SHADOWSERVER

Lighting the way to a more secure Internet

Securing Your Network Using Shadowserver Reports

@shadowserver

bgreene@shadowserver.org / david@shadowserver.org

SHADOWSERVER.ORG

What do the Bad Guys See?

Who is Scanning your Network?

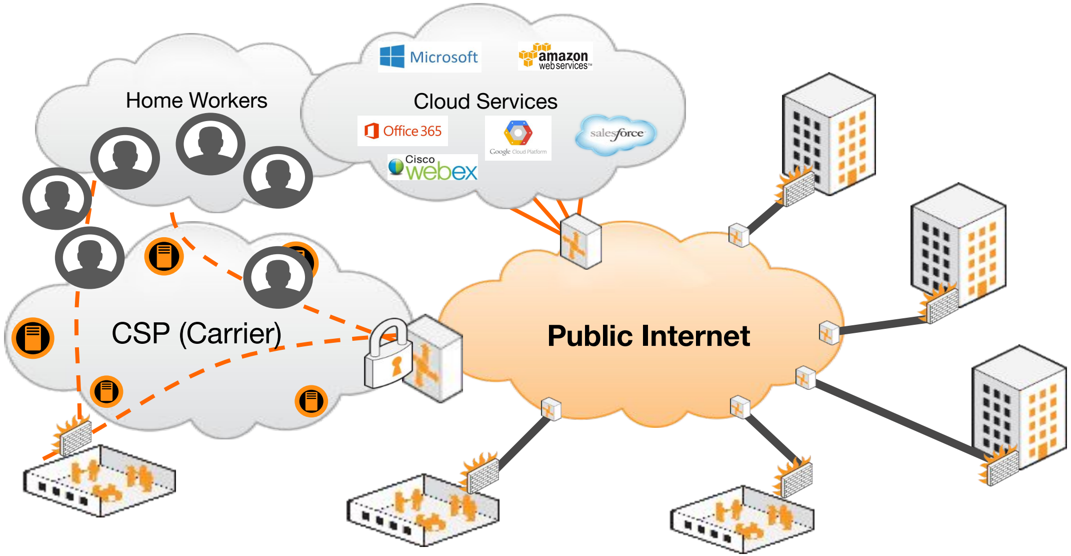
Reality of Today’s Risk!

- Miscreants are scanning your network. Assume they know your exposed risk.
- Miscreants have a list of vulnerabile systems on your network.
- Organizations are scanning your network, gaining intelligence on your organization’s risk.

The Miscreant’s Network Visibility

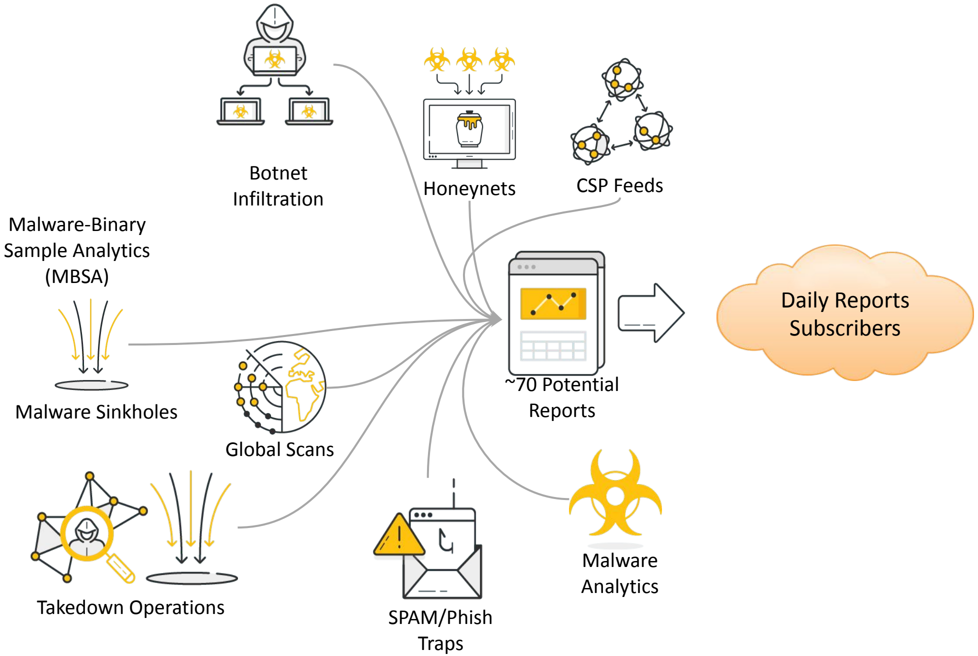
What can others see when looking into your network from the outside?

What is your organization’s risk?



SHADOWSERVER

Would it be nice ....



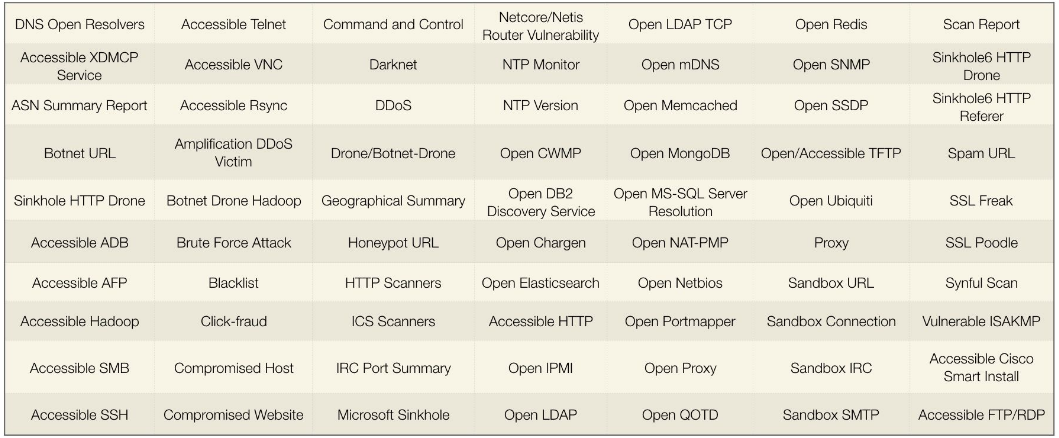
SHADOWSERVER

Public Service Reporting

Free Daily Remediation Reports - National CSIRTs and Network Owners

Network Reporting

Every day, Shadowserver sends custom remediation reports to more than 4600 vetted subscribers, including over 100 national governments and many Fortune 500 companies. These reports are detailed, targeted, relevant and free.



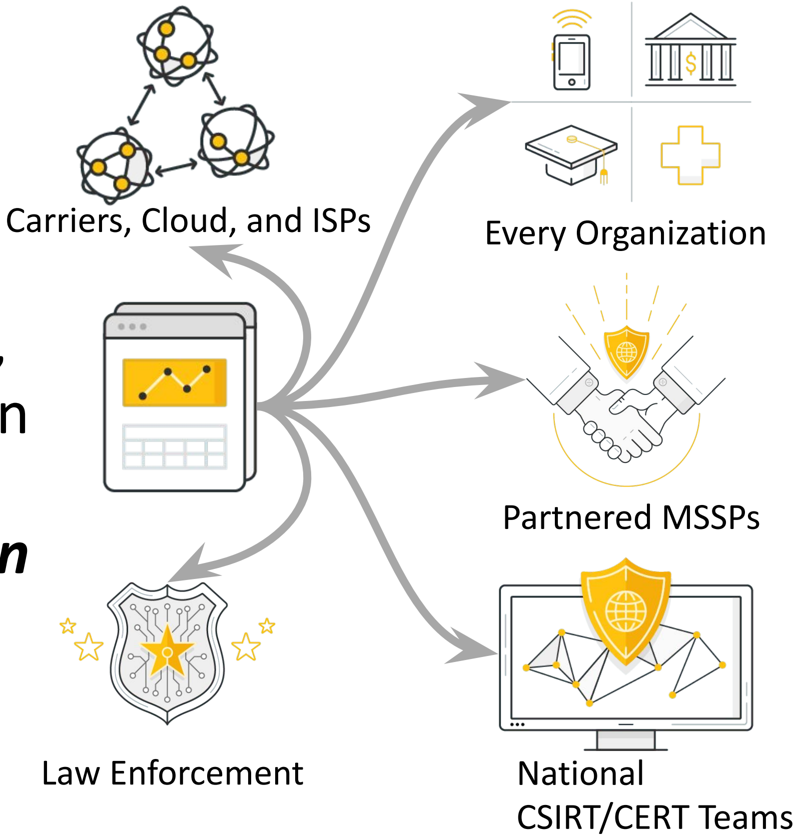
DNS Open Resolvers	Accessible Telnet	Command and Control	Netcore/Netis Router Vulnerability	Open LDAP TCP	Open Redis	Scan Report
Accessible XDMCP Service	Accessible VNC	Darknet	NTP Monitor	Open mDNS	Open SNMP	Sinkhole6 HTTP Drone
ASN Summary Report	Accessible Rsync	DDoS	NTP Version	Open Memcached	Open 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.

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

What Goes Into the Daily Network Reports?

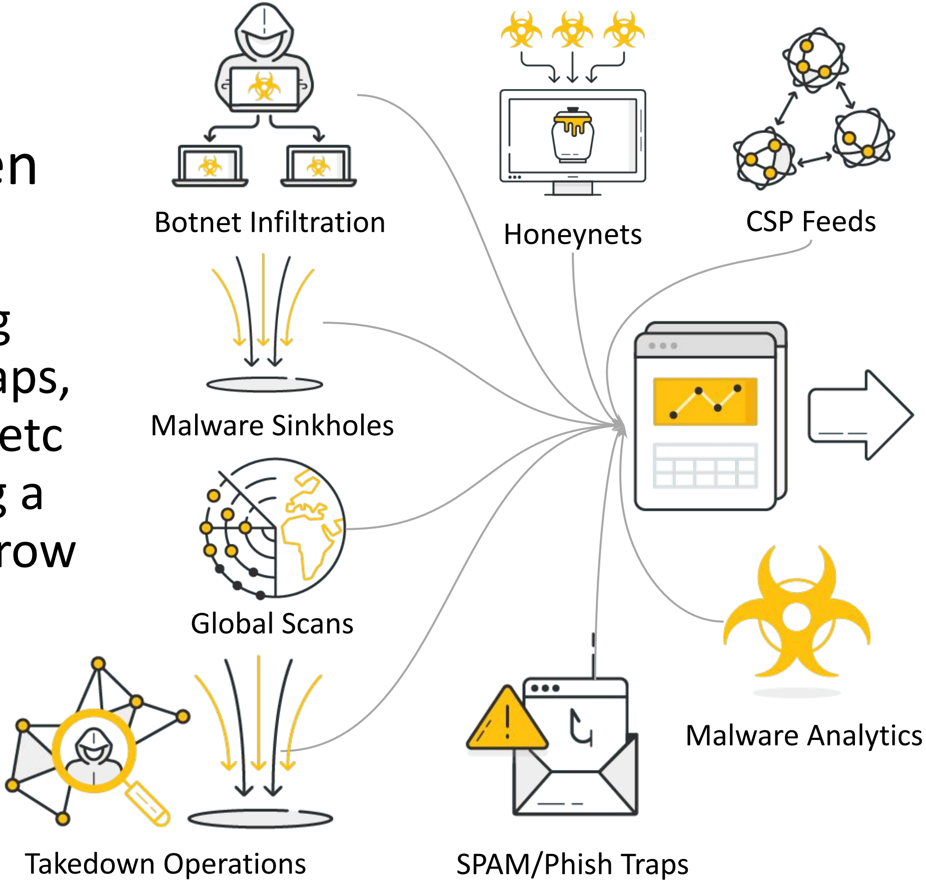
- Every day, Shadowserver sends free network reports to 4600+ organizations globally
- These emailed reports provide details of who is infected, violated, controlled and out of compliance in each organization
- ***If Shadowserver sees a problem on your network, then all Miscreants can exploit that problem***



What Goes Into the Daily Network Reports?

Scanning each network from the "outside-in" is a small part of a proven **Public Benefit Service:**

- 15 years of **Trust** that includes operating malware sinkholes, honeynets, spam traps, domain confiscation, malware analysis, etc
- **Industry Unique Perspective** - providing a wide range of Network Reports which grow and evolve with each new investigation, botnet take down and cybercrime disruption action

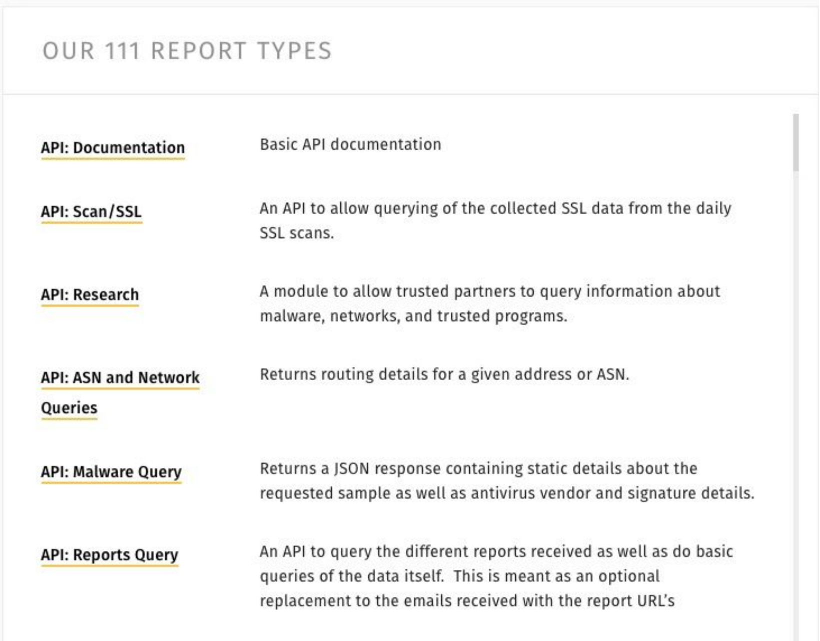


SHADOWSERVER

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 111 network report types and growing!

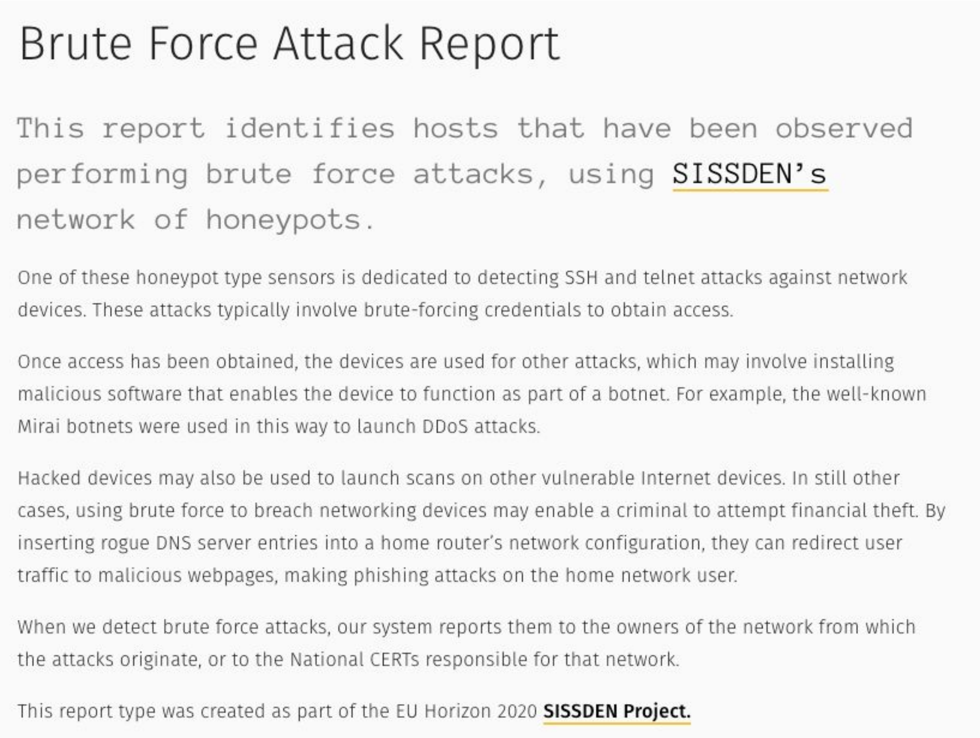


OUR 111 REPORT TYPES

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

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

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.

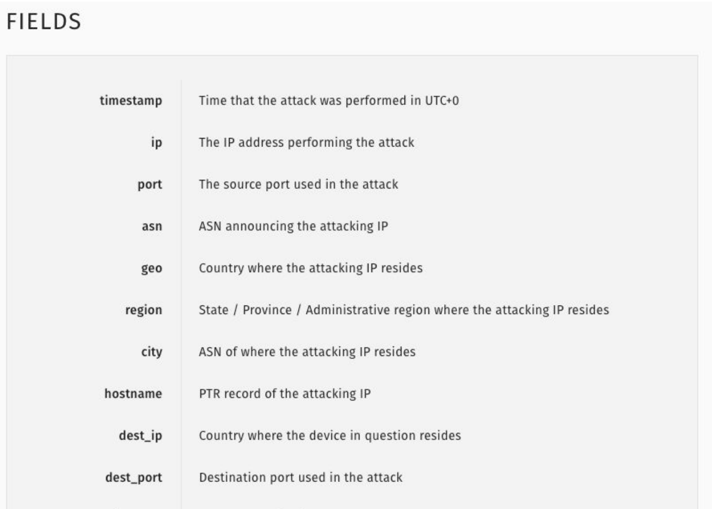
One of these honeypot type sensors is dedicated to detecting SSH and telnet attacks against network devices. These attacks typically involve brute-forcing credentials to obtain access.

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.

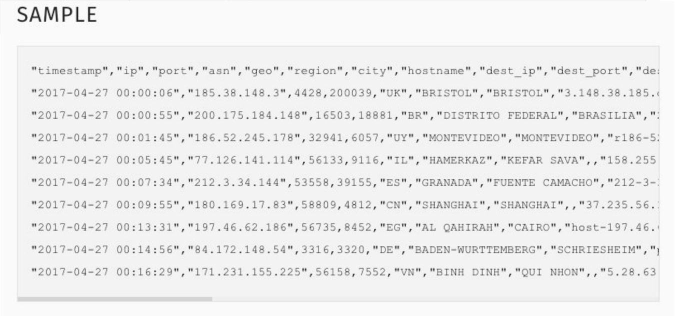
When we detect brute force attacks, our system reports them to the owners of the network from which the attacks originate, or to the National CERTs responsible for that network.

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

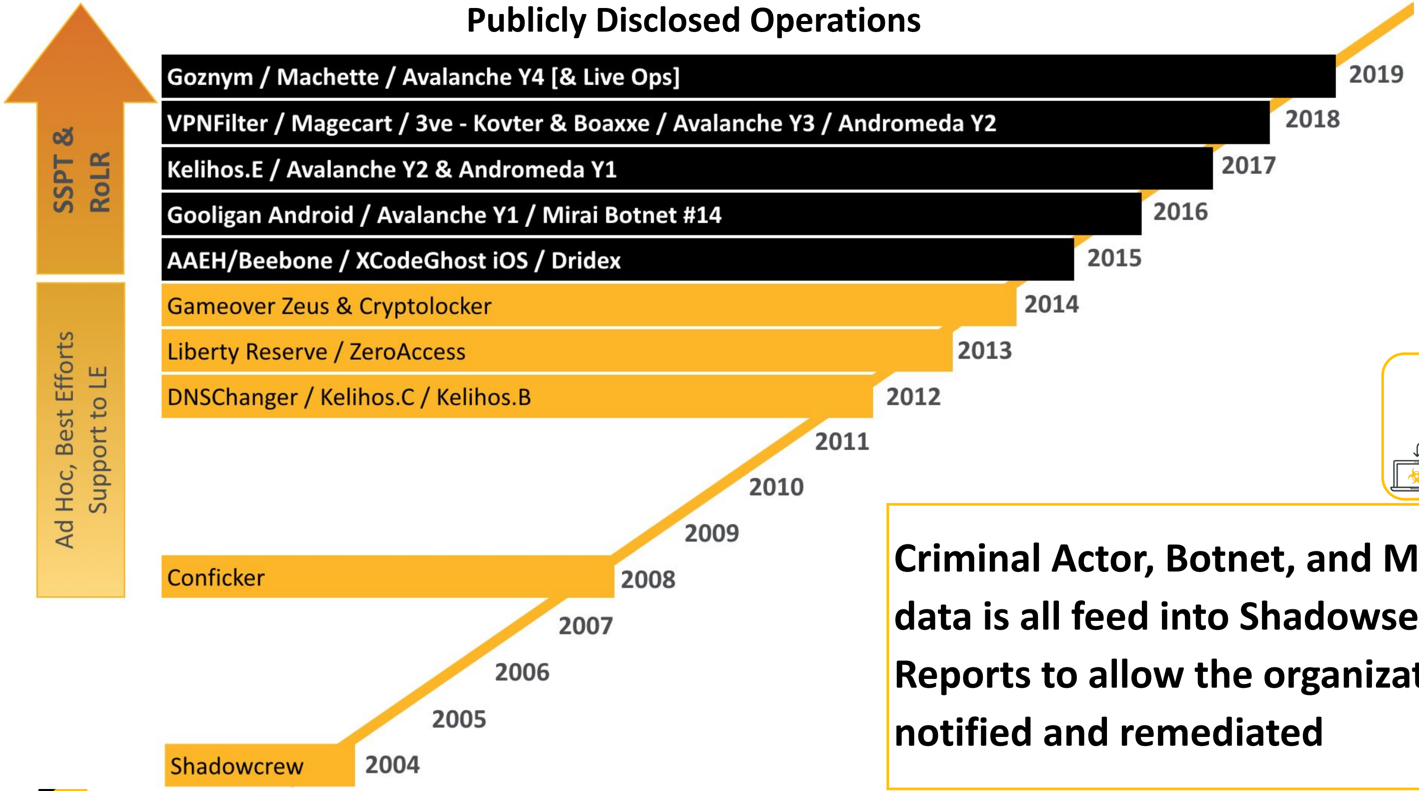


SAMPLE

```
"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

Botnet & Criminal Actor Takedown Operations



Publicly Disclosed Operations

SSPT & RoLR
Ad Hoc, Best Efforts Support to LE
Goznym / Machette / Avalanche Y4 [& Live Ops]
2019
VPNFilter / Magecart / 3ve - Kovter & Boaxxe / Avalanche Y3 / Andromeda Y2
2018
Kelihos.E / Avalanche Y2 & Andromeda Y1
2017
Gooligan Android / Avalanche Y1 / Mirai Botnet #14
2016
AAEH/Beebone / XCodeGhost iOS / Dridex
2015
Gameover Zeus & Cryptolocker
2014
Liberty Reserve / ZeroAccess
2013
DNSChanger / Kelihos.C / Kelihos.B
2012
2011
2010
2009
Conficker
2008
2007
2006
2005
Shadowcrew
2004

Criminal Actor, Botnet, and Malware Takedown data is all feed into Shadowserver's Daily Network Reports to allow the organizations and victims to be notified and remediated

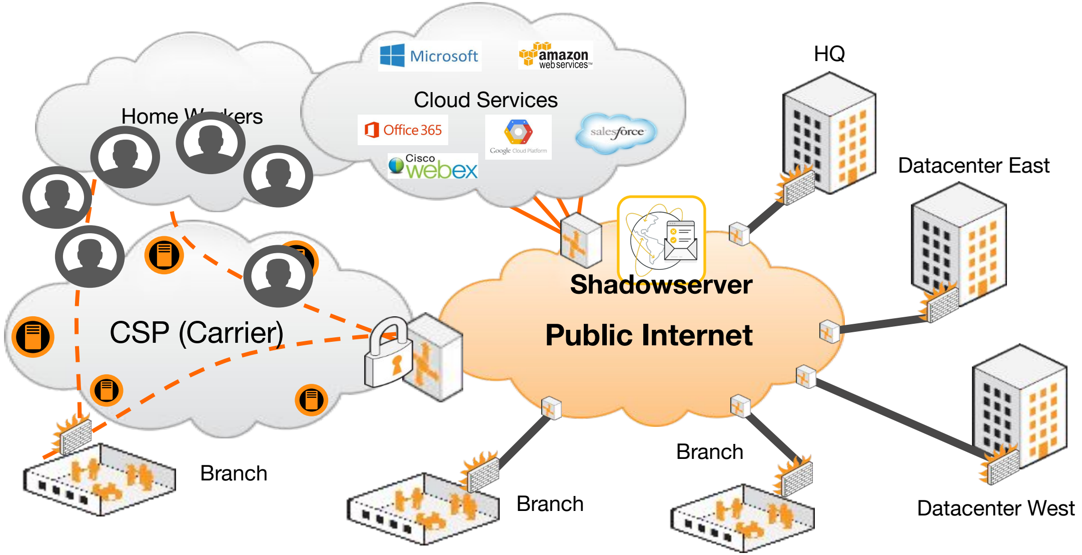
The Miscreant’s Network Visibility

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

What is your organization’s risk?

Shadowserver’s daily Network Reporting is tuned by:

- ASNs for the organization
- CIDR Blocks
- Delegated IP Blocks (Cloud)
- Domains



SHADOWSERVER

How do Get Started?

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

How will Shadowserver Validate Trust?

Shadowserver cannot “grant” people access to the data.

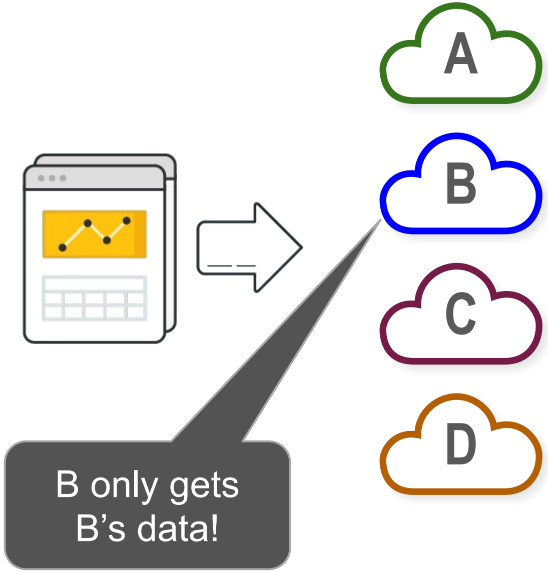
Shadowserver staff will work with you to validate that you have the authority and responsibility over the ASNs, CIDR Blocks (IP addresses), and Domain names.

Sometimes it is best to start small, establish trust, then add to the list of what is reported.

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).



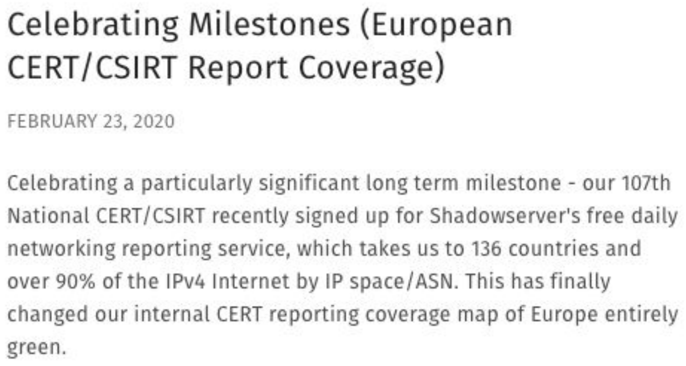
B only gets B’s data!

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

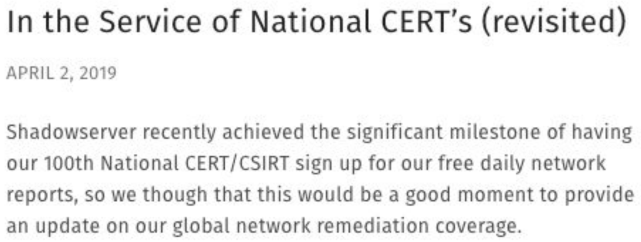
Shadowserver offers National CSIRTs a clear view of what’s happening on their networks, providing personalized support to interpret the data and leverage its impact. Whether you’re responsible for a specific set of networks or every network in your region, together we can make a positive impact on Internet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

Leveraging the Network Reports

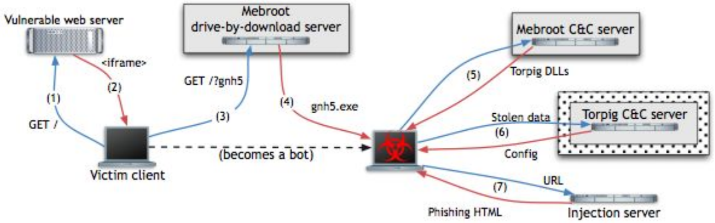
Hardware Vendor’s Network

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!

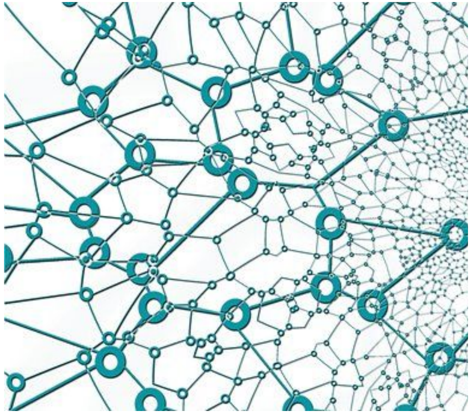
Mobile Telecom Operator Example

How are we going to monitor the security of our network?

Large Carrier in Indonesia sees their security risk, but does not yet have a big security budget.

Subscribes to Shadowserver’s Daily Network Reports. That provides +70 reports of an “outside scan,” malware, botnets, and other vulnerabilities.

Small team uses these reports to track down systems and equipment in the report. One problem, leads to another problem, which leads to several vulnerabilities and security incidents for which the “contracted vendors” neglected to patch.



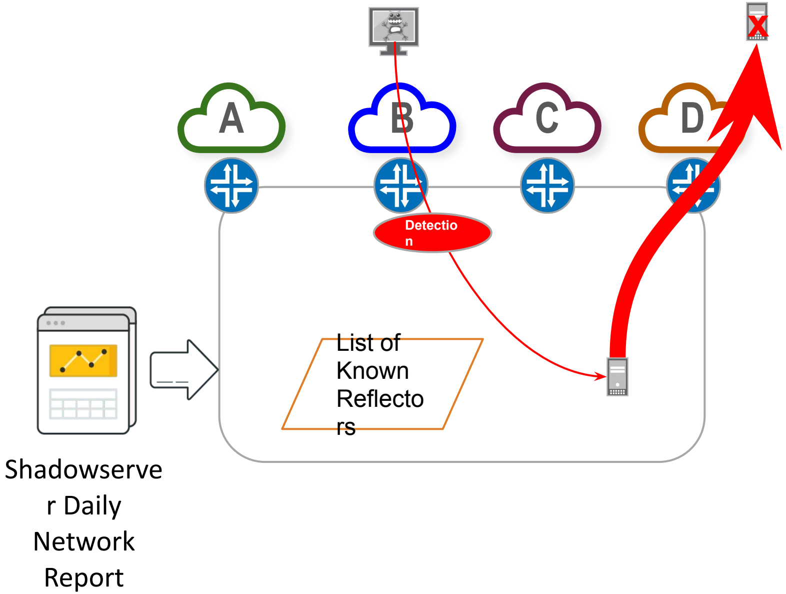
The Daily Network Reports cost effectively kick started the Mobile Operator’s Security Team - translating vast amounts of high-quality security data into actionable insights. These reports cleaned up the network and prevented major loss to the Carrier’s business.

Tracking Spoofed Traffic Into the Network

- Major us Carrier takes the Daily Network Reports specific reflection systems in their ASN
- Using Netflow and known spoofed triggered … compares that list to the Daily Report list.

Now Knows where the Spoofed traffic is originating!

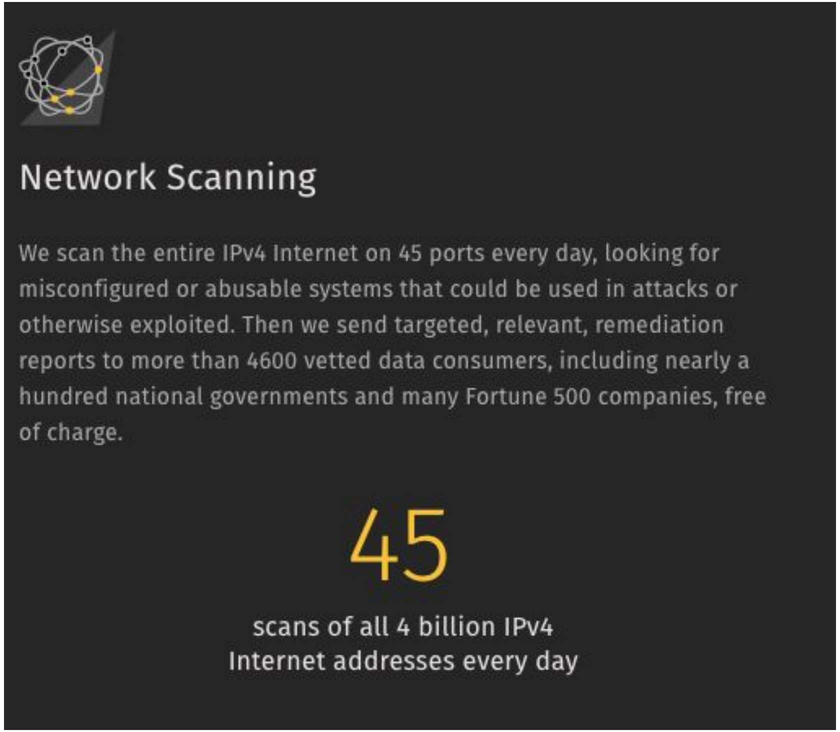
- Flowspec to block.
- Contact Peer to Backtrace



SHADOWSERVER

Shadowser’s Unique Source Data

Shadowserver’s Unique Sources

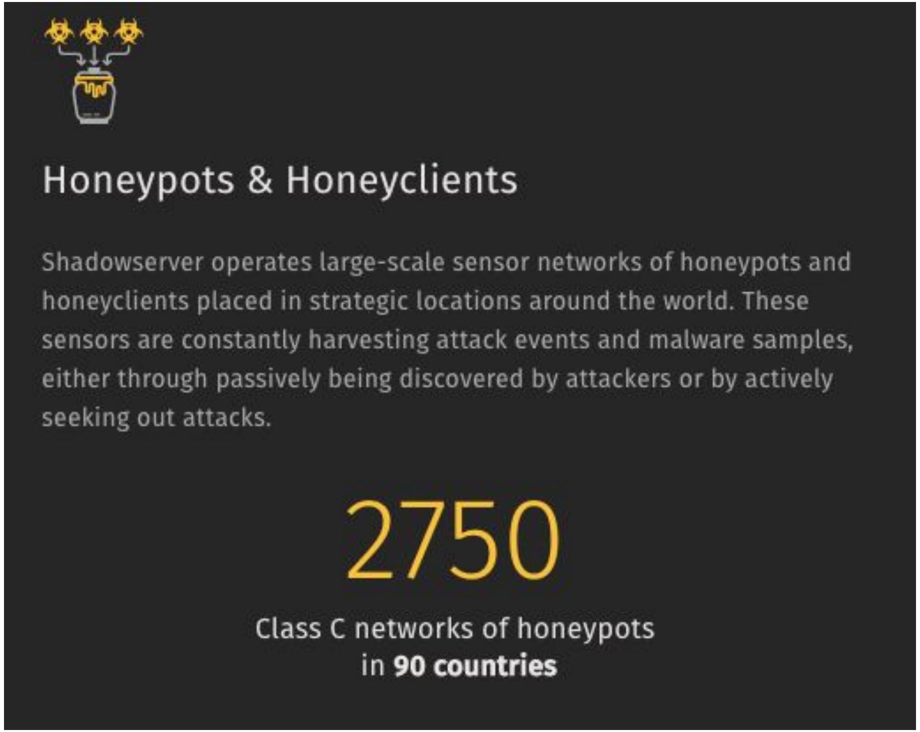


Network Scanning

We scan the entire IPv4 Internet on 45 ports every day, looking for misconfigured or abusable systems that could be used in attacks or otherwise exploited. Then we send targeted, relevant, remediation reports to more than 4600 vetted data consumers, including nearly a hundred national governments and many Fortune 500 companies, free of charge.

45

scans of all 4 billion IPv4
Internet addresses every day



Honeypots & Honeyclients

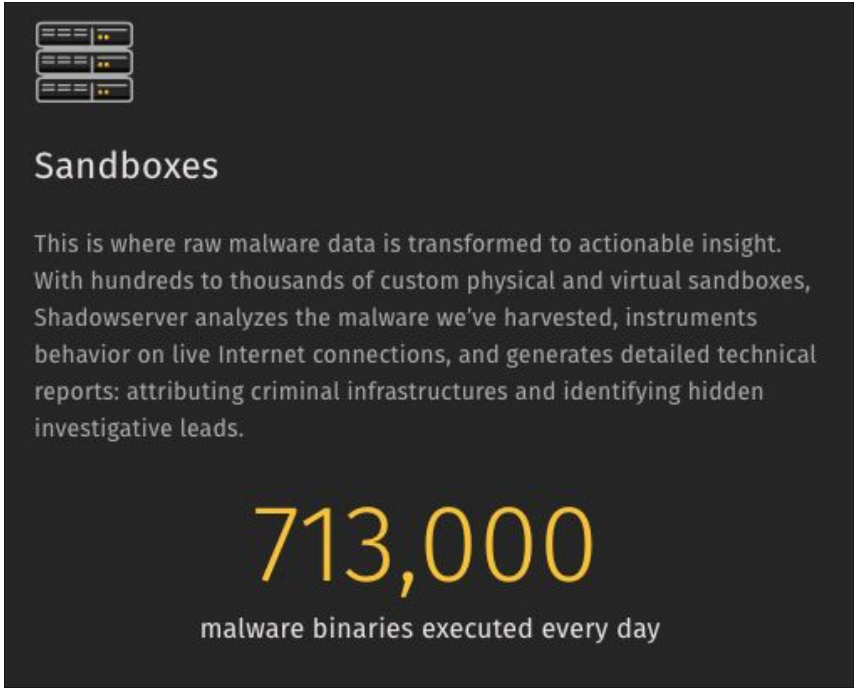
Shadowserver operates large-scale sensor networks of honeypots and honeyclients placed in strategic locations around the world. These sensors are constantly harvesting attack events and malware samples, either through passively being discovered by attackers or by actively seeking out attacks.

2750

Class C networks of honeypots
in **90 countries**

SHADOWSERVER

Shadowserver’s Unique Sources

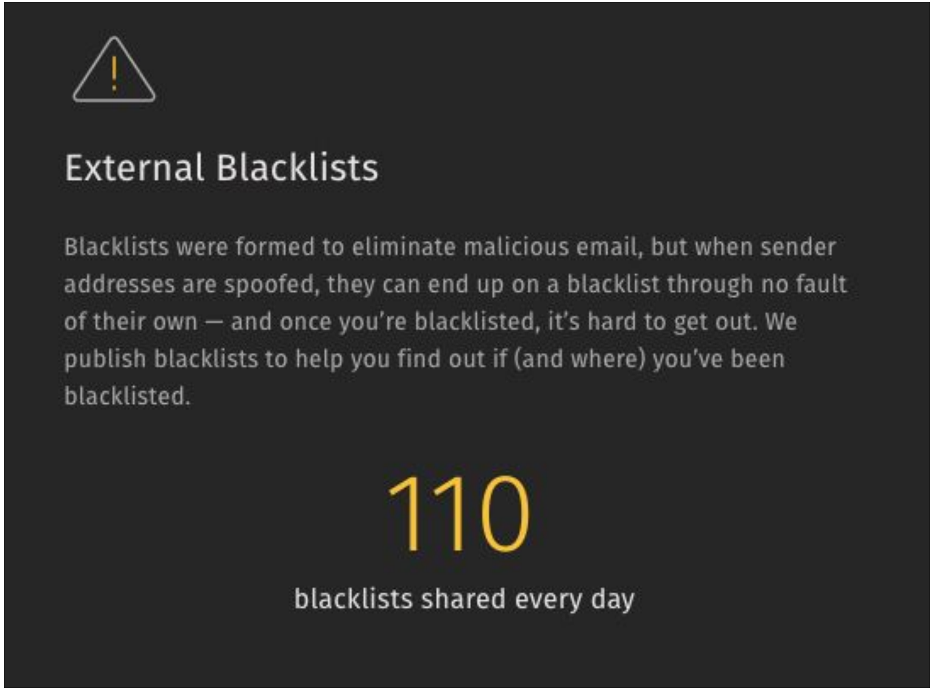


Sandboxes

This is where raw malware data is transformed to actionable insight. With hundreds to thousands of custom physical and virtual sandboxes, Shadowserver analyzes the malware we’ve harvested, instruments behavior on live Internet connections, and generates detailed technical reports: attributing criminal infrastructures and identifying hidden investigative leads.

713,000

malware binaries executed every day



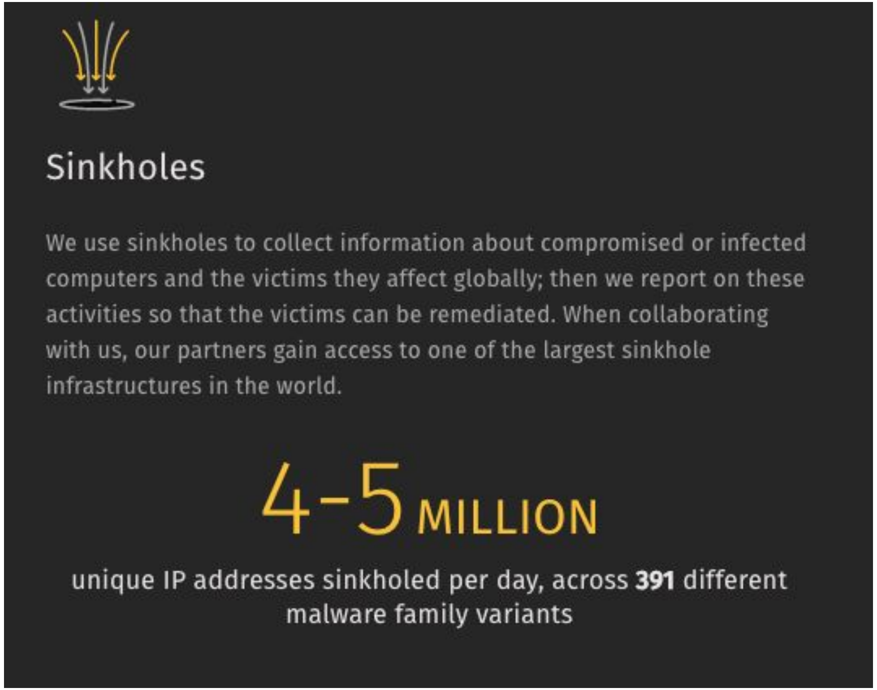
External Blacklists

Blacklists were formed to eliminate malicious email, but when sender addresses are spoofed, they can end up on a blacklist through no fault of their own — and once you’re blacklisted, it’s hard to get out. We publish blacklists to help you find out if (and where) you’ve been blacklisted.

110

blacklists shared every day

Shadowserver’s Unique Sources

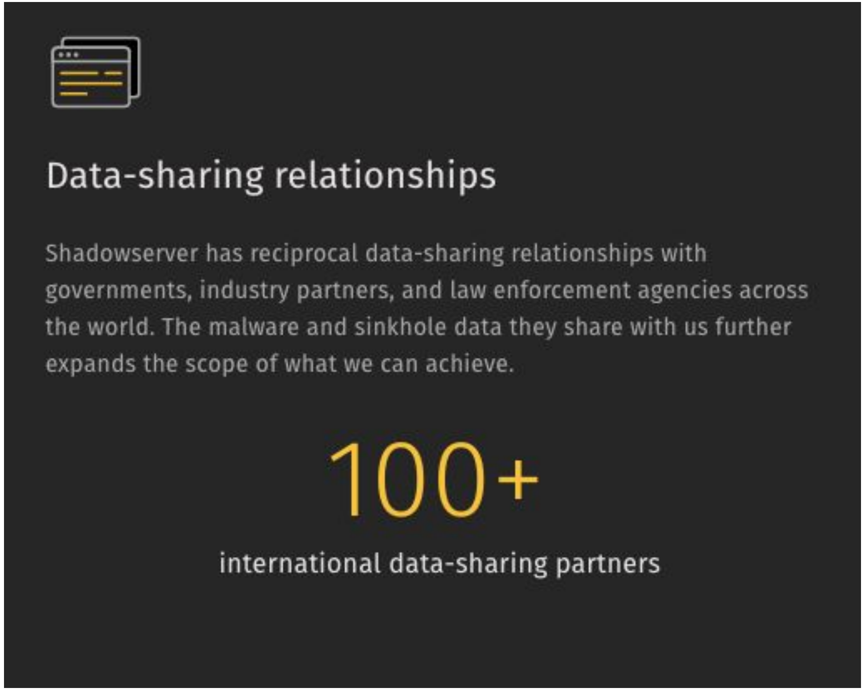


Sinkholes

We use sinkholes to collect information about compromised or infected computers and the victims they affect globally; then we report on these activities so that the victims can be remediated. When collaborating with us, our partners gain access to one of the largest sinkhole infrastructures in the world.

4-5 MILLION

unique IP addresses sinkholed per day, across **391** different malware family variants



Data-sharing relationships

Shadowserver has reciprocal data-sharing relationships with governments, industry partners, and law enforcement agencies across the world. The malware and sinkhole data they share with us further expands the scope of what we can achieve.

100+

international data-sharing partners

SHADOWSERVER

Who is Shadowserver?

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

Our mission is to make the Internet more secure by bringing to light vulnerabilities, malicious activity and emerging threats.

We promote a culture of sharing, equip organizations to improve their security, support criminal investigations, help protect victims, and offer free remediation reports.

We're driven by the vision of a secure, threat-free Internet.

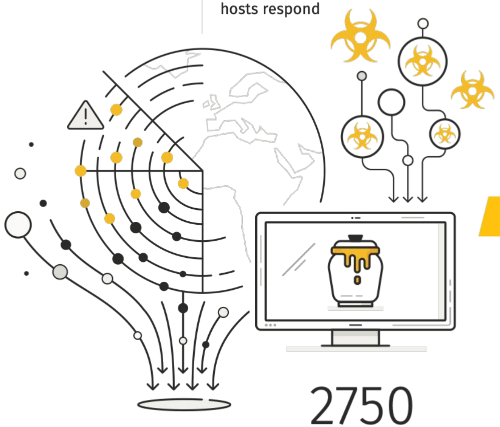
As security professionals, we understand there will always be obstacles on that path. Yet as passionate altruists committed to doing the right thing for the right reasons, we strive to that end: conducting leading-edge research and innovation with transparency, impartiality, and unassailable ethical standards.

https://www.shadowserver.org

Shadowserver by (some of the) numbers

4 BILLION

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



4-5 MILLION

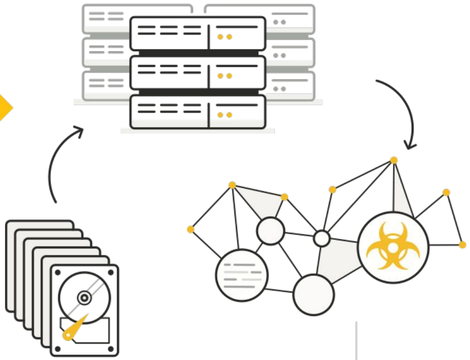
IP addresses per day sinkholed across **400** different malware variants

2750

Class C networks hosting honeypots & spampots

713K

unique malware samples ingested & analyzed **every day** by our sandboxes



11.6 PETABYTES

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

40 BILLION

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

4600

network owners & **106 National CSIRTs in 135 countries** rely on our **free** daily reports

Behind the scenes support for dozens of international Law Enforcement operations

Daily proactive security is in jeopardy unless you act.

SHADOWSERVER

Lighting the way to a more secure Internet

@shadowserver

freed0@shadowserver.org / david@shadowserver.org

SHADOWSERVER.ORG