Who is “Shadowserver?”

A security service for every Network!

Barry Greene - Shadowserver Volunteer

bgreene@shadowserver.org

SHADOWSERVER
Lighting the way to a more secure Internet

Shadow Who?

The Shadowserver Foundation is an Internet Critical not-for-profit organization (NPO) working to make the Internet more secure for everyone. They are the low-key, Cyber-Civil Defence service that is at the center of the push against Threat Actors on the Internet.

Unique insight into network security, a **global vantage point** and **proven TRUSTED partnerships**:

- *National Computer Security Incident Response Teams (nCSIRTs)*
- *Law Enforcement*
- *Industry and security researchers world-wide*

Shares information with Internet defenders at no cost to mitigate vulnerabilities, detect malicious activity and counter emerging threats.

SHADOWSERVER

Why is Shadowserver One of the Top Sources?

… and most people do not know about the free services the Shadowserver Alliance provides to the community.

Ask your teams "How are you leveraging Shadowserver's Tools & Reports?"

Ask your vendors, "Are you part of the Shadowserver Alliance? Are you helping to push back against the threat, or just making money from the threat?"

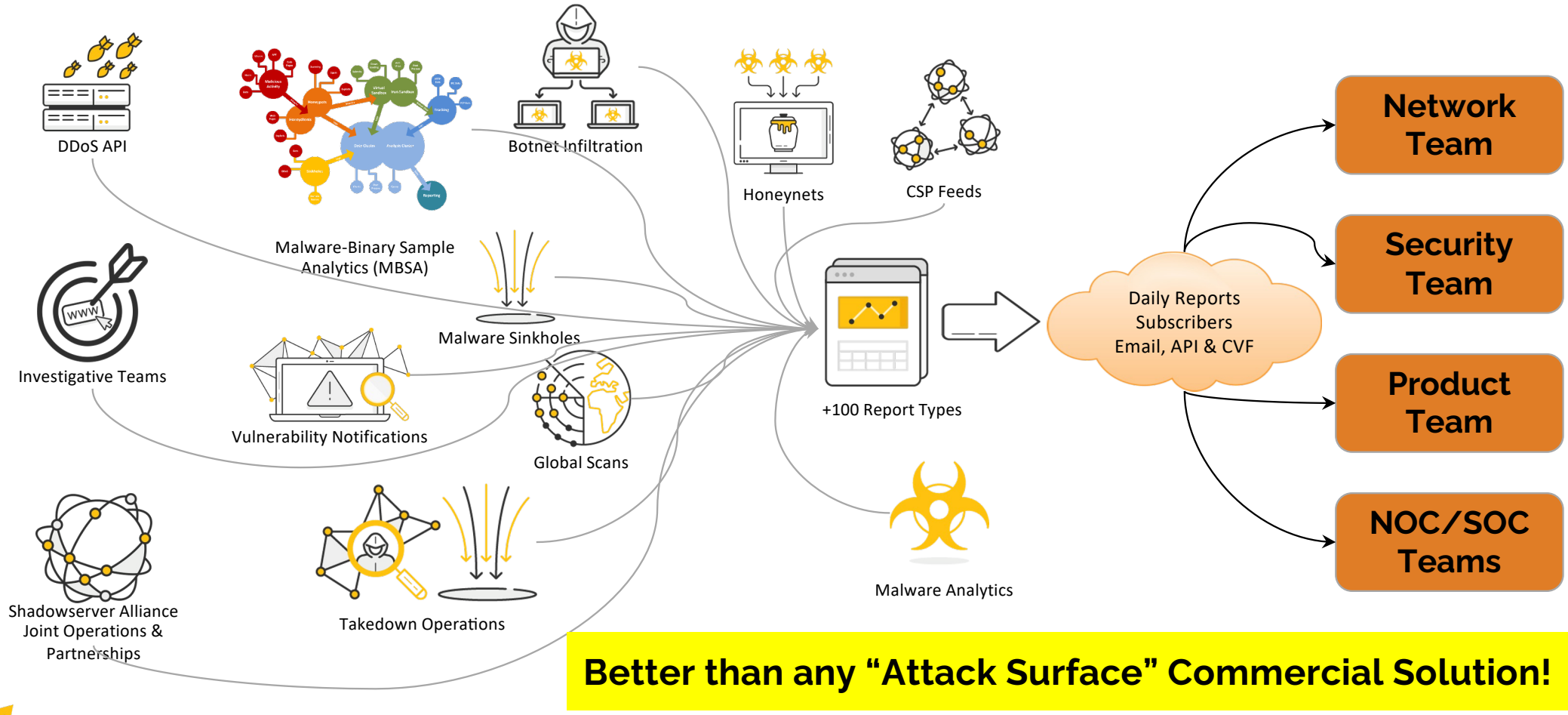
Ask your ISPs, Telcos, and Cloud Operators, "Are you working with Shadowserver to mitigate the threats on your network?"

SHADOWSERVER

An unparalleled combination of position, trusted information and 20 years of proven community partnerships enables Shadowserver to perform a critical role in Internet security - the world's largest provider of free cyber threat intelligence.

Shadowserver's "trust" is built on execution, confidentiality, & unique expert cybersecurity experience.

Shadowserver Providing the Tools



Better than any "Attack Surface" Commercial Solution!

SHADOWSERVER

The latest reports ....

Shadowserver @Shadowserver · Jun 16

A reminder we are sharing out daily data on accessible MOVEit instances in our Device Identification report - shadowserver.org/what-we-do/net...

You can track exposure on our Dashboard, for example - dashboard.shadowserver.org/statistics/iot...

1 11 16 4,151

Shadowserver @Shadowserver · Jun 16

Replying to @Shadowserver

You can track attacks against MOVEit instances as seen by our sensors (CVE-2023-34362) on our Exploited Vulnerabilities list dashboard.shadowserver.org/statistics/hon...

Make sure to patch against all 3 known vulns that allow for RCE, including the latest from June 15th

progress.com

MOVEit Transfer and MOVEit Cloud Vulnerability

Shadowserver @Shadowserver · Jun 13

At least 20.3K Fortinet devices likely vulnerable to CVE-2023-27997 (heap buffer overflow in sslvpn pre-authentication) seen in our scans (on 2023-06-12)

Fortinet advisory: fortiguard.com/psirt/FG-IR-23...
Dashboard: dashboard.shadowserver.org/statistics/com...

Make sure to update your FortiOS/FortiProxy!

4 101 211 53.6K

Shadowserver @Shadowserver · Jun 13

Replying to @Shadowserver

IP-specific data shared daily in our Vulnerable HTTP report - shadowserver.org/what-we-do/net...

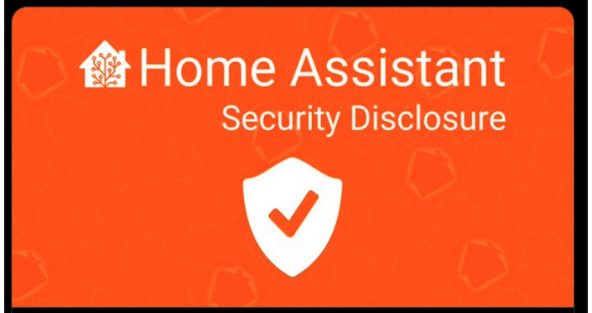
(tagged "cve-2023-27997")

Shadowserver
@Shadowserver

Since June 1st we are seeing scans for Home Assistant Supervisor API authentication bypass CVE-2023-27482.
dashboard.shadowserver.org/statistics/hon...

Make sure you run a fully patched Home Assistant, as the exploit details are public: home-assistant.io/blog/2023/03/0...

NVD entry: nvd.nist.gov/vuln/detail/CV....



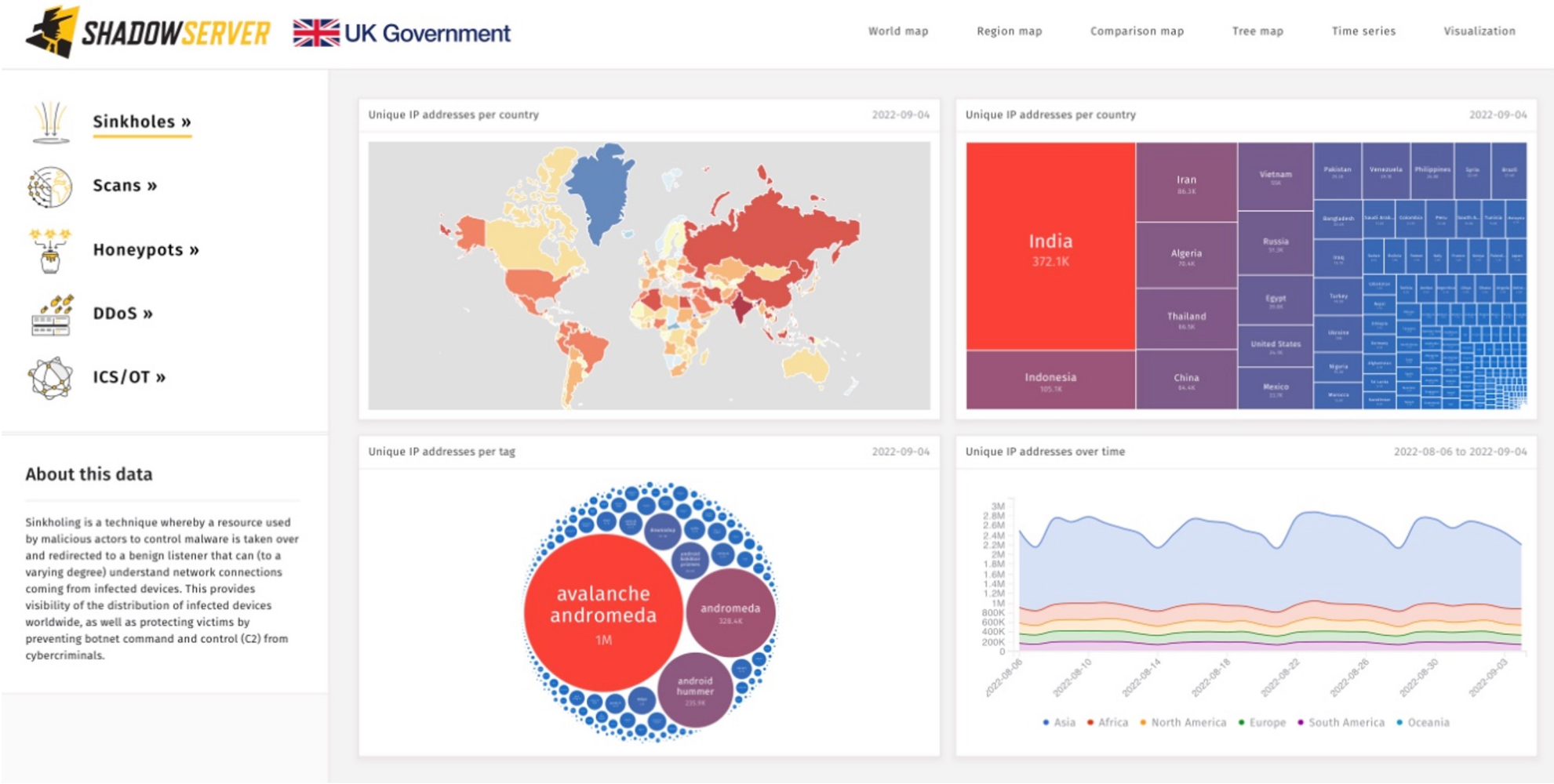
home-assistant.io

Disclosure: Supervisor security vulnerability

Disclosure of a security vulnerability found impacting installations using the Home Assistant Supervisor.

SHADOWSERVER

Shadowserver's Dashboard



SHADOWSERVER

Alliance Investment = Community Defense

Alliance investors include Philanthropist Craig Newmark who is “putting his money where his mouth is” by supporting a broad coalition of organizations dedicated to educating and protecting Americans amid escalating cybersecurity threats.

Cyber-Civil Defense helps the community, the customers, the business, and everyone on the Internet. Protect your country’s interest by investing and the Shadowserver Alliance and commissioning work that benefits your constituents. Anything you do for your constituents helps everyone on the Internet!

SHADOWSERVER

SHADOWSERVER

Using the Daily Reporting to Reduce your Security Risk

The Simple things Make a Big Difference

Security Best Common Practices (BCPs) are not hard, they are not expensive. They take time, persistence, and consistency.

- You do not need to pay to subscribe to any "security threat service."
- You do not need to buy expensive scanning services.
- You have access to the most advanced "surface area" security service to let you know what the "bad guy" threat actors can see.

All of this is free and a public service that provides daily reports on your ASN, IP Blocks, and Domain Names. The reports are delivered via email or APIs.

SHADOWSERVER

Example - No Budget for Security

2012 walking into a large Indonesian Cell Phone Company. There is no cybersecurity budget or team.

- Recruited two “fresh out of college” graduates to directly report to me (other VPs didn’t the workload of “new people.”)
- Had them pick one Shadowserver report a week.
- Their job was to track down the issues, find out how to fix the risk, document a process to minimize repeat, and then seek out and hunt for “how threat actors would have abused.”

Step-by-Step: We found the Nation State and Cyber Criminal threat actors and pushed them off our network. Each step built our resiliency, skills, capabilities, and capacity …. All using open source and public cyber civil defence tools!

SHADOWSERVER

Network Reports Highlight Actionable Risk

New Network Report types added by Community Action

- New network reports are added with each new category of incident
- Each network report type includes details of the source and recommended actions
- Over 90 network report types and growing!

OUR 137 REPORT TYPES

API: Documentation	Basic API documentation
API: Scan/SSL	An API to allow querying of the collected SSL data from the daily SSL scans.
API: Research	A module to allow trusted partners to query information about malware, networks, and trusted programs.
API: ASN and Network Queries	Returns routing details for a given address or ASN.
API: Malware Query	Returns a JSON response containing static details about the requested sample as well as antivirus vendor and signature details.
API: Reports Query	An API to query the different reports received as well as do basic queries of the data itself. This is meant as an optional replacement to the emails received with the report URL's
API: Trusted Programs Query	Returns a JSON response containing the details for the requested program.
Accessible ADB Report	This report identifies hosts that have the Android Debug Bridge (ADB) running, bound to a network port (5555/tcp) and accessible on the Internet. It's a Service Scan, and it's updated every 24 hours.
Accessible AFP Report	This report identifies hosts that have the Apple Filing Protocol (AFP) running and accessible on the Internet. It's a Service Scan, and it's updated every 24 hours.

SHADOWSERVER

Network Report Details (example)

Brute Force Attack Report

This report identifies hosts that have been observed performing brute force attacks, using SISSDEN's network of honeypots.

One of these honeypot type sensors is dedicated to detecting SSH and telnet attacks against network devices. These attacks typically involve brute-forcing credentials to obtain access.

Once access has been obtained, the devices are used for other attacks, which may involve installing malicious software that enables the device to function as part of a botnet. For example, the well-known Mirai botnets were used in this way to launch DDoS attacks.

Hacked devices may also be used to launch scans on other vulnerable Internet devices. In still other cases, using brute force to breach networking devices may enable a criminal to attempt financial theft. By inserting rogue DNS server entries into a home router's network configuration, they can redirect user traffic to malicious webpages, making phishing attacks on the home network user.

When we detect brute force attacks, our system reports them to the owners of the network from which the attacks originate, or to the National CERTs responsible for that network.

This report type was created as part of the EU Horizon 2020 **SISSDEN Project.**

FIELDS

timestamp	Time that the attack was performed in UTC+0
ip	The IP address performing the attack
port	The source port used in the attack
asn	ASN announcing the attacking IP
geo	Country where the attacking IP resides
region	State / Province / Administrative region where the attacking IP resides
city	ASN of where the attacking IP resides
hostname	PTR record of the attacking IP
dest_ip	Country where the device in question resides
dest_port	Destination port used in the attack

SAMPLE


```
"timestamp","ip","port","asn","geo","region","city","hostname","dest_ip","dest_port","de
"2017-04-27 00:00:06","185.38.148.3",4428,200039,"UK","BRISTOL","BRISTOL","3.148.38.185.
"2017-04-27 00:00:55","200.175.184.148",16503,18881,"BR","DISTRITO FEDERAL","BRASILIA",
"2017-04-27 00:01:45","186.52.245.178",32941,6057,"UY","MONTEVIDEO","MONTEVIDEO","r186-5
"2017-04-27 00:05:45","77.126.141.114",56133,9116,"IL","HAMERKAZ","KEFAR SAVA",,"158.255
"2017-04-27 00:07:34","212.3.34.144",53558,39155,"ES","GRANADA","FUENTE CAMACHO","212-3-
"2017-04-27 00:09:55","180.169.17.83",58809,4812,"CN","SHANGHAI","SHANGHAI",,"37.235.56.
"2017-04-27 00:13:31","197.46.62.186",56735,8452,"EG","AL QAHIRAH","CAIRO","host-197.46.
"2017-04-27 00:14:56","84.172.148.54",3316,3320,"DE","BADEN-WURTTEMBERG","SCHRIESHEIM",
"2017-04-27 00:16:29","171.231.155.225",56158,7552,"VN","BINH DINH","QUI NHON",,"5.28.63
```


SHADOWSERVER

Daily workflow with Shadowserver Reports

We have +50 reports with hundreds of issues! Where to we start?

Don't panic! Start daily action. Work with few of the simplistest first, then shift to reports that are CRITICAL and HIGH severity.

SHADOWSERVER

Example of the Daily - SNMP

timestamp	ip	protocol	port	hostname	sysdesc
2022-05-19 09:38:06		udp	161		Cisco IOS Software Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICESK9-M) Version 12.2(54)SG RELEASE SOFTWARE (fc3)Te
2022-05-19 09:49:18		udp	161		Cisco IOS Software C3560E Software (C3560E-UNIVERSALK9-M) Version 12.2(55)SE1 RELEASE SOFTWARE (fc1)Technical Support: htt
2022-05-19 10:03:53		udp	161		Cisco NX-OS(tm) n3000 Software (n3000-uk9) Version 6.0(2)U6(6) RELEASE SOFTWARE Copyright (c) 2002-2012 by Cisco Systems Inc.
2022-05-19 10:20:07		udp	161		Cisco IOS Software C3560E Software (C3560E-UNIVERSALK9-M) Version 12.2(55)SE1 RELEASE SOFTWARE (fc1)Technical Support: htt
2022-05-19 10:44:14		udp	161		Cisco IOS Software Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICESK9-M) Version 12.2(54)SG RELEASE SOFTWARE (fc3)Te
2022-05-19 11:15:39		udp	161		Cisco IOS Software C3560E Software (C3560E-UNIVERSALK9-M) Version 12.2(55)SE1 RELEASE SOFTWARE (fc1)Technical Support: htt
2022-05-19 11:58:20		udp	161		Cisco IOS XR Software (NCS-5500) Version 7.1.2 Copyright (c) 2013-2020 by Cisco Systems Inc.
2022-05-19 14:07:19		udp	161		Cisco IOS Software C3560E Software (C3560E-UNIVERSALK9-M) Version 12.2(55)SE1 RELEASE SOFTWARE (fc1)Technical Support: htt
2022-05-19 14:33:17		udp	161		Cisco IOS Software C3560E Software (C3560E-UNIVERSALK9-M) Version 12.2(55)SE1 RELEASE SOFTWARE (fc1)Technical Support: htt
2022-05-19 15:05:26		udp	161		Cisco IOS Software Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICESK9-M) Version 12.2(54)SG RELEASE SOFTWARE (fc3)Te
2022-05-19 15:12:21		udp	161		Cisco IOS Software Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICESK9-M) Version 12.2(54)SG RELEASE SOFTWARE (fc3)Te

Each of these devices have SNMP ports open to the Internet.

They are exposed for abuse.

https://www.shadowserver.org/what-we-do/network-reporting/open-snmp-report/

SHADOWSERVER

Example of the Daily - SNMP

sysname	asn	geo	region	city	version	naics	sic	sector	device_vendor	device_type	device_model	d
		US	OREGON	PORTLAND	2	517919		Communications, Service Provider, and Hosting Service	Cisco		IOS	
		JP	TOKYO	TOKYO	2	518210		Communications, Service Provider, and Hosting Service	Cisco		IOS	
		US	MASSACHUSETTS	CAMBRIDGE	2	517919		Communications, Service Provider, and Hosting Service				
		JP	TOKYO	TOKYO	2	518210		Communications, Service Provider, and Hosting Service	Cisco		IOS	
		US	WASHINGTON	SEATTLE	2	517919		Communications, Service Provider, and Hosting Service	Cisco		IOS	
		JP	TOKYO	TOKYO	2	518210		Communications, Service Provider, and Hosting Service	Cisco		IOS	
		AR	CAPITAL FEDERAL	BUENOS AIRES	2	517919		Communications, Service Provider, and Hosting Service				
		JP	TOKYO	TOKYO	2	518210		Communications, Service Provider, and Hosting S				
		JP	TOKYO	TOKYO	2	518210		Communications, Service Provider, and Hosting S				
		US	WASHINGTON	SEATTLE	2	517919		Communications, Service Provider, and Hosting S				
		US	WASHINGTON	SEATTLE	2	517919		Communications, Service Provider, and Hosting S				

device_sector	tag	community
enterprise	snmp	public
enterprise	snmp	public
	snmp	public
enterprise	snmp	public
enterprise	snmp	public
enterprise	snmp	public
	snmp	public
enterprise	snmp	public
enterprise	snmp	public
enterprise	snmp	public
enterprise	snmp	public

The Shadowserver reports using geolocation to provide the region and city.

Notice the “public” SNMP Community

SHADOWSERVER

Back to Basics - Do something - consistently every day!

Preventive Maintenance Inspection is Critical to the Mission. Any organization who needs to be always ready will alway inspect the daily habits of “PMI”

Example using Shadowserver’s Reports::

1. Organization with little to no security budget.
2. Grab new engineers right out of college.
3. Have them pick a Shadowserver report, hunt the problem, figure out how to sustainably fix, then act.

Reflect, learn, and repeat.

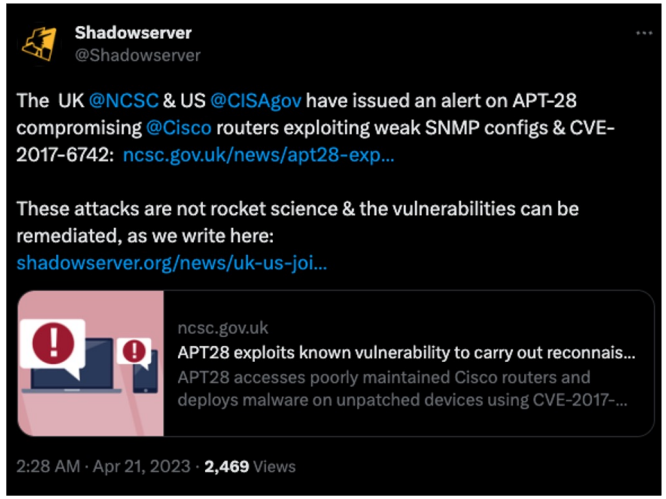
Each security issue found by Shadowserver is an “leading indicator of risk!

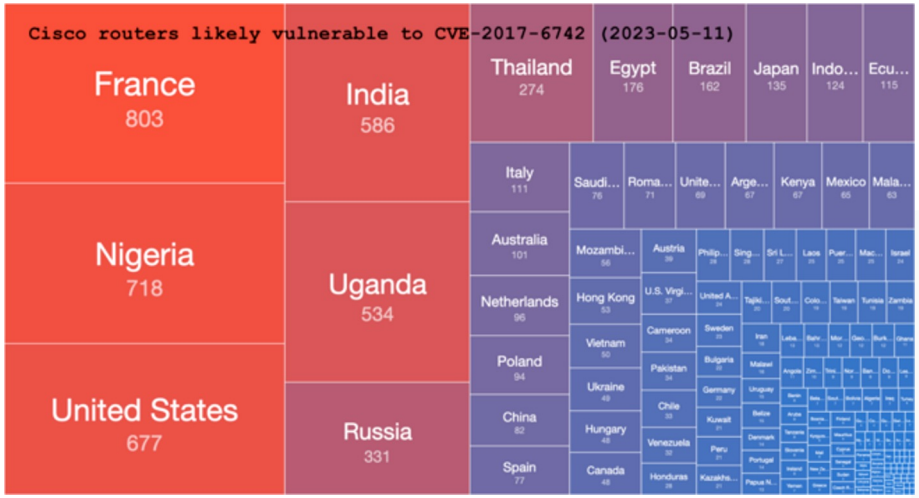
SHADOWSERVER

Watch for the Incident Reporting

Shadowserver alerts their constituents and the Internet on critical ACTIVE EXPLOITATION!

Shadowserver gives you the ability to quickly review the risk on your network and fix the vulnerability before it gets exploited.





NEWS

APT28 exploits known vulnerability to carry out reconnaissance and deploy malware on Cisco routers

APT28 accesses poorly maintained Cisco routers and deploys malware on unpatched devices using CVE-2017-6742.

UK/US Joint Announcements Remind Us That Un-Remediated Vulnerabilities Snowball

APRIL 20, 2023

The **UK's National Cyber Security Centre (NCSC)** and the **US Cybersecurity and Infrastructure Security Agency (CISA)** issued an alert on nation-state sponsored exploitation of router infrastructure.

The **"UK and US issue warning about APT28 actors exploiting poorly maintained Cisco routers" alert** called out SNMP public exposure and one vulnerability in particular – **CVE-2017-6742** which relates to a long known "remote code execution" opportunity on certain Cisco routers. Bad actors who find this vulnerability available to them can use it to execute any piece of code they choose. You can read more details **here**.

This alert is a timely reminder for all with unpatched equipment to think broadly!

Don't just consider your computer when patching – remember any device in your network (including your router) that connects to the Internet should be checked with a view to patching if a patch is available. If you fail to do this you are leaving yourself and your network's users potentially vulnerable.

SHADOWSERVER

Use the Exploited Vulnerabilities List

SHADOWSERVER UK Government

Dashboard | General statistics | IoT device statistics | Attack statistics

Attack statistics

Vulnerabilities

Category: Top
Statistic: Unique IPs
Date range: From – To
Country: Select an option...
IoT: Select an option...
CISA KEV: 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.

Exploited vulnerabilities - Top

Showing results for 2023-06-27

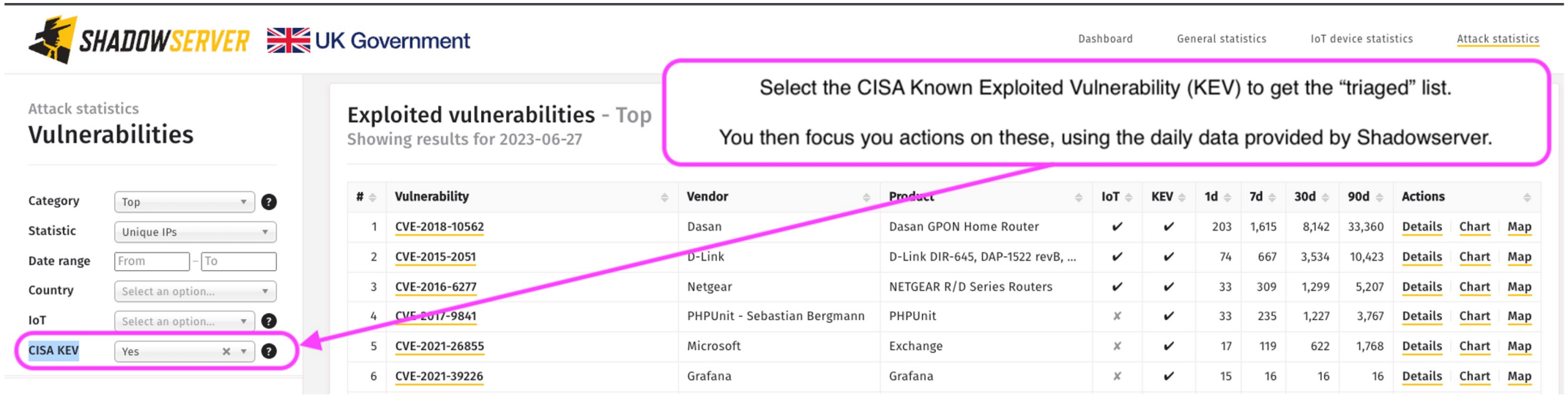
#	Vulnerability	Vendor	Product	IoT	KEV	1d	7d	30d	90d	Actions
1	CVE-2014-8361	Realtek	Realtek SDK	✔	✘	3,578	27,368	84,635	135,440	Details Chart Map
2	CVE-2017-17215	Huawei	Huawei Home Gateway HG532	✔	✘	3,298	27,661	121,057	438,802	Details Chart Map
3	CVE-2018-10562	Dasan	Dasan GPON Home Router	✔	✔	203	1,615	8,142	33,360	Details Chart Map
4	EDB-41471	MVPower	MVPower DVR	✔	✘	198	1,525	8,330	29,293	Details Chart Map
5	CVE-2016-10372	Zyxel	Eir D1000	✔	✘	156	1,222	6,061	20,970	Details Chart Map
6	EDB-25978	Netgear	Netgear DGN1000	✔	✘	149	1,216	5,840	18,030	Details Chart Map
7	CVE-2018-9995	TBK	DVR4104/DVR4216 and multiple...	✔	✘	128	215	536	1,289	Details Chart Map
8	CVE-2019-12780	Belkin	Wemo	✔	✘	85	444	2,351	9,495	Details Chart Map
9	EDB-39596	Shenzhen TVT	CCTV-DVR (rebranded by multi...	✔	✘	77	626	2,924	9,174	Details Chart Map
10	CVE-2015-2051	D-Link	D-Link DIR-645, DAP-1522 revB, ...	✔	✔	74	667	3,534	10,423	Details Chart Map
11	CVE-2017-18368	Zyxel/Billion	ZyXEL P660HN-T1A v1, ZyXEL P6...	✔	✘	34	371	2,361	4,783	Details Chart Map
12	OPENVAS-1361412562310107187	Vacron	Network Video Recorder (NVR)	✔	✘	34	260	1,292	4,213	Details Chart Map

https://dashboard.shadowserver.org/statistics/honeypot/monitoring/vulnerability/?category=monitoring&statistic=unique_ips

Focus on US CISA's KEV List

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

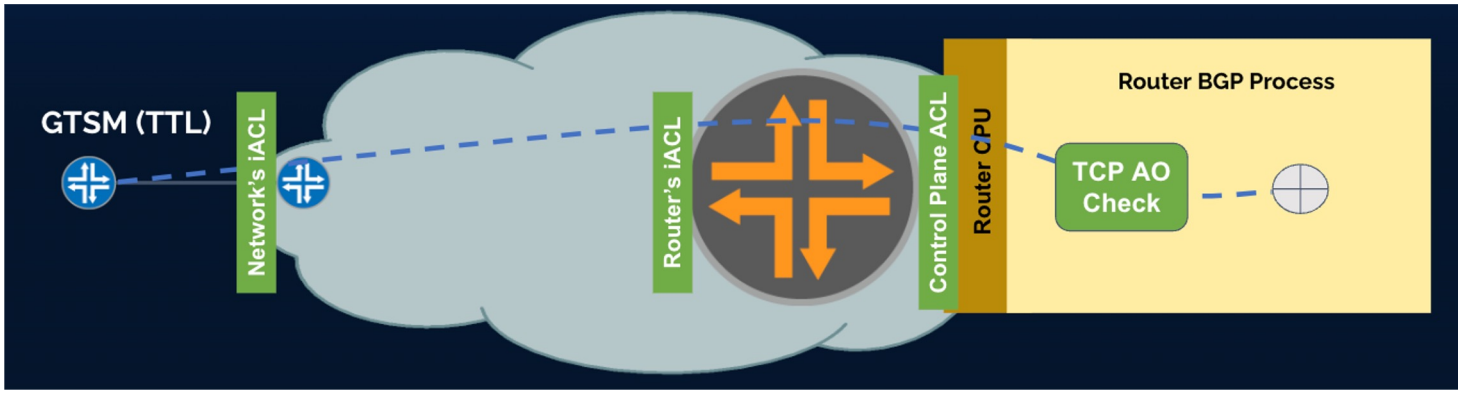
Shadowserver provides a public service to have an "outside-in" assessment of your network.



Example: Are you Protecting your BGP Session?

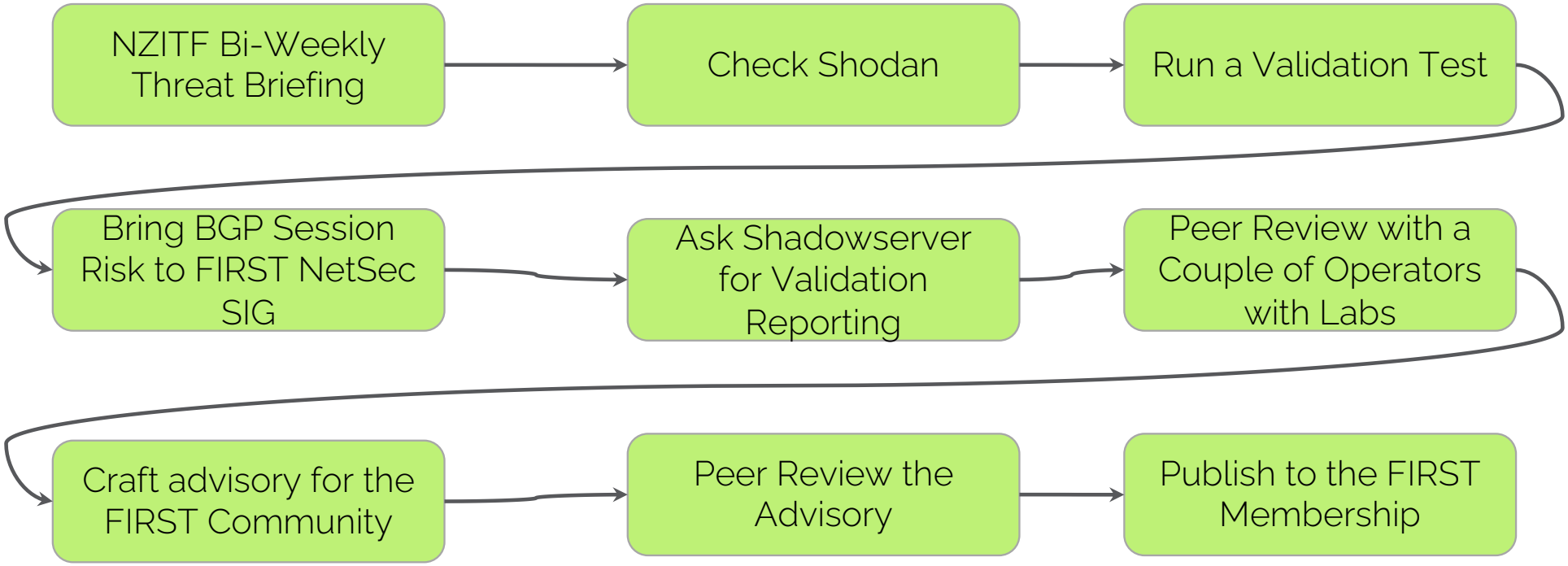
Networks that think they are "DDoS resilient" get surprised when their BGP Sessions go down from an easily crafted DDoS.

BGP port (179) is left open to the Internet and is an easy target for a low-level attack that will knock down your BGP session.
Shodan's BGP Report 325,082 open port 179 instances (June 2023). That is 325,082 organizations whose BGP sessions are at risk



SHADOWSERVER

What Happened?



And now we wait - as all teams are totally saturated with a sandstorm of security risk throw at them every day.

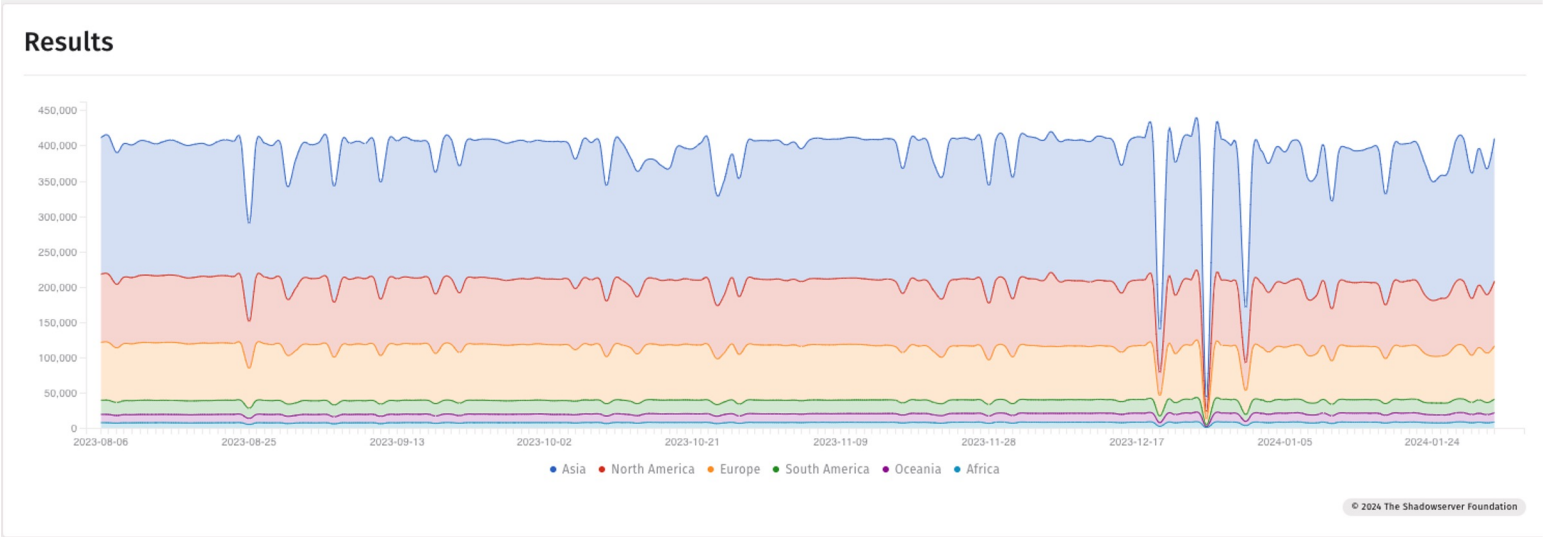
SHADOWSERVER

Check Shadowserver's New BGP Reports

Shadowserver has made it easy for organizations with two new reports:

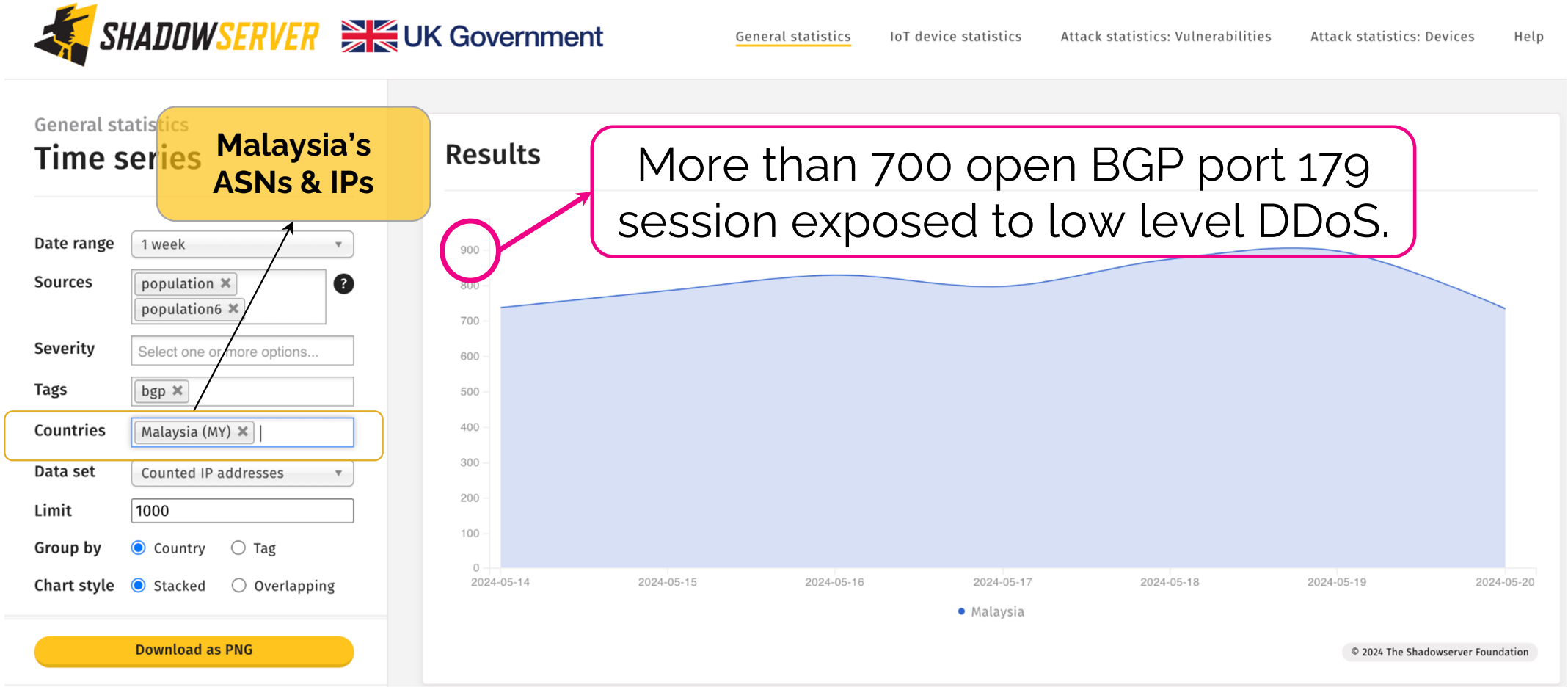
Accessible BGP service report: https://shadowserver.org/what-we-do/network-reporting/accessible-bgp-service-report/

Open BGP service report: https://shadowserver.org/what-we-do/network-reporting/open-bgp-service-report/



SHADOWSERVER

Malaysia's Current Risk



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.
- ✓ You can ask your "MSSPs" and "Managed Security" vendors to leverage these reports.
- ✓ ***Organizations have only used the Shadowserver Reports to build a security rhythm of action that uncovered & fixed risk in their organization.***

SHADOWSERVER

SHADOWSERVER

Lighting the way to a more secure Internet

Remember to Sign Up

dashboard.shadowserver.org

shadowserver.org/partner

@shadowserver

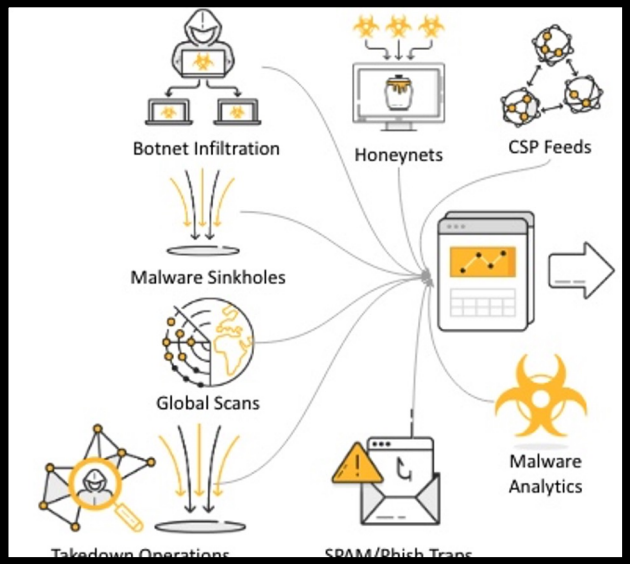
contact@shadowserver.org

SHADOWSERVER.ORG

Extras!

How to Sign Up and Get Started

Shadowserver's Daily Reports



SHADOWSERVER
Lighting the way to a more secure Internet

Plugging into the Shadowserver Alerts

Shadowserver Alliance Members: Will get pre-alerts, new report crafting, and ability to directly consult with the Shadowserver teams and fellow peers on as the public reporting is being curated (via the Alliance Mattermost).

Public Mailing List: https://mail.shadowserver.org/mailman/listinfo/public

X/Twitter: https://twitter.com/Shadowserver

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

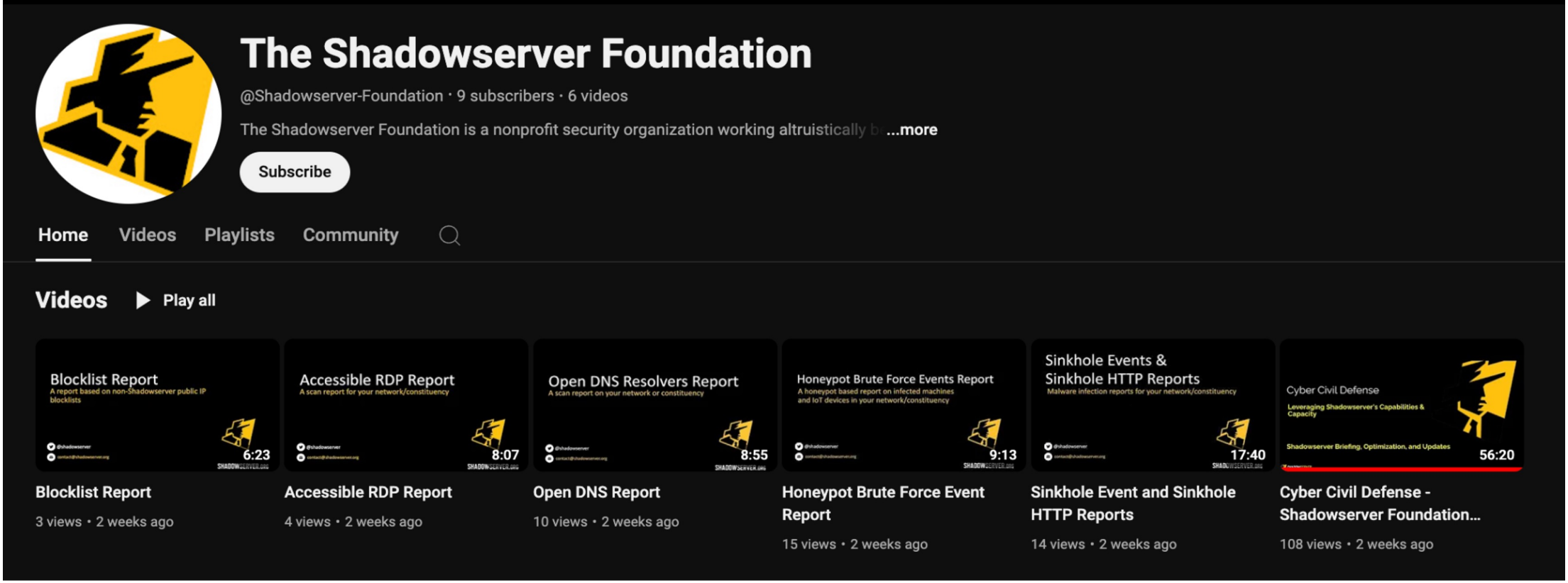
X (formerly Twitter)

Shadowserver (@Shadowserver) on X

We observed CVE-2024-21893 exploitation using '/dana-na/auth/saml-logout.cgi' on Feb 2nd hours before @Rapid7 posting & unsurprisingly lots to '/dana-ws/saml20.ws' after...

SHADOWSERVER

Shadowserver Youtube Channel



https://www.youtube.com/@Shadowserver-Foundation

SHADOWSERVER

Subscribing to the Daily Network Reports

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

Who Are you?

Your name

Your organization

Your role within the organization

Your email address

Your phone number

Your PGP key (for an encrypted reply)

Your Network?

Your ASNs and Customer ASNs

Your CIDR Blocks

Your Domain Names

If you are a national CERT, list your country.

If you are doing this on behalf of a another network, please explain.

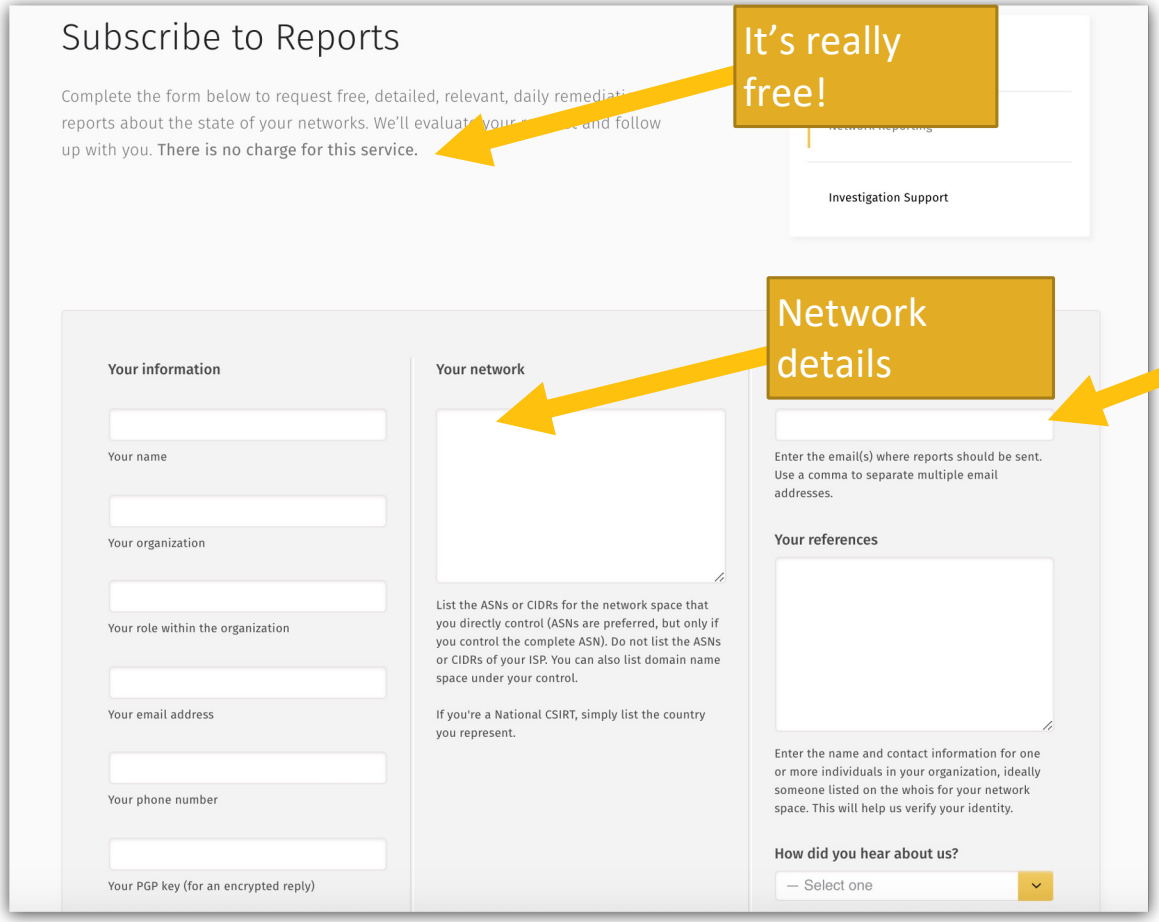
How do we Trust?

List of Emails to send the reports

List of references whom can vouch for you. 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.

SHADOWSERVER

Subscribing to the Daily Network Reports



It's really free!

Network details

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

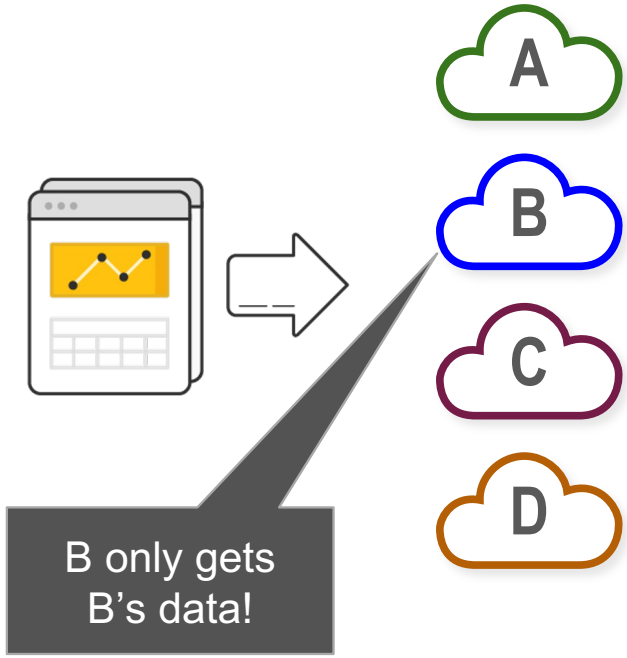
SHADOWSERVER

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

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 though 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/

SHADOWSERVER

Different Forms Of Data Access

- E-mail (must always be provided, even if only for notifications)
- Report file download links
- Webspace with report files
- API with report files
- Delta mode option (report changes only)

Reports are always files in CSV format

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

API: Reports Query

Last Updated: 2020-10-29

Reports API

An API to query the different reports received as well as to do basic queries of the data itself. This is meant as an optional replacement to the emails received with the report URL's. In all cases the queries and the data that is delivered is only from the reports that you would have normally received. You only get the data on the networks you are responsible for. You will not be able to get data on other networks or systems. Note refer to the **API: Documentation** pages for testing details and examples.

Modules

- reports/subscribed – List of reports that the user is subscribed to
- reports/types – List of all the types of reports that are available for the subscriber
- reports/list – List of actual reports that could be downloaded
- reports/download – Download specific report
- reports/query – Query the stored data

REPORTS METHODS

REPORTS/SUBSCRIBED

Note that most organizations will only have a single list they are subscribed to and can get data on.

Fields:

```
apikey : string : Your API key
```

SHADOWSERVER

Open Source Threat Intel Tool

IntelMQ is a solution for IT security teams (CERTs & CSIRTs, SOCs, abuse departments, etc.) for collecting and processing security feeds (such as log files) using a message queuing protocol.

It's a community driven initiative called IHAP (Incident Handling Automation Project) which was conceptually designed by European CERTs/CSIRTs during several InfoSec events.

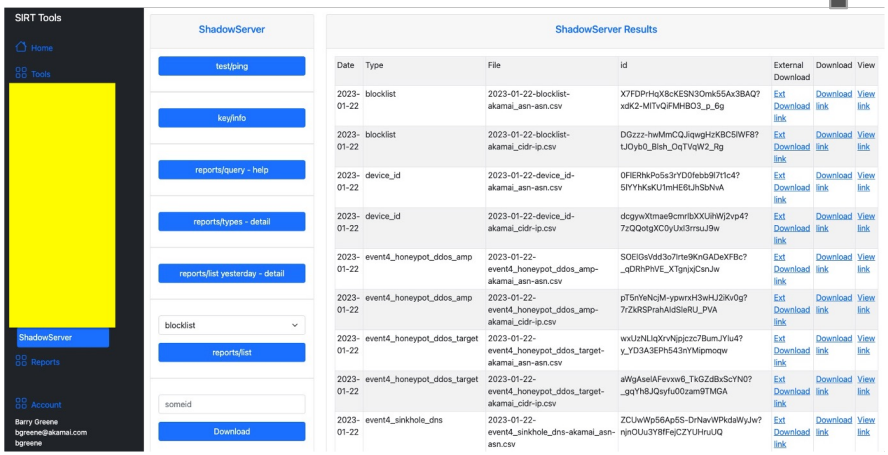
Its main goal is to give to incident responders an easy way to collect & process threat intelligence thus improving the incident handling processes of CERTs.

https://github.com/certtools/intelmq

Example of an API Tools (Akamai)

Shadowserver's API Tools allow for organization to build your own tools to leverage the security risk identified to you by Shadowserver.

Akamai gets daily update reports on all ASNs, IPv4, IPv4, and domain names …. All accessible via API.



Date	Type	File	id	External Download	Download	View
2023-01-22	blocklist	2023-01-22-blocklist-akamai_asn-asn.csv	X7FDPrHqX8cKESN3Omk55Ax3BAQ?xdK2-MTvQiFMHBO3_p_6g	Ext Download link	Download link	View link
2023-01-22	blocklist	2023-01-22-blocklist-akamai_cidr-ip.csv	DGzzz-hwMmCQJiqwgHzKBC5IWF8?tJOyb0_BIsh_OqTVqW2_Rg	Ext Download link	Download link	View link
2023-01-22	device_id	2023-01-22-device_id-akamai_asn-asn.csv	0FIERhkPo5s3rYD0febb9I7t1c4?5tYYhKsKU1mIHE6tJhSbNvA	Ext Download link	Download link	View link
2023-01-22	device_id	2023-01-22-device_id-akamai_cidr-ip.csv	dcgywXtmae9cmrlbXXUihWj2vp4?7zQQotgXC0yUxI3rrsuJ9w	Ext Download link	Download link	View link
2023-01-22	event4_honeypot_ddos_amp	2023-01-22-event4_honeypot_ddos_amp-akamai_asn-asn.csv	SOEIGsVdd3o7lrte9KnGADeXFBc?_qDRhPhVE_XTgnjxjCsnJw	Ext Download link	Download link	View link
2023-01-22	event4_honeypot_ddos_amp	2023-01-22-event4_honeypot_ddos_amp-akamai_cidr-ip.csv	pT5nYeNcjM-ypwrxH3wHJ2iKv0g?7rZkRSPrahAIdSleRU_PVA	Ext Download link	Download link	View link
2023-01-22	event4_honeypot_ddos_target	2023-01-22-event4_honeypot_ddos_target-akamai_asn-asn.csv	wxUznLlqXrvNjpjczc7BumJYIu4?y_YD3A3EPh543nYMipmoqw	Ext Download link	Download link	View link
2023-01-22	event4_honeypot_ddos_target	2023-01-22-event4_honeypot_ddos_target-akamai_cidr-ip.csv	aWgAseIAFevxw6_TkGZdBxScYN0?_gqYh8JQsyfu00zam9TMGA	Ext Download link	Download link	View link
2023-01-22	event4_sinkhole_dns	2023-01-22-event4_sinkhole_dns-akamai_asn-asn.csv	ZCUwWp56Ap5S-DrNavWPkdaWyJw?njnOUu3Y8fFejCZYUHruUQ	Ext Download link	Download link	View link

Alarms, tools, and other security capabilities can then be coded to protect Akamai, their customers, and the Internet.

In this case, Shadowserver's Sinkhole identified an Akamai customer who is using their CDN, but their "origin" datacenter has a Avalanche-NYMAIM infection.

SHADOWSERVER

Summary & Key Report Pages

Reports overview

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

Report Updates

- https://www.shadowserver.org/news-insights/
- Twitter @shadowserver or Linkedin: https://www.linkedin.com/company/the-shadowserver-foundation/
- Mailing list access send request to contact@shadowserver.org and request access to public@shadowserver.org
- Or subscribe directly at https://mail.shadowserver.org/mailman/listinfo/public
- Github: https://github.com/The-Shadowserver-Foundation

Reports API

- Request access to contact@shadowserver.org
- https://www.shadowserver.org/what-we-do/network-reporting/api-documentation/
- https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/

SHADOWSERVER