SHADOWSERVER

Shadowserver: Sharing Free Threat Intelligence at Scale

Piotr Kijewski, The Shadowserver Foundation

piotr@shadowserver.org, @piotrkijewski

7th December 2021
2021 FIRST & AfricaCERT Symposium for Africa and Arab Regions

SHADOWSERVER.ORG

What is The Shadowserver Foundation

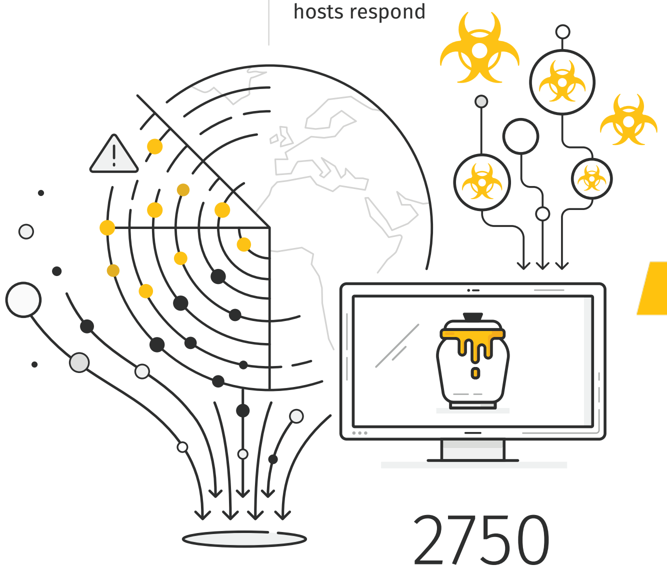
- A not-for-profit organisation (NPO) working to make the Internet more secure for everyone.
- **Unique sources**, a **global vantage point** and **proven partnerships** with:
  - *National Computer Security Incident Response Teams (nCSIRTs)*
  - *Law Enforcement*
  - *Industry and security researchers world-wide*
- **Shares information with Internet defenders at no cost** to mitigate vulnerabilities, detect malicious activity and counter emerging threats.
- An unparalleled combination of position, **trusted information** and **15 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

Shadowserver by (some of the) numbers

4 BILLION

IPv4 addresses scanned **45** times per day. **139 Million** hosts respond



4-5 MILLION

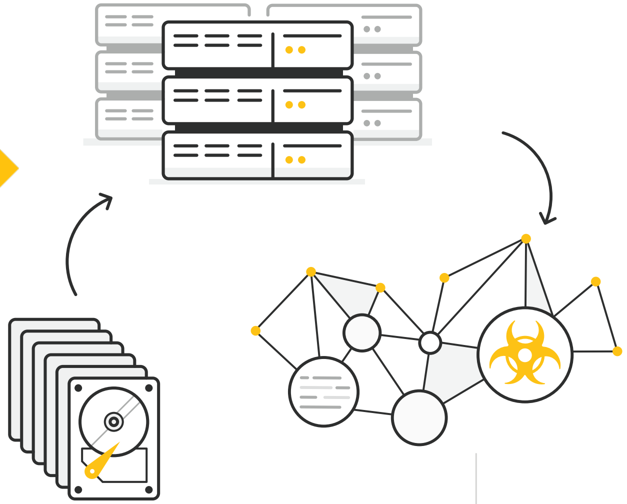
IP addresses per day sinkholed across **400** different malware variants

2750

Class C networks hosting honeypots & spampots

1,115,000

unique malware samples ingested & analyzed **every day** by our sandboxes. Over **1.5 billion samples** in our malware repository



11.6 PETABYTES

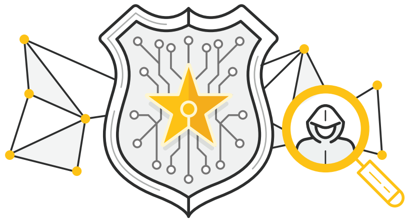
of malware & threat intel stored, **growing at 1+ PB/year**

40 BILLION

SSL certificates, indexed & searchable in our data & analysis clusters

6,020

network owners & **131 National CSIRTs in 173 countries and territories** rely on our **free** daily reports



Behind the scenes support for dozens of international Law Enforcement operations

SHADOWSERVER

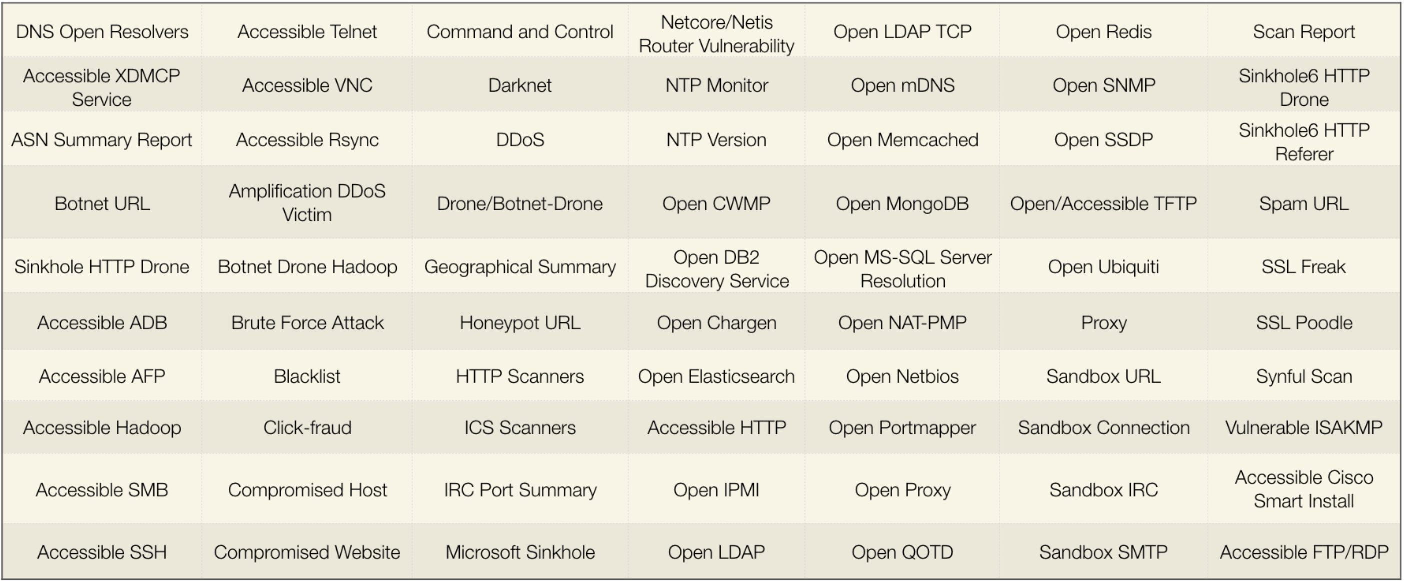
Free daily threat feeds

Providing CSIRTs with actionable information

Free Daily Remediation Reports - National CSIRTs and Network Owners

Network Reporting

Every day, Shadowserver sends custom remediation reports to more than 6000 vetted subscribers, including over 130 national governments and many Fortune 500 companies. These reports are detailed, targeted, relevant and free.

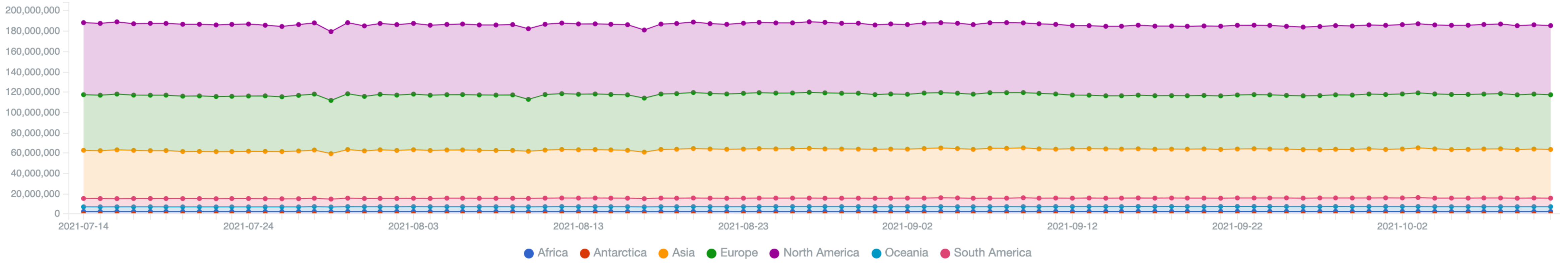


DNS Open Resolvers	Accessible Telnet	Command and Control	Netcore/Netis Router Vulnerability	Open LDAP TCP	Open Redis	Scan Report
Accessible XDMCP Service	Accessible VNC	Darknet	NTP Monitor	Open mDNS	Open SNMP	Sinkhole6 HTTP Drone
ASN Summary Report	Accessible Rsync	DDoS	NTP Version	Open Memcached	Open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

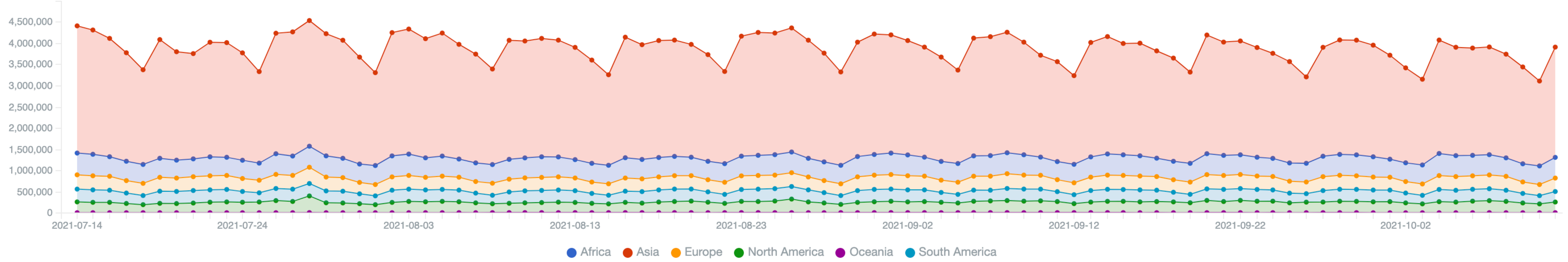
Much of the world uses these reports to receive rapid notification when computer networks globally are misconfigured, vulnerable, abusable, get compromised or become infected.

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

Shadowserver Daily Event Stats (Globally)



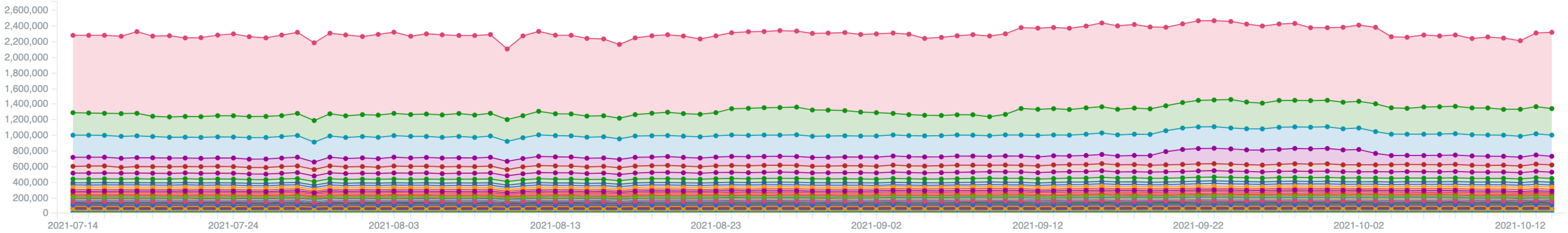
Over 180 million accessible/open/vulnerable services per day on average seen globally by our scans



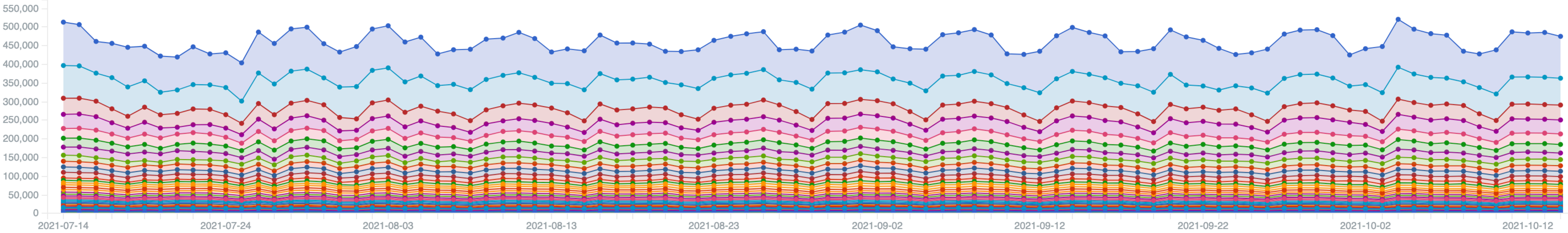
SHADOWSERVER

Approximately 4.5 million infected IP addresses per day on average seen globally in sinkholes

Shadowserver Daily Event Stats (Africa)



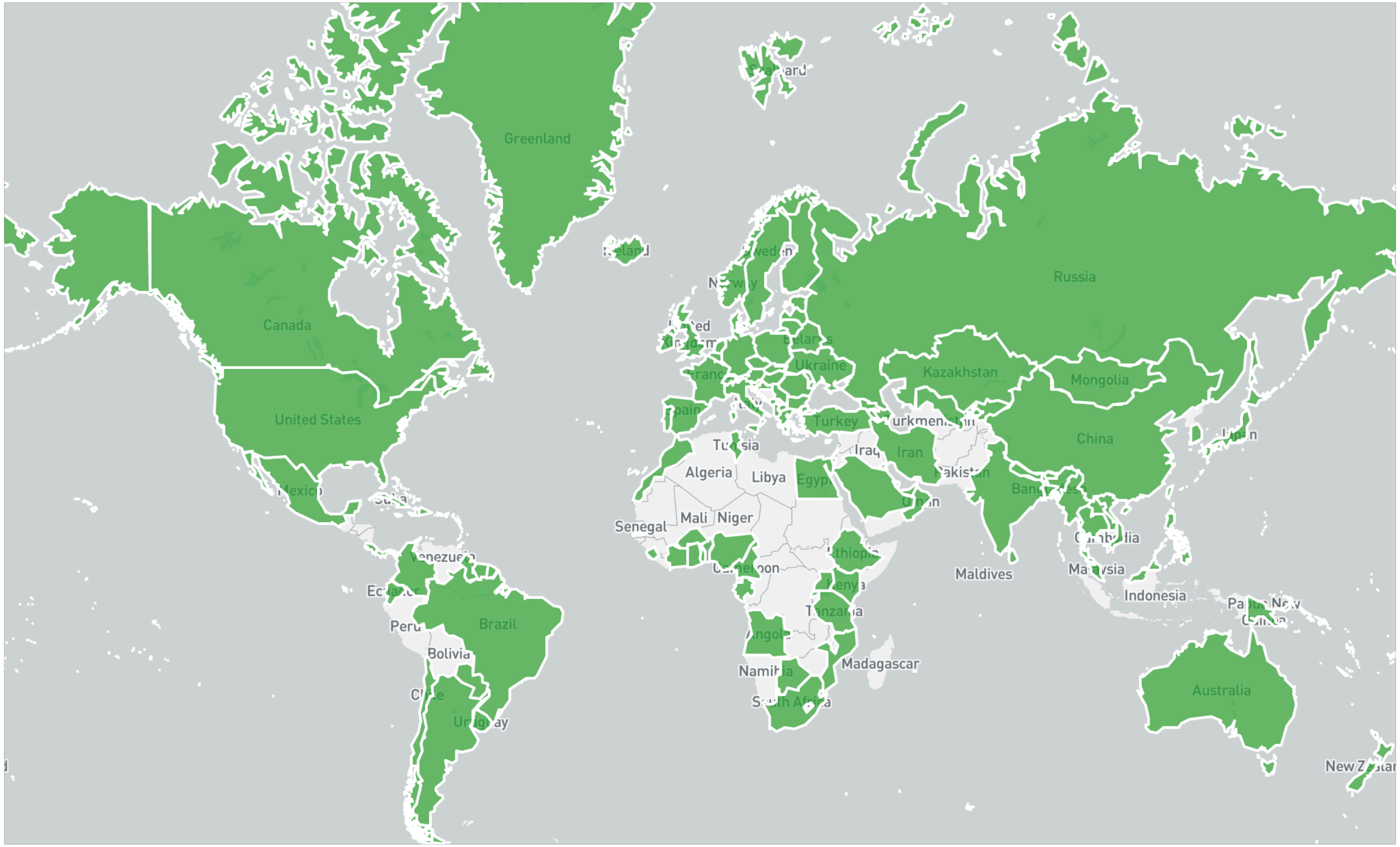
Around 2.2 million accessible/open/vulnerable services per day on average seen in Africa (scanning)



SHADOWSERVER

Over 450k infected IP addresses per day on average seen in Africa in our sinkhole data

National CSIRTs receiving feeds (Nov 2021)



Missing African National CSIRTs - 2021-12-01

Algeria	Comoros	Guinea-Bissau	Mauretania	Sao Tome and Principe
Burundi	Djibouti	Lesotho	Mauritius	Senegal
Cape Verde	Equatorial Guinea	Liberia	**Namibia (activated 2021-12-01)**	Somalia
Central African Republic	Eritrea	Libya	Niger	Western Sahara
Chad	Guinea	Mali	Republic of Congo	**Zambia (signing up 2021-12-01)**

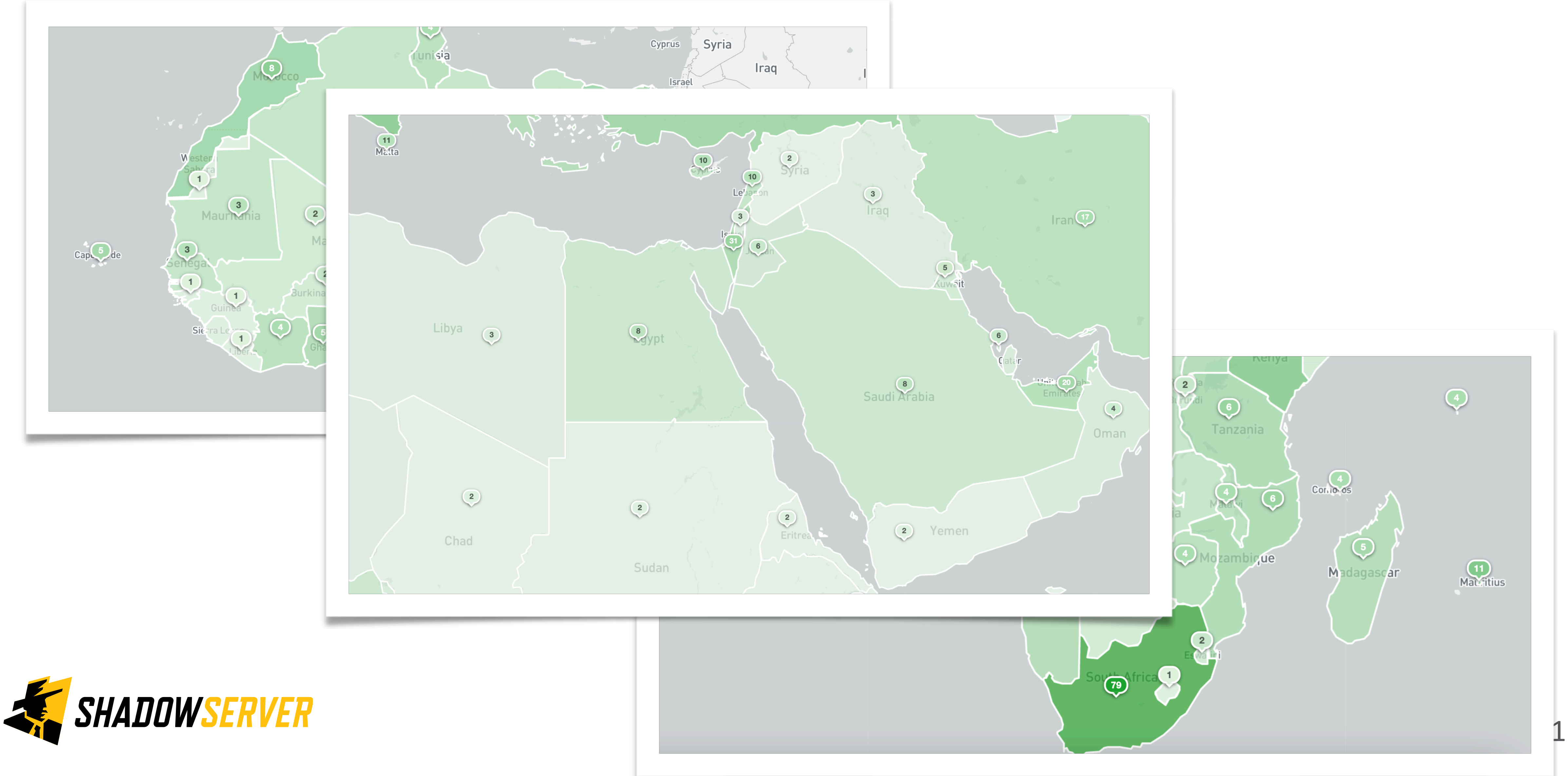
Can you help with the missing National CSIRTs?

Missing Arab Region National CSIRTs - 2021-12-01

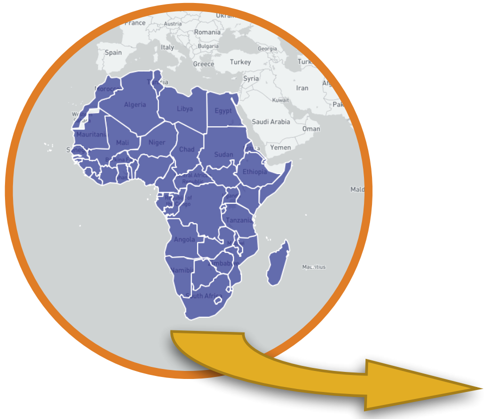
Algeria	Iraq	Mauretania
Bahrain	Jordan	Palestinian Territory
Comoros	Lebanon	Somalia
Djibouti	Libya	Sudan

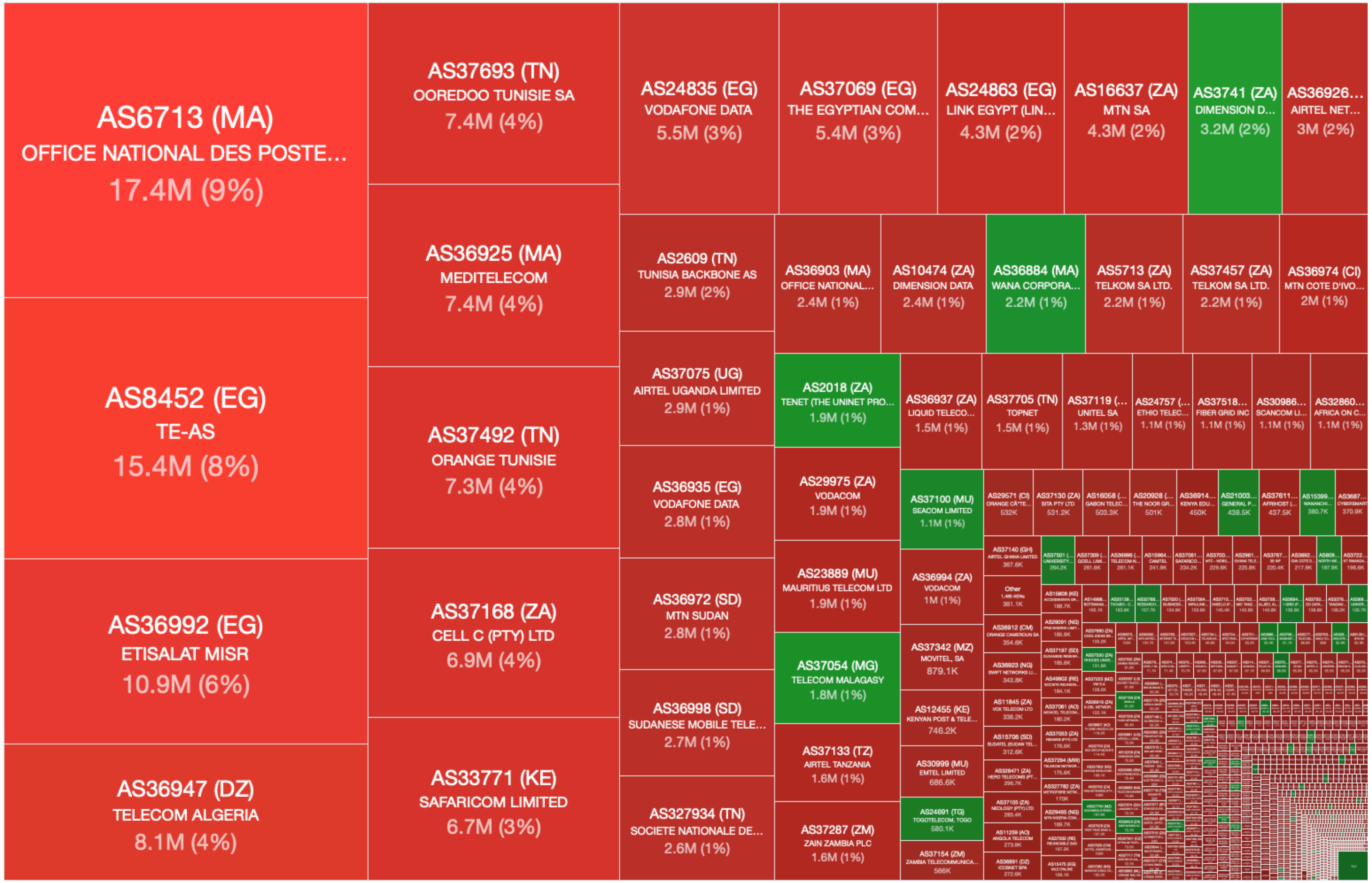
Can you help with the missing National CSIRTs?

Direct Feed recipients: African & Arab Region network owners (Nov 2021)



Shadowserver’s IPv4 View - Africa - ASN Reports

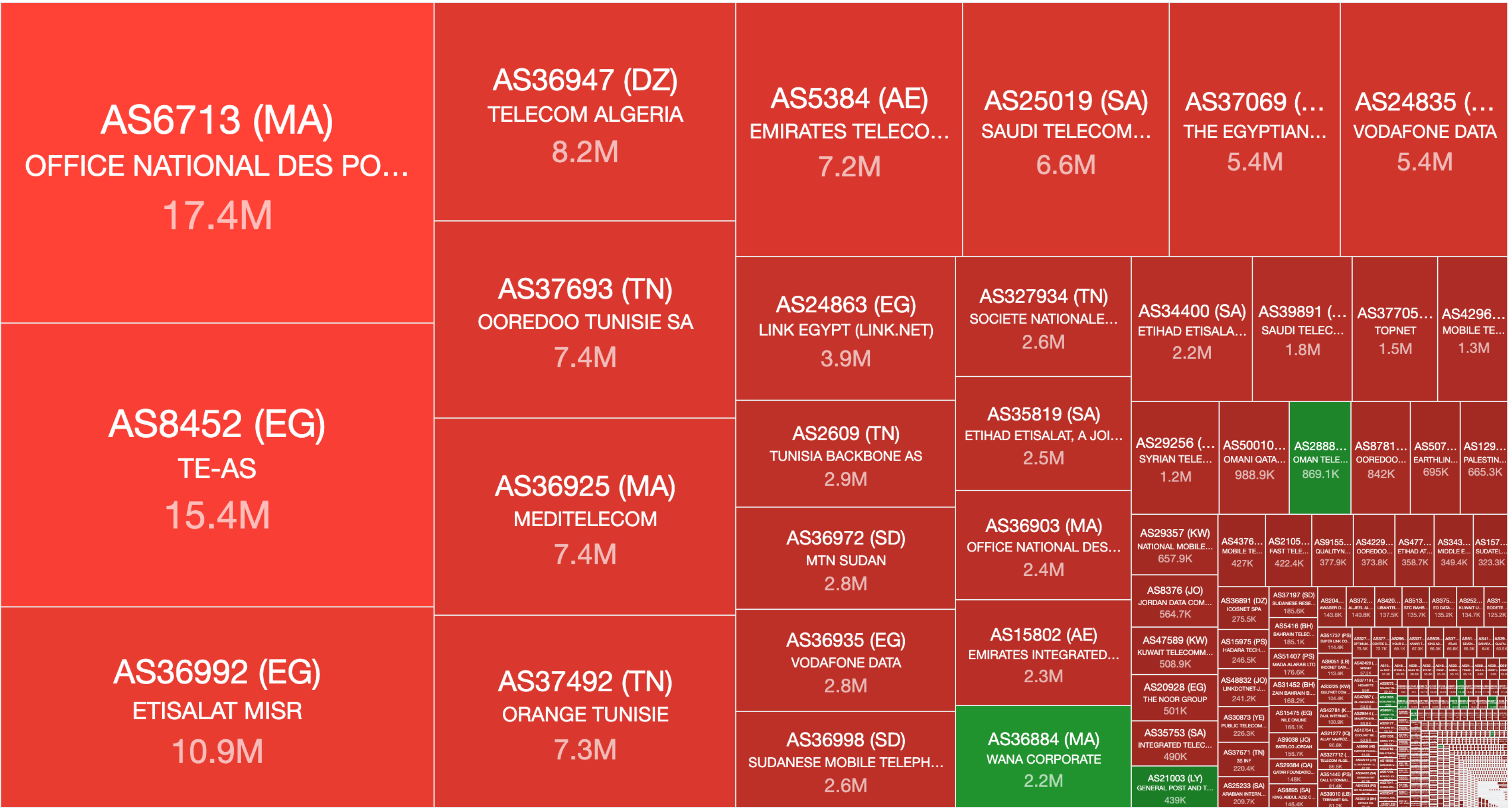




114,288,820 IPs
31,994 CIDRs
2,480 ASNs

Only 77 ASNs Currently Receiving Reports
- really want to improve that!

Shadowserver’s IPv4 View - Arab Region - ASN Reports



AS6713 (MA) OFFICE NATIONAL DES PO… 17.4M
AS8452 (EG) TE-AS 15.4M
AS36992 (EG) ETISALAT MISR 10.9M
AS36947 (DZ) TELECOM ALGERIA 8.2M
AS37693 (TN) OOREDOO TUNISIE SA 7.4M
AS36925 (MA) MEDITELECOM 7.4M
AS37492 (TN) ORANGE TUNISIE 7.3M
AS5384 (AE) EMIRATES TELECO… 7.2M
AS25019 (SA) SAUDI TELECOM… 6.6M
AS37069 (… THE EGYPTIAN… 5.4M
AS24835 (… VODAFONE DATA 5.4M
AS24863 (EG) LINK EGYPT (LINK.NET) 3.9M
AS2609 (TN) TUNISIA BACKBONE AS 2.9M
AS36972 (SD) MTN SUDAN 2.8M
AS36935 (EG) VODAFONE DATA 2.8M
AS36998 (SD) SUDANESE MOBILE TELEPH… 2.6M
AS327934 (TN) SOCIETE NATIONALE… 2.6M
AS35819 (SA) ETIHAD ETISALAT, A JOI… 2.5M
AS36903 (MA) OFFICE NATIONAL DES… 2.4M
AS15802 (AE) EMIRATES INTEGRATED… 2.3M
AS36884 (MA) WANA CORPORATE 2.2M
AS34400 (SA) ETIHAD ETISALA… 2.2M
AS39891 (… SAUDI TELEC… 1.8M
AS37705… TOPNET 1.5M
AS4296… MOBILE TE… 1.3M
AS29256 (… SYRIAN TELE… 1.2M
AS50010… OMANI QATA… 988.9K
AS2888… OMAN TELE… 869.1K
AS8781… OOREDOO… 842K
AS507… EARTHLIN… 695K
AS129… PALESTIN… 665.3K
AS29357 (KW) NATIONAL MOBILE… 657.9K
AS4376… MOBILE TE… 427K
AS2105… FAST TELE… 422.4K
AS9155… QUALITYN… 377.9K
AS4229… OOREDOO… 373.8K
AS477… ETIHAD AT… 358.7K
AS343… MIDDLE E… 349.4K
AS157… SUDATEL… 323.3K
AS8376 (JO) JORDAN DATA COM… 564.7K
AS36891 (DZ) ICOSNET SPA 275.5K
AS37197 (SD) SUDANESE RESE… 185.6K
AS204… AWASER O… 143.6K
AS372… ALJEEL AL… 140.8K
AS420… LIBANTEL… 137.5K
AS513… STC BAHR… 135.7K
AS375… EO DATA… 135.2K
AS252… KUWAIT U… 134.7K
AS31… SODETE… 125.2K
AS47589 (KW) KUWAIT TELECOMM… 508.9K
AS15975 (PS) HADARA TECH… 246.5K
AS5416 (BH) BAHRAIN TELEC… 185.1K
AS51407 (PS) MADA ALARAB LTD 176.6K
AS51737 (PS) SUPER LINK CO… 114.4K
AS9051 (LB) INCONET DATA… 113.4K
AS20928 (EG) THE NOOR GROUP 501K
AS48832 (JO) LINKDOTNET-J… 241.2K
AS31452 (BH) ZAIN BAHRAIN B… 168.2K
AS3225 (KW) GULFNET COM… 104.4K
AS35753 (SA) INTEGRATED TELEC… 490K
AS30873 (YE) PUBLIC TELECOM… 226.3K
AS15475 (EG) NILE ONLINE 166.1K
AS42781 (K… ZAJIL INTERNATI… 100.9K
AS9038 (JO) BATELCO JORDAN 156.7K
AS21277 (IQ) ALLAY NAWROZ… 96.8K
AS37671 (TN) 3S INF 220.4K
AS29384 (QA) QATAR FOUNDATIO… 148K
AS327712 (… TELECOM ALGE… 86.5K
AS21003 (LY) GENERAL POST AND T… 439K
AS25233 (SA) ARABIAN INTERN… 209.7K
AS8895 (SA) KING ABDUL AZIZ C… 146.4K
AS51440 (PS) CALL U COMMU… 81.4K
AS39010 (LB) TERRANET SAL 81.2K

75,869,846 IPs
31,440 CIDRs
1,246 ASNs

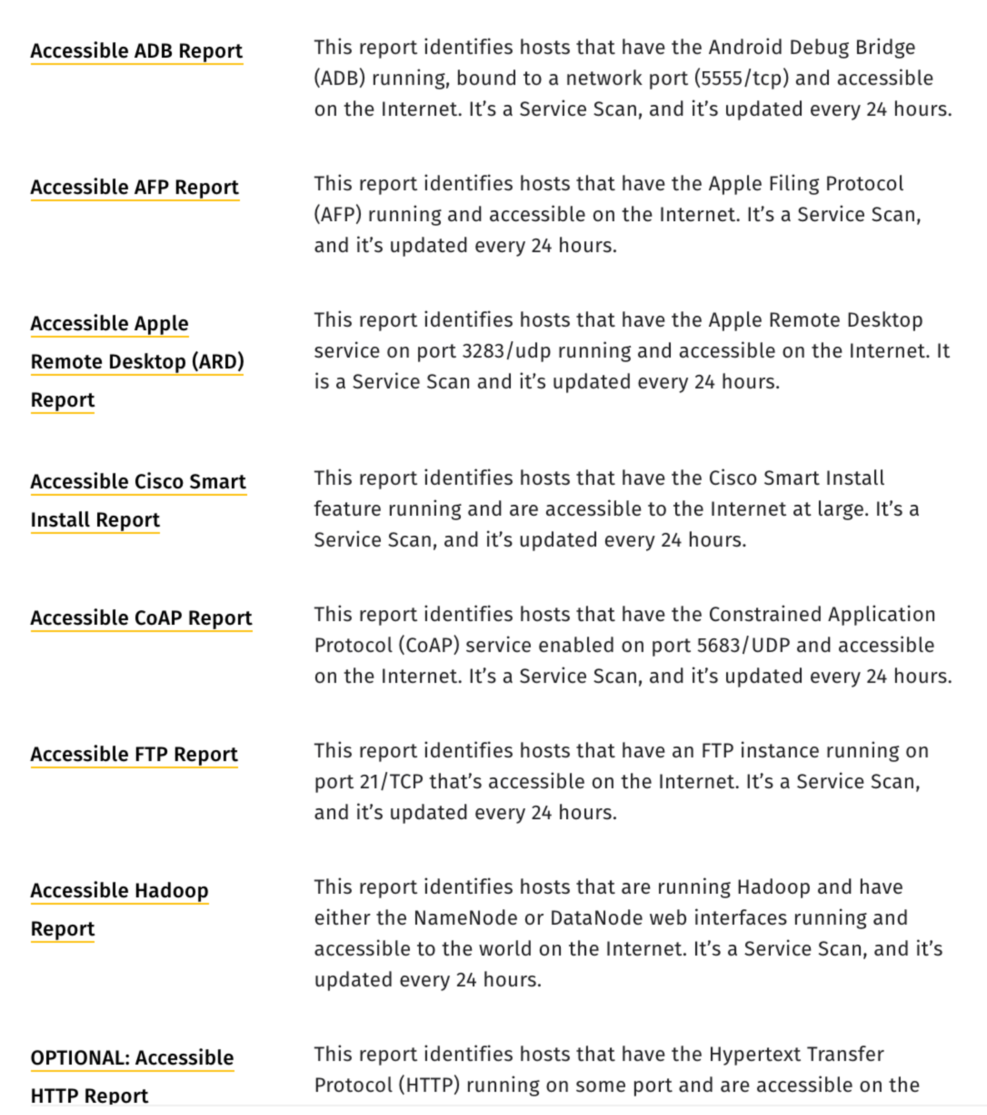
Only 17 ASNs Currently Receiving Reports **- really really want to improve that!**

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 70 network report types and growing!
- **Optional reports** for population type scans (like SSL certificate inventory, exposed SSH services etc, various IPv6 scans)
- API access (or e-mail/weblink delivery)

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



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.

Accessible Apple Remote Desktop (ARD) Report

This report identifies hosts that have the Apple Remote Desktop service on port 3283/udp running and accessible on the Internet. It is a Service Scan and it's updated every 24 hours.

Accessible Cisco Smart Install Report

This report identifies hosts that have the Cisco Smart Install feature running and are accessible to the Internet at large. It's a Service Scan, and it's updated every 24 hours.

Accessible CoAP Report

This report identifies hosts that have the Constrained Application Protocol (CoAP) service enabled on port 5683/UDP and accessible on the Internet. It's a Service Scan, and it's updated every 24 hours.

Accessible FTP Report

This report identifies hosts that have an FTP instance running on port 21/TCP that's accessible on the Internet. It's a Service Scan, and it's updated every 24 hours.

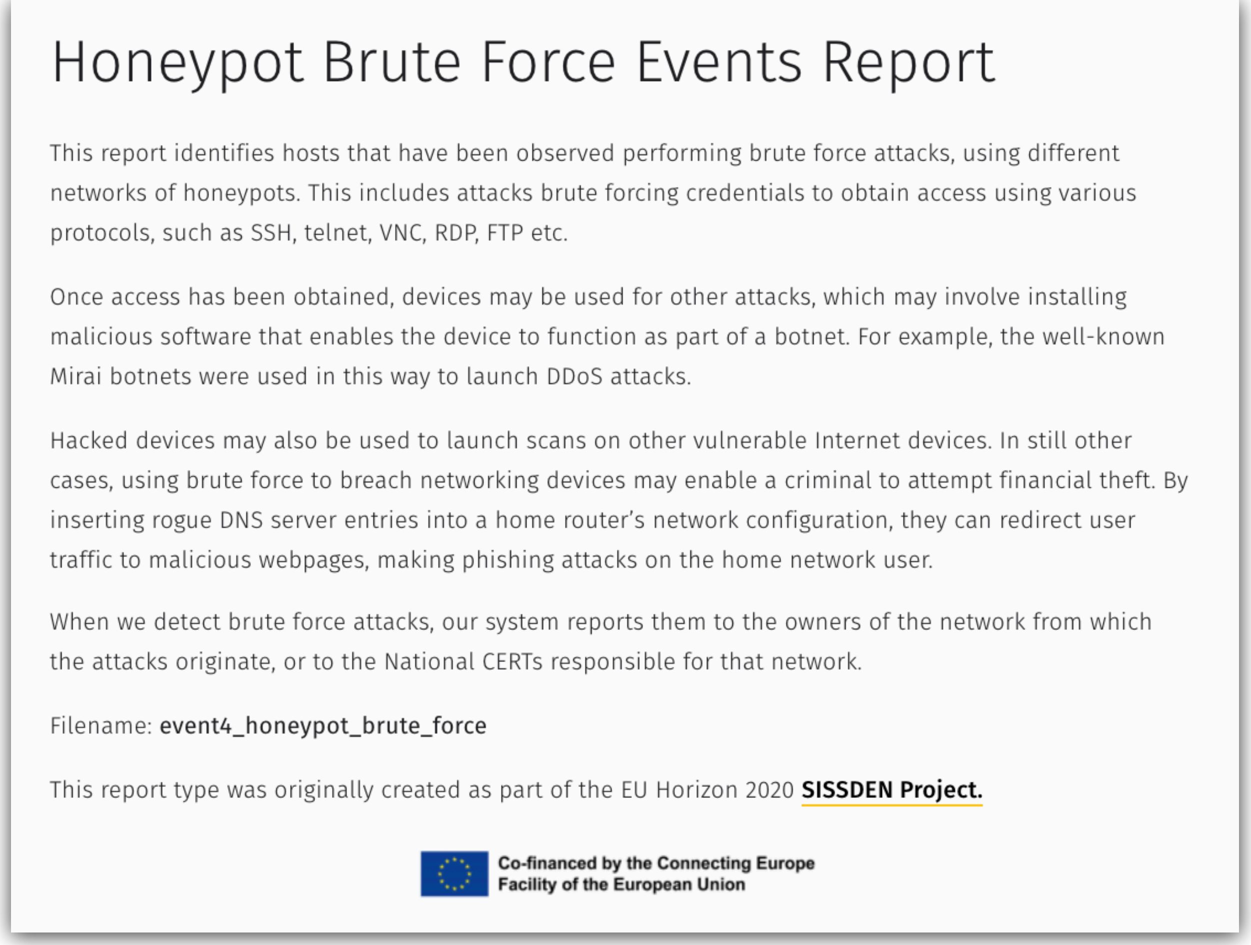
Accessible Hadoop Report

This report identifies hosts that are running Hadoop and have either the NameNode or DataNode web interfaces running and accessible to the world on the Internet. It's a Service Scan, and it's updated every 24 hours.

OPTIONAL: Accessible HTTP Report

This report identifies hosts that have the Hypertext Transfer Protocol (HTTP) running on some port and are accessible on the

Network Report Details (example)



Honeypot Brute Force Events Report

This report identifies hosts that have been observed performing brute force attacks, using different networks of honeypots. This includes attacks brute forcing credentials to obtain access using various protocols, such as SSH, telnet, VNC, RDP, FTP etc.

Once access has been obtained, devices may be 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.

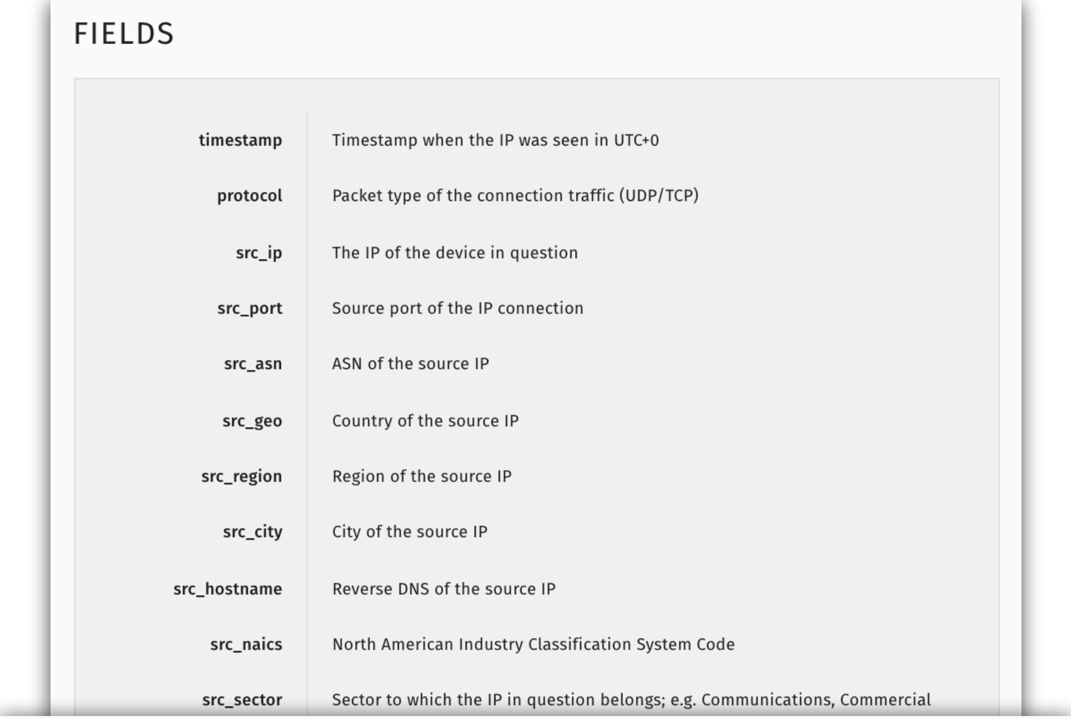
Hacked devices may also be used to launch scans on other vulnerable Internet devices. In still other cases, using brute force to breach networking devices may enable a criminal to attempt financial theft. By inserting rogue DNS server entries into a home router's network configuration, they can redirect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

Filename: **event4_honeypot_brute_force**

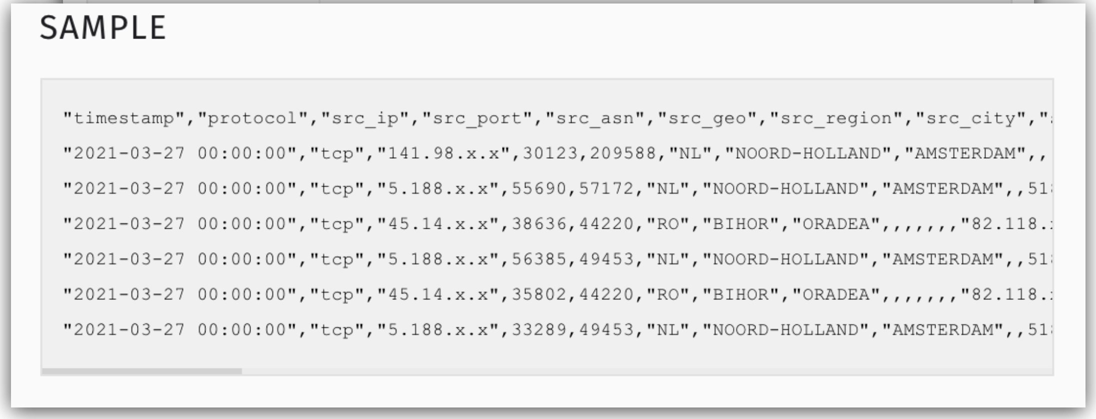
This report type was originally created as part of the EU Horizon 2020 **SISSDEN Project.**

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



FIELDS

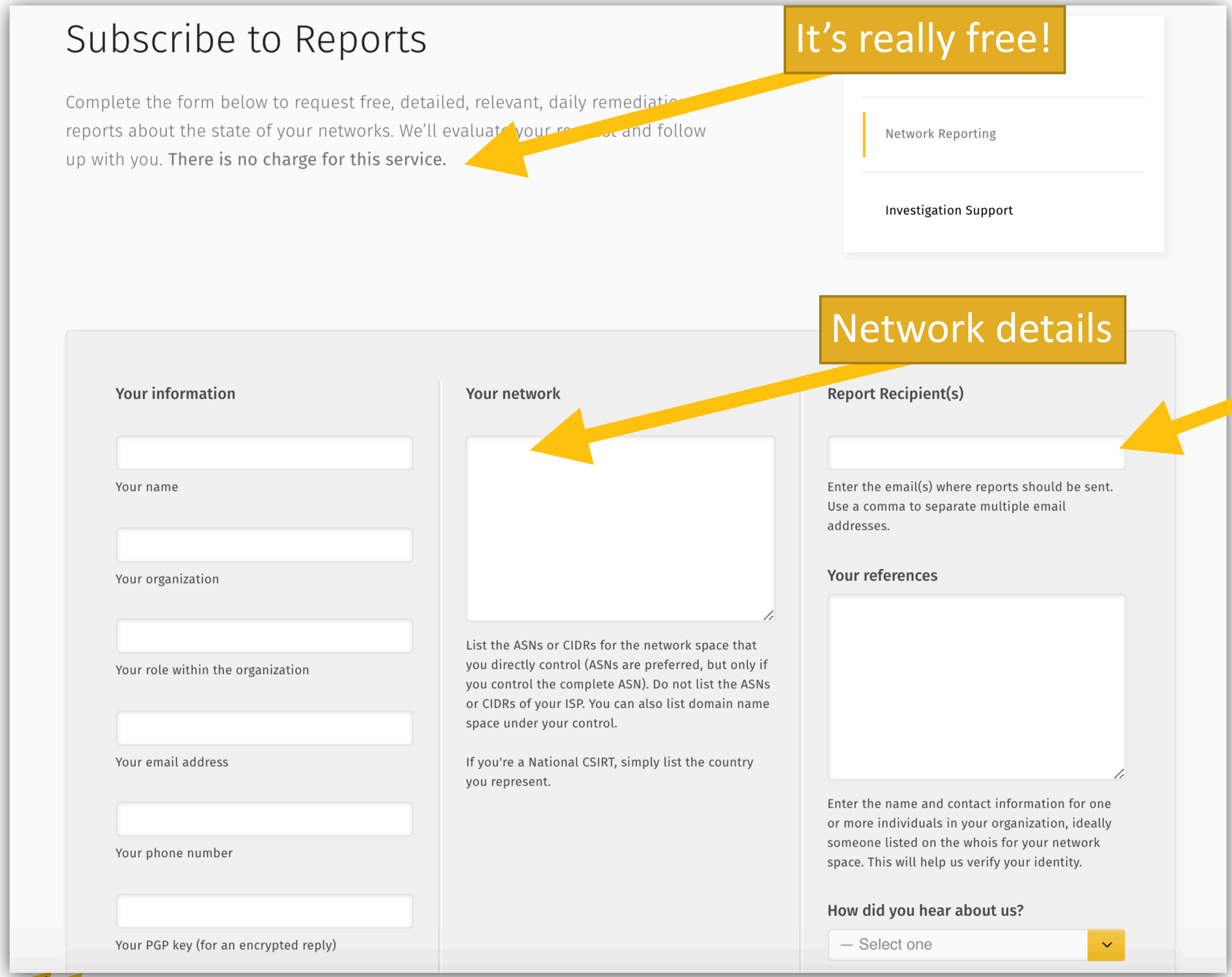
timestamp	Timestamp when the IP was seen in UTC+0
protocol	Packet type of the connection traffic (UDP/TCP)
src_ip	The IP of the device in question
src_port	Source port of the IP connection
src_asn	ASN of the source IP
src_geo	Country of the source IP
src_region	Region of the source IP
src_city	City of the source IP
src_hostname	Reverse DNS of the source IP
src_naics	North American Industry Classification System Code
src_sector	Sector to which the IP in question belongs; e.g. Communications, Commercial



SAMPLE

```
"timestamp","protocol","src_ip","src_port","src_asn","src_geo","src_region","src_city","
"2021-03-27 00:00:00","tcp","141.98.x.x",30123,209588,"NL","NOORD-HOLLAND","AMSTERDAM",,
"2021-03-27 00:00:00","tcp","5.188.x.x",55690,57172,"NL","NOORD-HOLLAND","AMSTERDAM",,51
"2021-03-27 00:00:00","tcp","45.14.x.x",38636,44220,"RO","BIHOR","ORADEA",,,,,,"82.118.
"2021-03-27 00:00:00","tcp","5.188.x.x",56385,49453,"NL","NOORD-HOLLAND","AMSTERDAM",,51
"2021-03-27 00:00:00","tcp","45.14.x.x",35802,44220,"RO","BIHOR","ORADEA",,,,,,"82.118.
"2021-03-27 00:00:00","tcp","5.188.x.x",33289,49453,"NL","NOORD-HOLLAND","AMSTERDAM",,51
```

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.**

Your information

Your name

Your organization

Your role within the organization

Your email address

Your phone number

Your PGP key (for an encrypted reply)

Your network

List the ASNs or CIDRs for the network space that you 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.

Report Recipient(s)

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

Your references

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

How did you hear about us?

— Select one

It's really free!

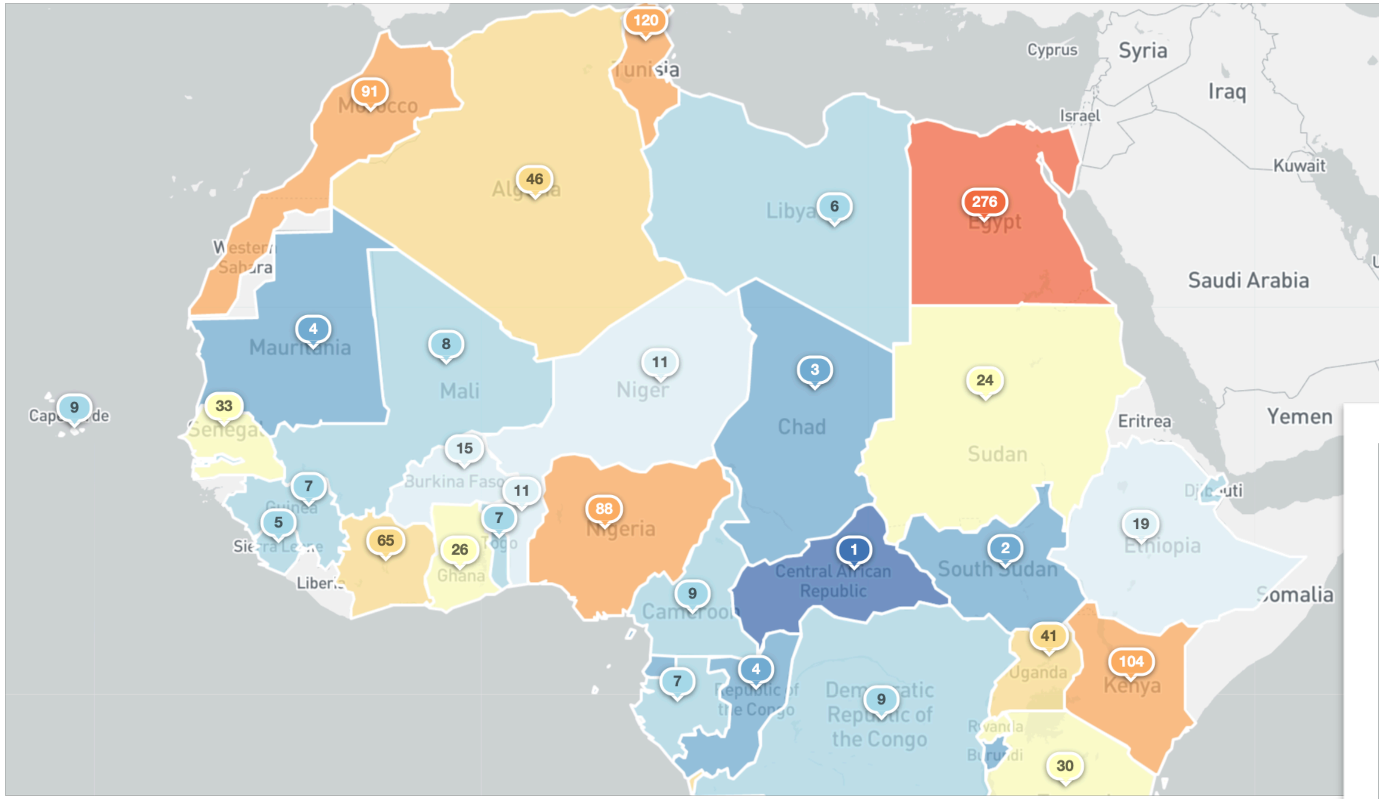
Network details

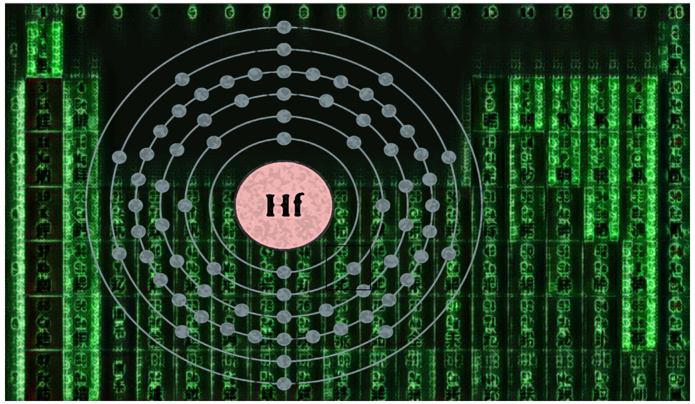
E-mail address where reports or download links will be sent

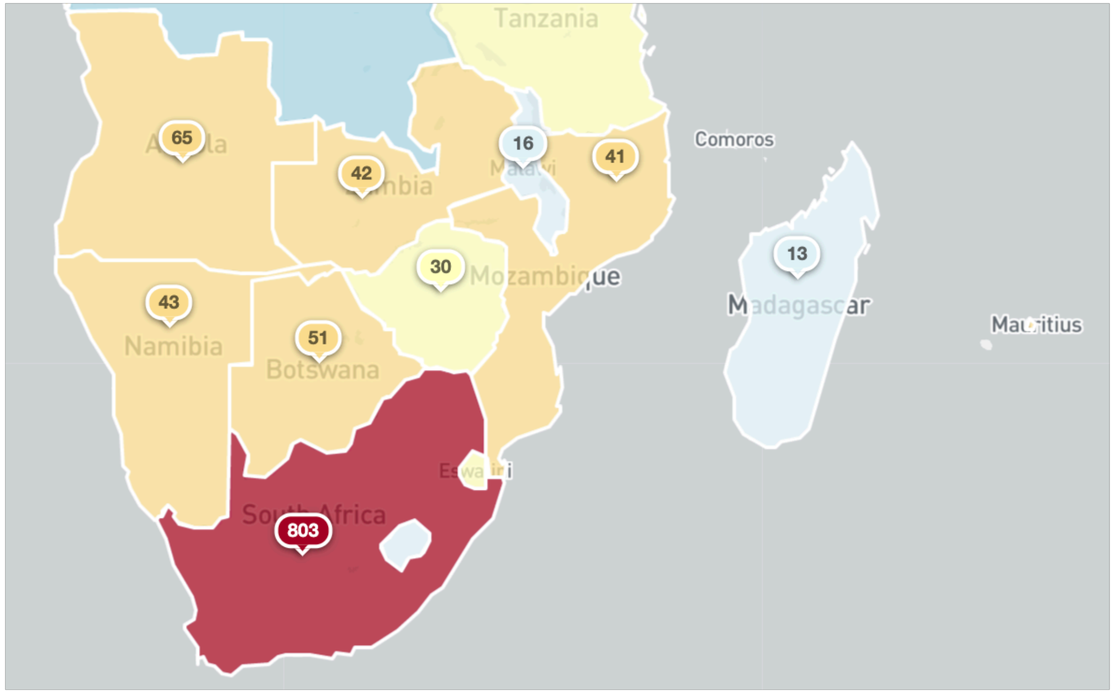
ASK FOR OPTIONAL REPORTS TOO!

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

Vulnerable Exchange Servers - 2021-03-14



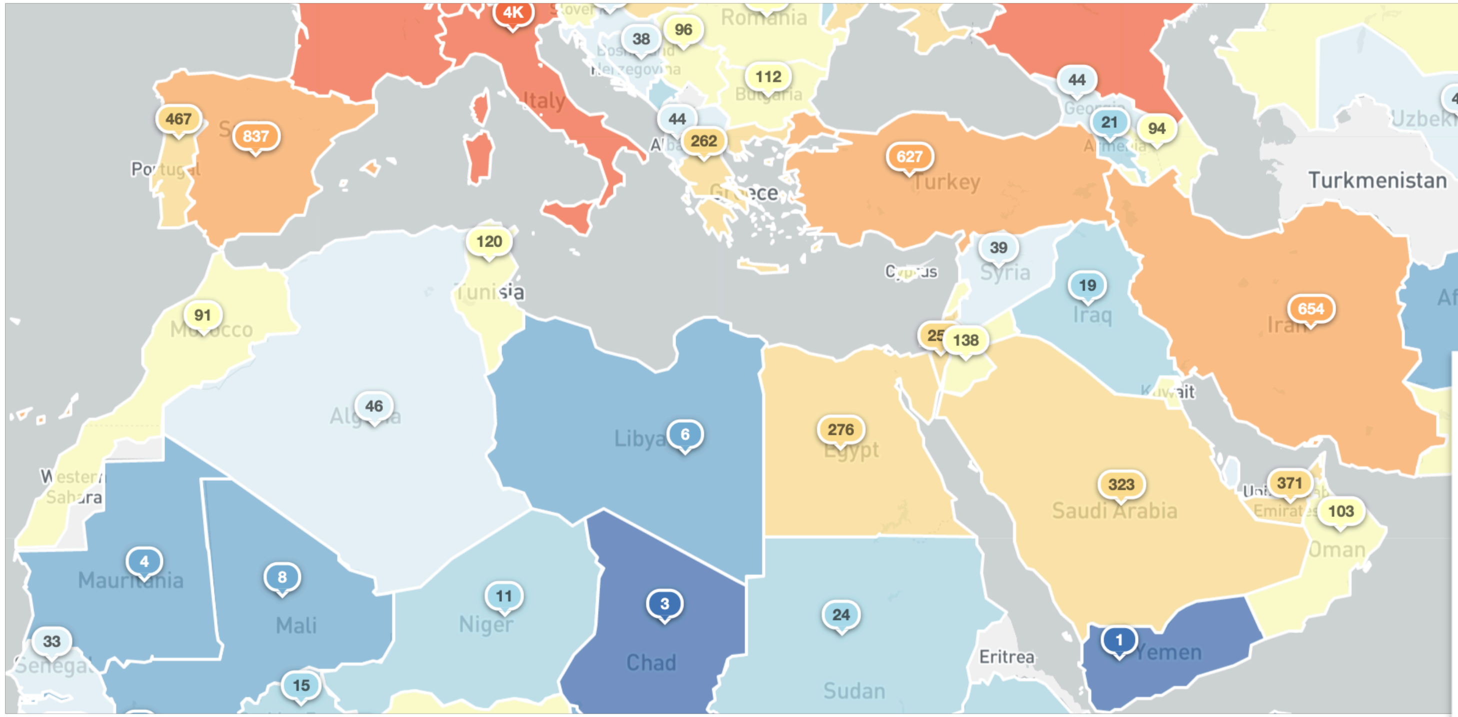


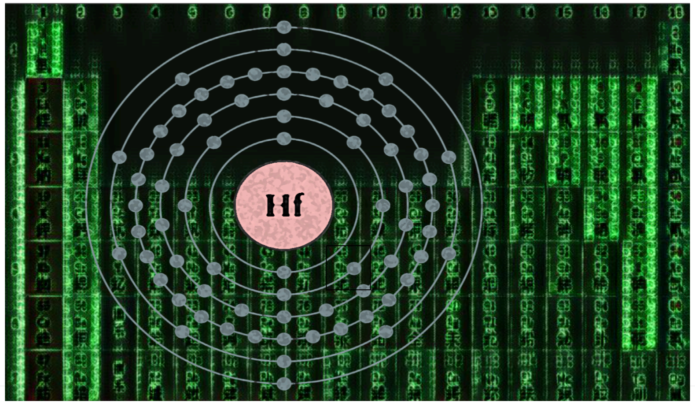


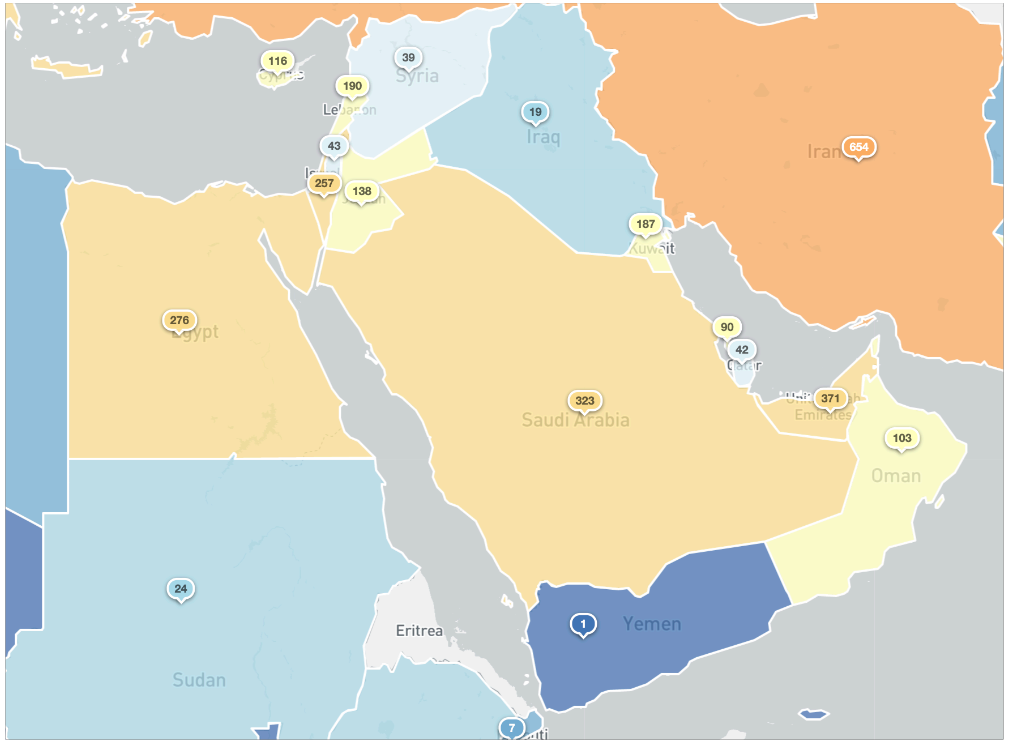
https://www.shadowserver.org/news/shadowserver-special-report-exchange-scanning-5/

SHADOWSERVER

Vulnerable Exchange Servers - 2021-03-14







https://www.shadowserver.org/news/shadowserver-special-report-exchange-scanning-5/

SHADOWSERVER

Tools for Automated Processing of Feeds

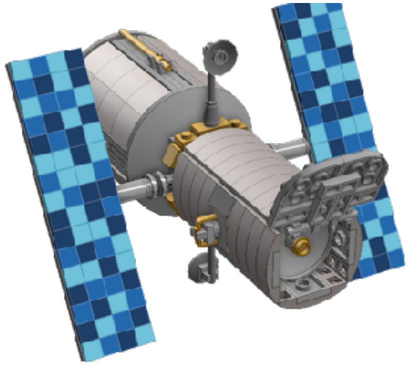
- Open source:
  - IntelMQ: https://github.com/certtools/intelmq
  - n6: https://github.com/CERT-Polska/n6
  - AbuseIO: https://abuse.io/
  - Megatron: https://github.com/cert-se/megatron-java
  - Collective Intelligence Framework: https://csirtgadgets.com/collective-intelligence-framework
- Commercial tools also exist!

Honeypot Sensor Networks

Not just IoT threats

Large Scale Sensor Networks - HaaS

- Existing open source honeypots & new honeypots developed by CSIRTs/ researchers and deployed under Honeypots-as-a-Service framework (**HaaS**), data fed to CSIRTs
- No need to maintain honeypot network by yourself
- Dynamic reconfiguration of honeypot personalities for more relevant attack data collection [future]
- "Observatory of IoT attacks for CSIRTs"
- Tighter integration with CSIRT/TI capabilities
    - MISP, The Hive/Cortex, etc [future]
    - Verification of IoC based sightings [future]



SHADOWSERVER

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

NASK

HaaS - Community Pool of Honeypots

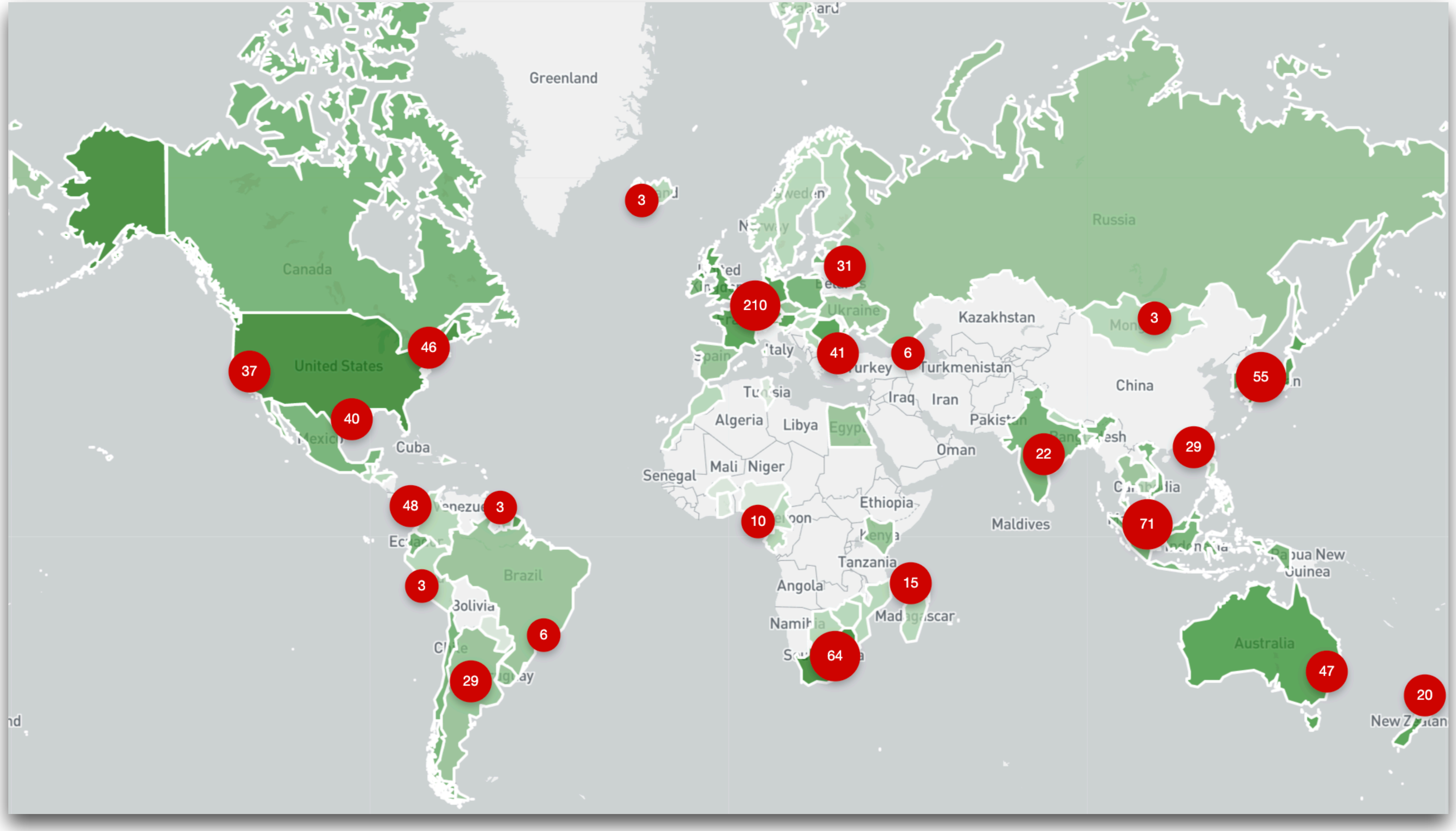
- 7 types of default honeypots that can be deployed
  - Agnus - Shadowserver proprietary honeypot, Web/IoT attacks
  - Cowrie - Open source, telnet/ssh honeypot
  - Conpot - Open source, ICS honeypot
  - Dionaea - Open source, multi-service honeypot
  - Glastopf - Open source, web-honeypot
  - Heralding - Open source, multi-service credential catching honeypot
  - Spampot - Shadowserver proprietary honeypot, spam catching honeypot

SHADOWSERVER

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

VARIOT

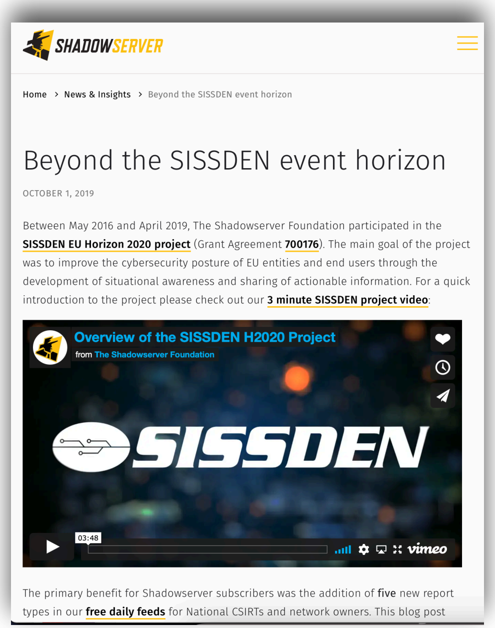
HaaS - Current honeypot distribution - 2021-12-01



HaaS/Africa - Current honeypot distribution - 2021-12-01

Foreign, Commonwealth
& Development Office

https://www.shadowserver.org/news/uk-foreign-commonwealth-development-office-funds-shadowserver-surge-in-africa-and-indo-pacific-regions/



SHADOWSERVER

Home › News & Insights › Beyond the SISSDEN event horizon

Beyond the SISSDEN event horizon

OCTOBER 1, 2019

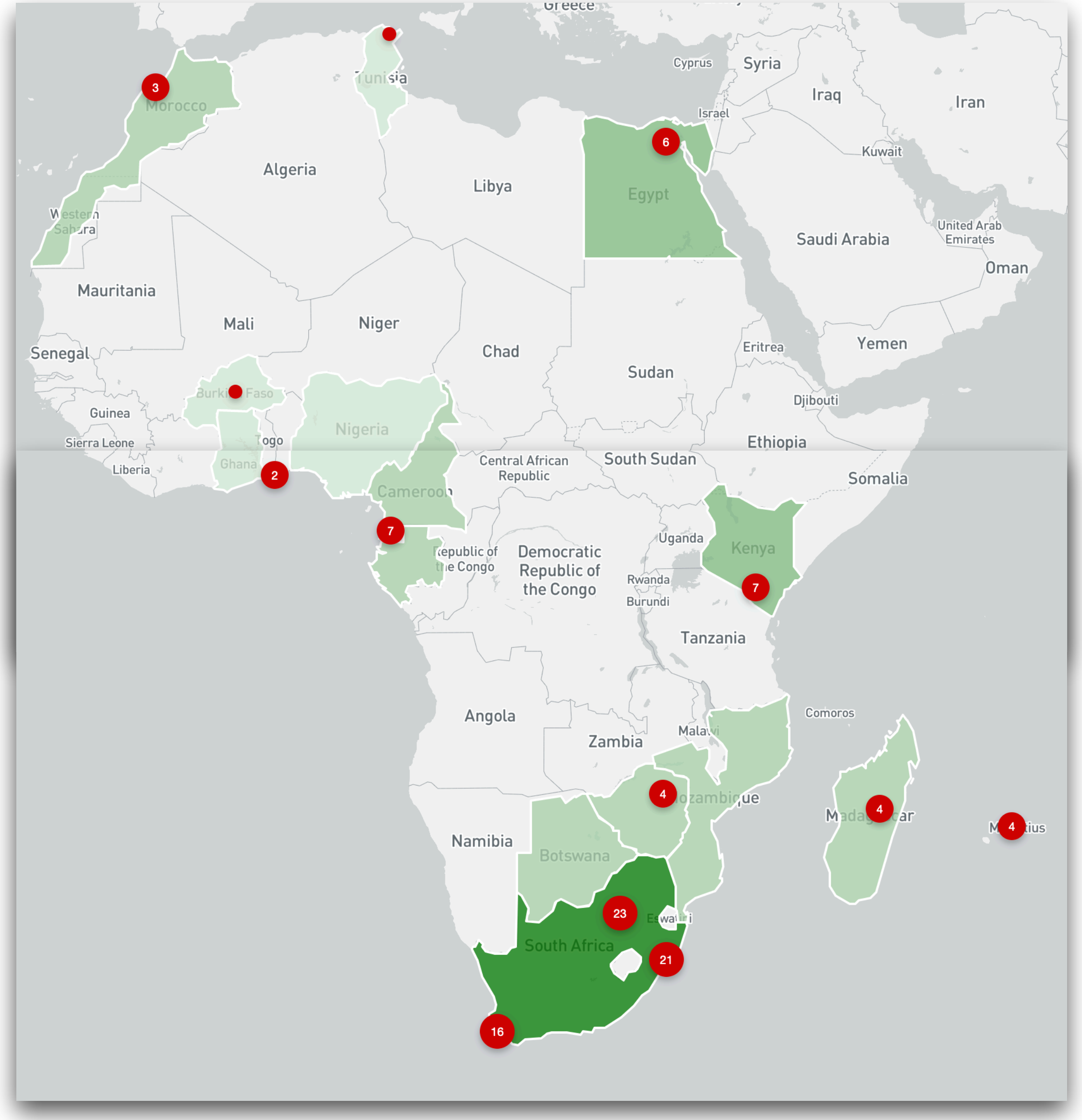
Between May 2016 and April 2019, The Shadowserver Foundation participated in the **SISSDEN EU Horizon 2020 project** (Grant Agreement **700176**). The main goal of the project was to improve the cybersecurity posture of EU entities and end users through the development of situational awareness and sharing of actionable information. For a quick introduction to the project please check out our **3 minute SISSDEN project video**:

Overview of the SISSDEN H2020 Project
from The Shadowserver Foundation
SISSDEN
03:48
vimeo

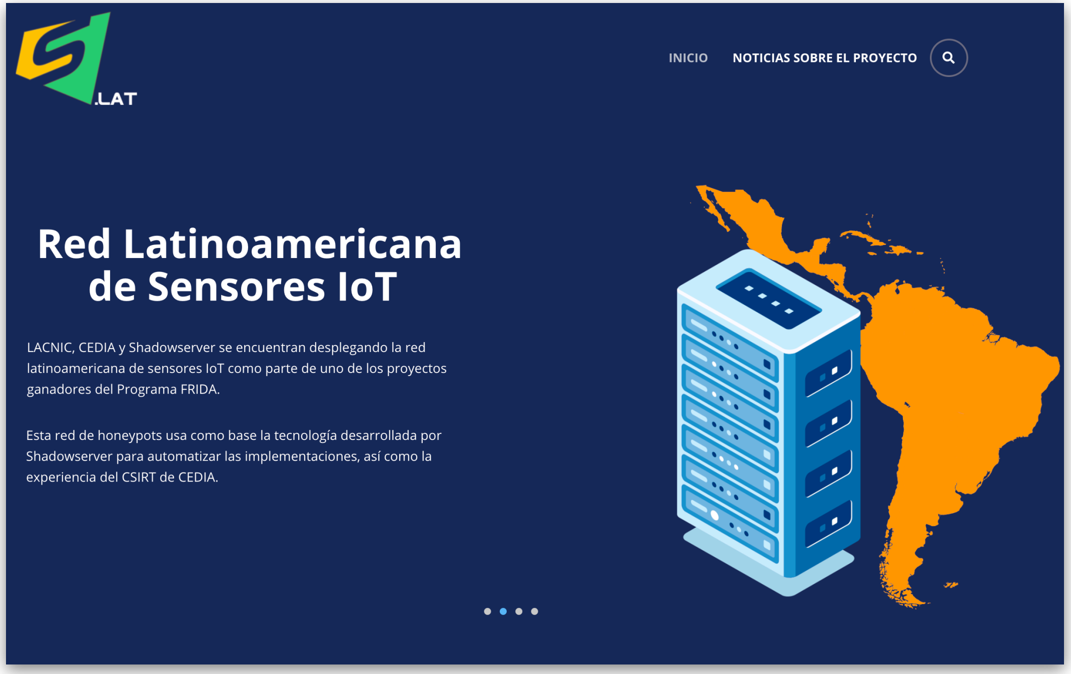
The primary benefit for Shadowserver subscribers was the addition of **five** new report types in our **free daily feeds** for National CSIRTs and network owners. This blog post

https://www.shadowserver.org/news/beyond-the-sissden-event-horizon/

SHADOWSERVER



Example collaboration: LACNIC CEDIA Shadowserver FRIDA IoT Honeypot Project



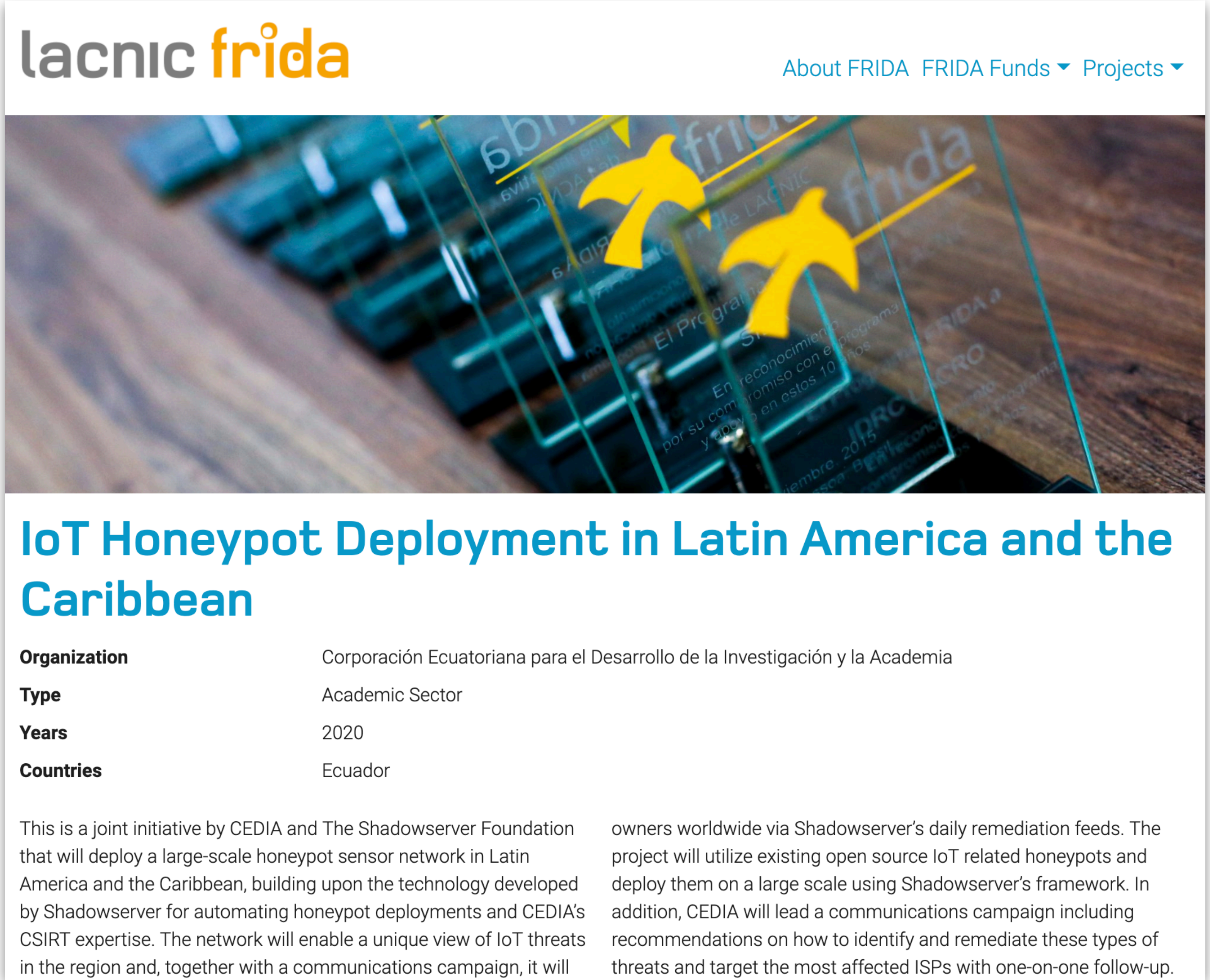
Red Latinoamericana de Sensores IoT

LACNIC, CEDIA y Shadowserver se encuentran desplegando la red latinoamericana de sensores IoT como parte de uno de los proyectos ganadores del Programa FRIDA.

Esta red de honeypots usa como base la tecnología desarrollada por Shadowserver para automatizar las implementaciones, así como la experiencia del CSIRT de CEDIA.

https://sensores.lat/

https://programafrida.net/en/archivos/project/iot-honeypot



IoT Honeypot Deployment in Latin America and the Caribbean

Organization	Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia
Type	Academic Sector
Years	2020
Countries	Ecuador

This is a joint initiative by CEDIA and The Shadowserver Foundation that will deploy a large-scale honeypot sensor network in Latin America and the Caribbean, building upon the technology developed by Shadowserver for automating honeypot deployments and CEDIA's CSIRT expertise. The network will enable a unique view of IoT threats in the region and, together with a communications campaign, it will owners worldwide via Shadowserver's daily remediation feeds. The project will utilize existing open source IoT related honeypots and deploy them on a large scale using Shadowserver's framework. In addition, CEDIA will lead a communications campaign including recommendations on how to identify and remediate these types of threats and target the most affected ISPs with one-on-one follow-up.

HaaS Sensor Specification

- VM Sensor node spec
  - Ubuntu 20.04 LTS
  - 1 GB RAM
  - 20 GB disk
  - At least 2 (preferably 4) publicly routable IPv4 (single NIC, no NAT, no network filtering)
  - 1 Mbit/s uplink

https://www.shadowserver.org/news/beyond-the-sissden-event-horizon

Focused Efforts in Africa: Collaboration!

- Training at Africa Internet Summit in Nairobi in 2017 for National CSIRTs
- Completed Q2 2021 FCDO project to expand Shadowserver recipient footprint, build up honeypot sensor networks in Africa & Indo-Pacific,
  - https://www.shadowserver.org/news/uk-foreign-commonwealth-development-office-funds-shadowserver-surge-in-africa-and-indo-pacific-regions/
- Started new FCDO Project in Q4 2021 to follow up on the above. We are therefore looking for:
  - More National CSIRTs & network owners (orgs) in Africa to sign-up to our free services
  - Orgs in Africa supplying VMs or physical machines for our honeypot sensors
- Will be focusing in 2022 on making it easier to benefit from our free services

SHADOWSERVER

Shadowserver in Africa - URLs

- April 2020 Africa blog

  https://www.shadowserver.org/news/the-shadowserver-foundation-threat-report-a-spotlight-on-africa/

- March 2021 FCDO funded project blog

  https://www.shadowserver.org/news/uk-foreign-commonwealth-development-office-funds-shadowserver-surge-in-africa-and-indo-pacific-regions/

- New Q4 2021 / Q1 2022 FCDO funded project (published Dec 1st):

  https://www.shadowserver.org/news/continuing-our-africa-and-indo-pacific-regional-outreach

- New 2021 Africa blog (being published soon):

  https://www.shadowserver.org/news/the-shadowserver-foundation-threat-report-a-spotlight-on-africa-2021

Foreign, Commonwealth
& Development Office

A Quick Win for New CSIRTs

- Ingesting and sharing Shadowserver (and other) feeds is a **quick win** in building up a new CSIRT
- Does not require significant investment in resources - maximize your limited budgets, take advantage of **free data** and **open source tools**
- Enables situational awareness = understanding of what is happening in your constituency (or network)
- Elevates the status of your CSIRT as it demonstrates you offer actionable information, even at early stages of cyber security journey
- Enables you to establish trust with your constituency and build new connections - you have valuable information to help defend them

SHADOWSERVER

Lighting the way to a more secure Internet

@shadowserver, @piotrkijewski

contact@shadowserver.org, piotr@shadowserver.org

SHADOWSERVER.ORG