



IP address reputation of Mongolia

TEAM

UNITEL LLC

Agenda

- Blacklist and their risk
- International statistic
- Research result
- Conclusion



Bilguun Ganchuluun

- Information security analyst
- OSCP
- Developer

Dashzeveg Baatartsogt

- Information security analyst

Mongolian ip addresses

Mongolia has a total of 215808 IP address assigned. (APNIC)

apnic, https://lite.ip2location.com/mongolia-ip-address-ranges?lang=en_US

Detail information

- 60 AS number
- Most ASN has the address 49920
- In 2021, just over 84.3 percent of the population in Mongolia had access to the Internet.
(<https://www.statista.com/>)
- 56.6 percent of all IP addresses are on the top 5 ASN

Blacklist

A blacklist is a process of creating a registration list by detecting abnormal behavior of users connected to the Internet on many sensors located around the world.

Detail information

- Download or distribute copyright-violating content. For example illegal content, such as pirated software, copyrighted material, or child exploitation material
- Abnormal behavior - Sending spam mail or information, sending malicious traffic from a user's device infected with a virus., or attempting to attack other networks, etc.

Many organizations use blacklist information as a source and take measures to limit services and block regularly.

Blacklist's risk

The impact of being blacklisted can be significant for individuals, organizations, and businesses. Here are some potential consequences:

Risks

- In a NAT network, there is a risk that all other users will be subject to content restrictions due to one abnormal event.
- Blocked email communication: If an IP address is blacklisted, emails sent from that address may be blocked or marked as spam by email providers, which can prevent important messages from being delivered.
- Reputational damage to your organization
- Difficulty accessing certain services: If an IP address is blacklisted, it may be blocked from accessing certain websites or services.
- Reduced website traffic if you provider of web service.

Case 1:

..161.122 copyrighted content distribution notification received at this address.

Dear Sir or Madam:

I certify under penalty of perjury that I am authorized to act on behalf of the Paramount Global companies CBS Broadcasting Inc., CBS Studios Inc., Paramount Pictures Corporation, Showtime Networks Inc., Viacom International, Inc., Black Entertainment Television LLC, and other Paramount Global subsidiaries and affiliates (collectively, the "Rights Owners"), the owners of certain exclusive intellectual property rights in the copyrighted work(s) identified in this notice. I have a good faith belief that the information in this notice is accurate.

We have become aware that the below IP addresses have been using your service for distributing video files, which contain infringing video content that is exclusively owned by the Rights Owners.

We have a good faith belief that the Rights Owners' video content that is described in the below report has not been authorized for sharing or distribution by the copyright owner, its agent, or the law. Such copying and use of this material constitutes clear infringement of the Rights Owners' rights under the Copyright Act and its counterpart laws around the world.

We are requesting your immediate assistance in removing and disabling access to the infringing material from your network. We also ask that you ensure the user and/or IP address owner refrains from future use and sharing of the Rights Owners' materials and property.

In complying with this notice, you should not destroy any evidence that may be relevant in a lawsuit relating to the infringement alleged; including all associated electronic documents and data relating to the presence of the infringing items on your site, which shall be preserved while disabling public access, irrespective of any document retention or corporate policy to the contrary.

Nothing in this letter shall be construed as a waiver or relinquishment of any right, remedy, or claims possessed by the Rights Owners, or any affiliated party, all of which are expressly reserved.

Should you have any questions, please contact me at the information below.

Ben Sodos
Vobile, Inc.
Address: 2880 Lakeside Drive, Suite 360
Santa Clara, CA 95054, United States
Email: p2p@copyright-notice.com
408.217.5000

Behalf of the Paramount Global

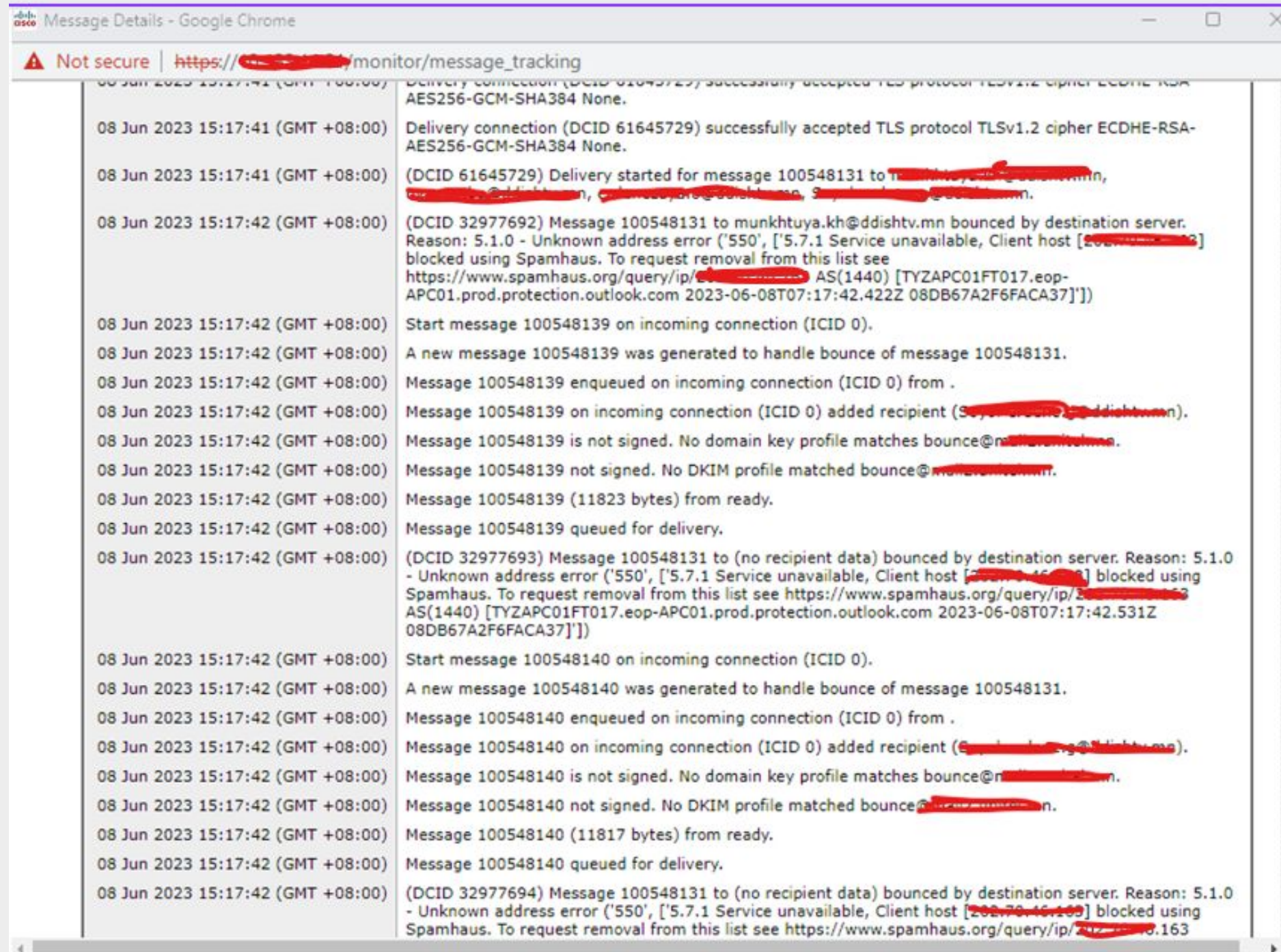
The ip address: Mobile network

<SubType BaseType="P2P" Protocol="BITTORRENT"/>

<FileName>Enemy At The Gates (2001) [1080p]</FileName>

Case 2:

Unable to send mail after blacklisted internal organization SMTP relay.



Case 3:

On average, this address (66.181.*.*) is blacklisted once every 4 days.

There is information that a botnet is working on that address. But the underlying problem is never fixed.

Subject: Spamhaus Notification | [REDACTED] - Botnet C&C Activity

Hello,

IP address: [REDACTED]

Issue: Botnet command and controller detection

Malware: win.qakbot

Inbox	MxToolbox Blacklist Summary - DELIVERABILITY MxToolbox Blacklist Summary 7/16/2023 - 7/23/2023 Dashboard Monitors Notifications History Mail Flow
Inbox	blacklist: [REDACTED] 6.181 - Removed from DRONE BL - here. blacklist:192.82.66.181 Removed from DRONE BL at 7/22/2023 5:22:53 PM (UTC+08:00) Ulaanbaatar after being down
Inbox	MxToolbox Blacklist Summary - DELIVERABILITY MxToolbox Blacklist Summary 7/9/2023 - 7/16/2023 Dashboard Monitors Notifications History Mail Flow
Inbox	MxToolbox Blacklist Summary - DELIVERABILITY MxToolbox Blacklist Summary 7/2/2023 - 7/9/2023 Dashboard Monitors Notifications History Mail Flow
Inbox	MxToolbox Blacklist Summary - DELIVERABILITY MxToolbox Blacklist Summary 6/25/2023 - 7/2/2023 Dashboard Monitors Notifications History Mail Flow
Inbox	blacklist: [REDACTED] - Removed from UCEPROTECTL3 - here. blacklist:192.82.66.181 Removed from UCEPROTECTL3 at 7/2/2023 3:12:54 PM (UTC+08:00) Ulaanbaatar after being
Inbox	blacklist: [REDACTED] - Removed from MAILSPIKE BL - here. blacklist:192.82.66.181 Removed from MAILSPIKE BL at 6/27/2023 2:44:19 PM (UTC+08:00) Ulaanbaatar after being
Inbox	blacklist: [REDACTED] - Added to UCEPROTECTL3 -) Ulaanbaatar Blacklist severity: Very Low MxRep Current Score: 89 Delisting link: http://email.mxtoolbox.com/c/eJwczEFu7CAMANDTwDICAw5ZsPi
Inbox	blacklist: [REDACTED] - Removed from MAILSPIKE Z - here. blacklist:192.82.66.181 Removed from MAILSPIKE Z at 6/27/2023 2:44:19 PM (UTC+08:00) Ulaanbaatar after being
Inbox	MxToolbox Blacklist Summary - DELIVERABILITY MxToolbox Blacklist Summary 6/18/2023 - 6/25/2023 Dashboard Monitors Notifications History Mail Flow
Inbox	blacklist: [REDACTED] - Added to MAILSPIKE Z -) Ulaanbaatar Blacklist severity: Low MxRep Current Score: 82 Delisting link: http://email.mxtoolbox.com/c/eJwczEFuHQANDTwNIMgWgsWHRj0IM
Inbox	blacklist: [REDACTED] - Added to MAILSPIKE BL -) Ulaanbaatar Blacklist severity: High MxRep Current Score: 82 Delisting link: http://email.mxtoolbox.com/c/eJwczD1uxCAQOHTQGkNjPkrKNJYyi
Inbox	MxToolbox Blacklist Summary - DELIVERABILITY MxToolbox Blacklist Summary 6/11/2023 - 6/18/2023 Dashboard Monitors Notifications History Mail Flow
Inbox	blacklist: [REDACTED] - Removed from UCEPROTECTL3 - here. blacklist:192.82.66.181 Removed from UCEPROTECTL3 at 6/12/2023 1:02:52 PM (UTC+08:00) Ulaanbaatar after being
Inbox	MxToolbox Blacklist Summary - DELIVERABILITY MxToolbox Blacklist Summary 6/4/2023 - 6/11/2023 Dashboard Monitors Notifications History Mail Flow
Inbox	blacklist: [REDACTED] - Added to UCEPROTECTL3 -) Ulaanbaatar Blacklist severity: Very Low MxRep Current Score: 89 Delisting link: http://email.mxtoolbox.com/c/eJwczEFuHQANDTwNIMwwi4
Inbox	blacklist: [REDACTED] - Removed from MAILSPIKE BL - here. blacklist:192.82.66.181 Removed from MAILSPIKE BL at 6/7/2023 12:30:42 PM (UTC+08:00) Ulaanbaatar after being
Inbox	blacklist: [REDACTED] - Removed from MAILSPIKE Z - here. blacklist:192.82.66.181 Removed from MAILSPIKE Z at 6/7/2023 12:30:42 PM (UTC+08:00) Ulaanbaatar after being
Inbox	MxToolbox Blacklist Summary - DELIVERABILITY MxToolbox Blacklist Summary 5/28/2023 - 6/4/2023 Dashboard Monitors Notifications History Mail Flow

Check the blacklist

There are many sources where you can see if your public address is blacklisted.



- Checked from 82 different sources.
- All of your MX record, DNS, blacklist and SMTP diagnostics in one integrated tool



- Defines ip reputation according to AbuseIPDB customer's report.

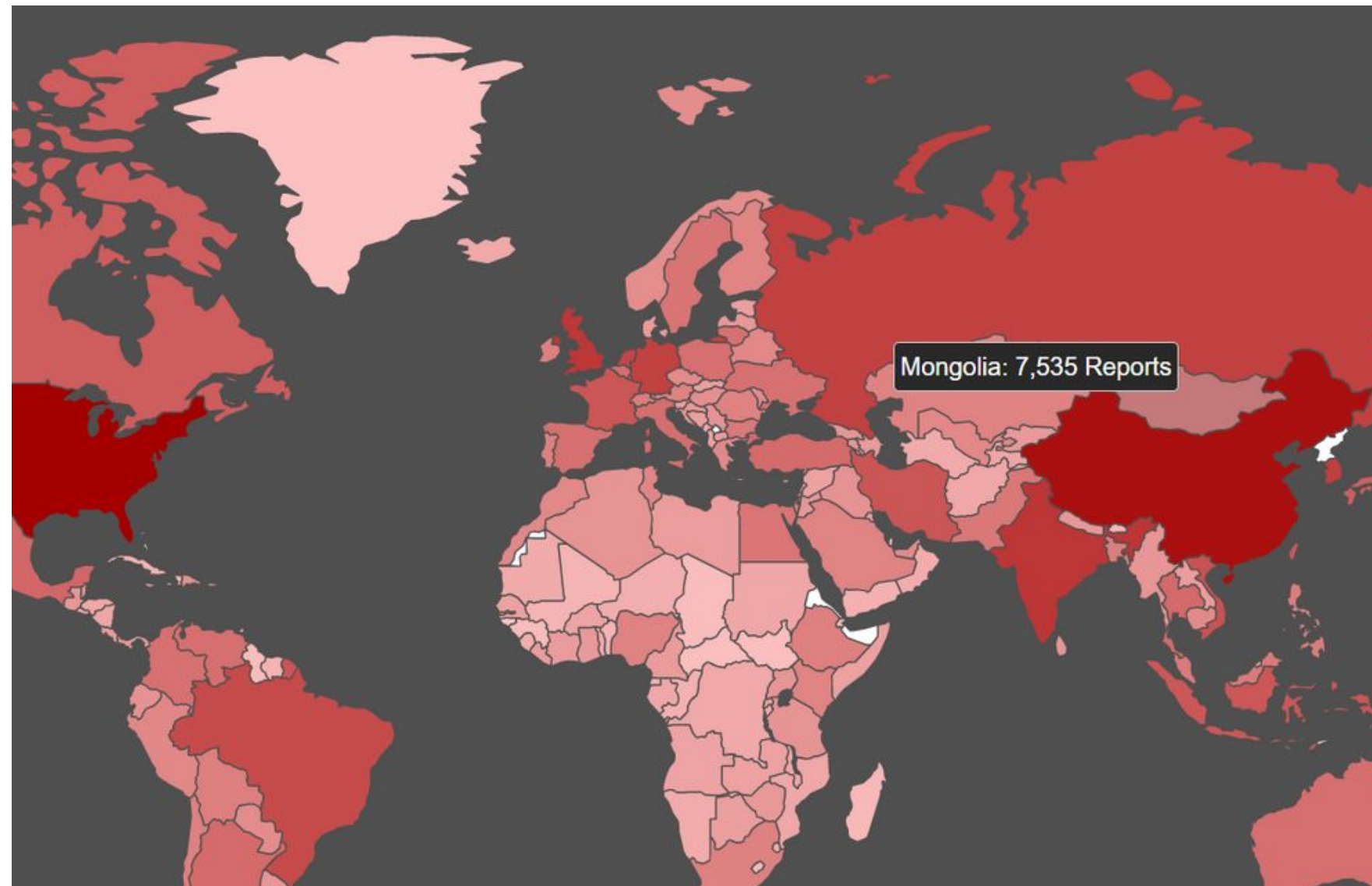


- Checked from 66 different sources.

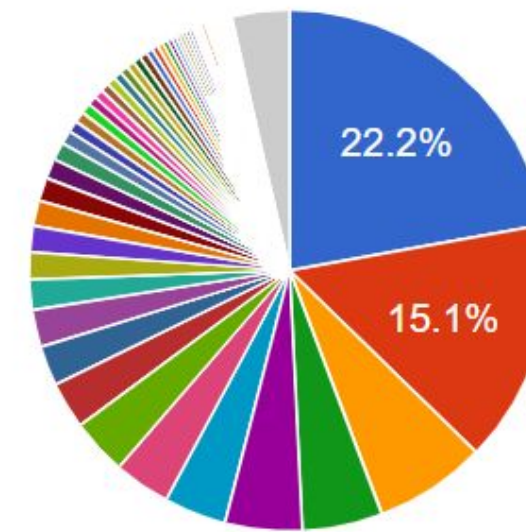
International statistics

In the report coming to abuseipdb, The number of IP addresses being reported is in 54th place.

<https://www.abuseipdb.com/statistics>



Reported IP Addresses By Country (Last 7 Days)



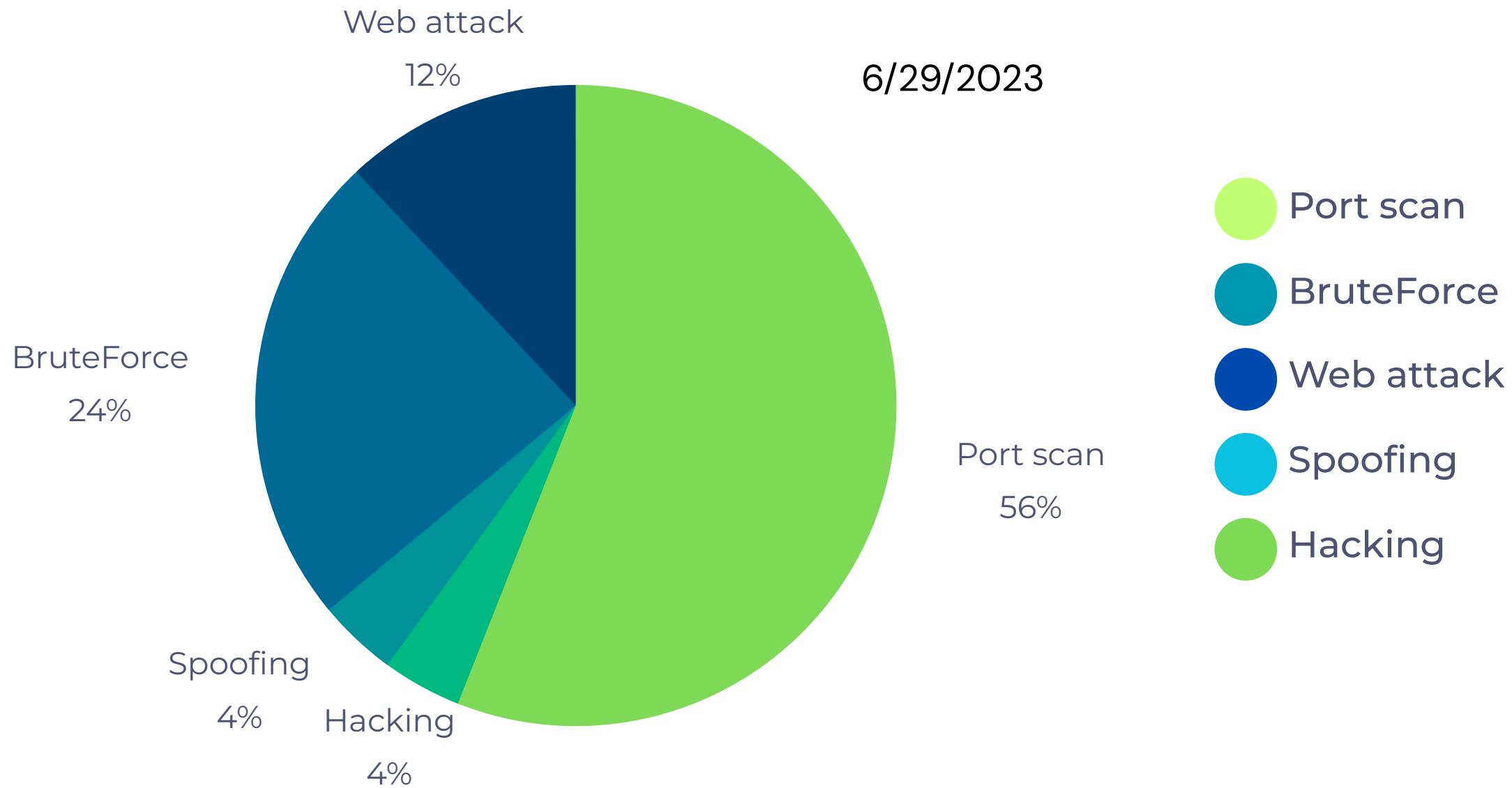
6/28/2023

- Romania
 - Saudi Arabia
 - Finland
 - Kenya
 - Mongolia
 - Tunisia
 - Peru
- ▲ 8/9 ▼

In that week, 7,535 addresses were reported in abuseipdb, which is 3.7 percent of the total number of addresses.

International statistics

Checked the ABUSE reason in the Top 10 ASN for 25244 ip's address.



127.0.0.1:8000/subnet_reputation?subnet=49.0.129.0/24

Update

```
{"data": [{"networkAddress": "49.0.129.0", "netmask": "255.255.255.0", "minAddress": "49.0.129.1", "maxAddress": "49.0.129.254", "numPossibleHosts": 254, "addressSpaceDesc": "Internet", "reportedAddress": [{"ipAddress": "49.0.129.3", "numReports": 328, "mostRecentReport": "2023-06-28T12:37:49+00:00", "abuseConfidenceScore": 100, "countryCode": "MN"}, {"ipAddress": "49.0.129.9", "numReports": 782, "mostRecentReport": "2023-06-29T02:19:58+00:00", "abuseConfidenceScore": 100, "countryCode": "MN"}, {"ipAddress": "49.0.129.10", "numReports": 4, "mostRecentReport": "2023-06-05T20:21:38+00:00", "abuseConfidenceScore": 0, "countryCode": "MN"}, {"ipAddress": "49.0.129.25", "numReports": 1, "mostRecentReport": "2023-06-21T08:50:34+00:00", "abuseConfidenceScore": 3, "countryCode": "MN"}, {"ipAddress": "49.0.129.27", "numReports": 32, "mostRecentReport": "2023-06-27T23:12:51+00:00", "abuseConfidenceScore": 100, "countryCode": "MN"}]}]}
```

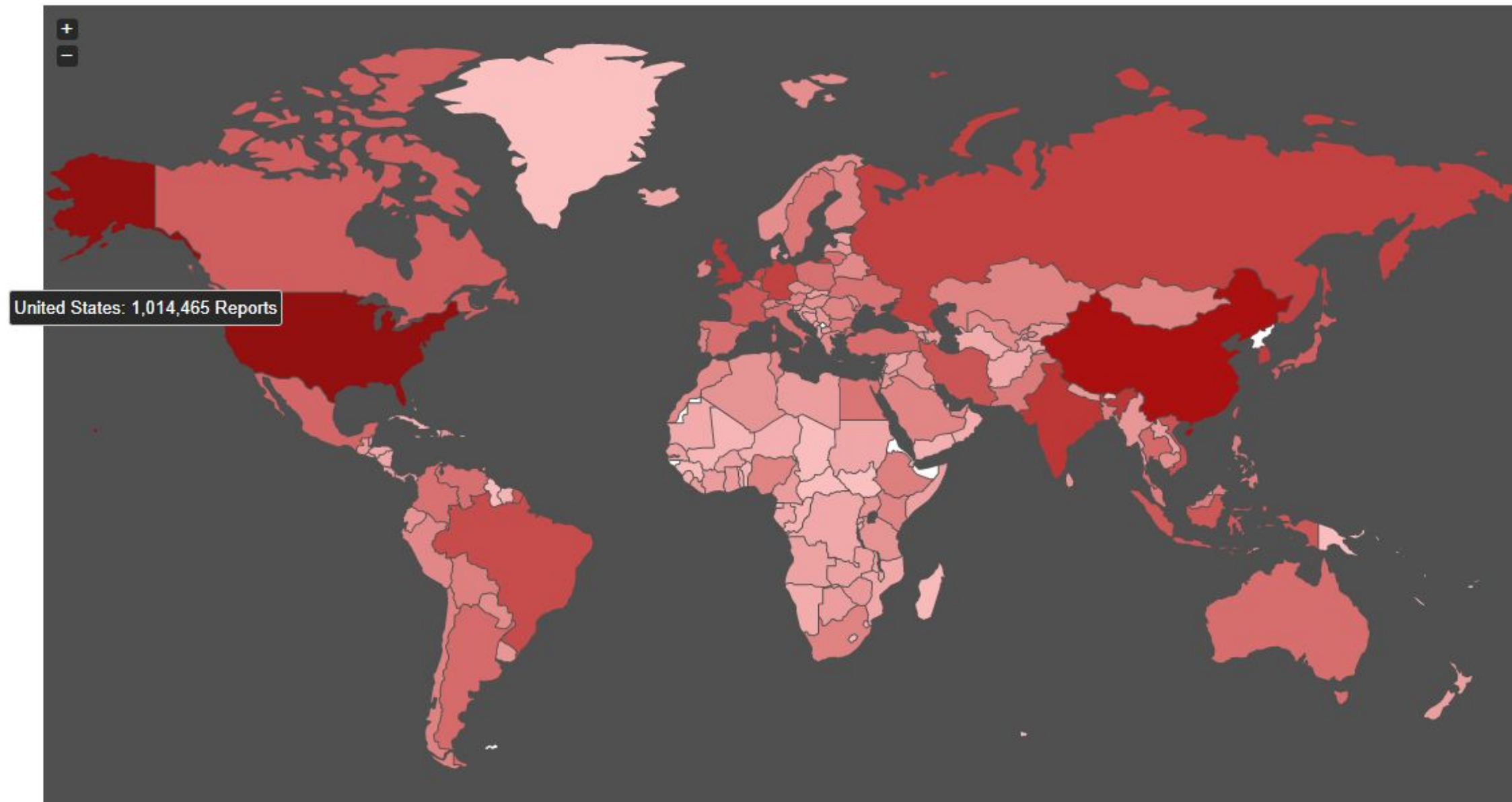

International statistics

Top 3 countries where the most addresses are blacklisted

- USA - 1014465 - 0.06%
- China - 687366 - 0.19%
- Singapore - 315696 - 1.5%

<https://www.abuseipdb.com/statistics>

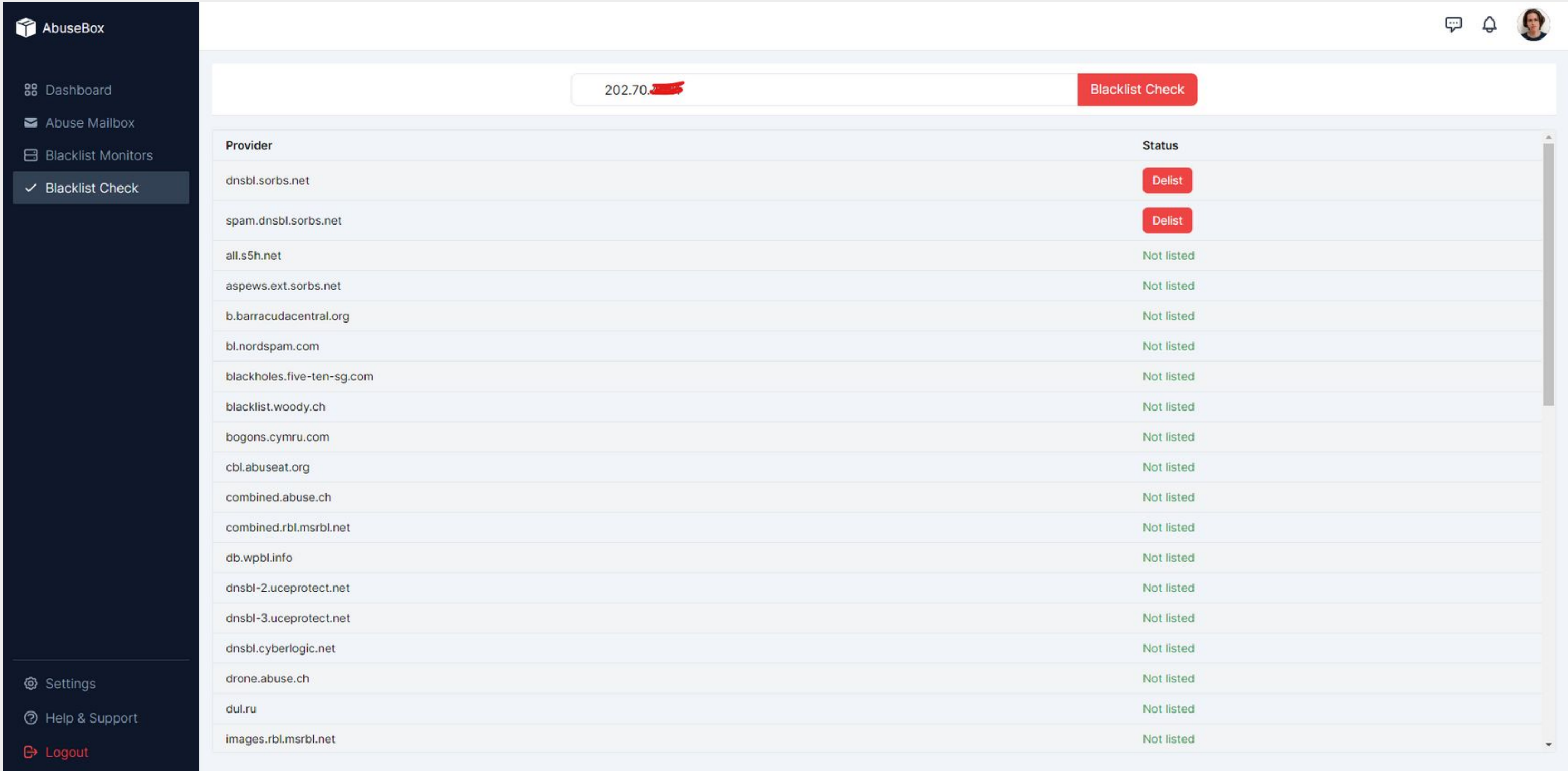
<https://ipinfo.io/>



6/29/2023

Our research & solution

As an ISP organization, we receive complaints about addresses being blacklisted every day. Because of this, there have been several incidents of malfunctions. So, the first step is we want to monitor it regularly.



The screenshot displays the AbuseBox interface for performing a blacklist check. A search bar at the top contains the IP address "202.70. [redacted]" and a "Blacklist Check" button. Below the search bar is a table with two columns: "Provider" and "Status". The table lists various providers and their current status.

Provider	Status
dnsbl.sorbs.net	Delist
spam.dnsbl.sorbs.net	Delist
all.s5h.net	Not listed
aspews.ext.sorbs.net	Not listed
b.barracudacentral.org	Not listed
bl.nordspam.com	Not listed
blackholes.five-ten-sg.com	Not listed
blacklist.woody.ch	Not listed
bogons.cymru.com	Not listed
cbl.abuseat.org	Not listed
combined.abuse.ch	Not listed
combined.rbl.msrb1.net	Not listed
db.wpbl.info	Not listed
dnsbl-2.uceprotect.net	Not listed
dnsbl-3.uceprotect.net	Not listed
dnsbl.cyberlogic.net	Not listed
drone.abuse.ch	Not listed
dul.ru	Not listed
images.rbl.msrb1.net	Not listed

Ip addresses of surveyed

We checked 156976 addresses of the almost all ISP. For examples are below:

AS17882 Univision LLC

AS9484 Mobinet LLC. AS Mobinet Internet Service Provider

AS38805 STXCitinet, Leading Internet & VOIP Service Provider, Ulaanbaatar, Mongolia

AS45204 GEMNET LLC

AS38818 YOKOZUNANET LLC

AS10219 SKYMEDIA CORPORATION LLC

AS9934 Mongolia Telecom

AS58439 ICNC LLC

AS10076 ERDEMNET Mongolian National Research and Education Network education

AS24559 G-Mobile Corporation

https://lite.ip2location.com/mongolia-ip-address-ranges?lang=en_US

Statistics according to research

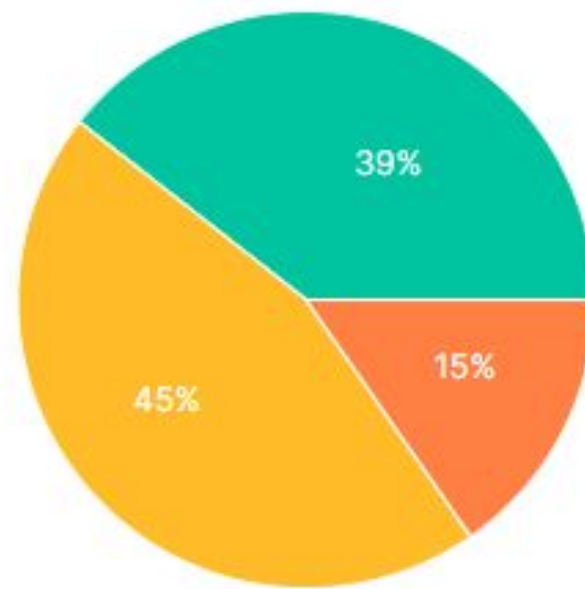
38.39% of the total addresses are included in the blacklist, which is a very high percentage.

Total IP Addresses
156976

Not blacklisted IP Addresses
96709

Blacklisted IP Addresses
60267

Categories

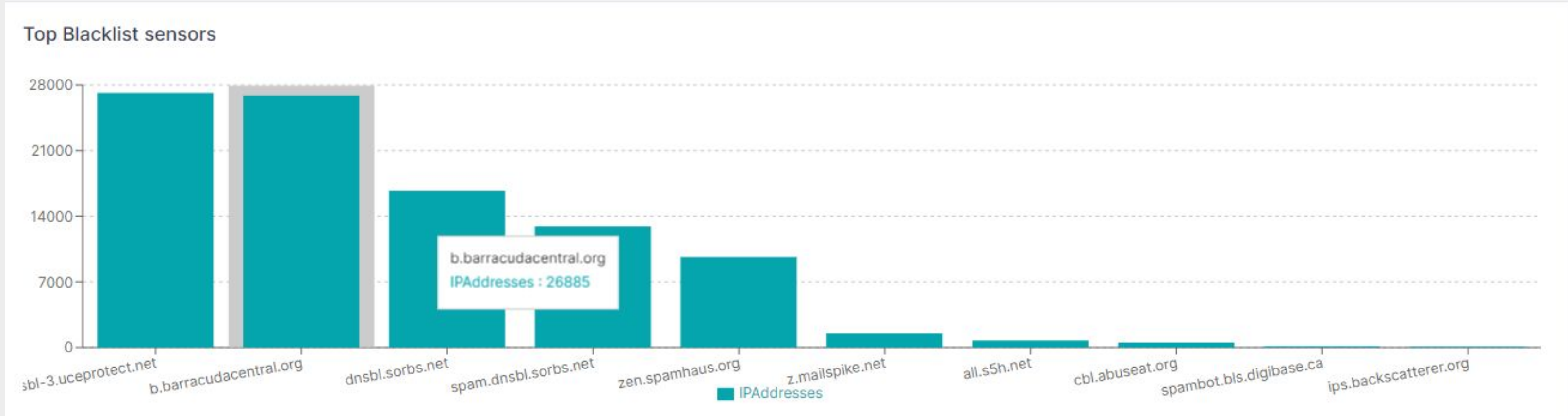


Spam IPS Unknown

8/31/2023

Statistics according to research

Below are the sensors with the most blacklisted Mongolian addresses.



DB & Backend

The information will be stored in DB and monitored regularly.

DelistRequests object (41)

Hostname:

103.2

Delist requests:

```
{"b.barracudacentral.org": {"status": "sent",  
"confirmation_number": "BBR21693472143-94613-17997"}}
```

Status:

processing

Created:

Date: 2023-08-31

Today | 📅

Time: 08:56:54

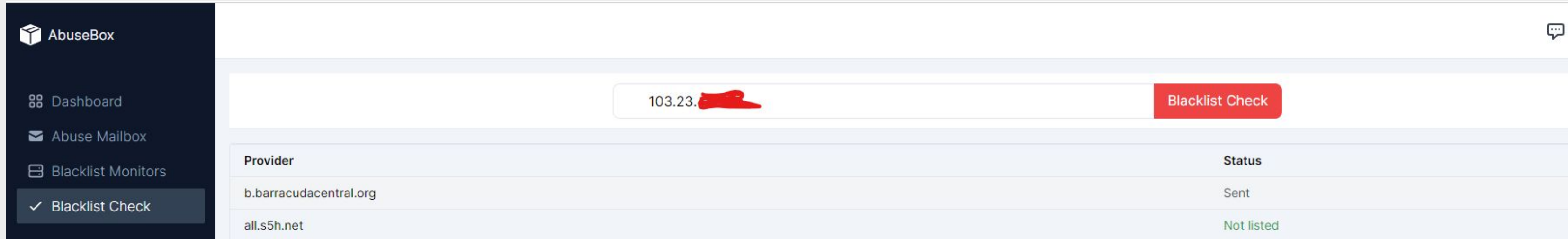
Now | 🕒

Note: You are 8 hours ahead of server time.

- 103.119.92.107 {'blacklists': [['singular.ttk.pte.hu', ['unknown']]]}
- 103.119.92.106 {'blacklists': []}
- 103.119.92.105 {'blacklists': []}
- 103.119.92.104 {'blacklists': []}
- 103.119.92.103 {'blacklists': []}
- 103.119.92.102 {'blacklists': []}
- 103.119.92.101 {'blacklists': []}
- 103.119.92.100 {'blacklists': []}
- 103.119.92.99 {'blacklists': []}
- 103.119.92.98 {'blacklists': []}
- 103.119.92.97 {'blacklists': []}
- 103.119.92.96 {'blacklists': []}
- 103.119.92.95 {'blacklists': []}
- 103.119.92.94 {'blacklists': []}
- 103.119.92.93 {'blacklists': [['all.s5h.net', ['unknown']], ['singular.ttk.pte.hu', ['unknown']]]}
- 103.119.92.92 {'blacklists': []}
- 103.119.92.91 {'blacklists': []}
- 103.119.92.90 {'blacklists': []}
- 103.119.92.89 {'blacklists': [['all.s5h.net', ['unknown']]]}

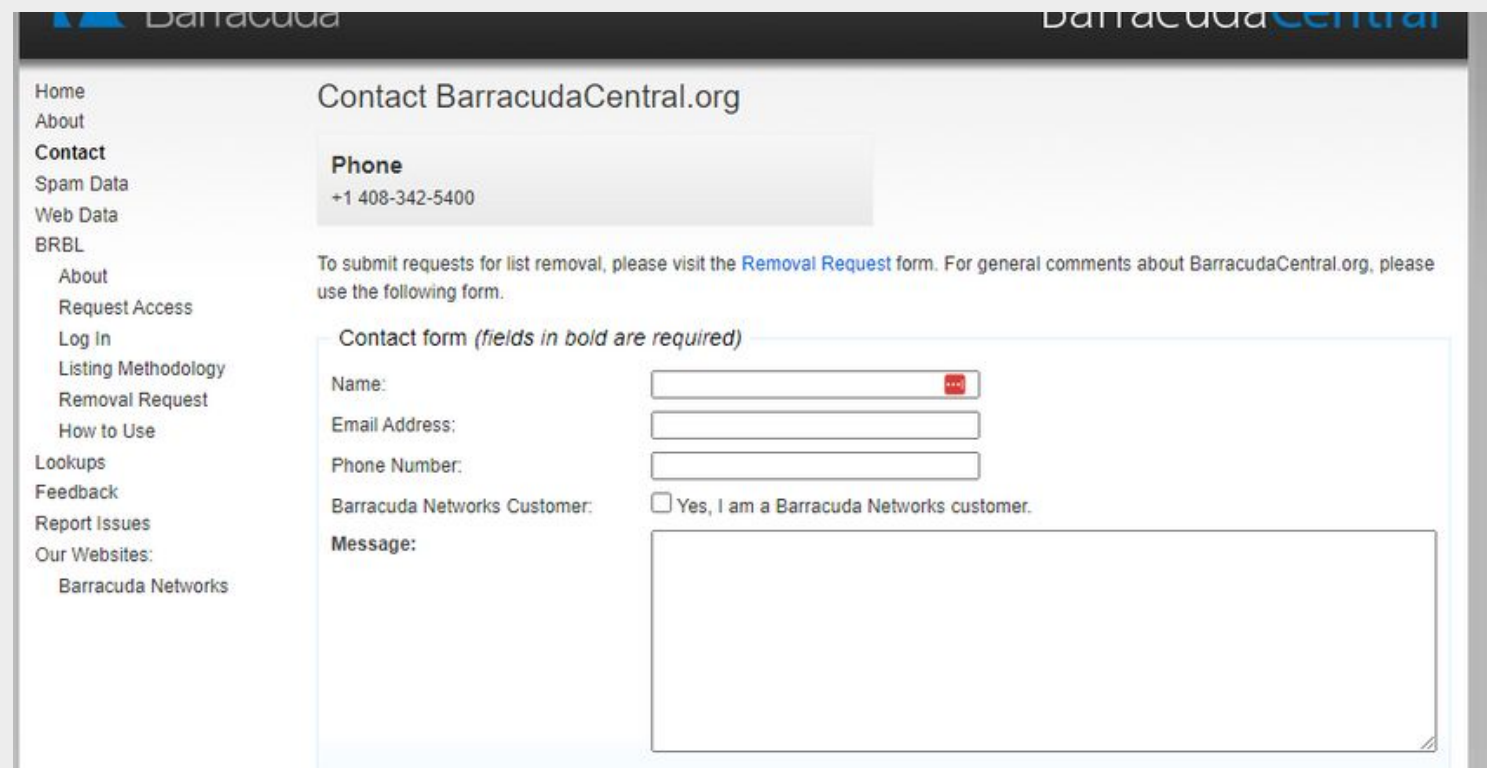
Automate delist process

A request was made to delist the address that was on the list. This makes it easier to request a manual on the web



The screenshot shows the AbuseBox interface. On the left is a dark sidebar with navigation items: AbuseBox, Dashboard, Abuse Mailbox, Blacklist Monitors, and Blacklist Check (highlighted with a checkmark). The main content area features a search bar with the IP address "103.23. [redacted]" and a red "Blacklist Check" button. Below this is a table with two columns: "Provider" and "Status".

Provider	Status
b.barracudacentral.org	Sent
all.s5h.net	Not listed



The screenshot shows the contact page for BarracudaCentral.org. The page title is "Contact BarracudaCentral.org". A "Phone" field displays "+1 408-342-5400". Below this is a message: "To submit requests for list removal, please visit the [Removal Request](#) form. For general comments about BarracudaCentral.org, please use the following form." The form is titled "Contact form (fields in bold are required)" and includes the following fields:

- Name:
- Email Address:
- Phone Number:
- Barracuda Networks Customer: Yes, I am a Barracuda Networks customer.
- Message:

Delist and their risks

In order to delist an IP address registered in the blacklist, the organization maintaining the list is contacted and a request for de-listing is submitted manually.

1

Some time is needed after sending the request.

2

If you don't find out the reason, you will be blacklisted again in a short time

3

Unable to get out of the blacklist due to repeated requests.

Кибер аюулгүй байдлын тухай хууль

According to the law, the citizen will assume the following obligations.

18 дугаар зүйл.Иргэн

18.1.Иргэн кибер аюулгүй байдлыг хангах талаар дараах үүргийг хүлээнэ:

18.1.1.өөрийн болон өөрийн асрамжид байгаа хүний кибер аюулгүй байдлыг хариуцах;

18.1.2.холбогдох байгууллагаас гаргасан зөвлөмжийг дагах, шаардлагыг биелүүлэх;

18.1.3.хууль тогтоомжид заасан бусад.

18.2.Кибер халдлага, зөрчил үүссэн, үүссэн байж болзошгүй тохиолдолд Нийтийн төвд даруй мэдэгдэж болно.

Our ideas for this issue

ISPs and law enforcement agencies can work together to take the following actions.

1

United

- Provide recommendations to consumers in accordance with Article 18 of the said law.
- Recommend security solutions such as anti-virus to users.
- When the risk is repeated many times, demand fulfillment of obligations according to the above law

2

Implement a campaign to educate users

- What risks Copyright-Infringing and unauthorized cracked content may pose to
you

3

Ability to correctly determine the cause of the blacklist and use dynamic NAT addresses.

Demo

Blacklist check

