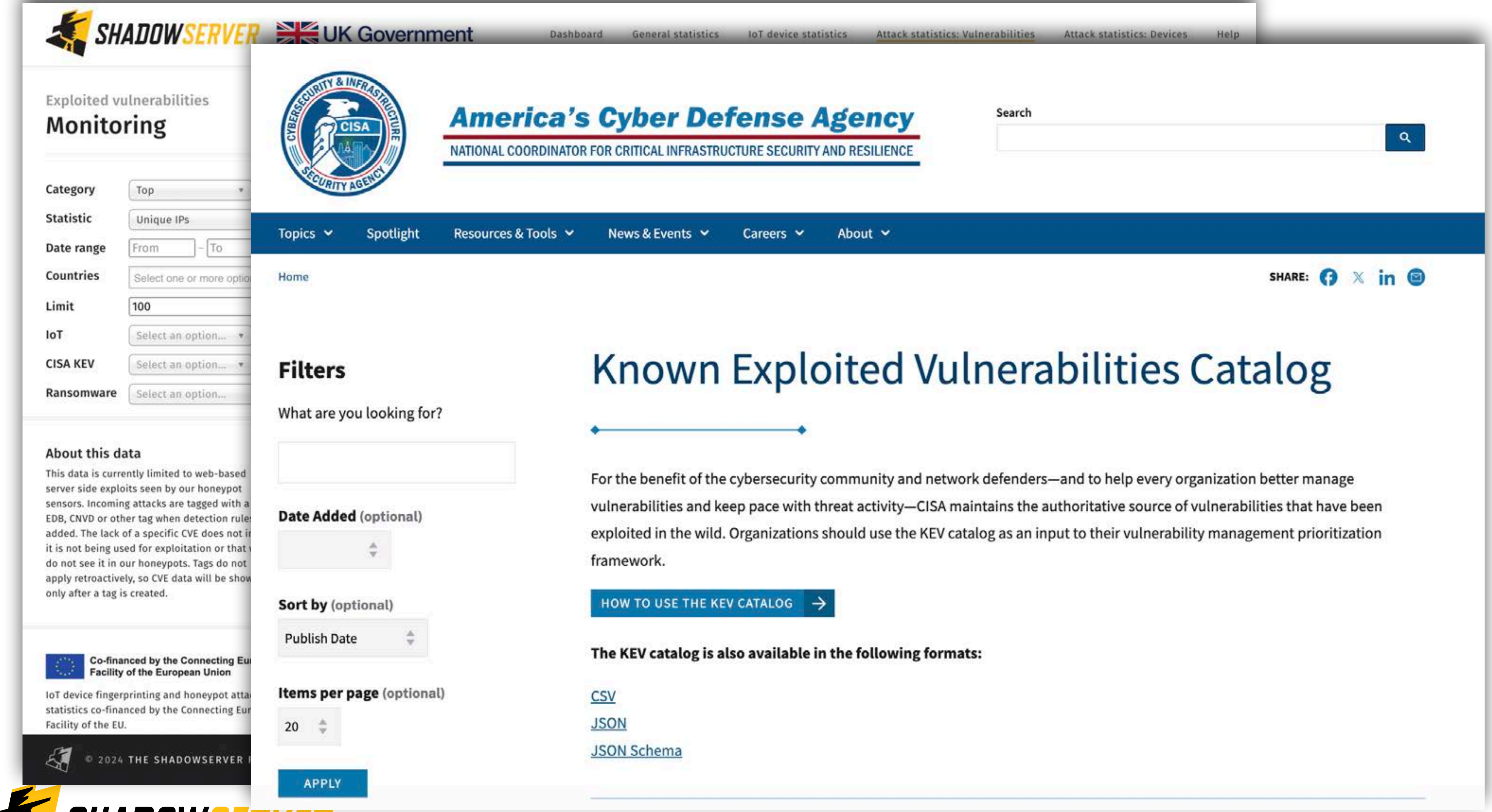
#	Vulnerability	Vendor	Product	IoT	KEV	Ransomware	1d	7d avg	30d avg	90d avg	Actions
1	CVE-2017-17215	Huawei	Huawei Home...	✓	✗	-	2,141	1,958	1,916	2,959	Details ≡
2	CVE-2019-9670	Synacor	Zimbra Collab...	✗	✓	Unknown	339	204	50	40	Details ≡
3	CVE-2023-20198	Cisco	Cisco IOS XE	✗	✓	Unknown	244	213	222	245	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

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 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 rule 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 Eu Facility of the EU.

© 2024 THE SHADOWSERVER F

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

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

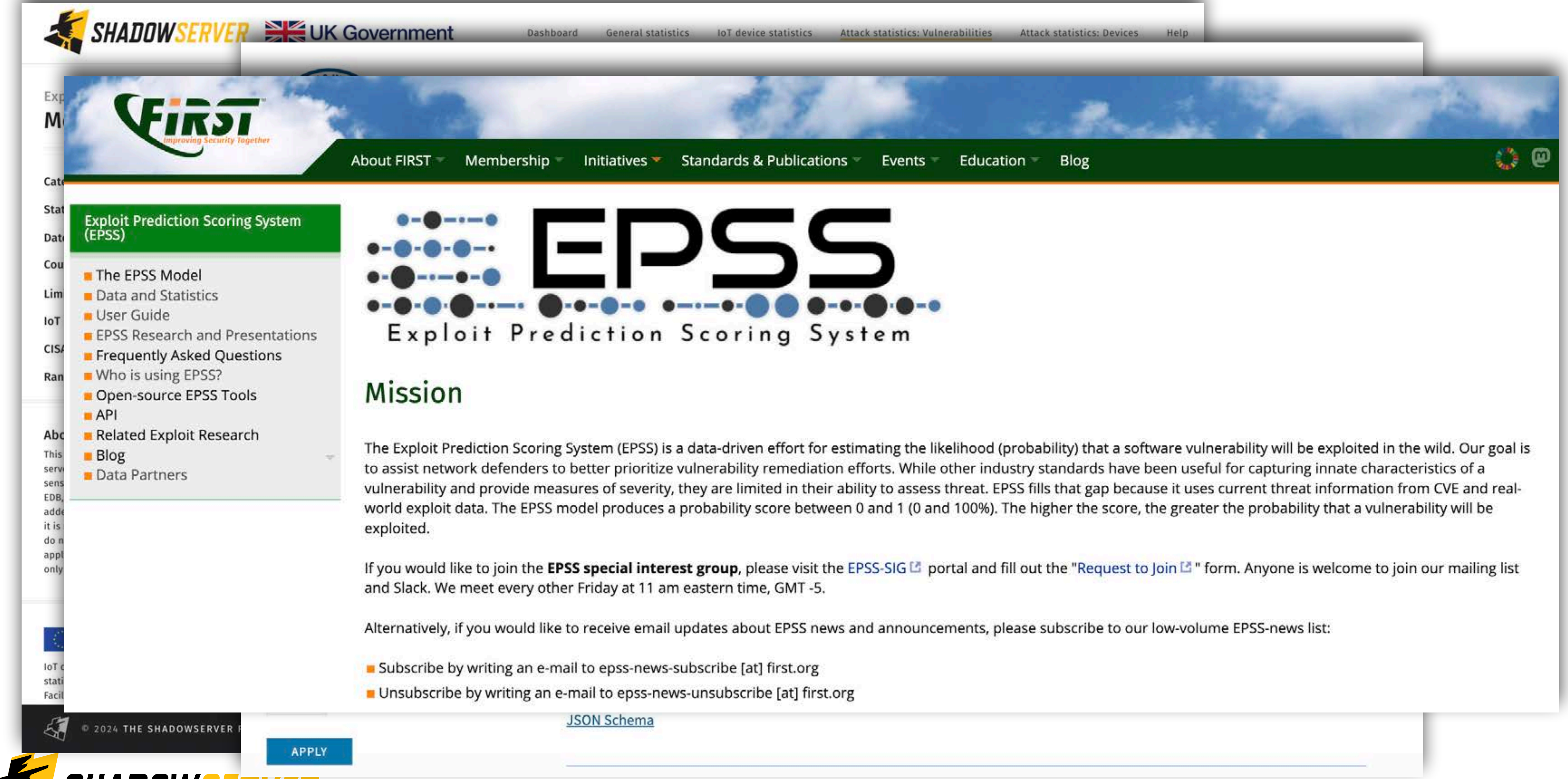
JSON

JSON Schema

SHADOWSERVER

Exploitation tracking (by CVE or similar)

TLP CLEAR



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.

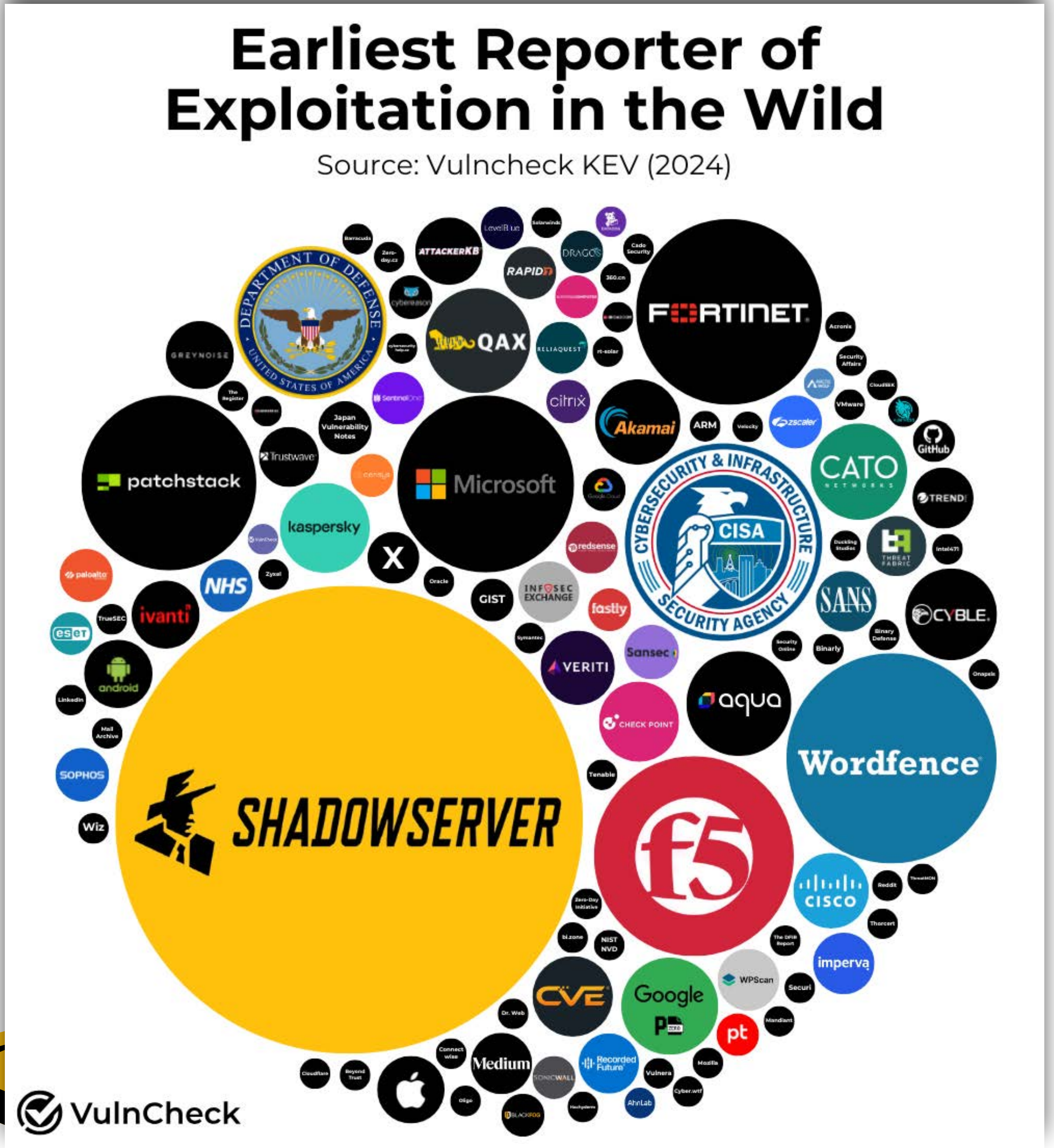
If you would like to join the **EPSS special interest group**, please visit the EPSS-SIG portal and fill out the "Request to Join" form. Anyone is welcome to join our mailing list and Slack. We meet every other Friday at 11 am eastern time, GMT -5.

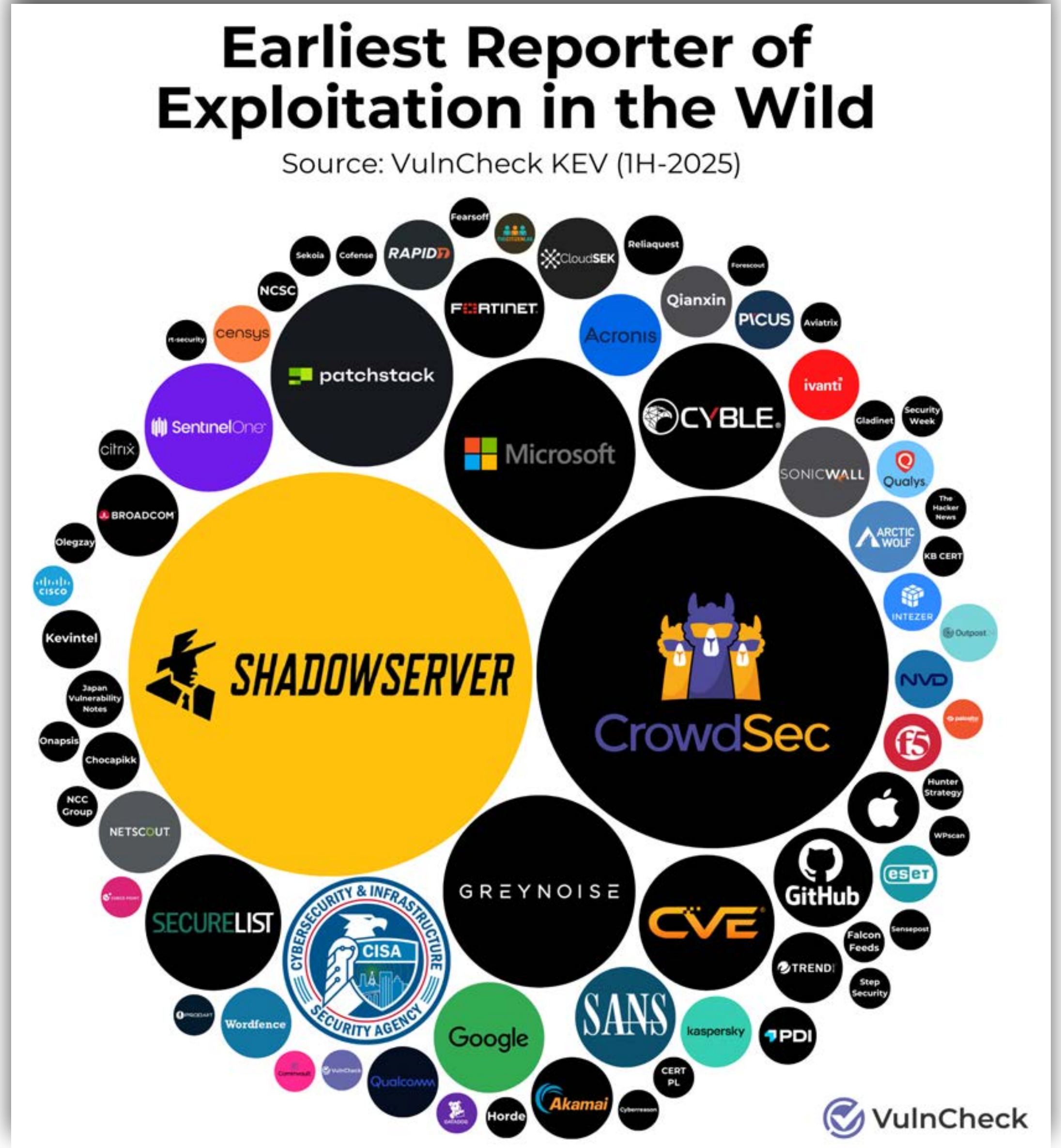
Alternatively, if you would like to receive email updates about EPSS news and announcements, please subscribe to our low-volume EPSS-news list:

- 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

TLP
CLEAR

Earliest Reporter of Exploitation in the Wild


Earliest Reporter of Exploitation in the Wild
Source: Vulncheck KEV (2024)


Earliest Reporter of Exploitation in the Wild
Source: VulnCheck KEV (1H-2025)

TLP CLEAR

Better Insights? Host a 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 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

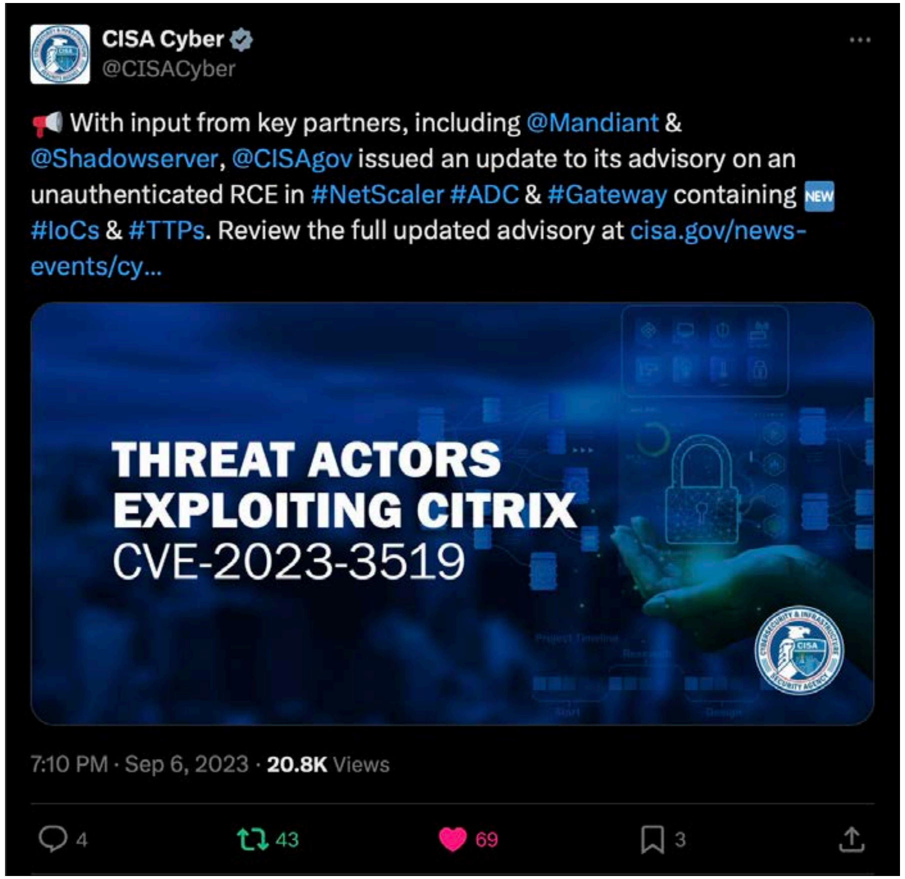
Case studies

Collaborative Response to Emerging Critical RCE Vulnerabilities in Exposed Assets

TLP
CLEAR

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-2025-53770)
- Working with Alliance partners & incident responder communities on the ground to understand vulnerable populations, compromised assets



CISA Cyber
@CISACyber

📢 With input from key partners, including @Mandiant & @Shadowserver, @CISAgov issued an update to its advisory on an unauthenticated RCE in #NetScaler #ADC & #Gateway containing 🆕 #IoCs & #TTPs. Review the full updated advisory at cisa.gov/news-events/cy…

7:10 PM · Sep 6, 2023 · 20.8K Views

4 43 69 3

SHADOWSERVER

Cisco IOS XE

BadCandy implants (Autumn 2023 - ongoing)

TLP CLEAR

Cisco IOS XE BadCandy

TLP CLEAR

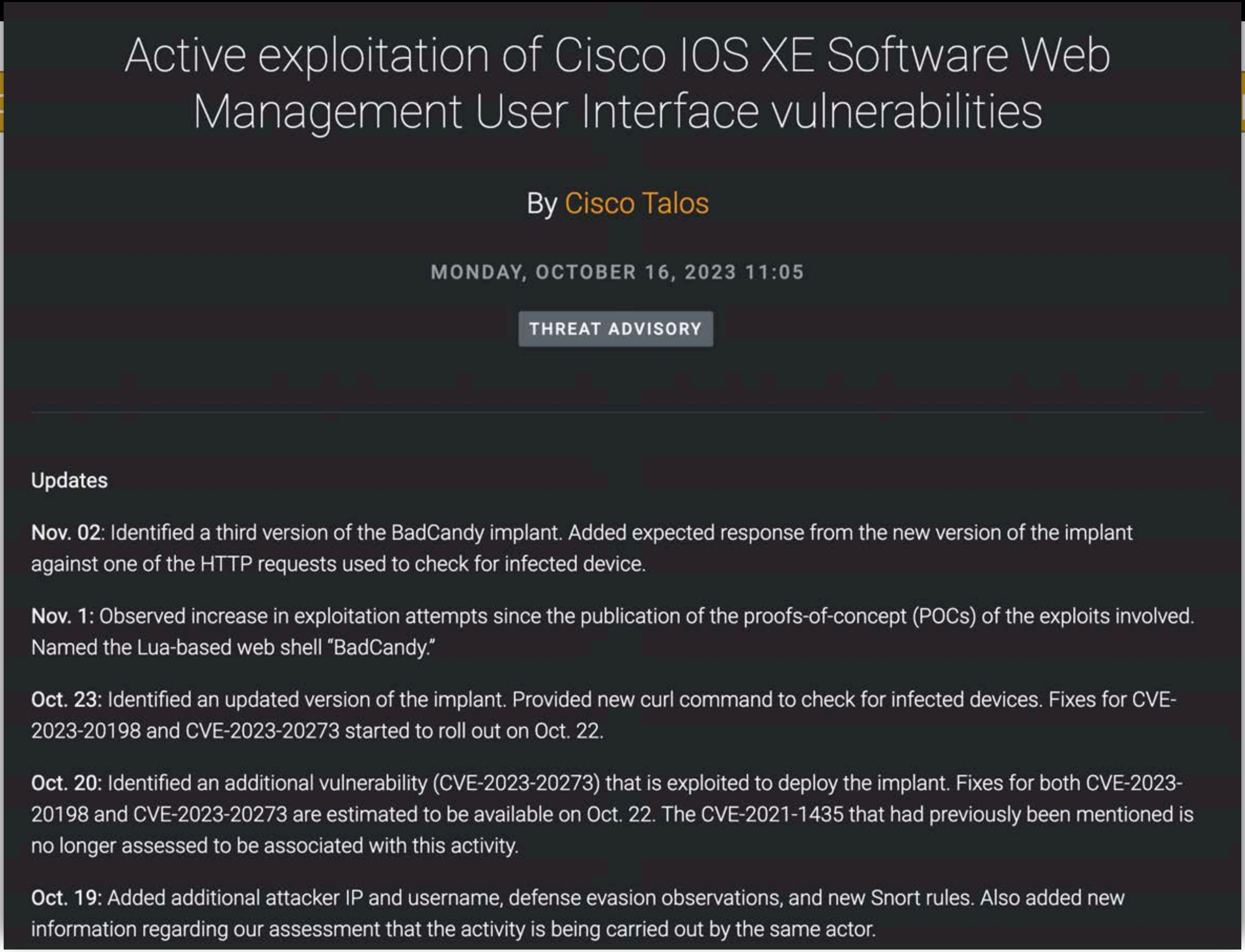
Cisco IOS XE BadCandy

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

TLP CLEAR

Cisco IOS XE BadCandy

Oct 16th: Cisco Talos publicatic 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

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

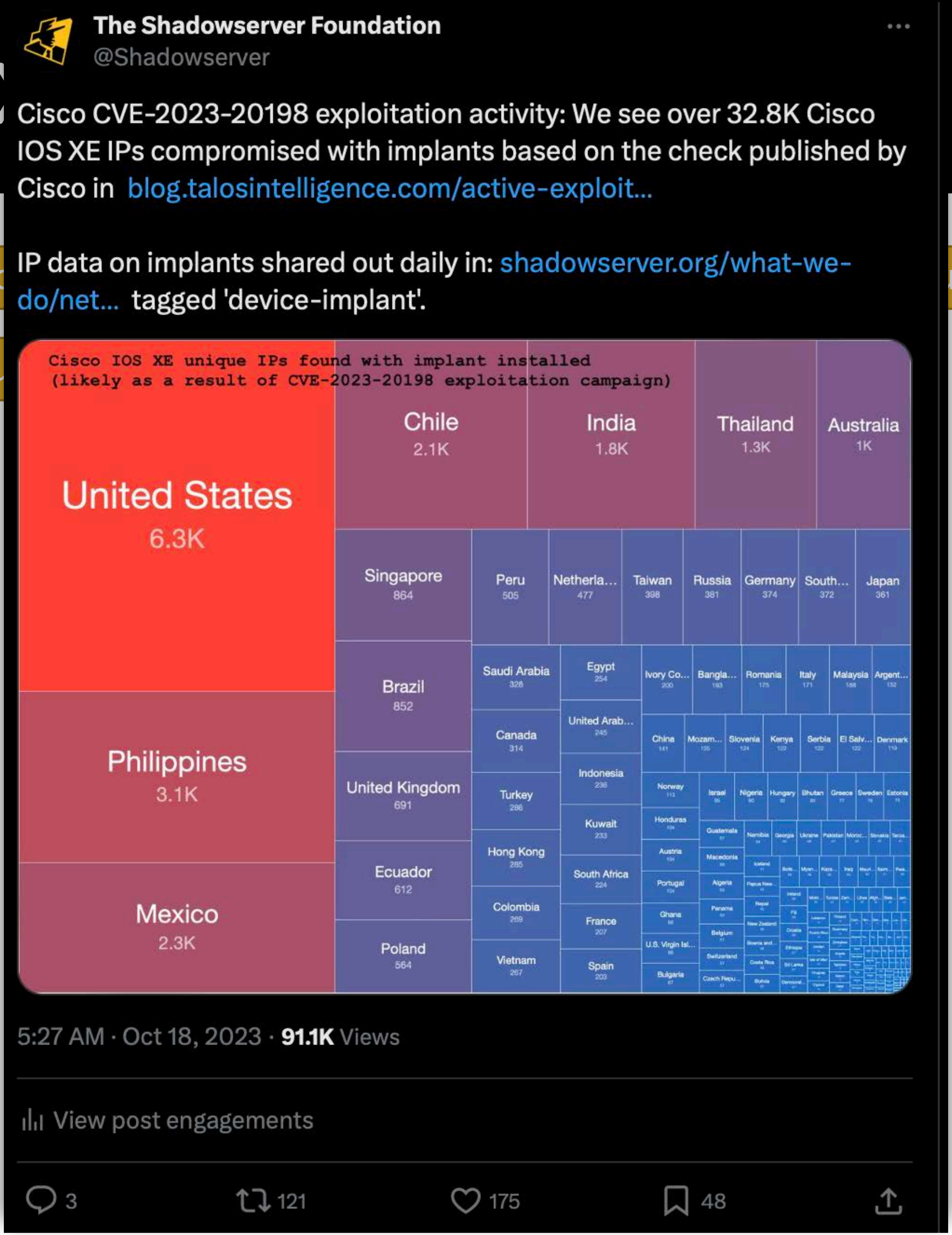
SHADOWSERVER

TLP
CLEAR

Cisco IOS

Oct 16th: Cisco Talos publicati lnerabilities. 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'.

```
Cisco IOS XE unique IPs found with implant installed
(likely as a result of CVE-2023-20198 exploitation campaign)
```

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

View post engagements

3 121 175 48

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 for Cisco IOS XE

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 for Cisco IOS XE

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 for Cisco IOS XE

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 for Cisco IOS XE

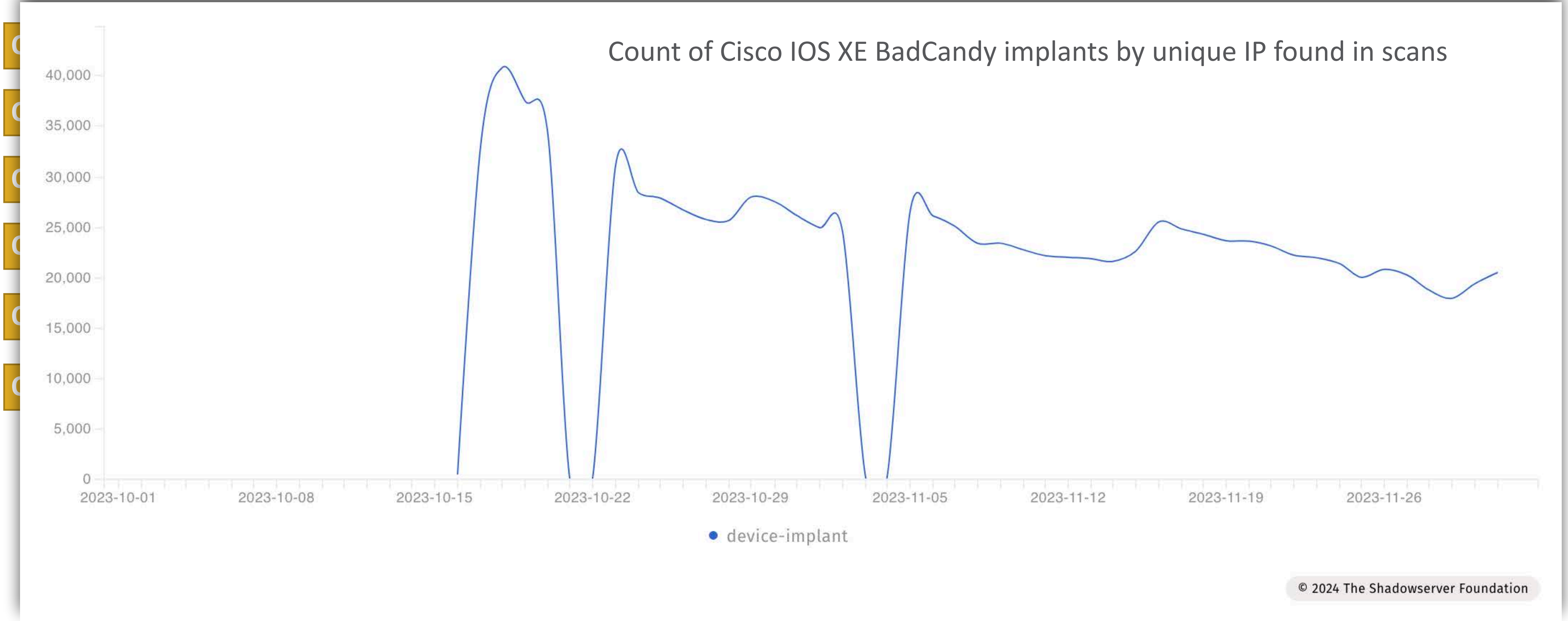
Oct 19th: First implant scans immediately detected after rollout

Oct 22nd: Implant updated by attackers

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

TLP CLEAR

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

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

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 for Cisco IOS XE

Oct 19th: First implant scans immediately detected after rollout

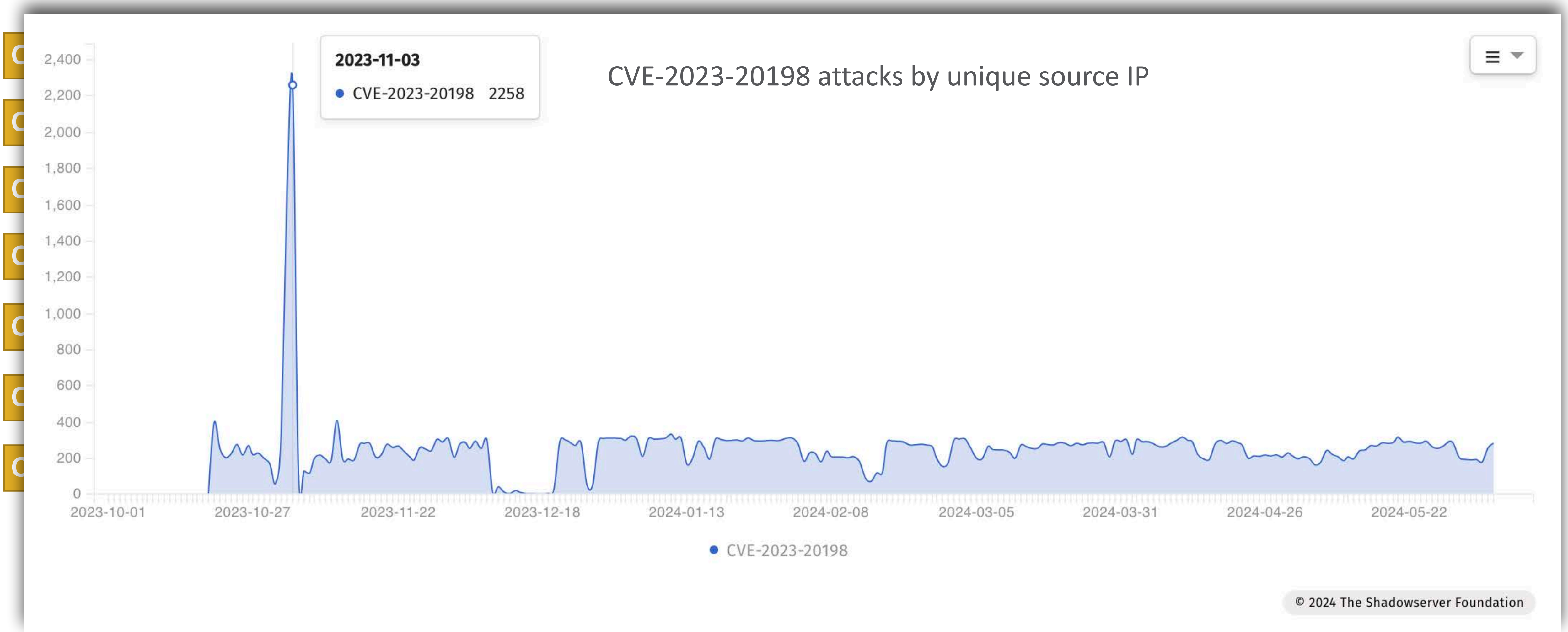
Oct 22nd: Implant updated by attackers

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

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 for Cisco IOS XE

Oct 19th: First implant scans immediately detected after rollout

Oct 22nd: Implant updated by attackers

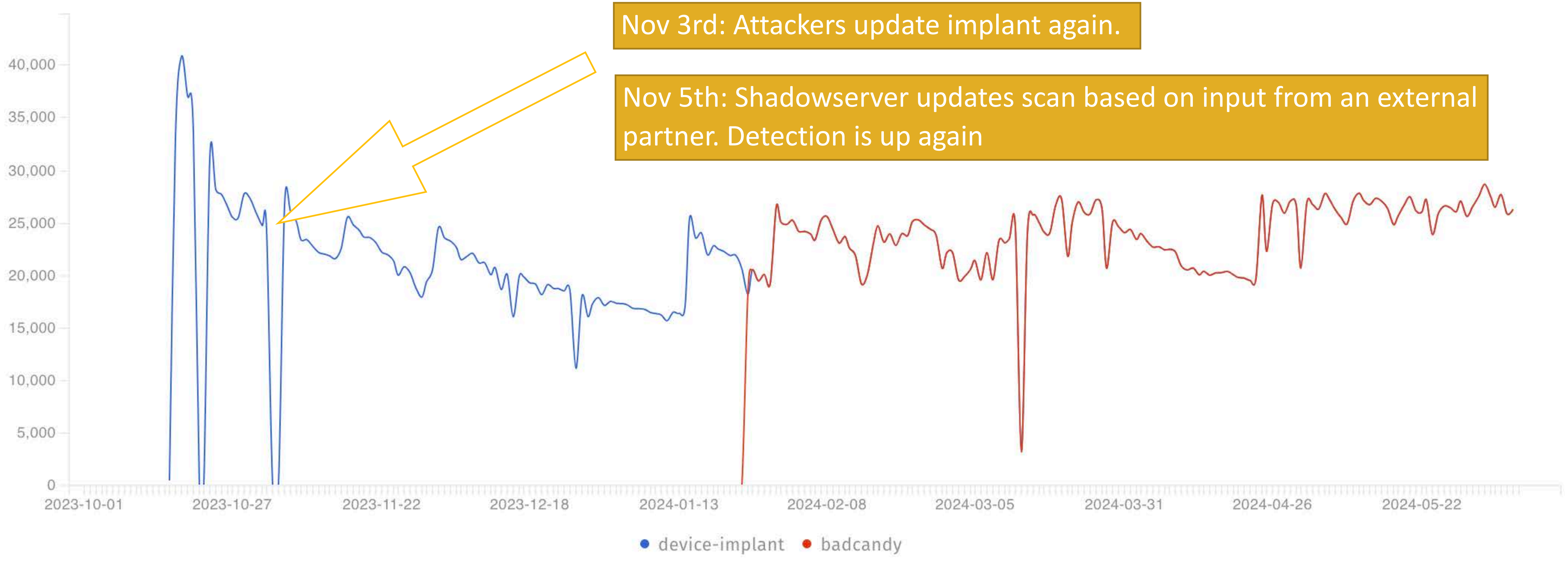
Oct 23rd: Cisco updates advisory with new implant details. Shadowserver scans updated

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

SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy



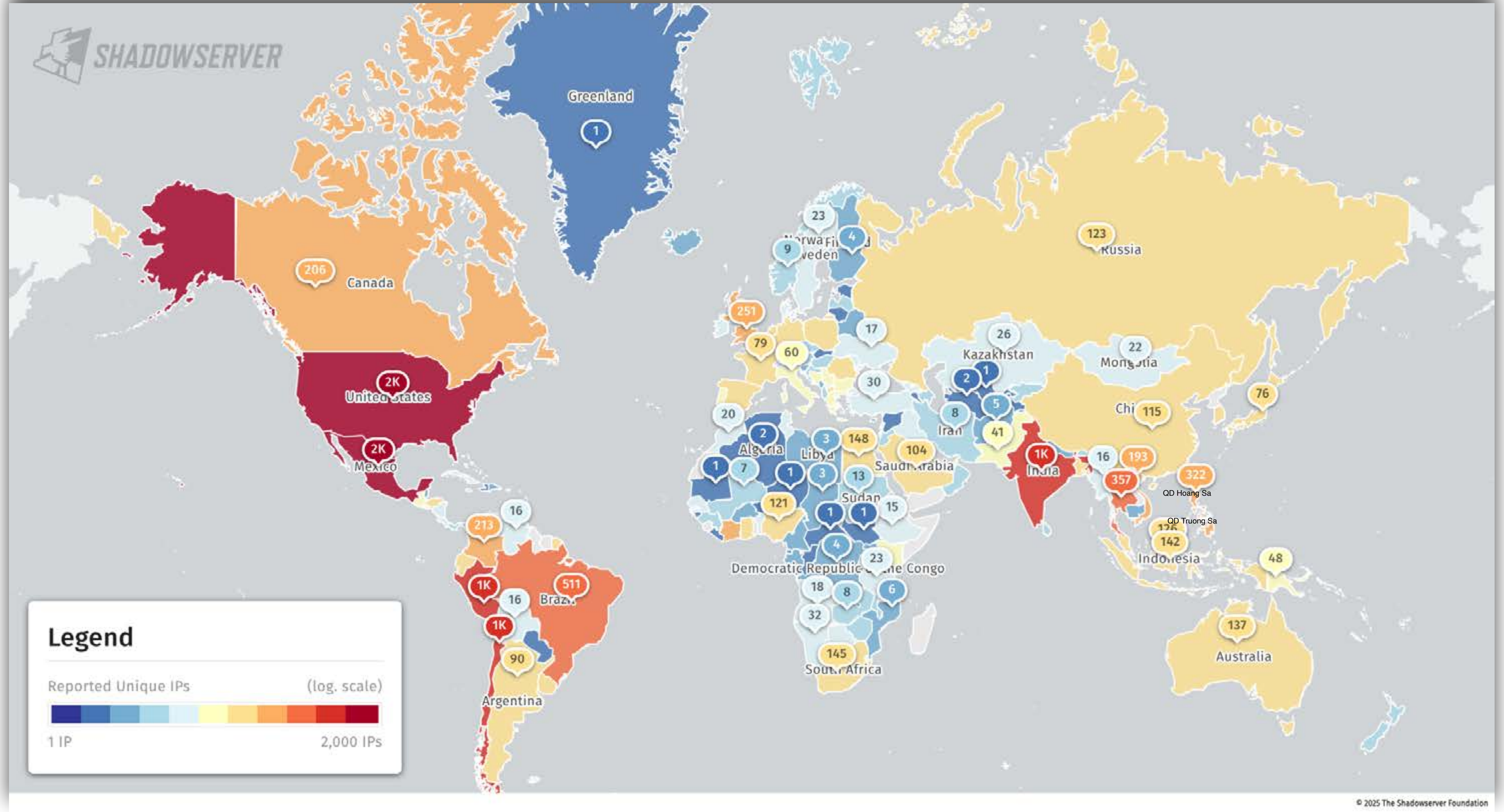
Nov 3rd: Attackers update implant again.

Nov 5th: Shadowserver updates scan based on input from an external partner. Detection is up again

SHADOWSERVER

TLP CLEAR

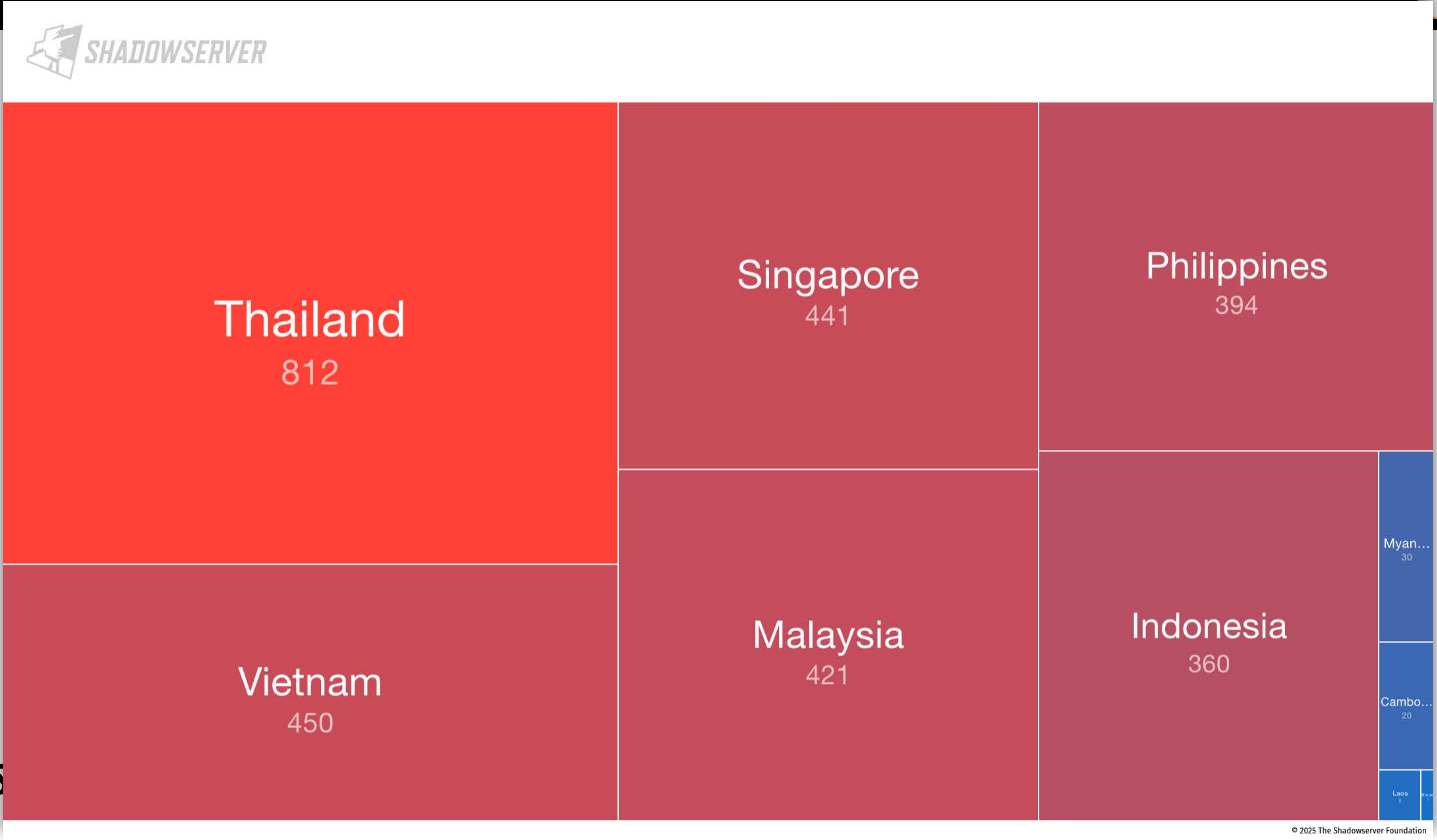
Cisco IOS XE BadCandy - 2025-09-06 - Still ongoing!



SHADOWSERVER

TLP CLEAR

Cisco IOS XE BadCandy - 2025-09-06 - Still ongoing!



© 2025 The Shadowserver Foundation

Palo Alto PAN-OS

CVE-2024-0012 (Autumn 2024 - Current)

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012

TLP
CLEAR

Palo Alto PAN-OS CVE-2024-0012

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

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012

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

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012

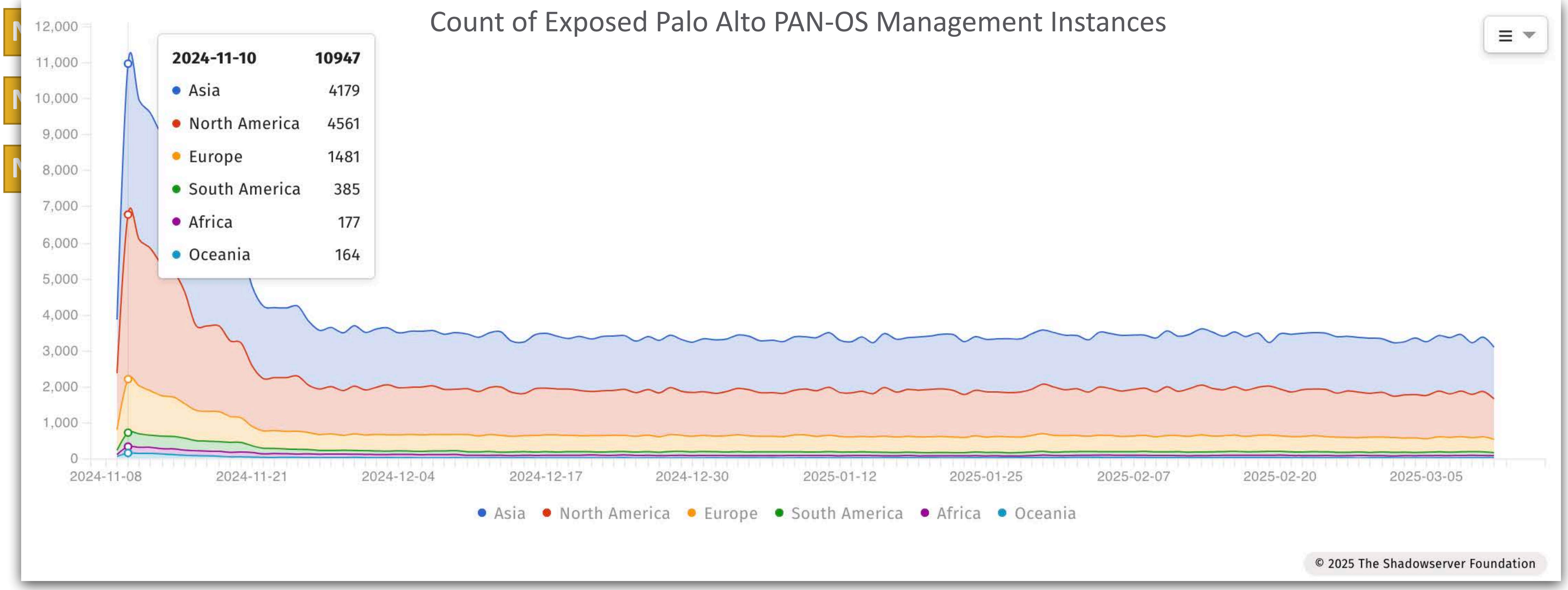
November 8th: Tipped off that exposed PAN-OS management interfaces may be vulnerable to a 0-day

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



SHADOWSERVER

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012

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

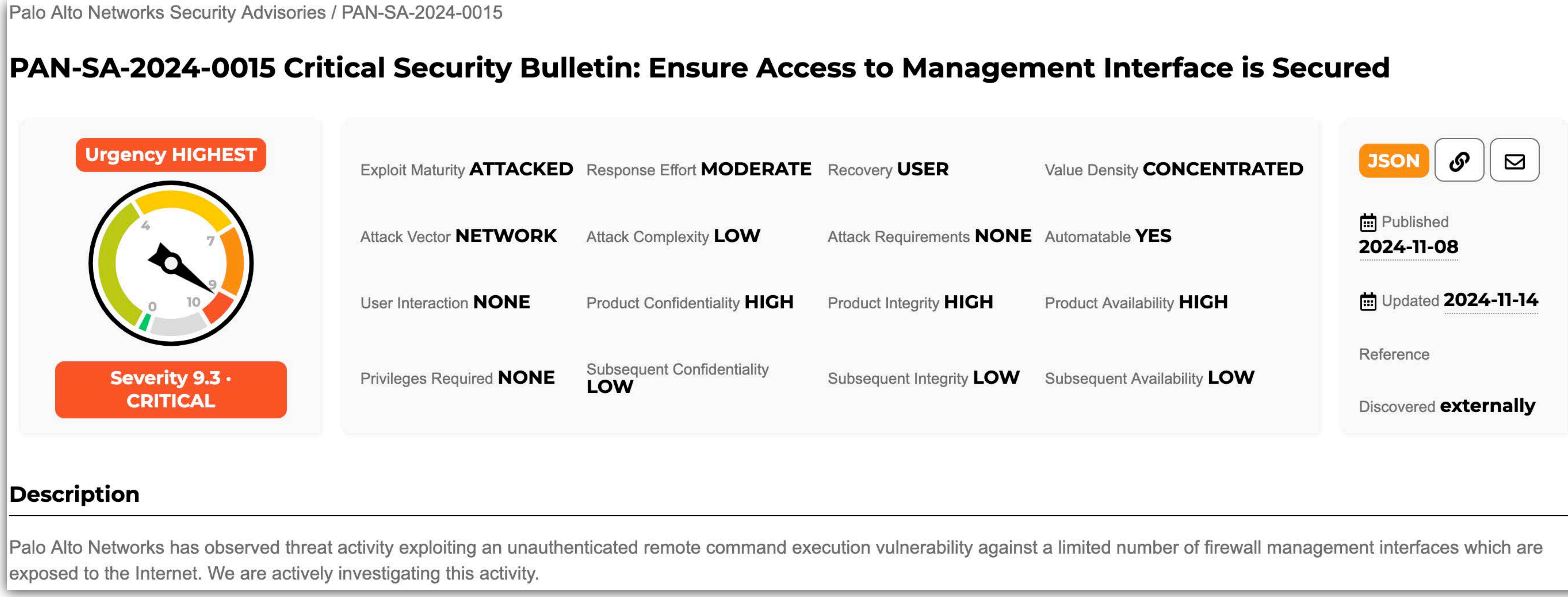
November 8th: Detections added and device id rules generated. Palo Alto issues initial advisory about potential 0day

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

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

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012



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**

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.

TLP
CLEAR

Palo Alto PAN-OS CVE-2024-0012

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

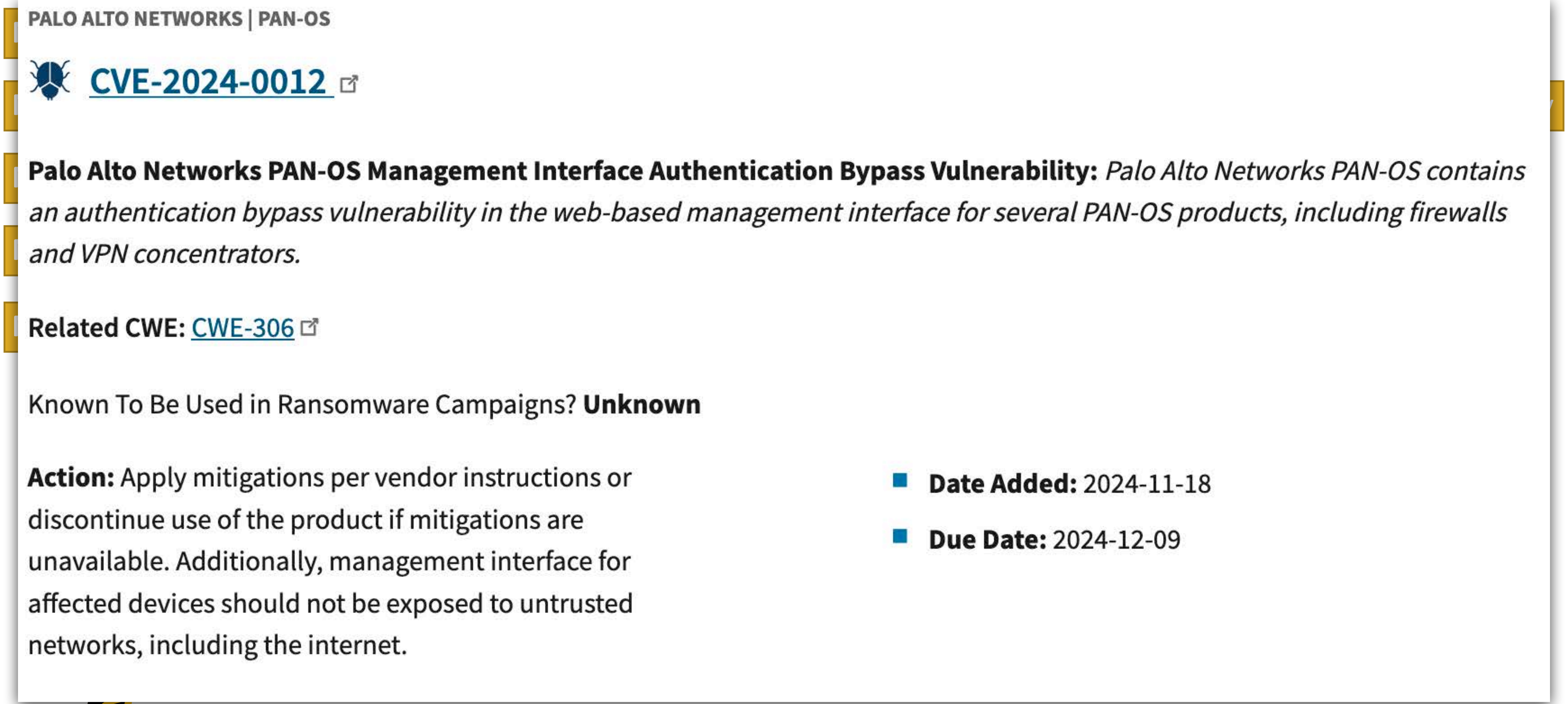
November 10th: Data on exposed interfaces goes out to report recipients

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

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

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012



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

TLP
CLEAR

Palo Alto PAN-OS CVE-2024-0012

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

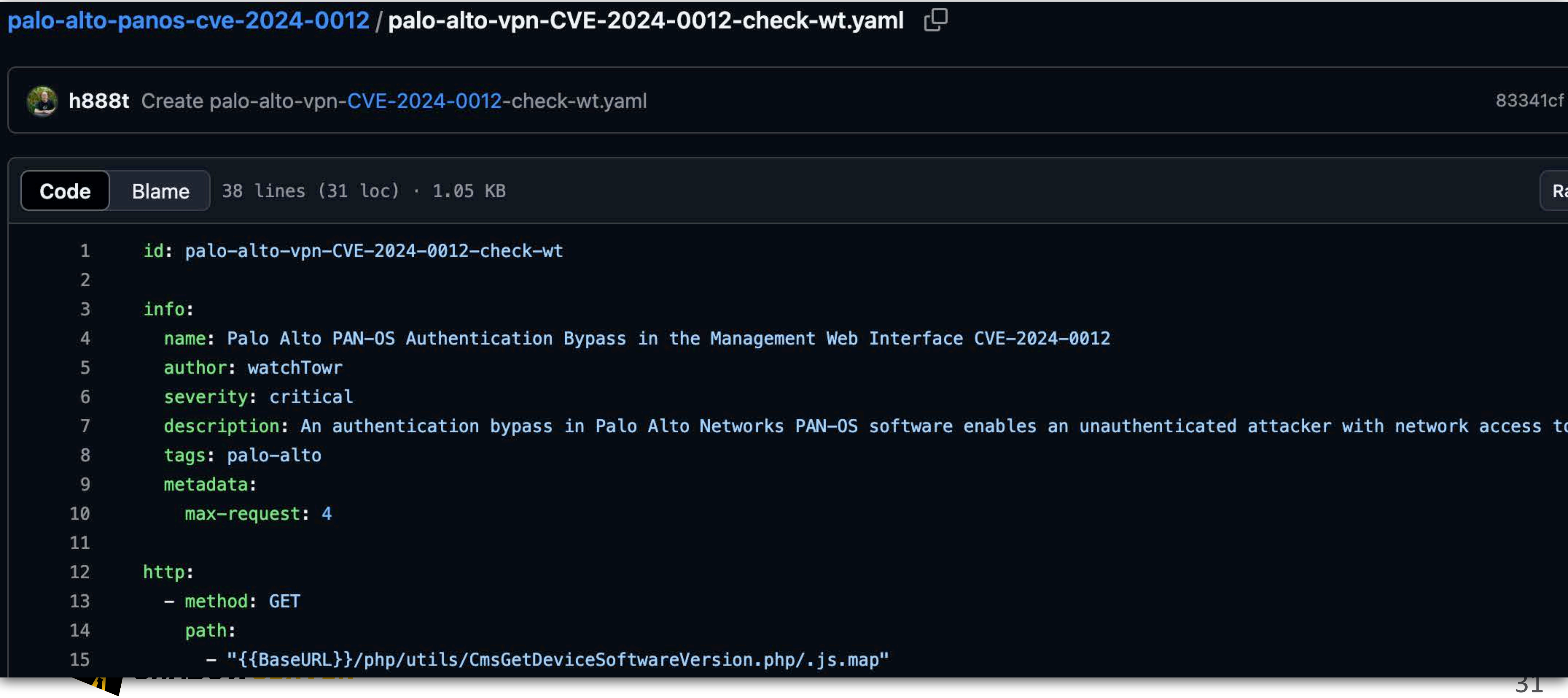
November 14th: Palo Alto issues updated notice that there is a vulnerability

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



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

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 t
  tags: palo-alto
  metadata:
    max-request: 4

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

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012

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

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

Nove

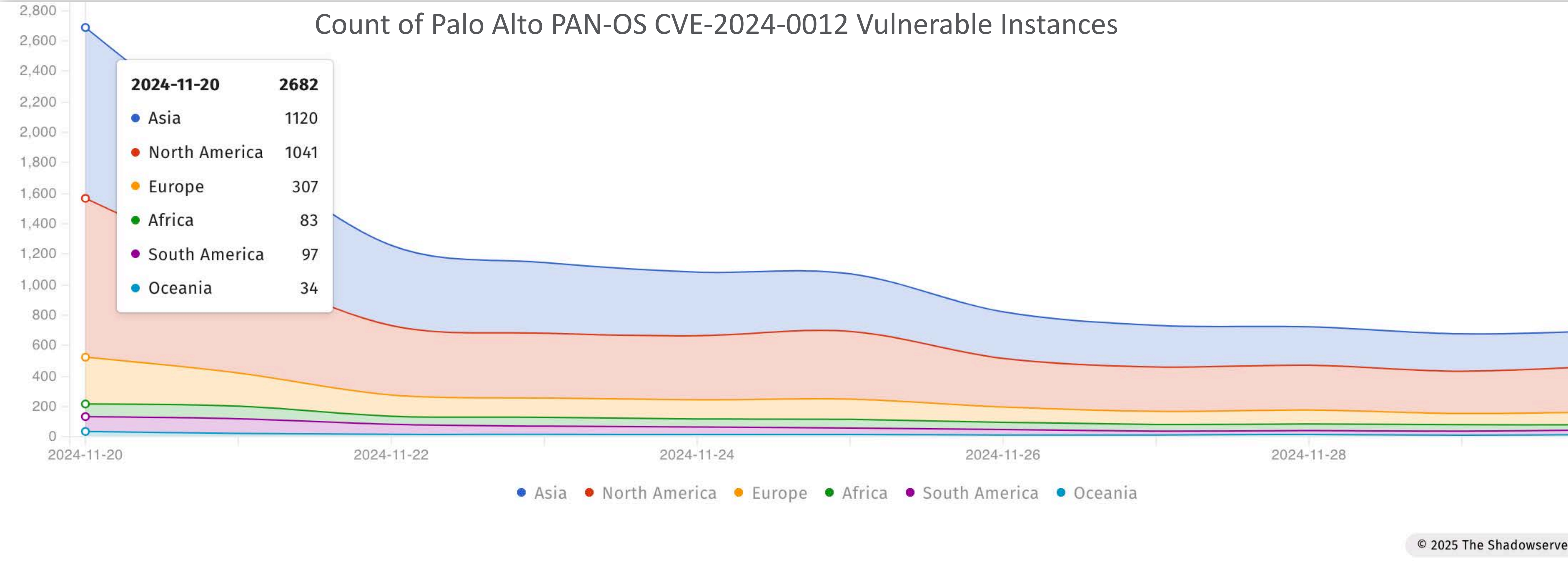
Nove

Nove

Nove

Nove

Nove



2024-11-20	**2682**
● Asia	1120
● North America	1041
● Europe	307
● Africa	83
● South America	97
● Oceania	34

SHADOWSERVER

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012

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

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

TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012

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

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

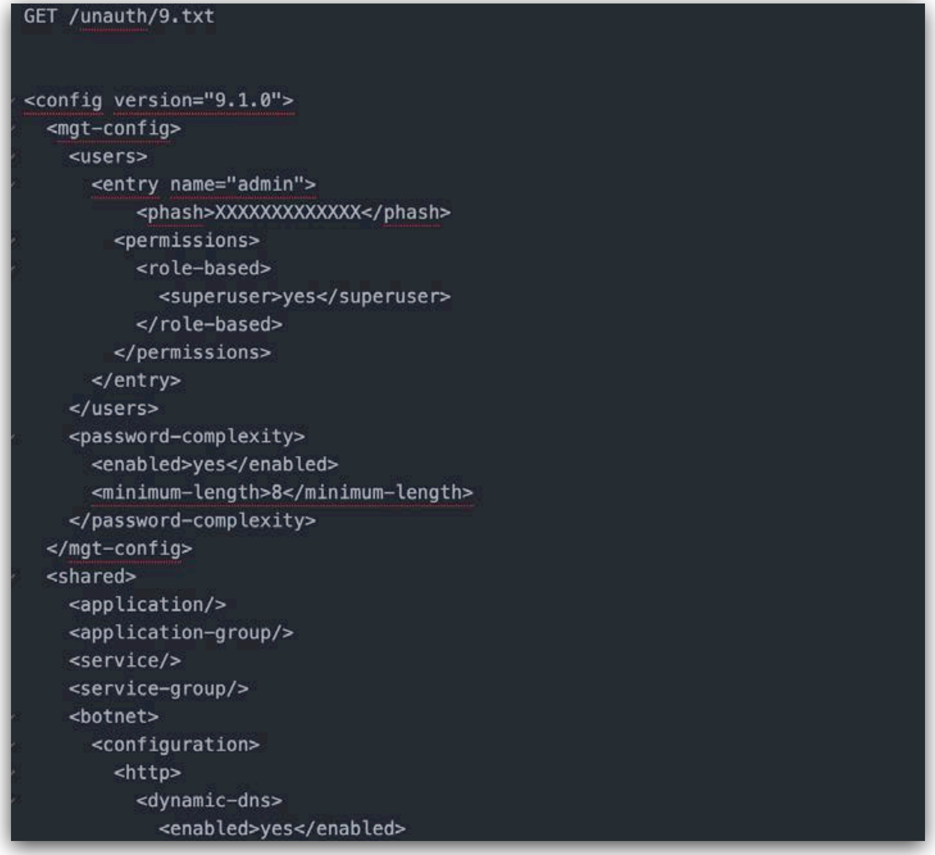
Palo Alto PAN-OS CVE-2024-0012

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

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



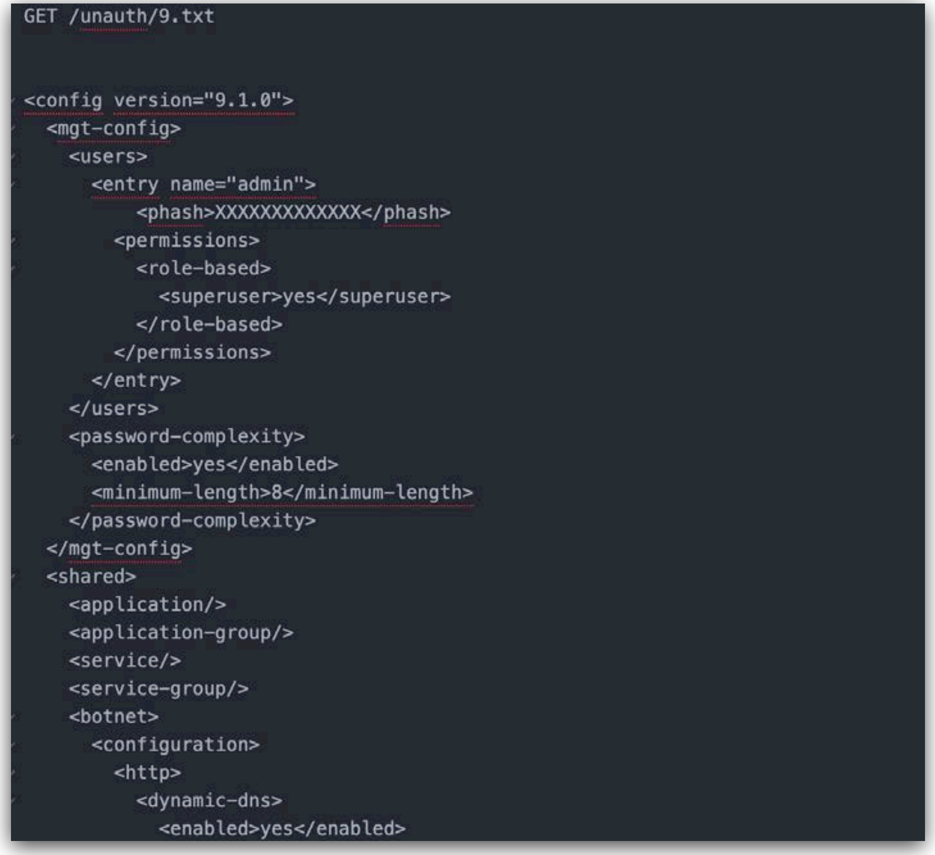
```
GET /unauth/9.txt


<config version="9.1.0">
  <mgt-config>
    <users>
      <entry name="admin">
          <phash>XXXXXXXXXXXXX</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

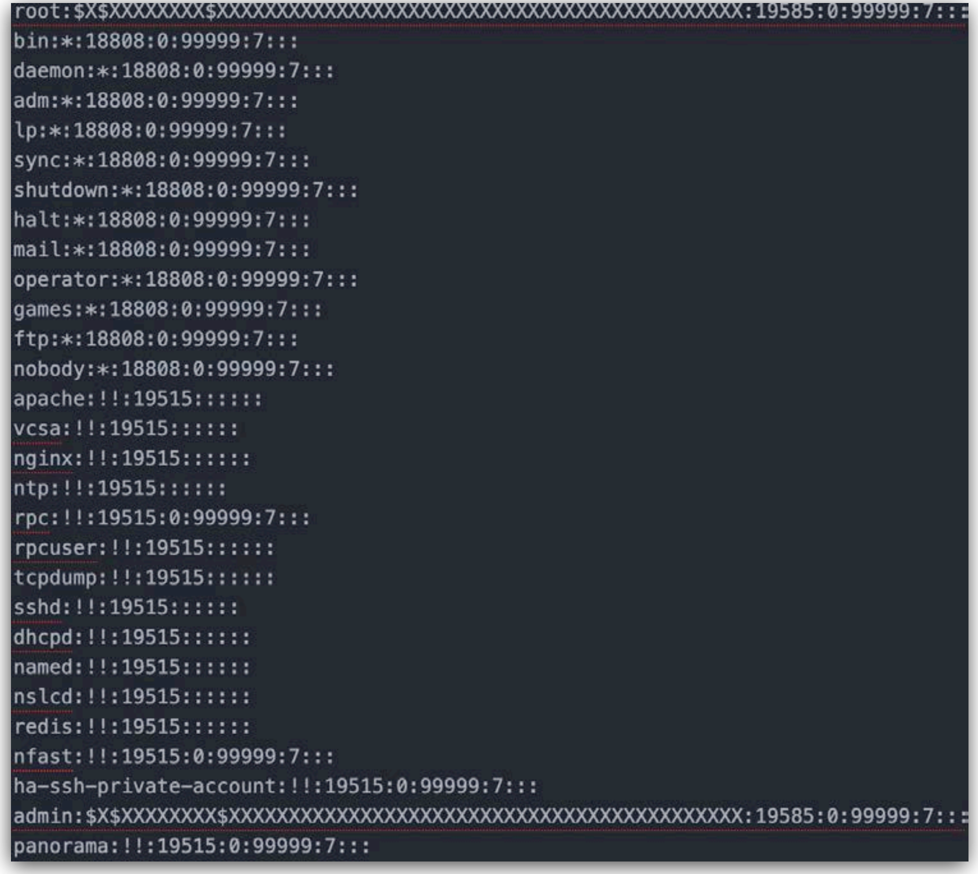
TLP CLEAR

Palo Alto PAN-OS CVE-2024-0012

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

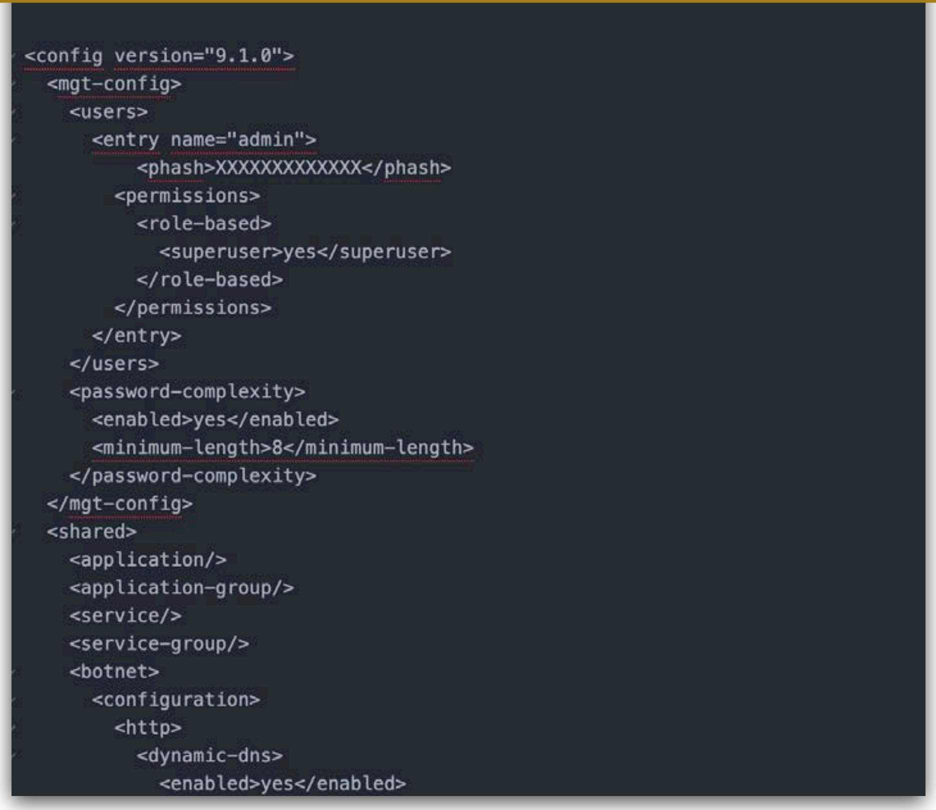
SHADOWSERVER

TLP CLEAR

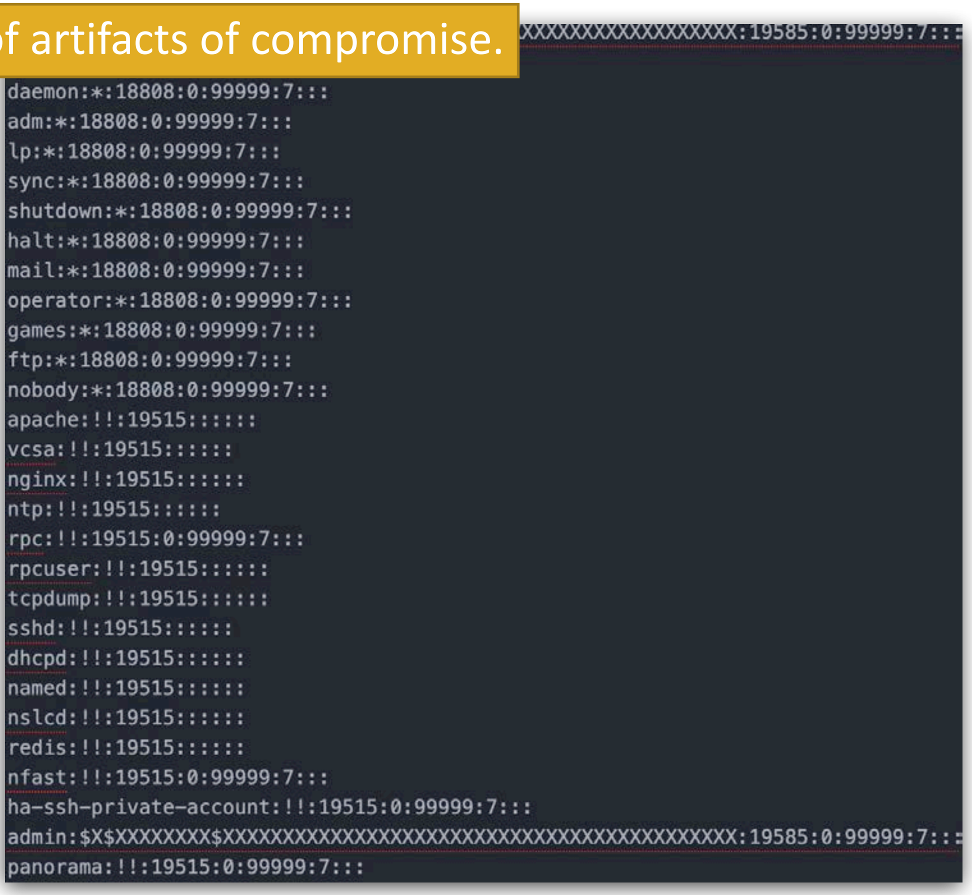
Palo Alto PAN-OS CVE-2024-0012

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>XXXXXXXXXXXXX</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>
```

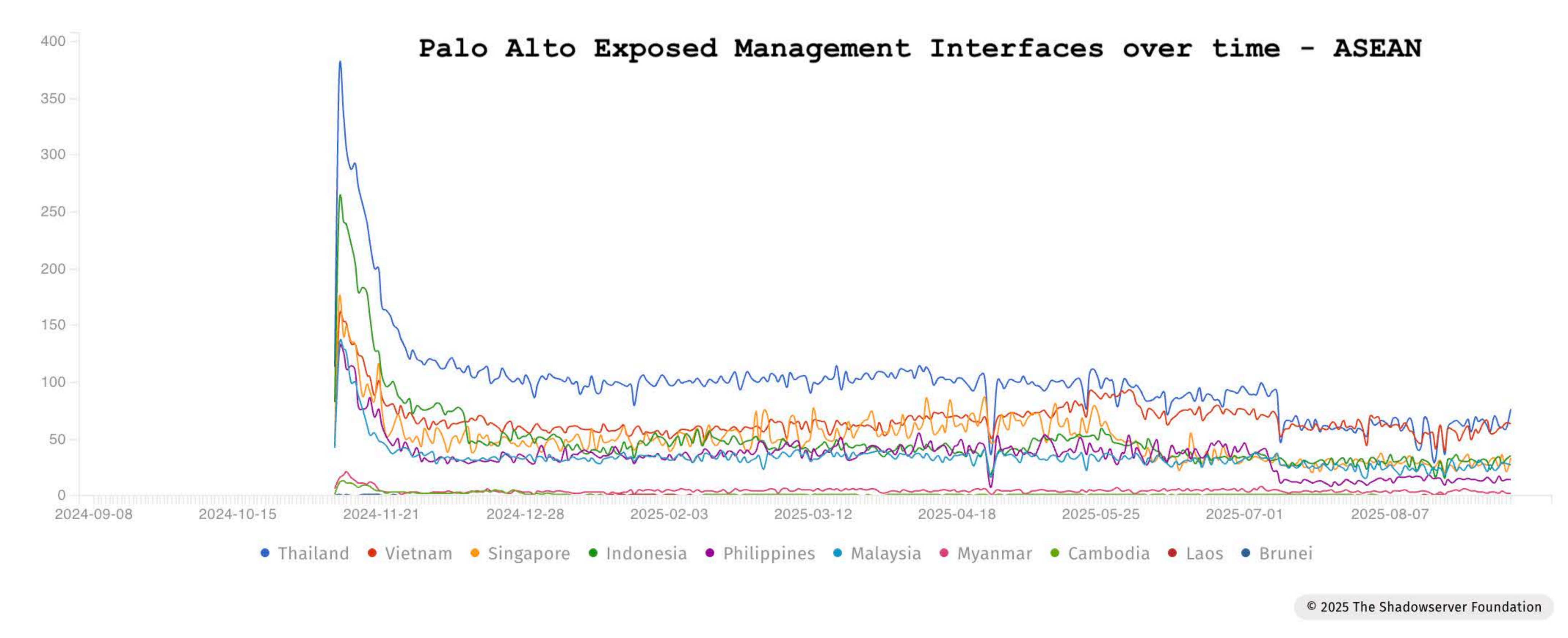


```
XXXXXXXXXXXXXXXXXX:19585:0:99999:7:::
daemon:*:18808:0:99999:7:::
adm:*:18808:0:99999:7:::
lp:*:18808:0:99999:7:::
sync:*:18808:0:99999:7:::
shutdown:*:18808:0:99999:7:::
halt:*:18808:0:99999:7:::
mail:*:18808:0:99999:7:::
operator:*:18808:0:99999:7:::
games:*:18808:0:99999:7:::
ftp:*:18808:0:99999:7:::
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$XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:19585:0:99999:7:::
panorama:!!:19515:0:99999:7:::
```

SHADOWSERVER

TLP CLEAR

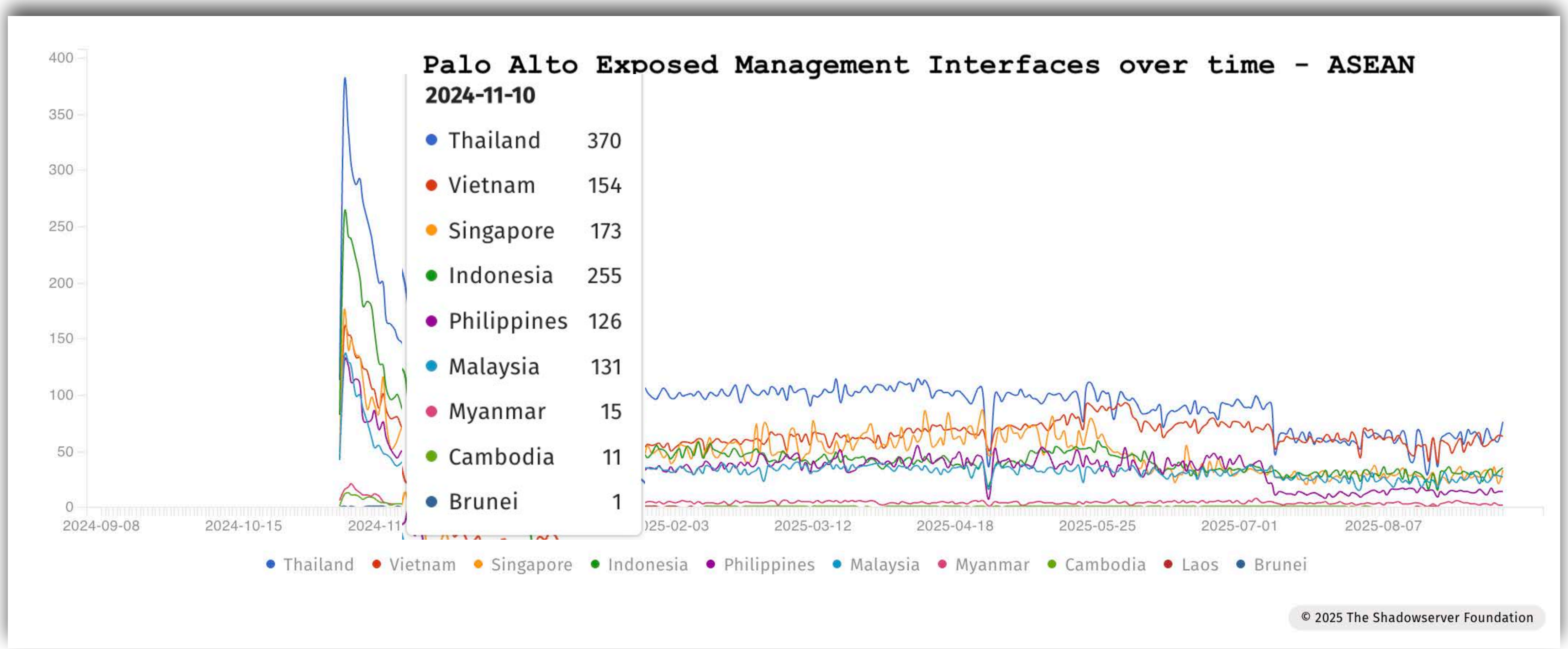
Palo Alto PAN-OS CVE-2024-0012 (ASEAN)



SHADOWSERVER

TLP CLEAR

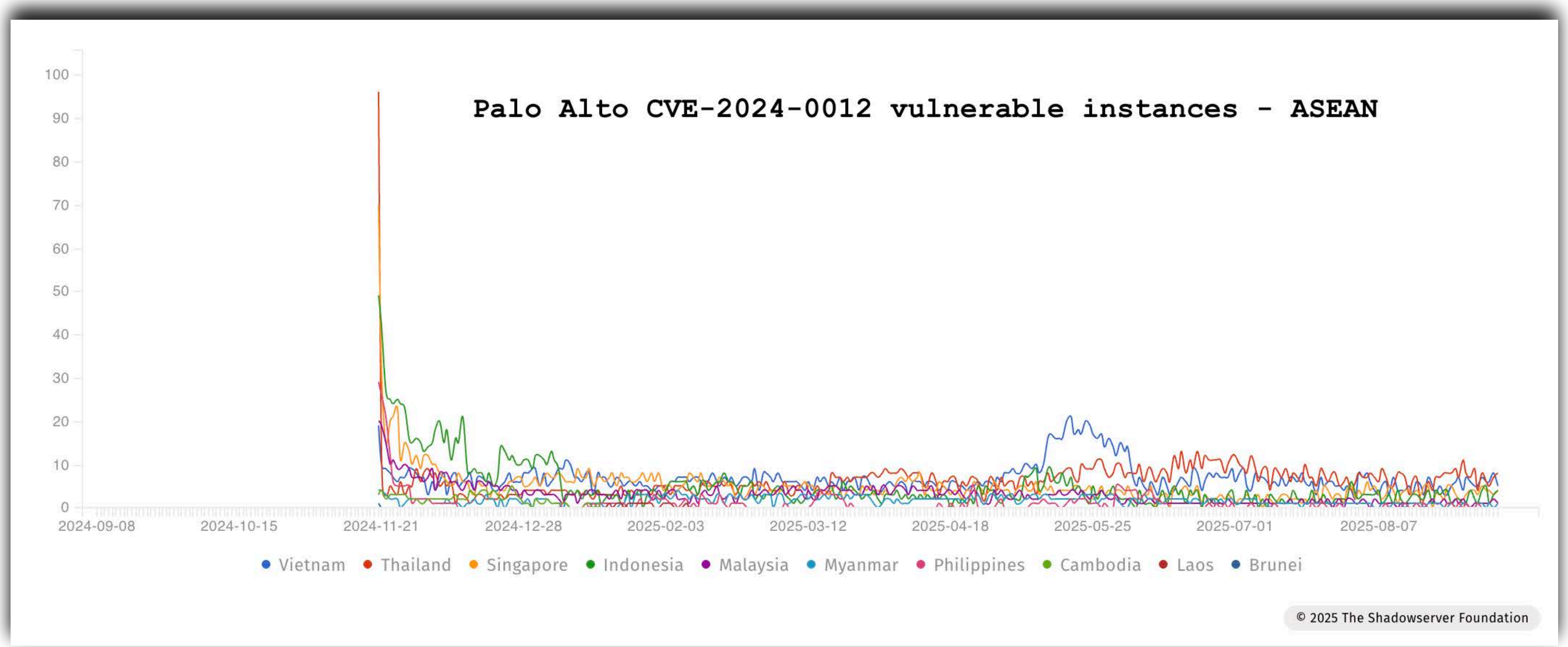
Palo Alto PAN-OS CVE-2024-0012 (ASEAN)



SHADOWSERVER

TLP CLEAR

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

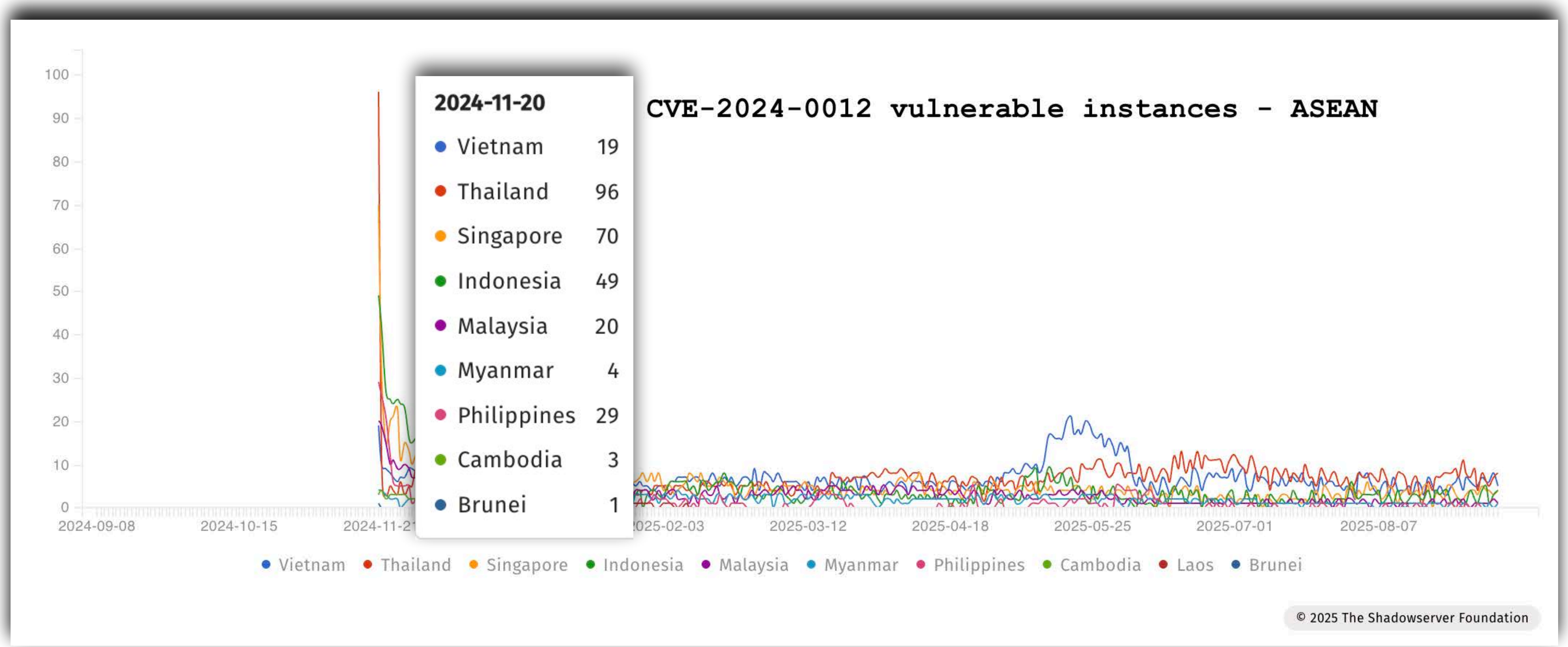


© 2025 The Shadowserver Foundation

SHADOWSERVER

TLP CLEAR

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



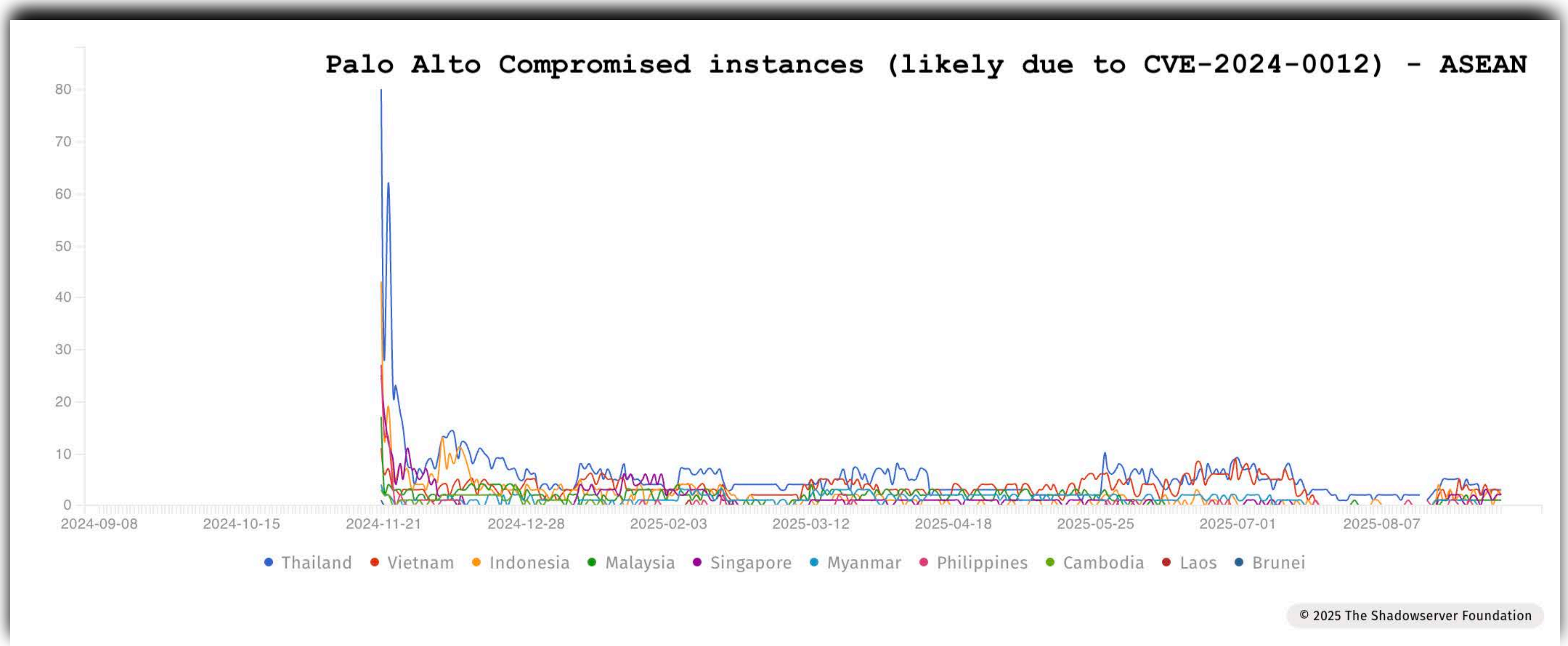
2024-11-20

● Vietnam	19
● Thailand	96
● Singapore	70
● Indonesia	49
● Malaysia	20
● Myanmar	4
● Philippines	29
● Cambodia	3
● Brunei	1

SHADOWSERVER

TLP CLEAR

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

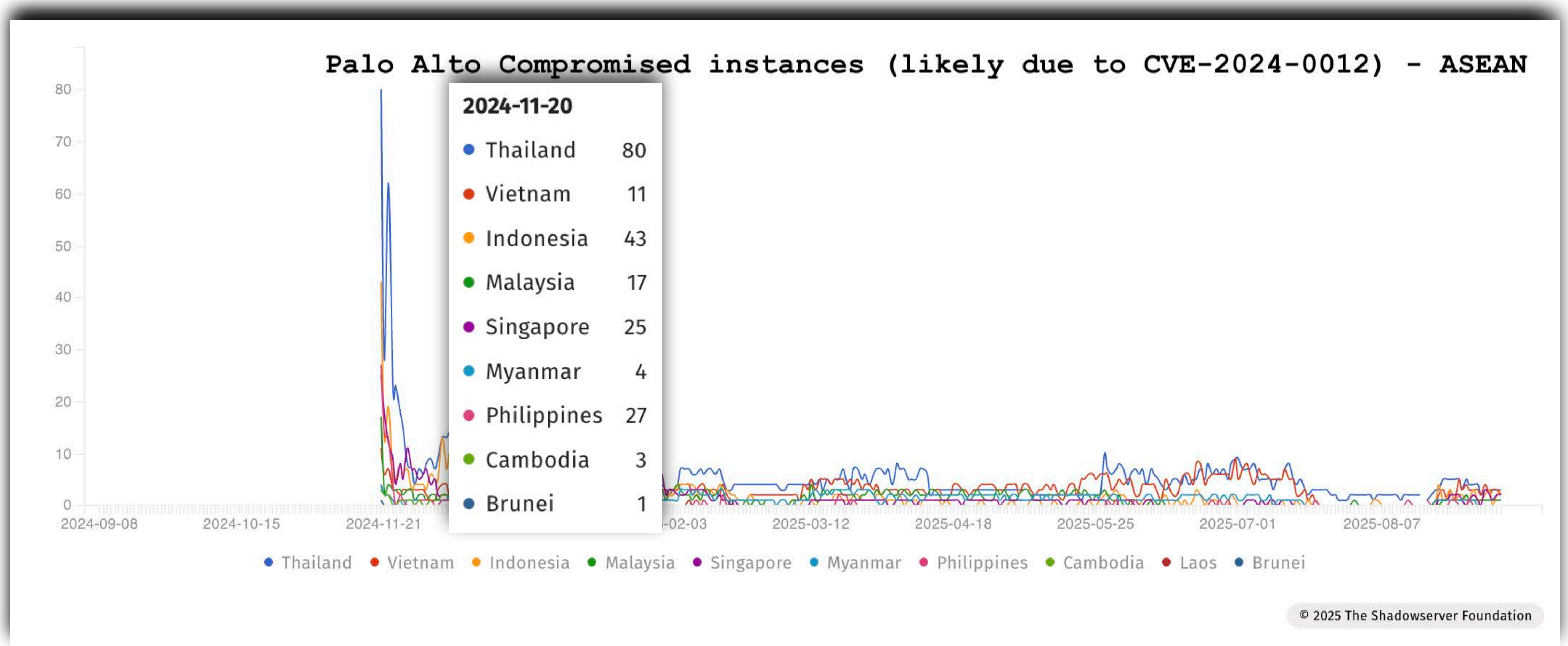


© 2025 The Shadowserver Foundation

SHADOWSERVER

TLP CLEAR

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



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!
- If your receive a report from Shadowserver **please act!**

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