

Cybersecurity start with the basics



Safeguard your organization with Daily Cybersecurity habits using Shadowserver Foundation's Free Public Services

Shadowserver Team for this Briefing



Barry Greene

Security & Resiliency Architect

bgreene@senki.org or bgreene@shadowserver.org

Linkedin:

<https://www.linkedin.com/in/barryrgreene/>

More on Senki.org (see

<https://www.senki.org/about-senki/barrys-bio/>)

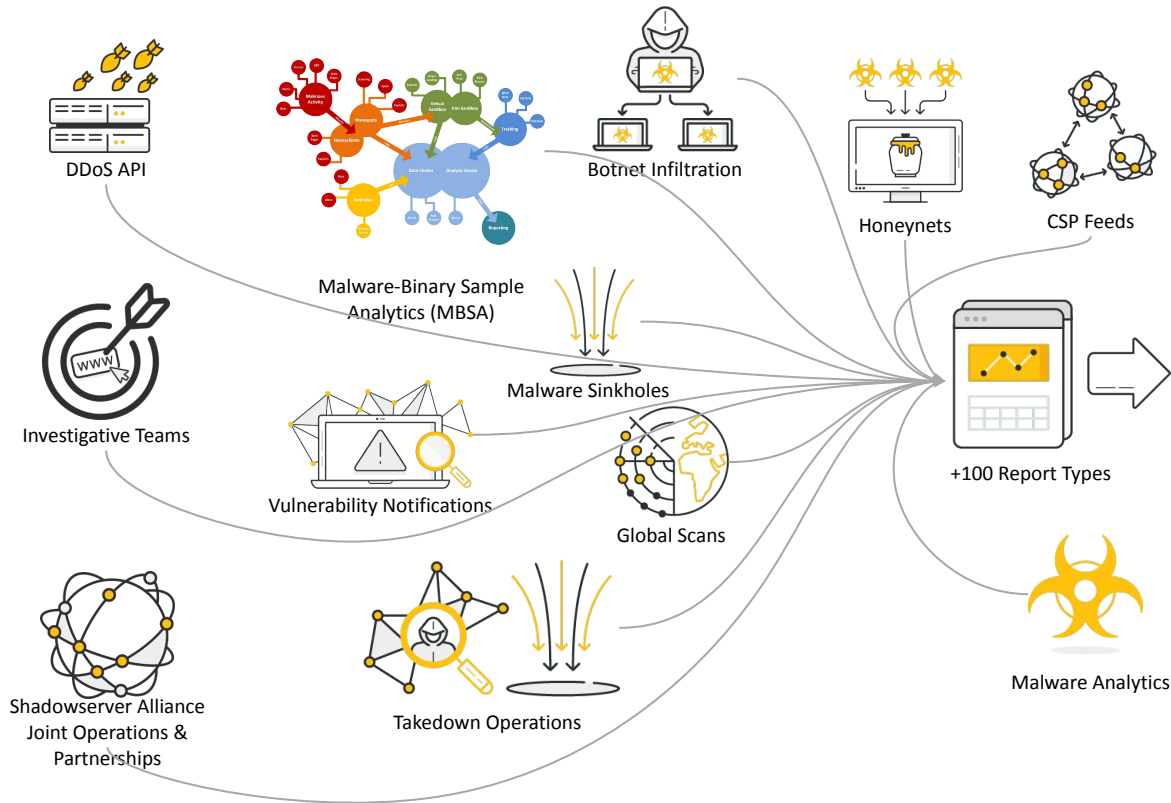
Confidentiality

FIRST TRAFFIC LIGHT PROTOCOL (TLP) Version 2.0	TLP: CLEAR	TLP: GREEN	TLP: AMBER	TLP: AMBER+STRICT	TLP: RED
May be shared with those with a need-to-know within a formal organization of which the recipient is a member (company, ISAC, ...)	✓	✓	✓	✓	✗
May be shared with those with a need-to-know in organizations to which the recipient provides cybersecurity services	✓	✓	✓	✗	✗
May be shared with members of wider security community	✓	✓	✗	✗	✗
May be shared without limits	✓	✗	✗	✗	✗

<https://www.first.org/tlp/>

The Shadowserver Foundation is a nonprofit security organization working altruistically behind the scenes to make the Internet more secure for everyone.

What is Shadowserver Providing You



Shadowserver provide an Security Attack Surface Report on your Network as a Public Service?

Why are you ignoring this critical tool that will help you reduce your security exposure?

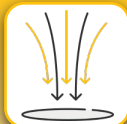


What Shadowserver can deliver NOW!

What is the Shadowserver
Foundation & what does it
do?



What does The Shadowserver Foundation do?



Sinkholes

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



Scanning

We call out to nearly every IPv4 (~3.7 billion) and ~1.7 Billion IPv6 addresses many times a day looking for over 150 different types of misconfiguration or potentially abusable systems



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



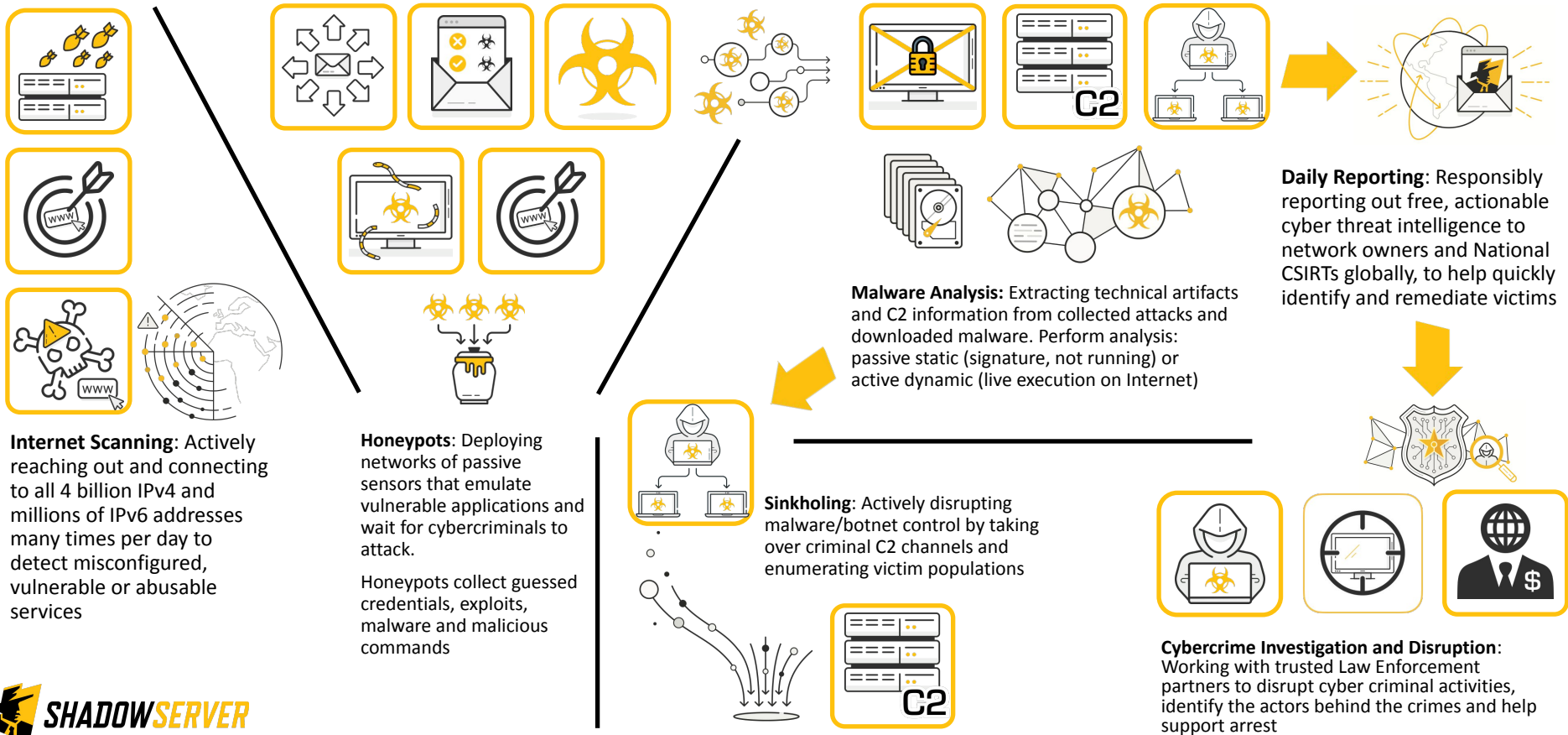
For
network
owners +
focus on
CSIRT & LE
support



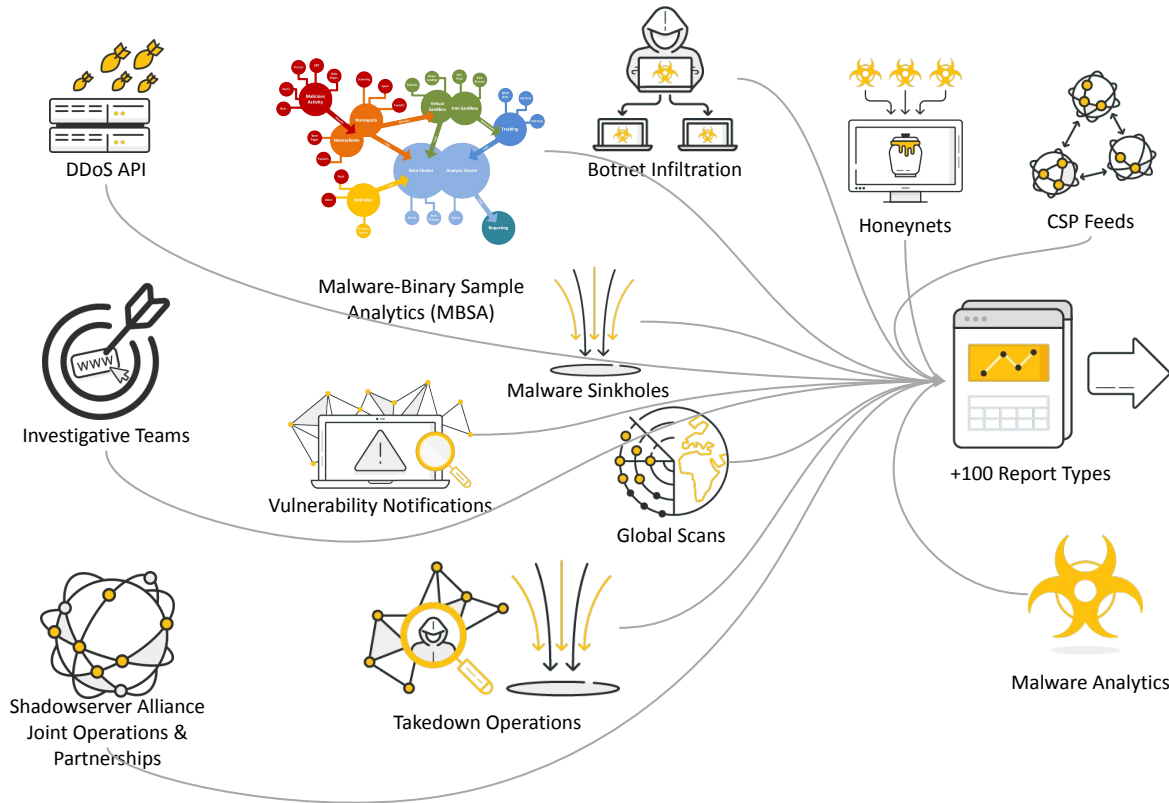
+ a host of other
interesting things!



How Shadowserver Counters Key Internet Threats



What is Shadowserver Providing You

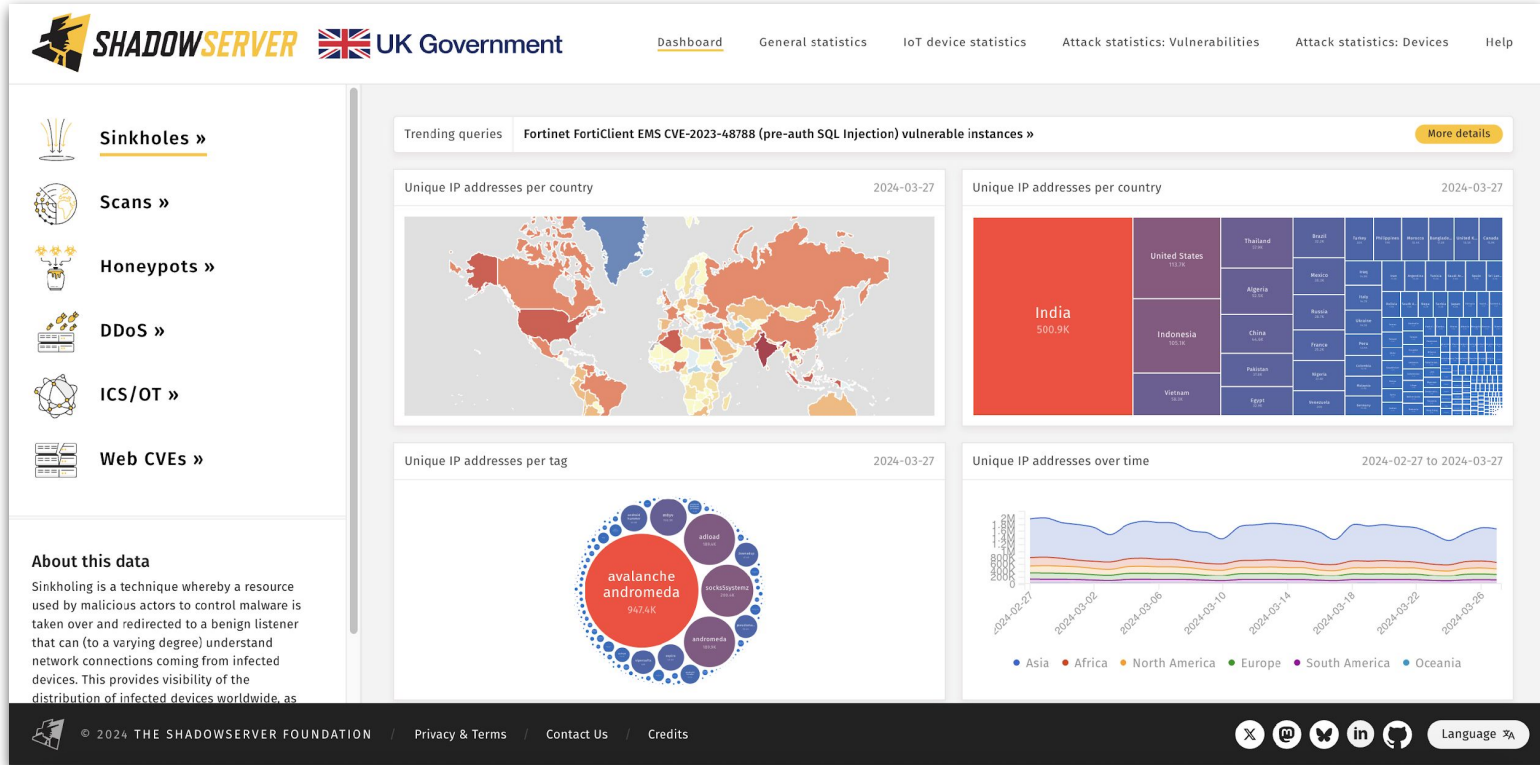


Shadowserver provide an Security Attack Surface Report on your Network as a Public Service?

Daily Reports
Subscribers
Email, API & CVF

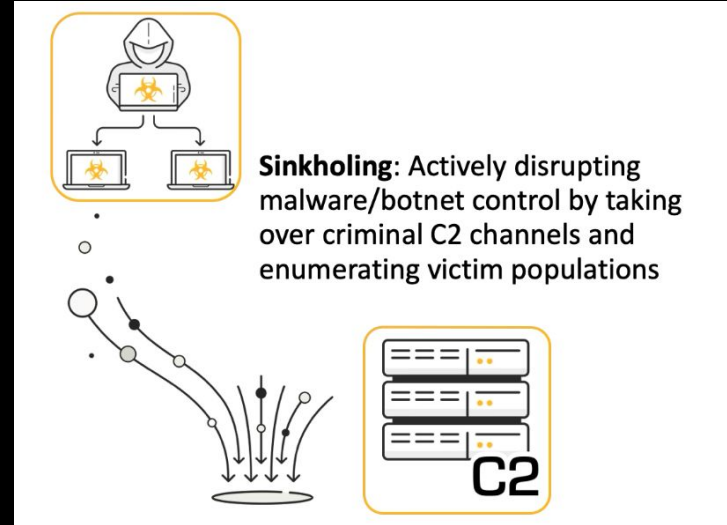
Why are you ignoring this critical tool that will help you reduce your security exposure?

Shadowserver Public Dashboard



Malware in Your Network!

Using the Shadowserver Foundation's Sinkhole Reporting to find malware in your network.



Sinkhole Botnet/Malware C&C

Shadowserver Alliance Team, Security Trust Groups, Law Enforcement, and Partnered Security Organizations taking down malware command and control.

 Sinkholes »

 Scans »

 Honeypots »

 DDoS »

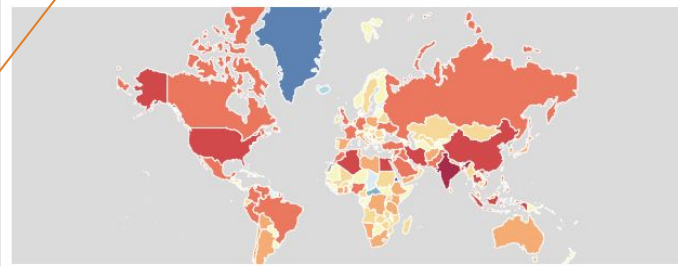
 ICS/OT »

 Web CVEs »

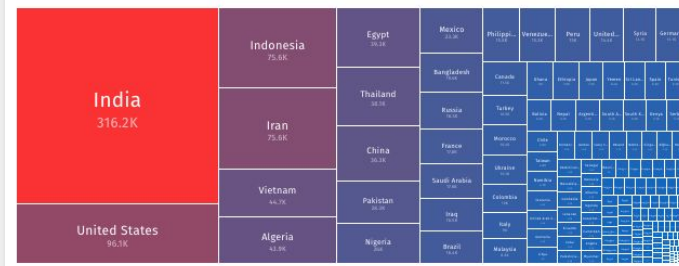
Trending queries VMW

More details

Unique IP addresses per country 2024-08-18



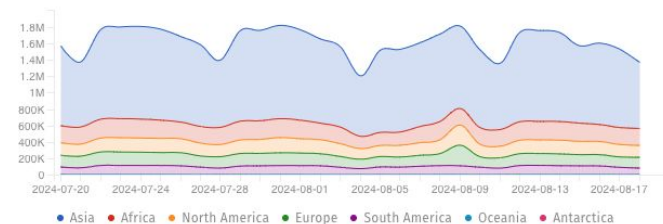
Unique IP addresses per country 2024-08-18



Unique IP addresses per tag 2024-08-18



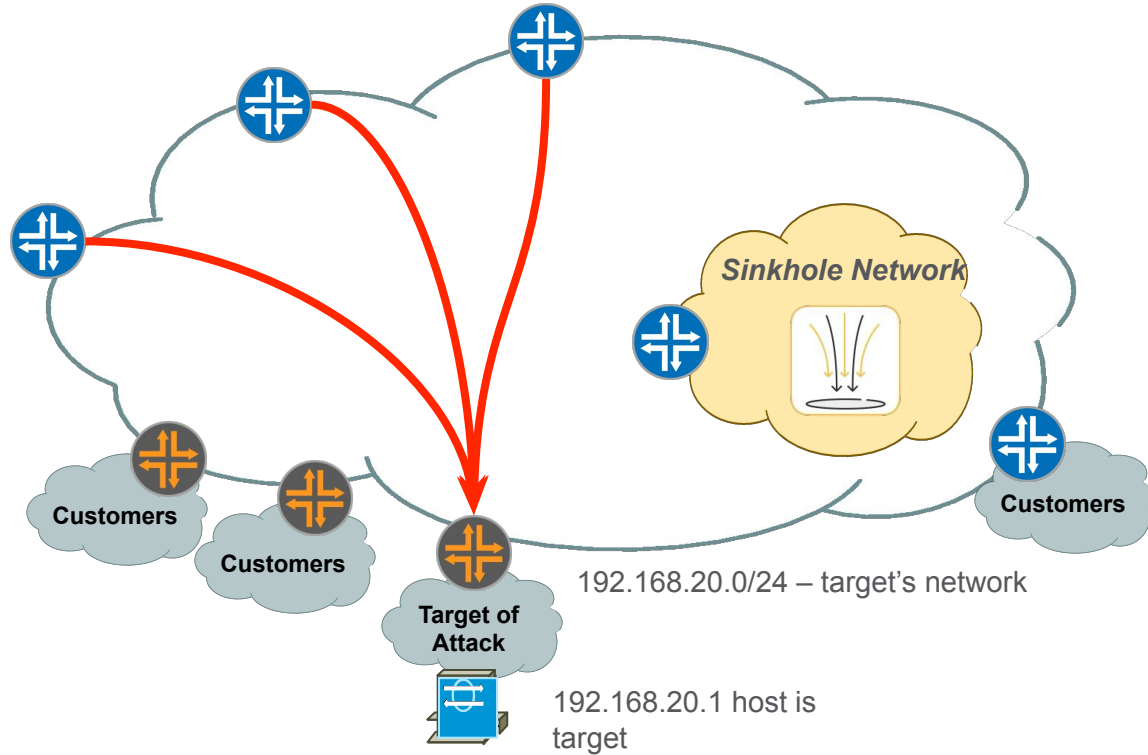
Unique IP addresses over time 2024-07-20 to 2024-08-18



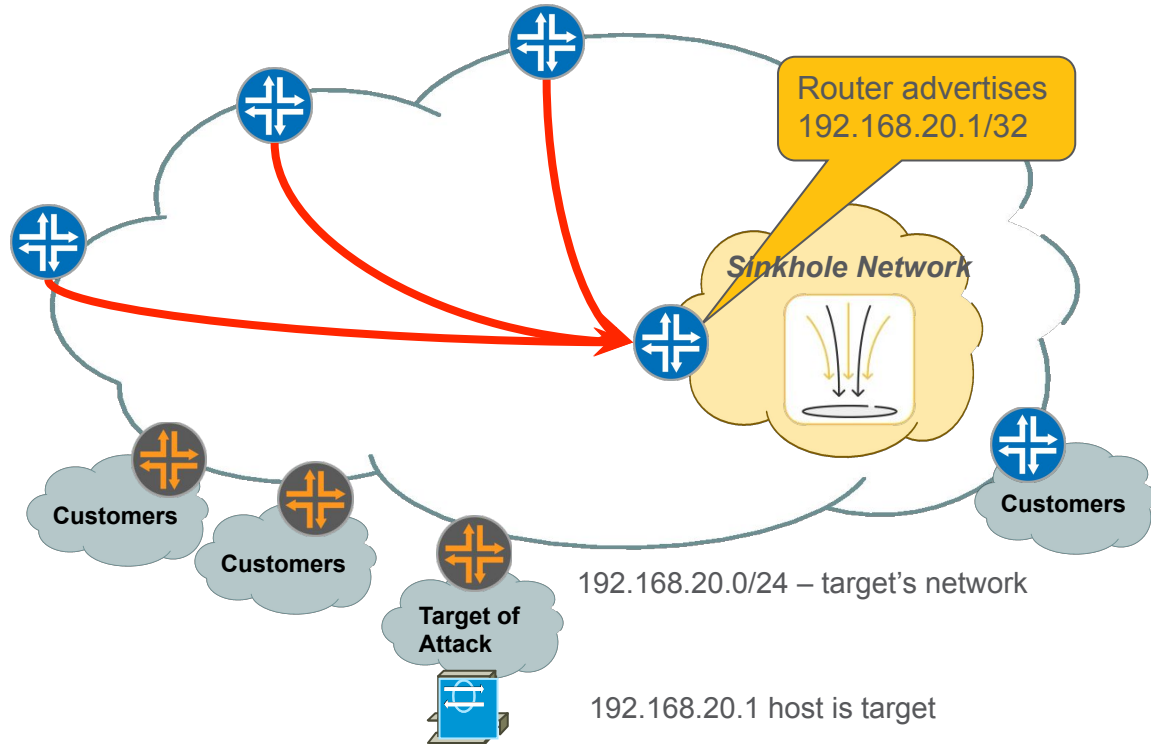
About this data

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 network connections coming from infected devices. This provides visibility of the distribution of infected devices worldwide, as well as protecting victims by preventing botnet command and control (C2) from cybercriminals.

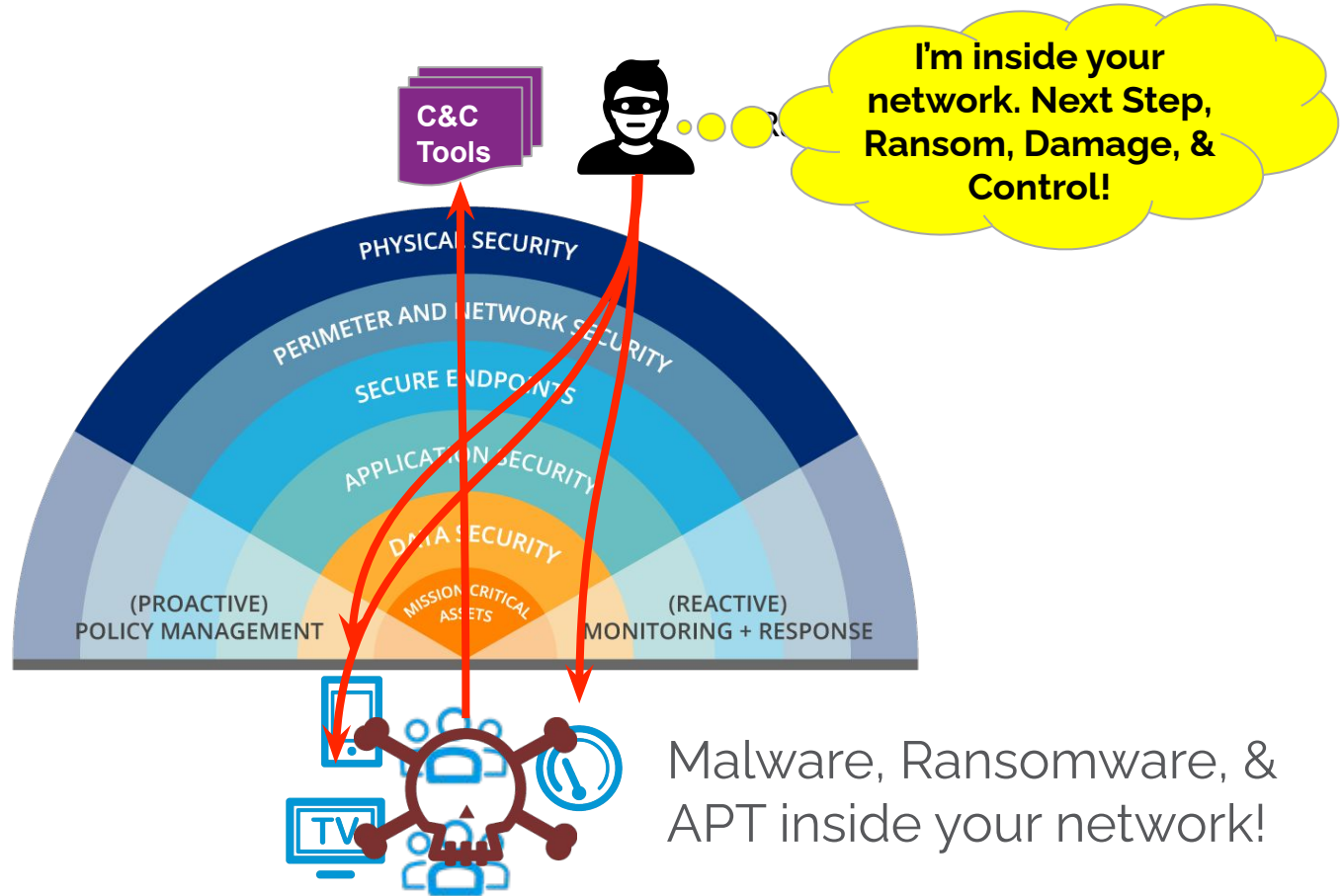
Sinkhole Routers/Networks



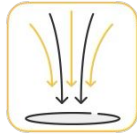
Sinkhole Routers/Networks



DNS Based Sinkhole Operation



DNS Based Sinkhole Operation



Shadowserver Foundation's
Sinkhole Operations

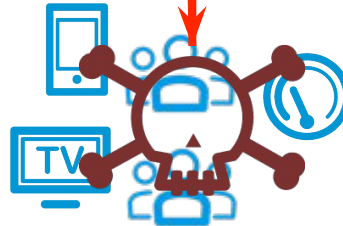
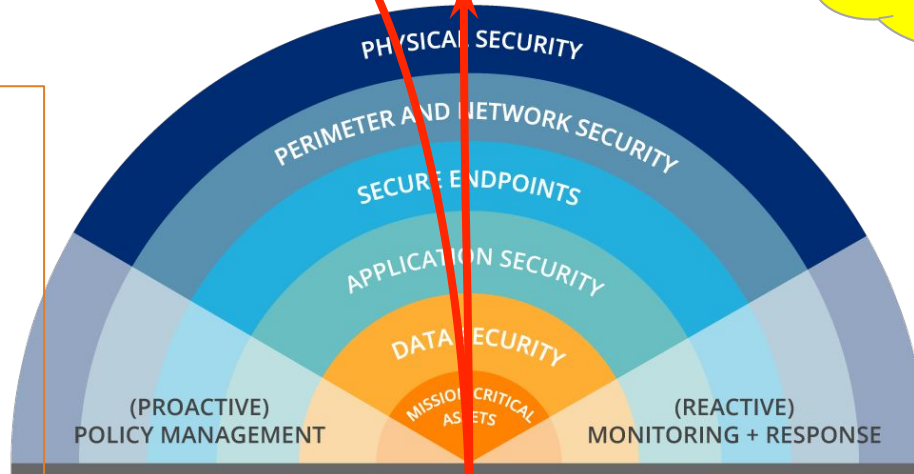
Intercept the C&C
Domain Names

C&C
Tools



I'm inside your
network. Next Step,
Ransom, Damage, &
Control!

Cyber Civil Defence
Community works
together to find the
C&C details and set
up a lawful
disruption.

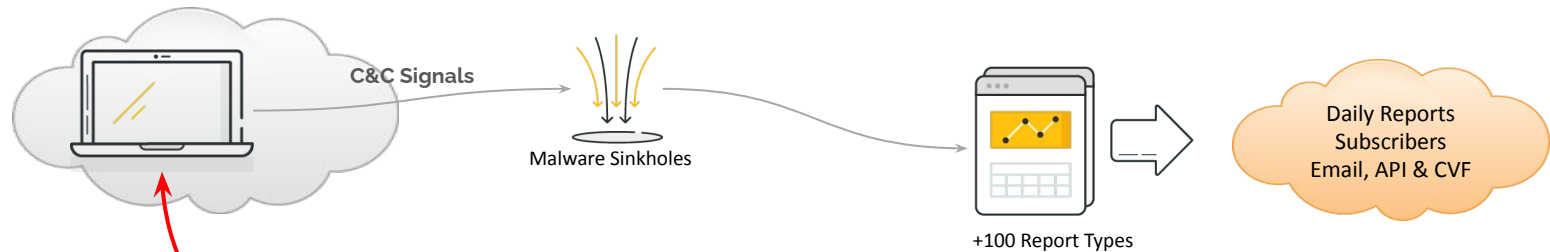


Malware, Ransomware, &
APT inside your network!

Find the Malware inside your Network

All the data from the “sinkholed” malware, botnets, APT, Ransomware, and etc is now added to the daily reports send to organizations a part of a FREE DAILY REPORTS!

Are you signed up for these daily reports?



Malware used for Ransomware

THIS DOMAIN HAS BEEN SEIZED

911 S5
PROXY

OPERATION TUNNEL RAT

This domain has been seized by the Defense Criminal Investigative Service, the Federal Bureau of Investigation, and the Bureau of Industry and Security, Office of Export Enforcement, pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Texas as part of a coordinated international law enforcement action taken against the 911 S5 residential proxy service.



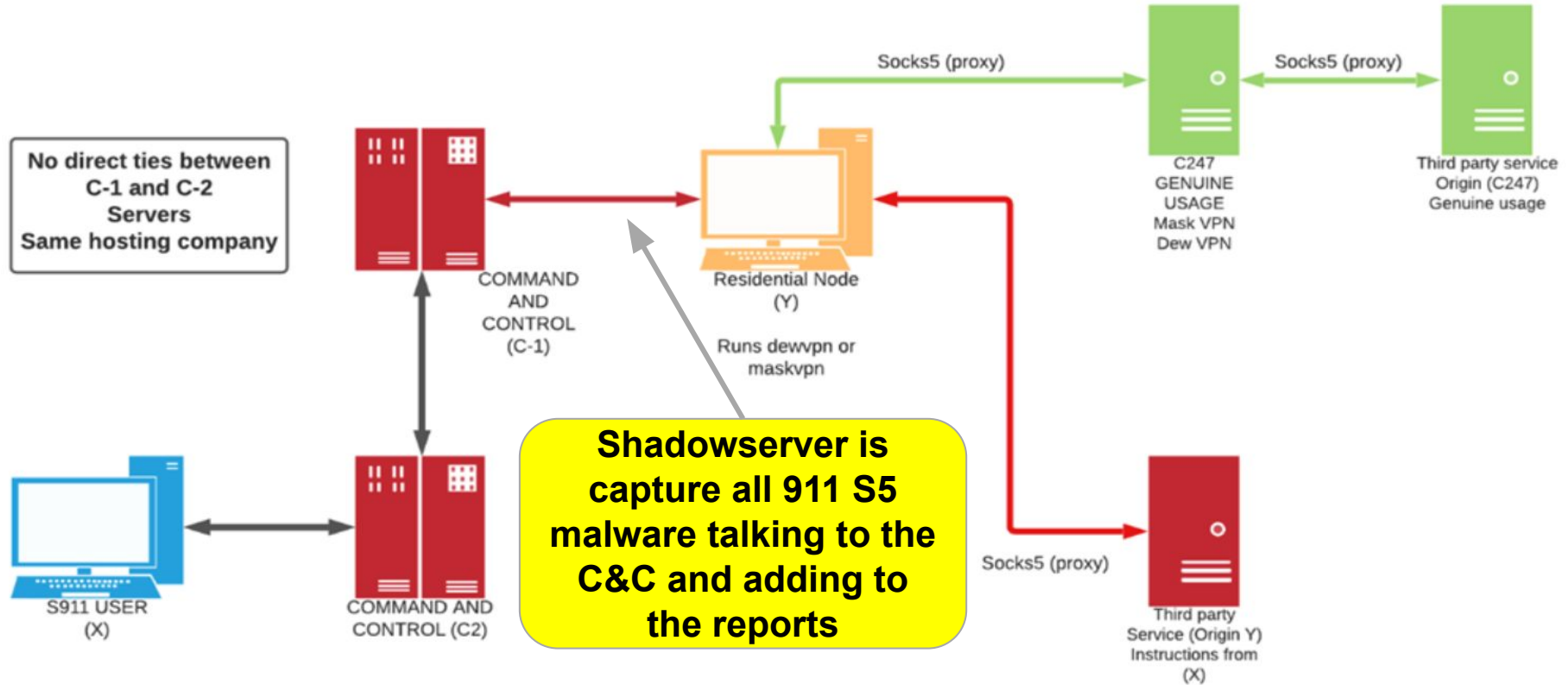
For more information or to determine if you are a victim of 911S5 malware, please visit

[fbi.gov/911S5](https://www.fbi.gov/911S5)

For more details behind the recent disruption led by the US Department of Justice see:

<https://justice.gov/opa/pr/911-s5-botnet-dismantled-and-its-administrator-arrested-coordinated-international-operation>

Shadowserver's 911 S5 Sinkhole



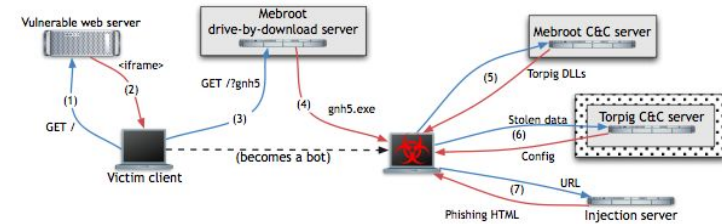
Hardware Vendor's Network Saved!

Why are their 19 Computer infected with MBROOT?

Shadowserver's Daily Network Report arrives with a new report on Torpig botnet (also called Sinowal or Mebroot). It is now part of the "victim notification" of a malware takedown.

19 computers in the network are infected!

Those computer were immediately pull off the network. They were fully patched, had the latest antivirus versions, and several were running extra browser security tool.



The potential damage to the organization was prevented by Shadowserver's Network Report. The infection vector was identified and extra network protections were put in place to protect the organization. All from a public benefit report!

Sinkhole Infections in PACNOG Community

General statistics

Tree map

Filters

Day < >

Sources

Severity

Tags

Countries

Population

GDP

Data set

Download as PNG

These are INFECTED & COMPROMISED Devices that trigger an alarm on Shadowserver's Globally Distributed Sinkholes.

They are a RISK on YOUR NETWORK!

PG: Papua New Guinea: 471

Vanuatu
1%

Solomon Islands
3

Samoa
6

Papu
1

Marshall Islands
9

Marx
1

© 2024 The Shadowserver foundation

Sinkhole Infection in PACNOG Community

General statistics

Time series

Date range: 1 month

Sources: sinkhole, sinkhole6

Severity: Select one or more options...

Tags: Select one or more options...

Countries: PaCSON - no AU/NZ

Data set: Counted IP addresses

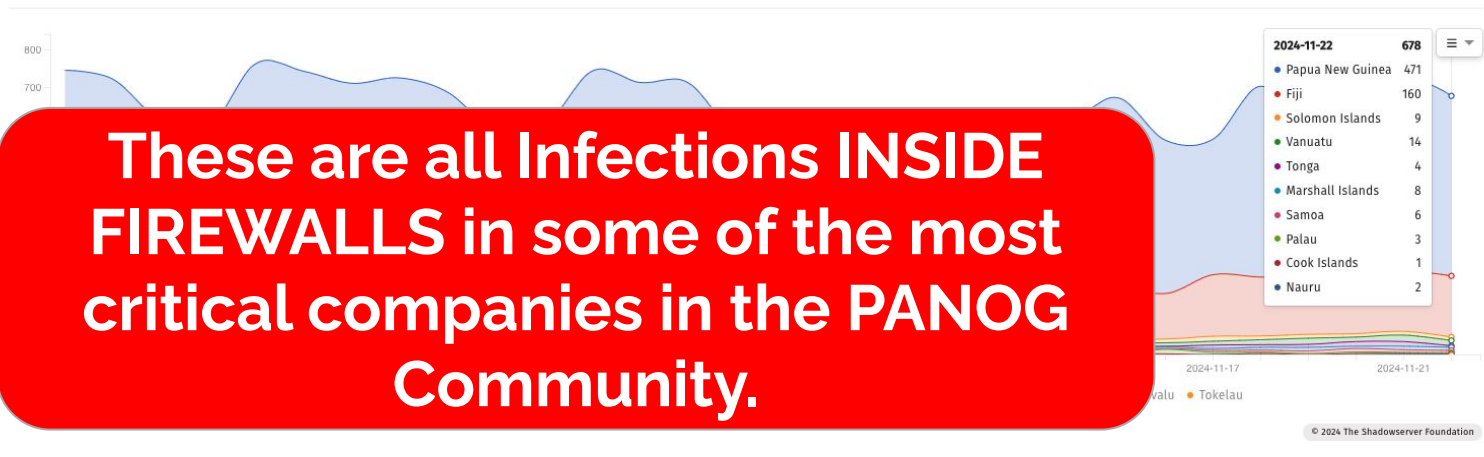
Limit:

Group by: Country Tag

Chart style: Stacked Overlapping

Download as PNG

Results



These are all Infections INSIDE FIREWALLS in some of the most critical companies in the PANOG Community.

Internet Detailed v4/v6 Scanning

Scanning for risk on network providing detailed attack surface reporting on what can be seen on your network.

 Sinkholes »

 **Scans »**

 Honey pots »

 DDoS »

 ICS/OT »

 Web CVEs »

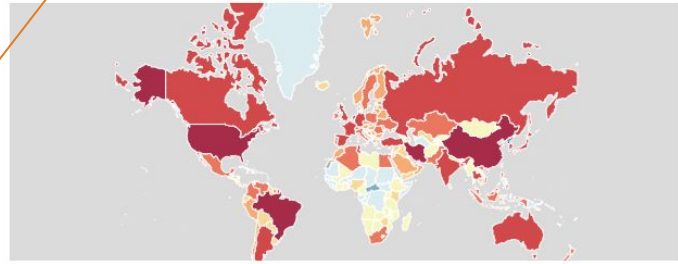
About this data

Shadowserver scans the entire IPv4 Internet for over 100 different network protocols every day, and also performs IPv6 scans based on IPv6 hitlists for selected protocols. These are "hello" type port scans that do not exploit any vulnerability. They enable identification of misconfigured, vulnerable or abusable devices, unnecessarily exposed attack surfaces, or simply just population enumeration. Population enumeration results can be found under the "population" source type.

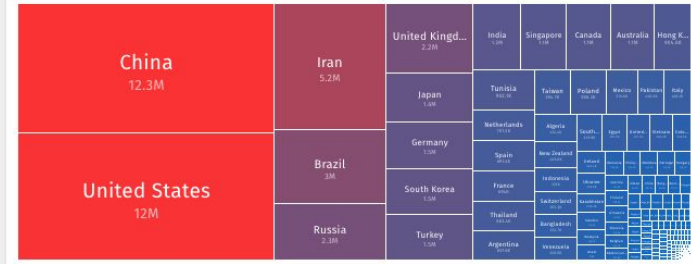
Trending queries VMware ESXi hypervisor CVE-2024-37063 (authentication bypass) exploited by ransomware operators »

More details

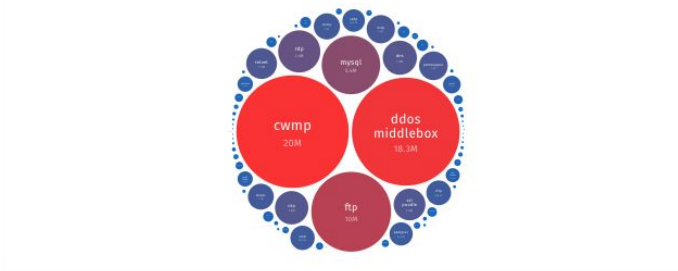
Unique IP addresses per country 2024-08-18



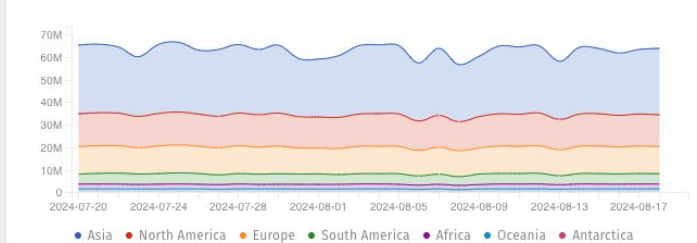
Unique IP addresses per country 2024-08-18



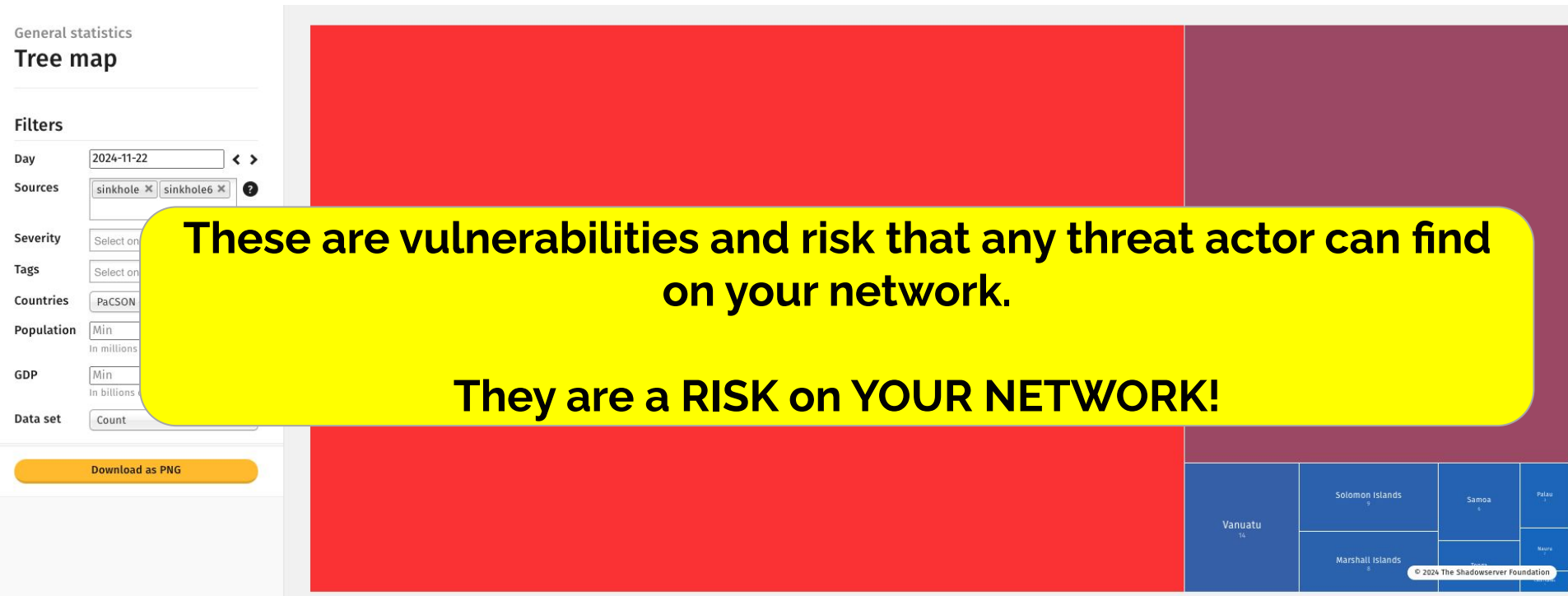
Unique IP addresses per tag 2024-08-18



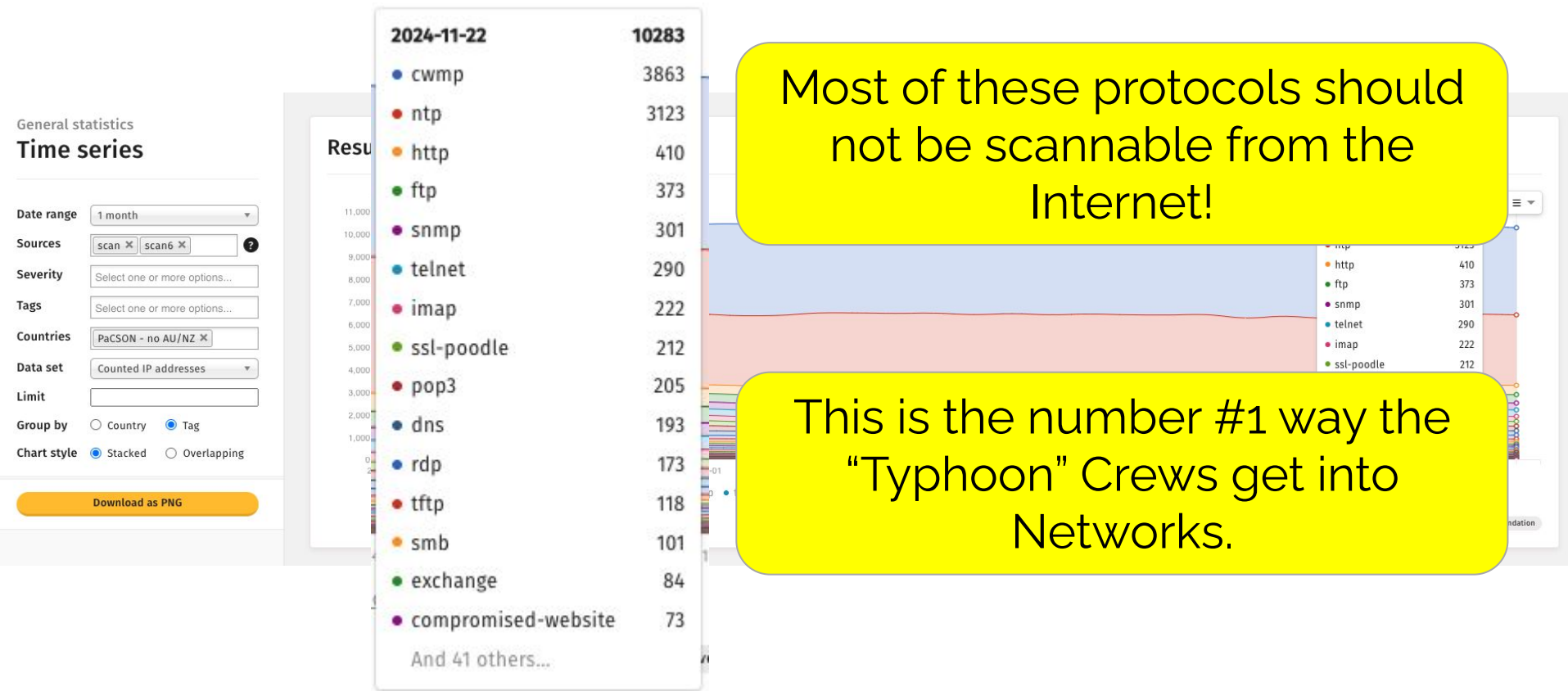
Unique IP addresses over time 2024-07-20 to 2024-08-18



Scanned Risk in PACNOG Community the Bad Guys See



What are the top Scanned Risk in PACNOG Community?



Honeybots - Monitoring KEVs

Honeybots are a means to know when a risk is "actively exploited" and to track where the 'probing/attacking' device is located

Sinkholes »

Scans »

Honeybots »

DDoS »

ICS/OT »

Web CVEs »

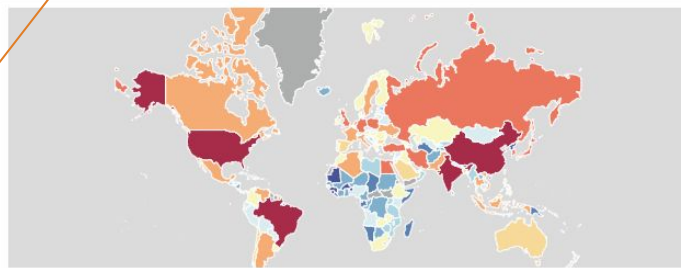
About this data

Networks of honeypots can be used to observe hosts performing various server-side attacks, such as exploits targeting externally exposed services, or brute-forcing of credentials on IoT devices to obtain access via remote access protocols such as SSH, telnet, VNC, RDP and FTP. They can also be used to observe network scanning activity and amplification DDoS attempts.

Trending queries VMware ESX Hypervisor CVE-2024-38005 (authentication bypass) exploited by ransomware operators

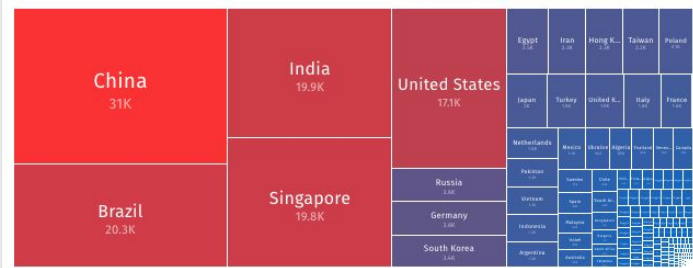
Unique IP addresses per country

2024-08-18



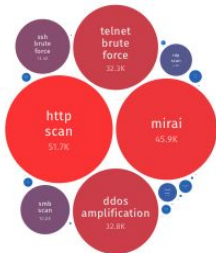
Unique IP addresses per country

2024-08-18



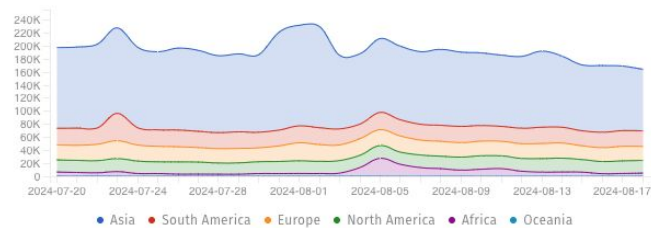
Unique IP addresses per tag

2024-08-18



Unique IP addresses over time

2024-07-20 to 2024-08-18



How are PACNOG Community Infections Scanning?

Date range

Sources

Severity

Tags

Countries

Data set

Limit

Group by Country Tag

Count as Daily average Total

Style

These are devices in networks used to attack other networks.

That means someone inside your network is using your resources to attack others - and most likely attacking you.

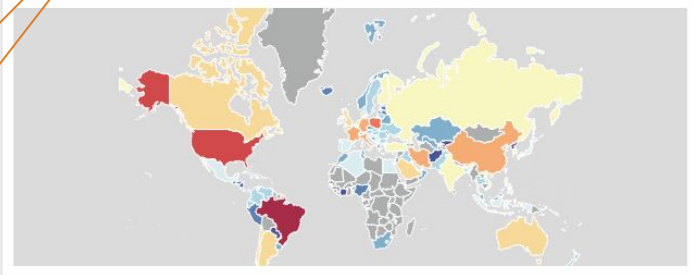
DDoS Sources

Where are the DDoS Reflection Amplification and DDoS Bots? Are they on your network?

- Sinkholes »
- Scans »
- Honeypots »
- DDoS »**
- ICS/OT »
- Web CVEs »

Trending queries VMware ESXi hypervisor CVE-2024-37085 (authentication bypass), exploited by ransomware operators

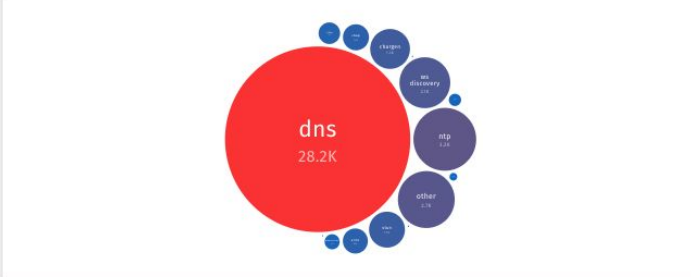
Unique IP addresses per country 2024-08-18



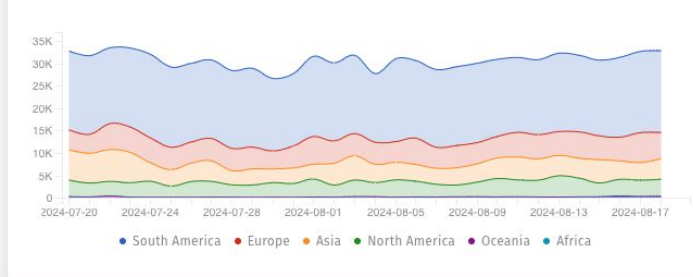
Unique IP addresses per country 2024-08-18



Unique IP addresses per tag 2024-08-18



Unique IP addresses over time 2024-07-20 to 2024-08-18



About this data
Observations from honeypots about reflected Distributed Denial of Service (DDoS) amplification events. This category of DDoS attacks utilizes UDP-based, publicly exposed, amplifiable network services to reflect packets to a victim, by spoofing the source IP address of the packets sent by the amplifier to the victim's IP address.

ICS/OT - Critical Infrastructure

Industrial Control Systems (ICS) and Operational Technologies (OT) should not be exposed to the Internet.



Sinkholes »



Scans »



Honey pots »



DDoS »



ICS/OT »



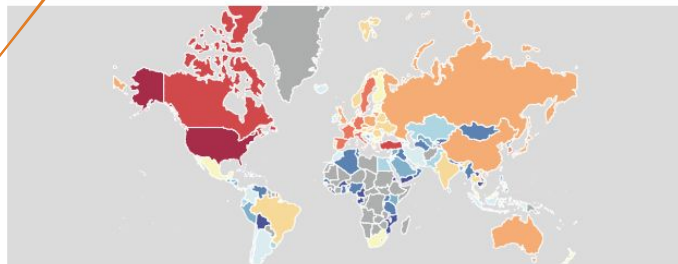
Web CVEs »

About this data

Shadowserver scans the entire IPv4 address space for multiple native Industrial Control System / Operation Technology (ICS/OT) services and network protocols. The devices identified should probably not be exposed publicly on the Internet.

Trending queries: VMware ESXi hypervisor CVE=2024-37085 (authentication bypass) exploited by ransomware operators » [More details](#)

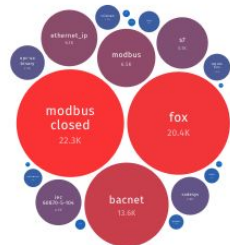
Unique IP addresses per country 2024-08-18



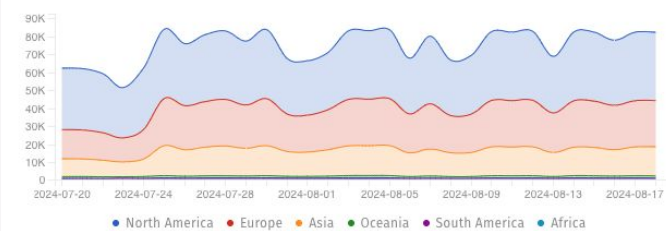
Unique IP addresses per country 2024-08-18



Unique IP addresses per tag 2024-08-18



Unique IP addresses over time 2024-07-20 to 2024-08-18



Web Exposure Risk



Microsoft Exchange, Web Vulnerabilities, and other risk are visible to Shadowserver's telemetry and are part of the daily updates.



Sinkholes »



Scans »



Honey pots »



DDoS »



ICS/OT »



Web CVEs »

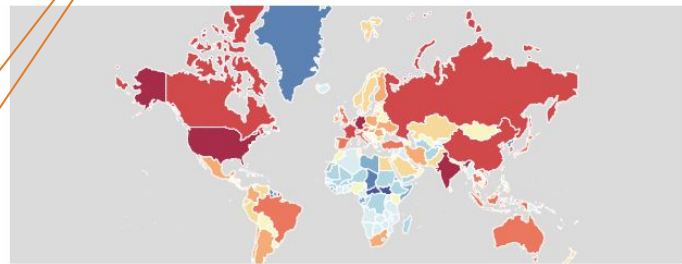
About this data

Shadowserver scans for critical pre-auth Web-based remote code execution (RCE) vulnerabilities (or vulnerabilities that can be chained together by attackers to remotely execute code) in high-profile or otherwise popular software that is often exposed to the public Internet. These vulnerabilities, identified by their CVE entry are often exploited in the wild and should be remediated as quickly as possible.

Trending queries VMwa

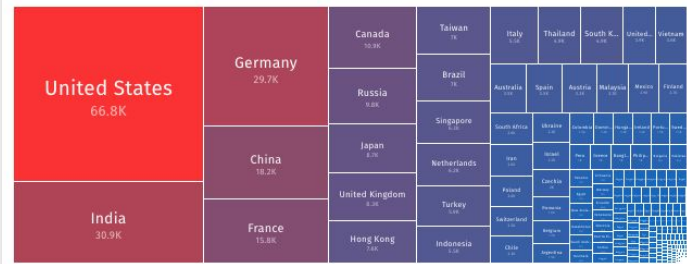
Unique IP addresses per country

2024-08-18



Unique IP addresses per country

2024-08-18



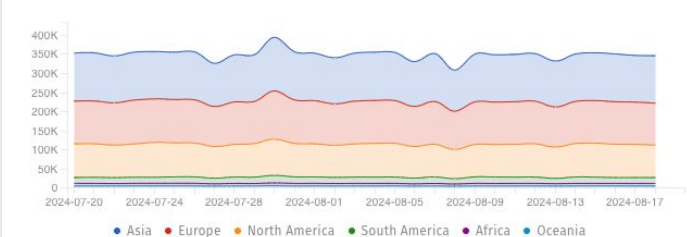
Unique IP addresses per tag

2024-08-18

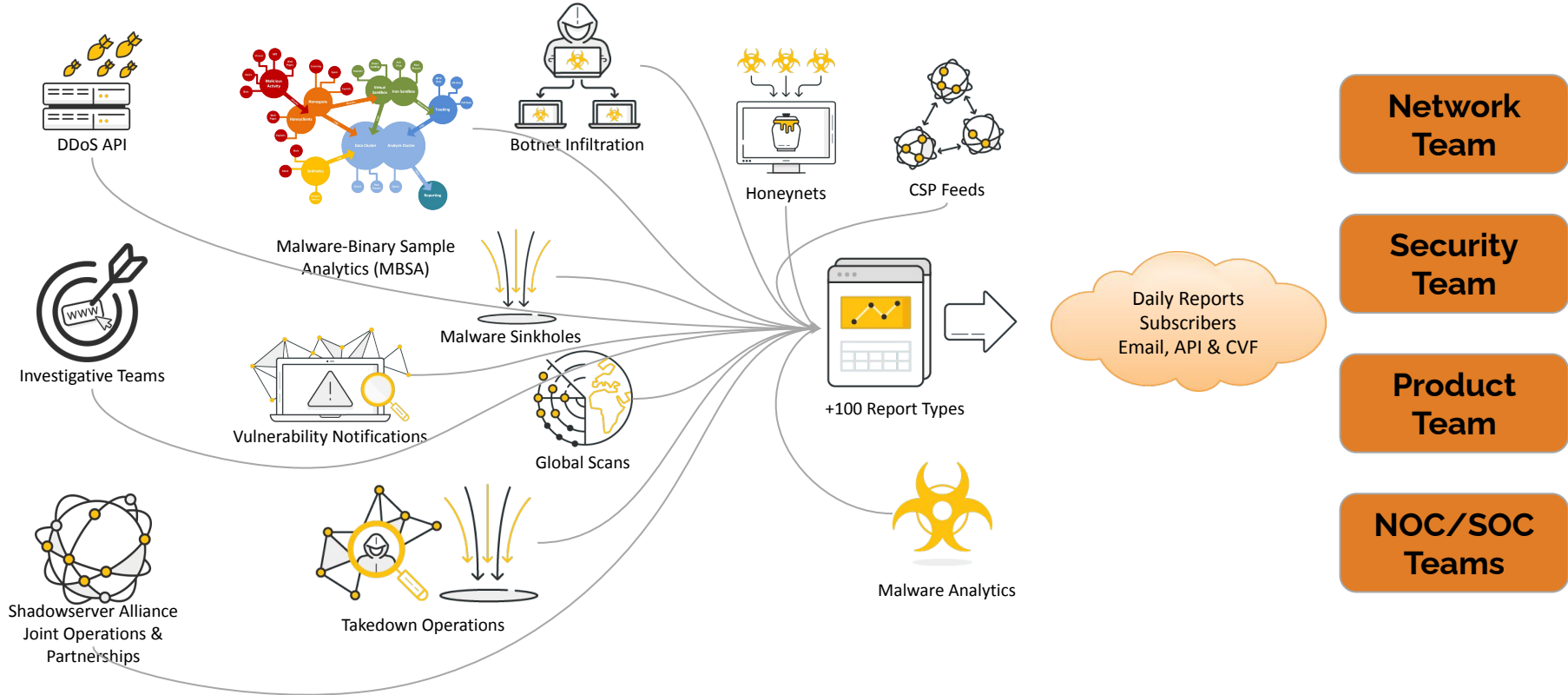


Unique IP addresses over time

2024-07-20 to 2024-08-18



Shadowserver Providing the Tools



Focus on US CISA's KEV List

CISA provides the KEV list as a tool to help organizations focus REDUCING RISK!

Shadowserver provides a public service to have an “outside-in” assessment of your network.



AMERICA'S CYBER DEFENSE AGENCY

- Topics ▾
- Spotlight
- Resources & Tools ▾
- News & Events ▾
- Careers ▾
- About ▾

[Home](#)

Known Exploited Vulnerabilities Catalog



- Dashboard
- General statistics
- IoT device statistics
- [Attack statistics](#)

Attack statistics Vulnerabilities

Category: ?

Statistic:

Date range: From To

Country:

IoT: ?

CISA KEV x ?

Exploited vulnerabilities - Top

Showing results for 2023-06-27

#	Vulnerability	Vendor	Product	IoT	KEV	1d	7d	30d	90d	Actions
1	CVE-2018-10562	Dasan	Dasan GPON Home Router	✓	✓	203	1,615	8,142	33,360	Details Chart Map
2	CVE-2015-2051	D-Link	D-Link DIR-645, DAP-1522 revB, ...	✓	✓	74	667	3,534	10,423	Details Chart Map
3	CVE-2016-6277	Netgear	NETGEAR R/D Series Routers	✓	✓	33	309	1,299	5,207	Details Chart Map
4	CVE-2017-9841	PHPUnit - Sebastian Bergmann	PHPUnit	x	✓	33	235	1,227	3,767	Details Chart Map
5	CVE-2021-26855	Microsoft	Exchange	x	✓	17	119	622	1,768	Details Chart Map
6	CVE-2021-39226	Grafana	Grafana	x	✓	15	16	16	16	Details Chart Map

Select the CISA Known Exploited Vulnerability (KEV) to get the “triaged” list.
You then focus you actions on these, using the daily data provided by Shadowserver.

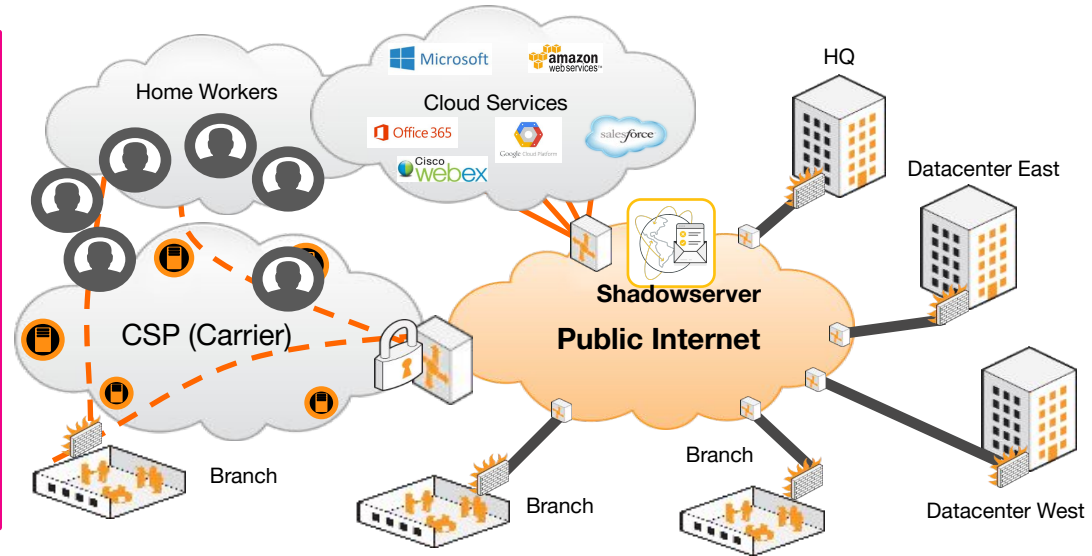


The Bad Actor's Network Visibility

What can others see when looking into your network from the outside?
What is your organisation's risk?

Shadowserver's daily Network Reporting is tuned by:

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



Reports - Multiple Times a Week

- * Operation Endgame: Smoke Loader malware sinkhole infections
- * 911 SOCKS5 Proxy sinkhole infection data
- * Zyxel NAS CVE-2024-29973 RCE botnet exploitation activity
- * Microsoft MSMQ CVE-2024-30080 update: Increased Scanning Activity
- * Alert: Critical Microsoft Message Queuing (MSMQ) Remote Code Execution (RCE) vulnerability CVE
- * Now scanning/sharing VMware vCenter CVE-2024-37079 & CVE-2024-37078
- * SolarWinds Serv-U Directory Transversal Vulnerability CVE-2024-28995 scanning and reporting

What do you get?

Dear All,

P2Pinfect malware has been making the rounds recently infecting vulnerable Redis installations to drop cryptominers and ransomware: <https://cadosecurity.com/blog/from-dormant-to-dangerous-p2pinfect-evolves-to-deploy-new-ransomware-and-cryptominer>

As a reminder, we scan for open Redis installations & now see over 40K daily (with no auth in place): https://dashboard.shadowserver.org/statistics/combined/time-series/?date_range=365&source=scan&source=scan6&tag=redis&dataset=unique_ips&style=stacked

The vast majority of vulnerable Redis servers are on networks of major cloud providers. Sadly, these numbers are steadily going up.

If you run Redis in a cloud environment especially please read https://redis.io/docs/latest/operate/oss_and_stack/management/security/ & ensure adequate access controls!

We share IP data in Open Redis report: <https://www.shadowserver.org/what-we-do/network-reporting/open-redis-report/> ← especially if you represent a cloud/hosting provider please have a look

Social media with stats:

<https://x.com/Shadowserver/status/1806311519543595177>

<https://infosec.exchange/@shadowserver/112688720367882572>

<https://www.linkedin.com/feed/update/urn:li:activity:7212079165229961216>

<https://bsky.app/profile/shadowserver.bsky.social/post/3kvvetmie324>

kind regards,
Piotr



We welcome your Questions

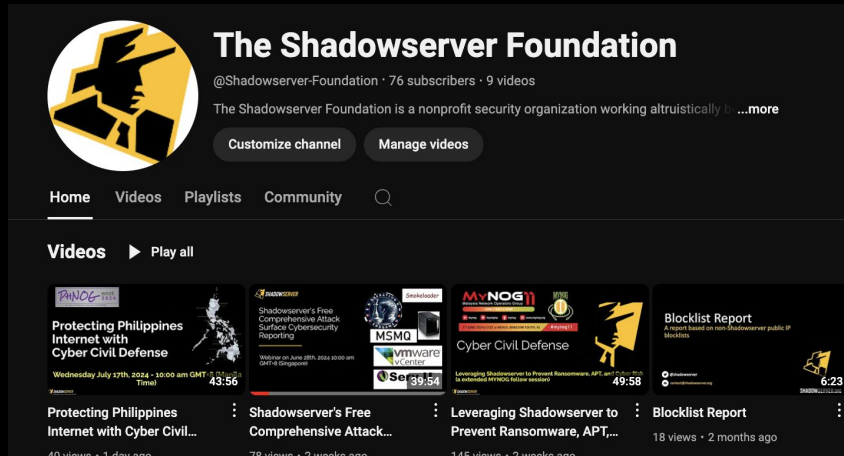
Are you ready to get started?



Follow-up Webinars

Step 1: Subscribe to the Shadowserver's public mailing list
<https://mail.shadowserver.org/mailman/listinfo/public>.

Step 2: Subscribe to the Shadowserver Foundation's Youtube Channel: <https://youtube.com/@shadowserver-foundation>



The screenshot shows the YouTube channel page for 'The Shadowserver Foundation'. The channel name is 'The Shadowserver Foundation' with the handle '@Shadowserver-Foundation', 76 subscribers, and 9 videos. The bio states it is a nonprofit security organization. Below the bio are buttons for 'Customize channel' and 'Manage videos'. The navigation bar includes 'Home', 'Videos', 'Playlists', and 'Community'. The 'Videos' section is active, showing a grid of video thumbnails. The first video is 'Protecting Philippines Internet with Cyber Civil Defense' (43:56). Other visible video titles include 'Shadowserver's Free Comprehensive Attack Surface Cybersecurity Reporting', 'Leveraging Shadowserver to Prevent Ransomware, APT...', and 'Blocklist Report'.

Immediate Action for Everyone

Step 1: Subscribe to the Shadowserver Foundation's public mailing list at <https://mail.shadowserver.org/mailman/listinfo/public>. The mailing list is used to make service announcements, share information, and facilitate open security discussions. You can also ask questions on the mailing list.

Step 2: Subscribe to Shadowserver's Social Media. This is another way of getting updates and notices for new Webinars.

<https://x.com/Shadowserver/>

<https://infosec.exchange/@shadowserver/>

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

<https://bsky.app/profile/shadowserver.bsky.social/>

Step 3: Subscribe to the Shadowserver Foundation's Youtube Channel:

<https://youtube.com/@shadowserver-foundation>

Sign up to our YouTube Channel



The Shadowserver Foundation

@Shadowserver-Foundation · 112 subscribers · 9 videos

The Shadowserver Foundation is a nonprofit security organization working altruistically b...more

🔔 **Subscribed** ▾

Home Videos Playlists 🔍

Videos ▶ Play all



Protecting Philippines Internet with Cyber Civil...

65 views · 1 month ago



Shadowserver's Free Comprehensive Attack...

108 views · 1 month ago



Leveraging Shadowserver to Prevent Ransomware, APT,...

153 views · 1 month ago



Blocklist Report

28 views · 3 months ago



Accessible RDP Report

16 views · 3 months ago



Open DNS Report

31 views · 3 months ago

Subscribe to the FREE Reports!

**Click Here to Subscribe to your FREE Reports that
... If you take action ... will reduce your cyber-risk!**

The Shadowserver Foundation is a nonprofit security organization working altruistically behind the scenes to make the Internet more secure for everyone.

[Our Story](#)

www.shadowserver.org

Subscribing to the Daily Network Reports

Subscribe to Reports

Complete the form below to request free, detailed, relevant, daily remediation reports about the state of your networks. We'll evaluate your request and follow up with you. There is no charge for this service.

It's really free!

Network details

E-mail address where reports or download links will be sent

Your information

Your name

Your organization

Your role within the organization

Your email address

Your phone number

Your PGP key (for an encrypted response)

Your network

List the ASNs or CIDRs for the network space that you directly control (ASNs are preferred, but only if you control the complete ASN). Do not list the ASNs or CIDRs of your ISP. You can also list domain name space under your control.

If you're a National CSIRT, simply list the country you represent.

Investigation Support

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.

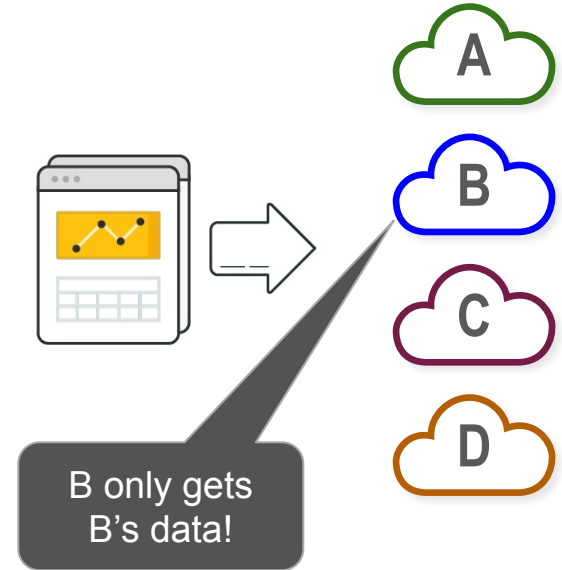
How did you hear about us?

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

Shadowserver's Data Sharing Principles

General Theme - You only get free daily remediation reports for the networks or country(ies) that you can prove your authority (by ASNs, CIDRs, DNS Zones and national authorities).

Any organization may use any of the data that Shadowserver provides to them for free each day concerning their own network space, without any restrictions - we consider the data to be theirs, to do with as they want. We do not give Google's data to Microsoft, or US data to the UK. We only give each network's data to that network's owner (plus their responsible national CERT/CSIRT and LE agencies).



Privacy & Terms has further details: <https://www.shadowserver.org/privacy-and-terms/>

Shadowserver's Data Sharing Principles

Nationals CERTs with Legitimate Authority can request access to Country Data

Shadowserver offers National CSIRTs a clear view of what's happening on their networks, providing personalized support to interpret the data and leverage its impact. Whether you're responsible for a specific set of networks or every network in your region, together we can make a positive impact on Internet security.

Celebrating Milestones (European CERT/CSIRT Report Coverage)

FEBRUARY 23, 2020

Celebrating a particularly significant long term milestone - our 107th National CERT/CSIRT recently signed up for Shadowserver's free daily networking reporting service, which takes us to 136 countries and over 90% of the IPv4 Internet by IP space/ASN. This has finally changed our internal CERT reporting coverage map of Europe entirely green.

In the Service of National CERT's (revisited)

APRIL 2, 2019

Shadowserver recently achieved the significant milestone of having our 100th National CERT/CSIRT sign up for our free daily network reports, so we thought that this would be a good moment to provide an update on our global network remediation coverage.

Privacy & Terms has further details: <https://www.shadowserver.org/privacy-and-terms/>

Home

elseif2 edited this page on Sep 6, 2023 · 10 revisions

Introduction

The following pages represent the different documentation details on what API's Shadowserver provides to different parties. Some of these are available to the public and most are private for partners and our direct data consumers. If you feel you fit any of those descriptions please then request access here: <https://www.shadowserver.org/contact/>

Program Document Pages

- [Programs for accessing the API's](#)
- [Program for managing Reports](#)

API Document Pages

- [ASN and Network Queries](#)
- [Honeypot](#)
- [Malware Query](#)
- [Malware Research](#)
- [Reports Query](#)
- [Scan](#)
- [Trusted Programs Query](#)
- [Filters](#)

Related

- [IntelMQ](#)

Pages 12

Home

- Introduction
- Program Document Pages
- API Document Pages
- Related

▶ [API: ASN and Network Queries](#)

▶ [API: Honeypot](#)

▶ [API: Malware Query](#)

▶ [API: Malware Research](#)

▶ [API: Reports Query](#)

▶ [API: Scan](#)

▶ [API: Trusted Programs Query](#)

▶ [API:Filters](#)

▶ [call_api Documentation](#)

▶ [IntelMQ](#)

▶ [report manager Documentation](#)

Email contacts@shadowserver.org to request an API key,



Summary

Shadowserver's Non-Profit Mission, Community Trust, and provides any organization with data to minimize their cybersecurity risk.

- ✓ The **Daily Network Reporting** is a **free - public service** to organizations with a ASN, IP addresses, and domain names.
- ✓ These reports are **delivered** via **Email or APIs** - allowing for easy integration with your current security tools.
- ✓ ***Organizations have only used the Shadowserver Reports to build a security rhythm of action that uncovered & fixed risk in their organization.***



SHADOWSERVER

Lighting the way to a more secure Internet

Remember to Sign Up

dashboard.shadowserver.org

shadowserver.org/partner



@shadowserver



contact@shadowserver.org

SHADOWSERVER.ORG