Blocklist Report

A report based on non-Shadowserver public IP blocklists

@shadowserver

contact@shadowserver.org

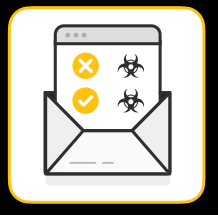
SHADOWSERVER.ORG

Presentation Aims & Objectives

- Introduce Blocklist reports
- Highlight a sample Blocklist report
- Describe key features of the report
- Demonstrate how a National CERT can action a Blocklist report
- Offer guidance on how to protect and remove Blocklists
- Provide a key list of Shadowserver online resources to enable report subscription and use

SHADOWSERVER

Blocklists

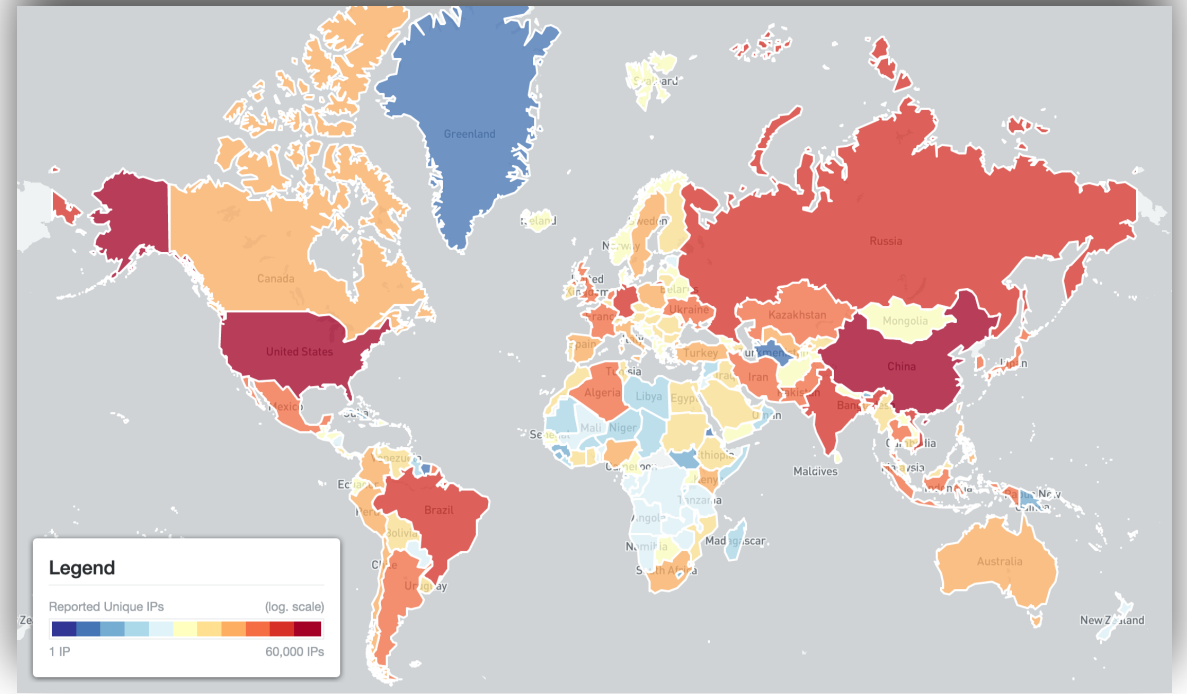


- Blocklists are a popular mechanism for protecting against cyber attacks, often meant to be used directly in firewalls or IDS/IPS systems
- The sources and mechanisms behind the blocklists may be very varied
- Shadowserver monitors over 110 public lists daily, aggregates the data and shares it
- None of the data is actually sourced from Shadowserver itself and Shadowserver do not control these lists in any way

SHADOWSERVER

Blocklists

- IP blocklists commonly name mail server IP addresses and/or domains suspected of :
  - sending SPAM
  - acting as an open proxy
  - an improperly configured mail server
- Variety of sites that collate lists of spam-sending entities
- Spamhaus is perhaps the most established
- List owners have different views on why an IP constitutes a block such as
  - the speed and number of emails or server requests sent
  - mail settings
  - spam reports filed



SHADOWSERVER

Blocklist Report

- Block List Report: https://www.shadowserver.org/what-we-do/network-reporting/blocklist-report/
- Report is available as a file in CSV format
- The report filename contains blocklist
- Reports can be sent as e-mail attachments, downloaded via HTTP or obtained via a RESTful API
- All timestamps are in UTC
- For more documentation on API access, please visit the below URLs and send a request for 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

Example Blocklists Report

Block List Report

This report is the aggregation of a variety of different Block/Deny list providers, for end-users' reference.

The purpose in sharing this information is to alert end-users that specific IP addresses of theirs have been flagged by providers as possibly malicious, and different services might be affected because of this listing.

The option to remove any system from a block list will vary by the provider. Some will have a well documented process, and some will demand payment for removal.

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

SHADOWSERVER

FIELDS

timestamp	Date and time of the tracked event in UTC+0
ip	IP Address of the device in question
hostname	Reverse DNS of the device in question
source	Block list source
reason	Given reason of the block list by the source
asn	ASN of where the device in question resides
geo	Country where the device in question resides
region	State / Province / Administrative region where the device in question resides
city	City in which the device in question resides

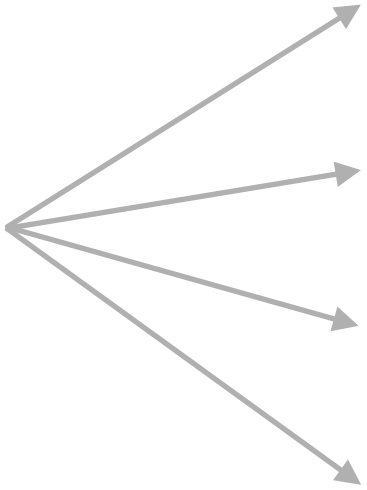
SAMPLE

```
"timestamp","ip","hostname","source","reason","asn","geo","region","city","naics","sic"
"2015-09-21 01:13:38","50.62.177.14",,"blocklist.de","apache abuse",26496,"US","ARIZONA"
"2015-09-21 01:13:38","46.29.2.166",,"blocklist.de","apache abuse",6663,"SK","BRATISLAVSI
"2015-09-21 01:13:38","50.62.177.208",,"blocklist.de","apache abuse",26496,"US","ARIZONA
"2015-09-21 01:13:38","5.141.52.232",,"blocklist.de","apache abuse",28719,"RU","KHANTY-M
"2015-09-21 01:13:38","5.141.229.165",,"blocklist.de","apache abuse",12705,"RU","PERMSKI
"2015-09-21 01:13:38","50.62.161.15",,"blocklist.de","apache abuse",26496,"US","ARIZONA"
"2015-09-21 01:13:38","46.219.242.192",,"blocklist.de","apache abuse",31148,"UA","KYIV",
"2015-09-21 01:13:38","46.200.239.116",,"blocklist.de","apache abuse",6849,"UA","L'VIVS'
"2015-09-21 01:13:38","46.63.78.85",,"blocklist.de","apache abuse",51784,"UA","KHMEL'NYT
```

Action a Blocklist Report

timestamp	ip	Hostname	source	reason	asn	geo	region	city
07/03/2022 00:02	46.29.2.XX	XXX	blocklist.de	apache abuse	6663	SK	BRATISLAVA KRAJ	BRATISLAVA

Key event fields



timestamp	Date and time of the tracked event in UTC+0
ip	IP Address of the device in question
hostname	Reverse DNS of the device in question
source	Block list source
reason	Given reason of the block list by the source
asn	ASN of where the device in question resides
geo	Country where the device in question resides
region	State / Province / Administrative region where the device in question resides
city	City in which the device in question resides

SHADOWSERVER

Action a Blocklist Report

timestamp	ip	Hostname	source	reason	asn	geo	region	city
07/03/2022 00:02	46.29.2.XX	XXX	blocklist.de	apache abuse	6663	SK	BRATISLAVA KRAJ	BRATISLAVA

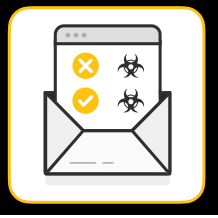
IP WHOIS
46.29.2.XX

```
% Abuse contact for '46.29.2.0 - 46.29.2.255' is 'abuse@enahost.com'

inetnum:        46.29.2.0 - 46.29.2.255
netname:        LERTAS-NET
descr:          Lertas network
country:        SK
admin-c:        LL5900-RIPE
tech-c:         LL5900-RIPE
mnt-domains:    TTISK-MNT
status:         ASSIGNED PA
mnt-by:         TTISK-MNT
mnt-routes:     MNT-EWRO
created:        2013-07-17T21:37:12Z
last-modified:  2018-05-16T07:47:27Z
source:         RIPE
abuse-c:        LAH26-RIPE
```

SHADOWSERVER

Verifying results



- Shadowserver provides the report “as-is” based on data published by others
- Some blocklists may contain false positives
- Some blocklists may have stale data
- Questions on blocklist content should be directed to the source of the particular list (mentioned in the report)

SHADOWSERVER

Blocklist - Removal

- Visit the provider and confirm the IP - our reports often only report out the wider CIDR block
- List owners will provide a general listing reason (as shown in our report)
- Removal policies vary by provider :
  - Self-Service Removal - some list owners operate a self-service removal feature
  - Time-Based Removal - most lists have a built-in, automatic process that removes IP addresses on different time periods if they are suspecting of sending SPAM multiple times
  - At Cost Removal - some providers may charge a removal fee

- Ensure you provide a review of mail server settings and look for issues such as :
  - missing or incorrect reverse DNS records
  - missing or incorrect banner greetings

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

Report Updates

- https://www.shadowserver.org/news-insights/
- Twitter @shadowserver
- 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

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

SHADOWSERVER

Lighting the way to a more secure Internet

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG