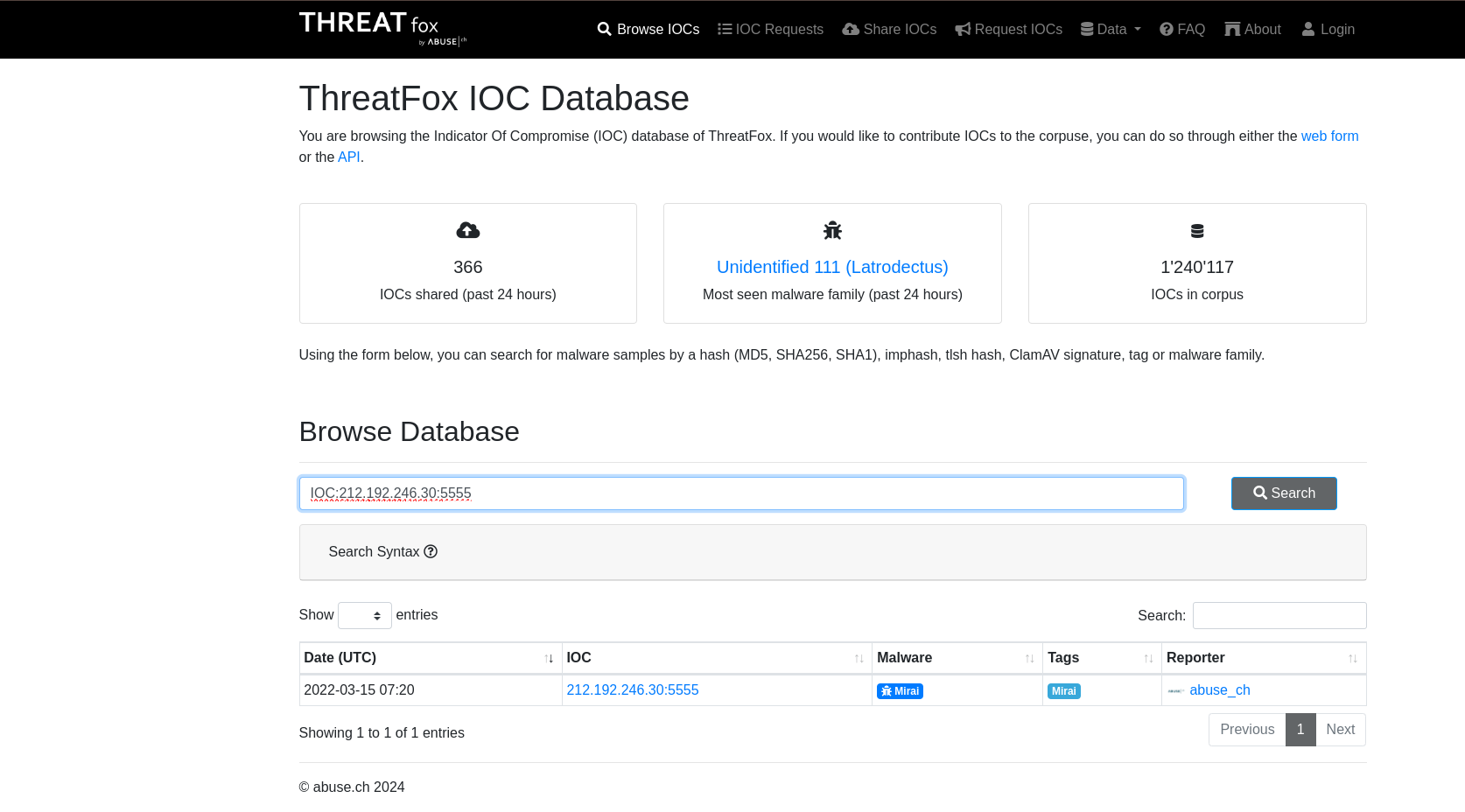
**Using Abuse.ch Platforms**

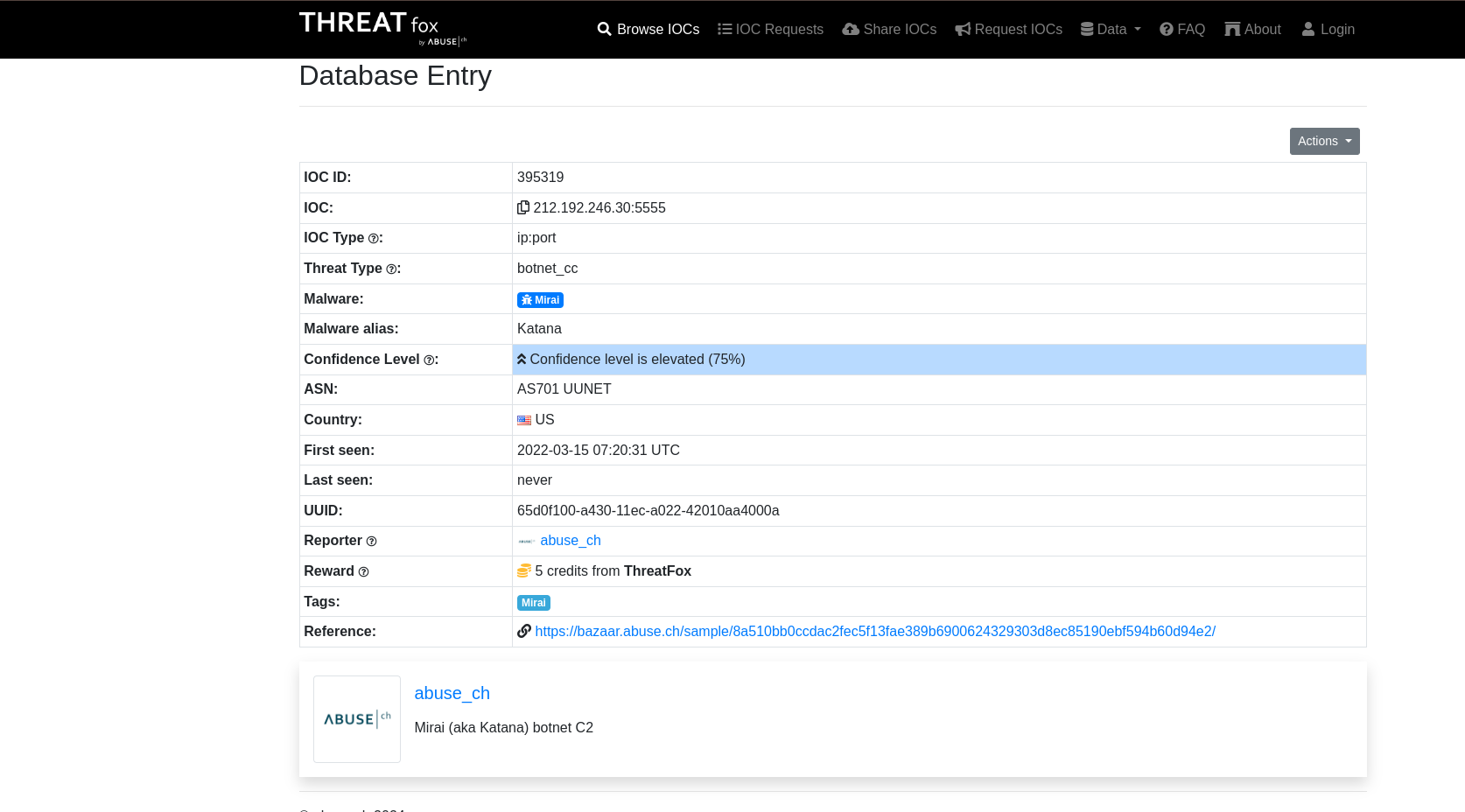
1. ThreatFox

It has a library of IOCs that assist security analysts to search for, share and export IOCs related to their search.

I am searching for the IOC **212.192.246.30:5555**

Here is the result:



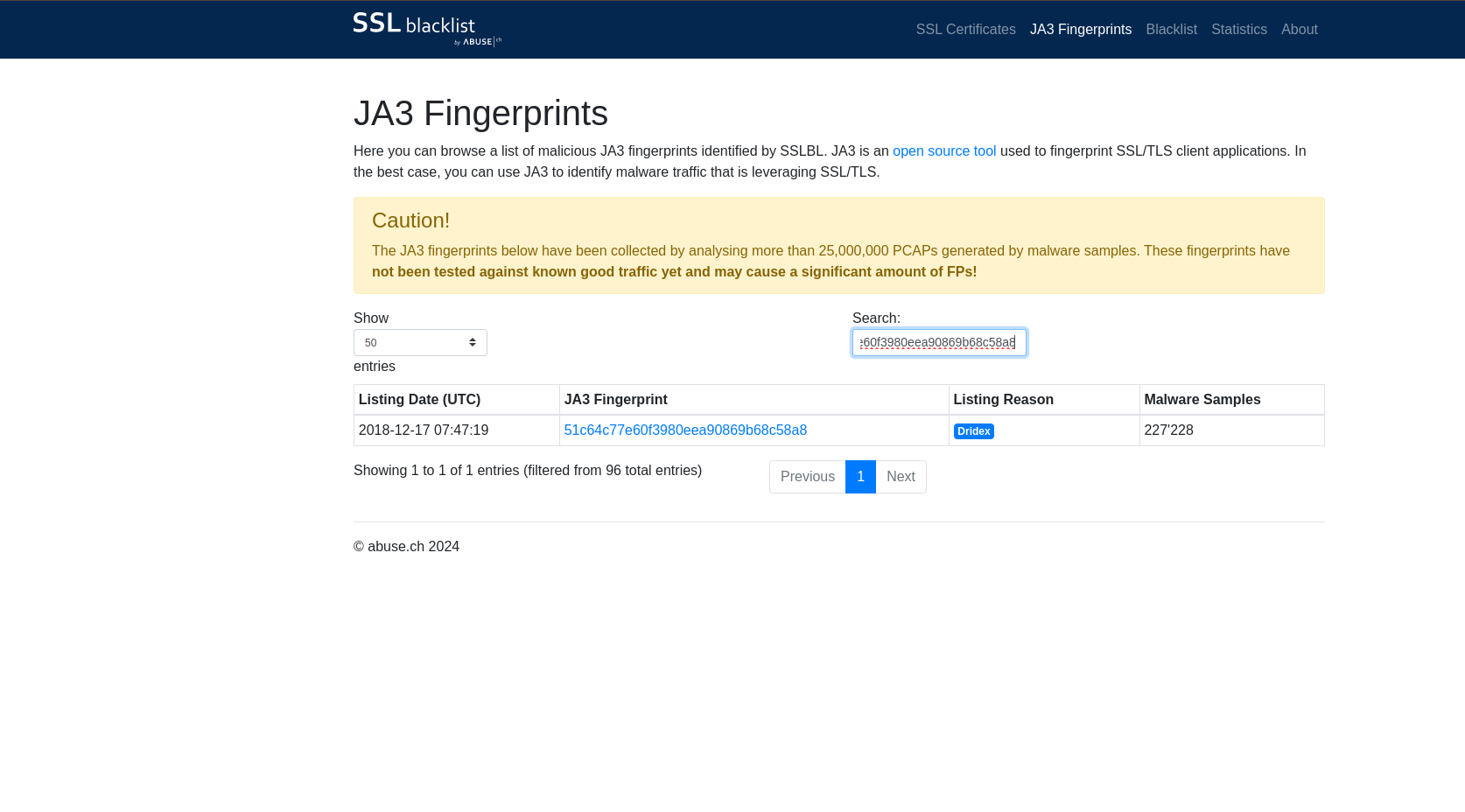


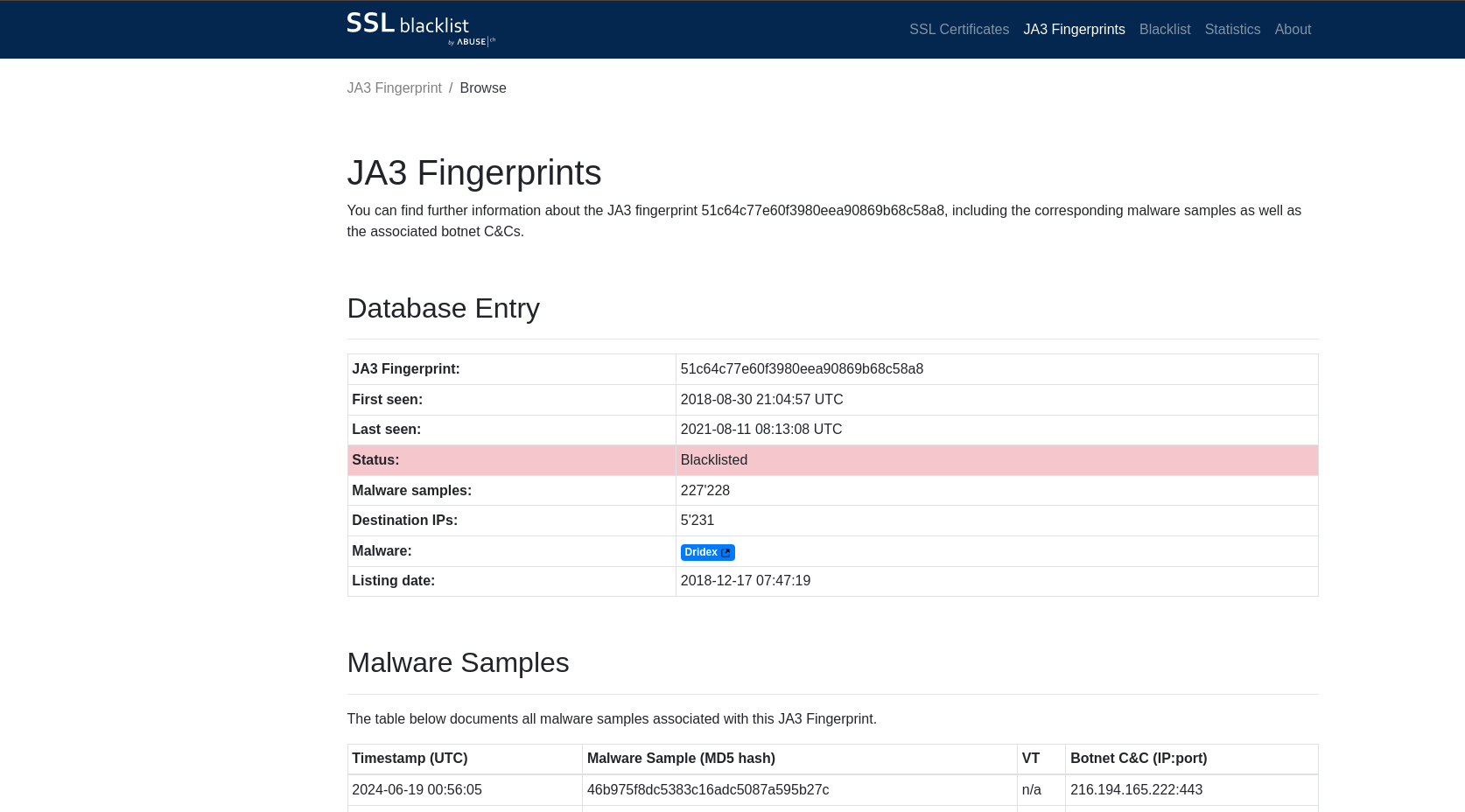
1. SSL Blacklist

A tool used to identify and detect malicious SSL connections.

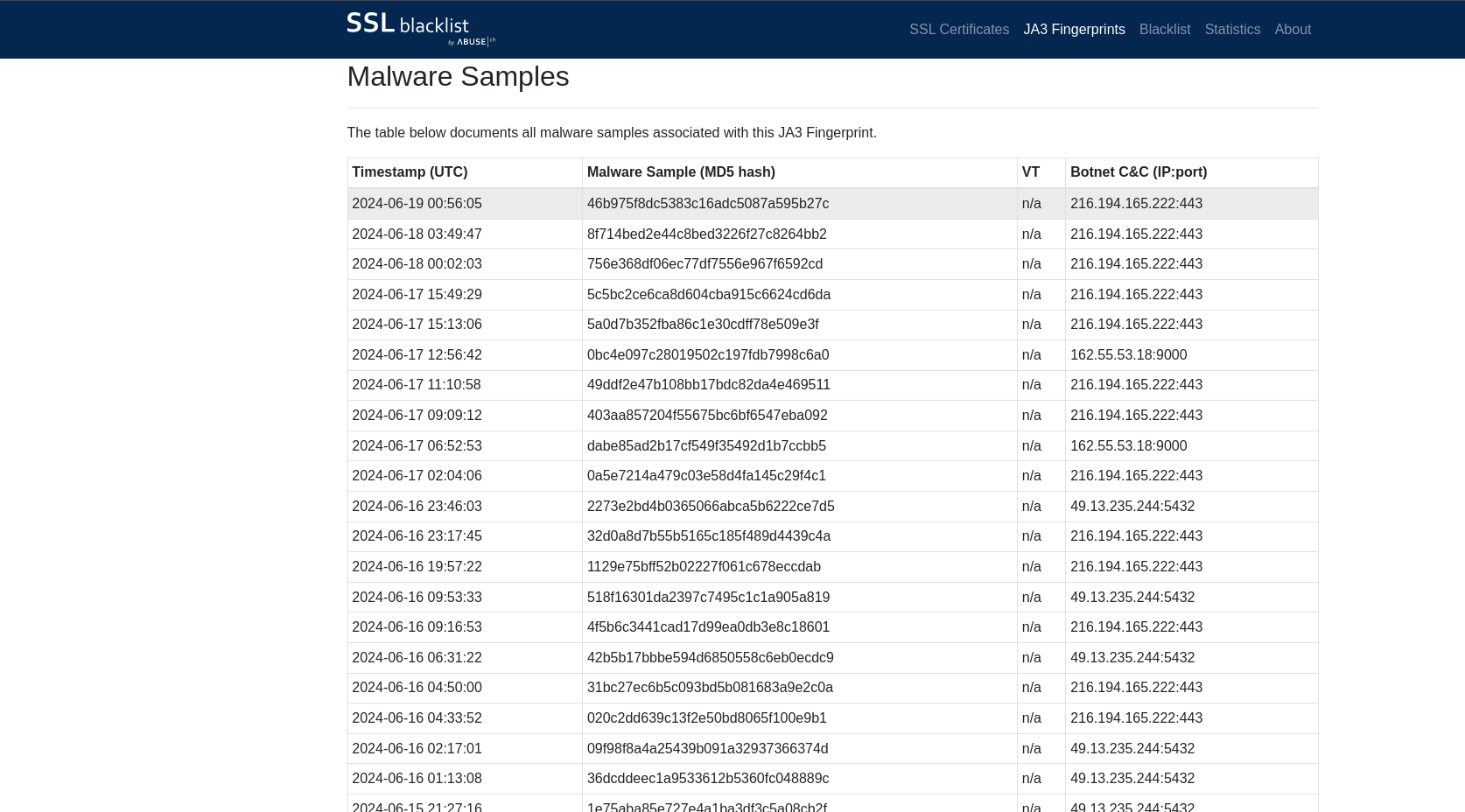
I am searching for a JA3 Fingerprint **51c64c77e60f3980eea90869b68c58a8**

Here are the results:





The JA3 Fingerprint I inserted was last seen in 2021. However there are newer Fingerprints of the same malware as shown in samples below:



Since the malware uses encrypted C&C servers, “network-based measures such as blocking C&C IPs is only effective in the short term” according to Malpedia.

According to MalwareBytes, “Dridex uses an older tactic of infection by attaching a Word document that utilizes macros to install malware. However, once new versions of Microsoft Office came out and users generally updated, such a threat subsided because it was no longer simple to infect a user with this method.”

Encouraging windows users to update their system will mitigate the risk of the windows system.

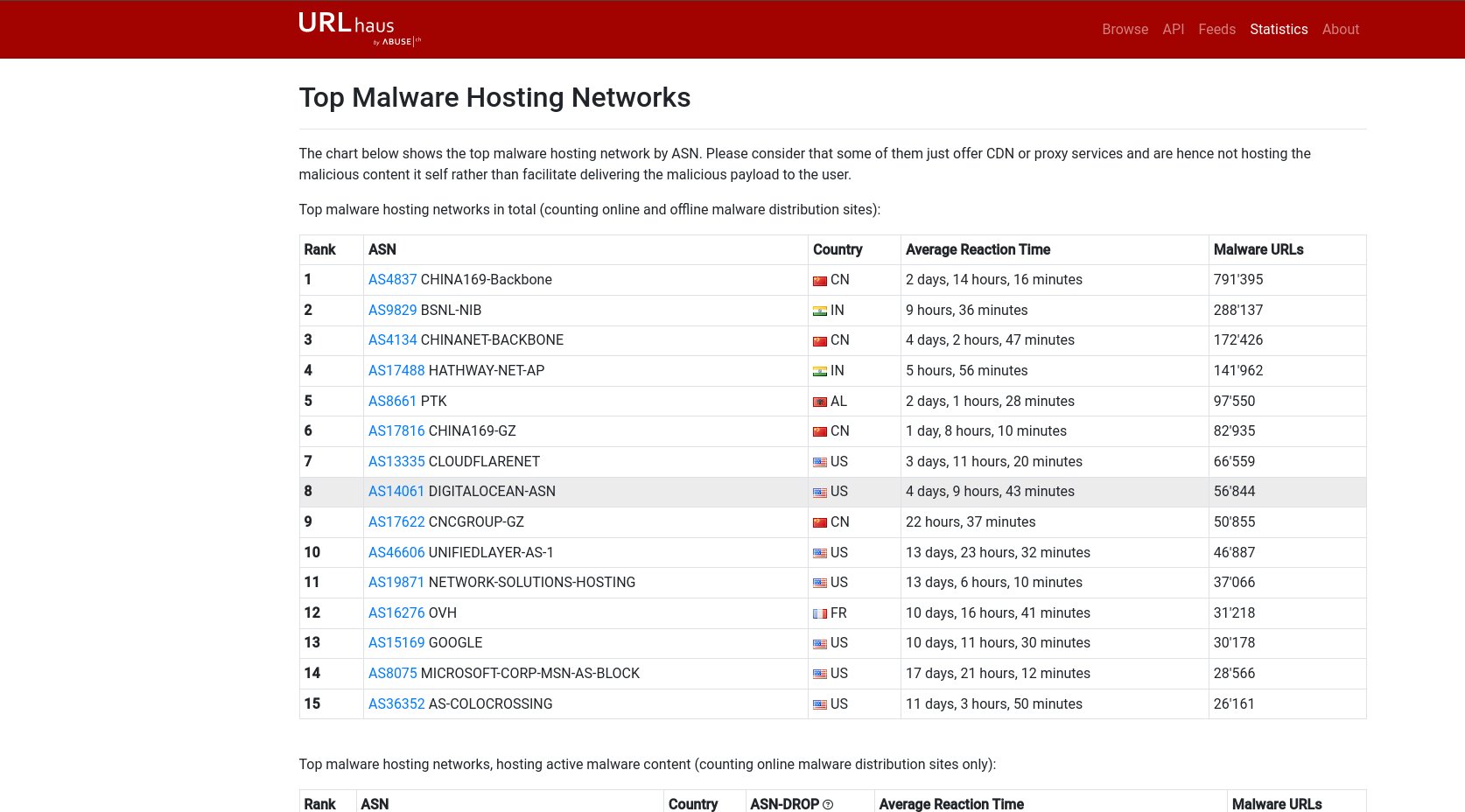
Further information on Dridex malware can be found at [Malpedia](https://malpedia.caad.fkie.fraunhofer.de/details/win.dridex).

1. URLhaus

The focus of the tool is on sharing malicious URLs used for malware distribution. As a security analyst, I can leverage the tool to validate my investigations on filetypes suspected to be malicious.

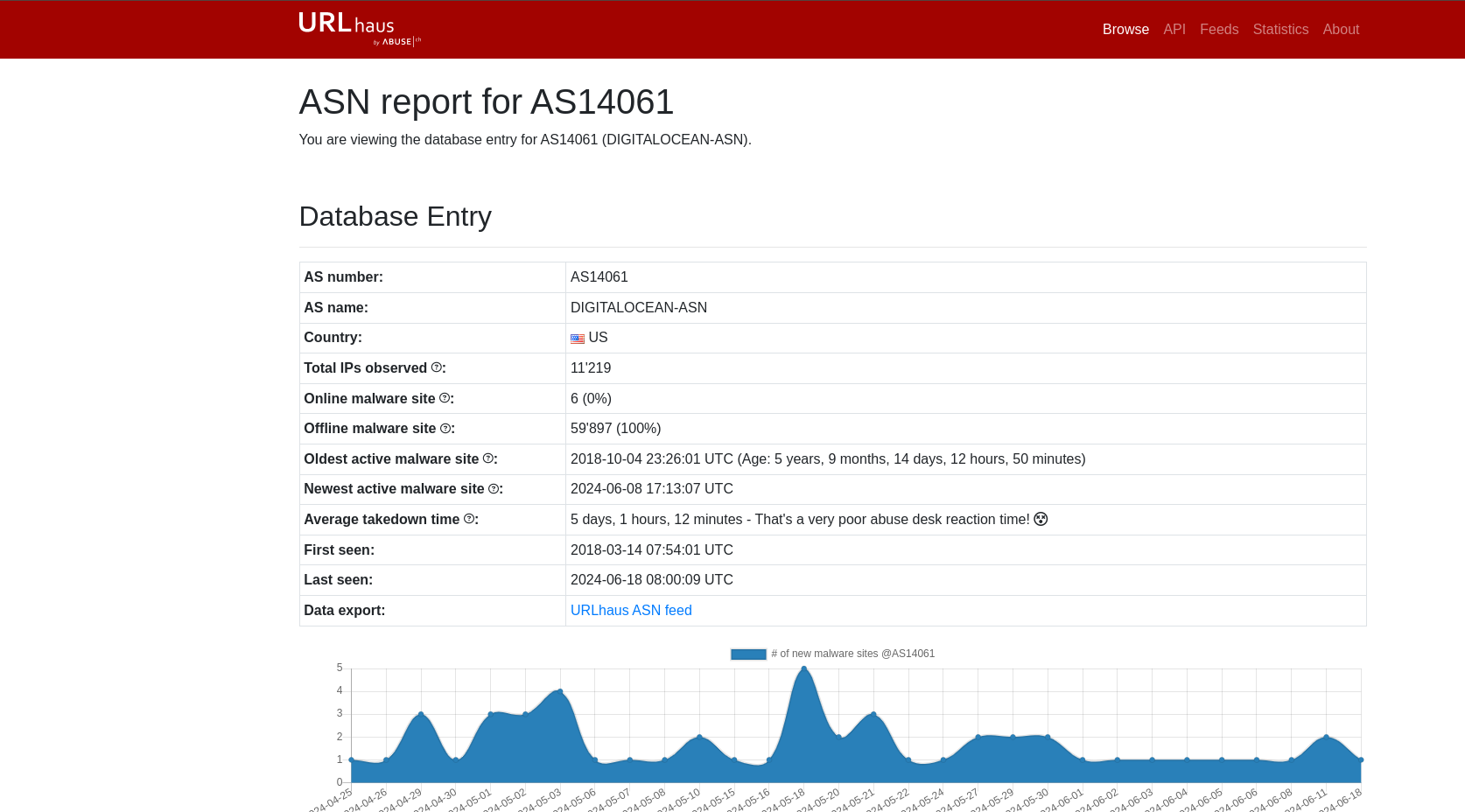
I am looking up ASN number **AS14061** in the Statistics page. The task is to identify the malware-hosting network with that ASN number.

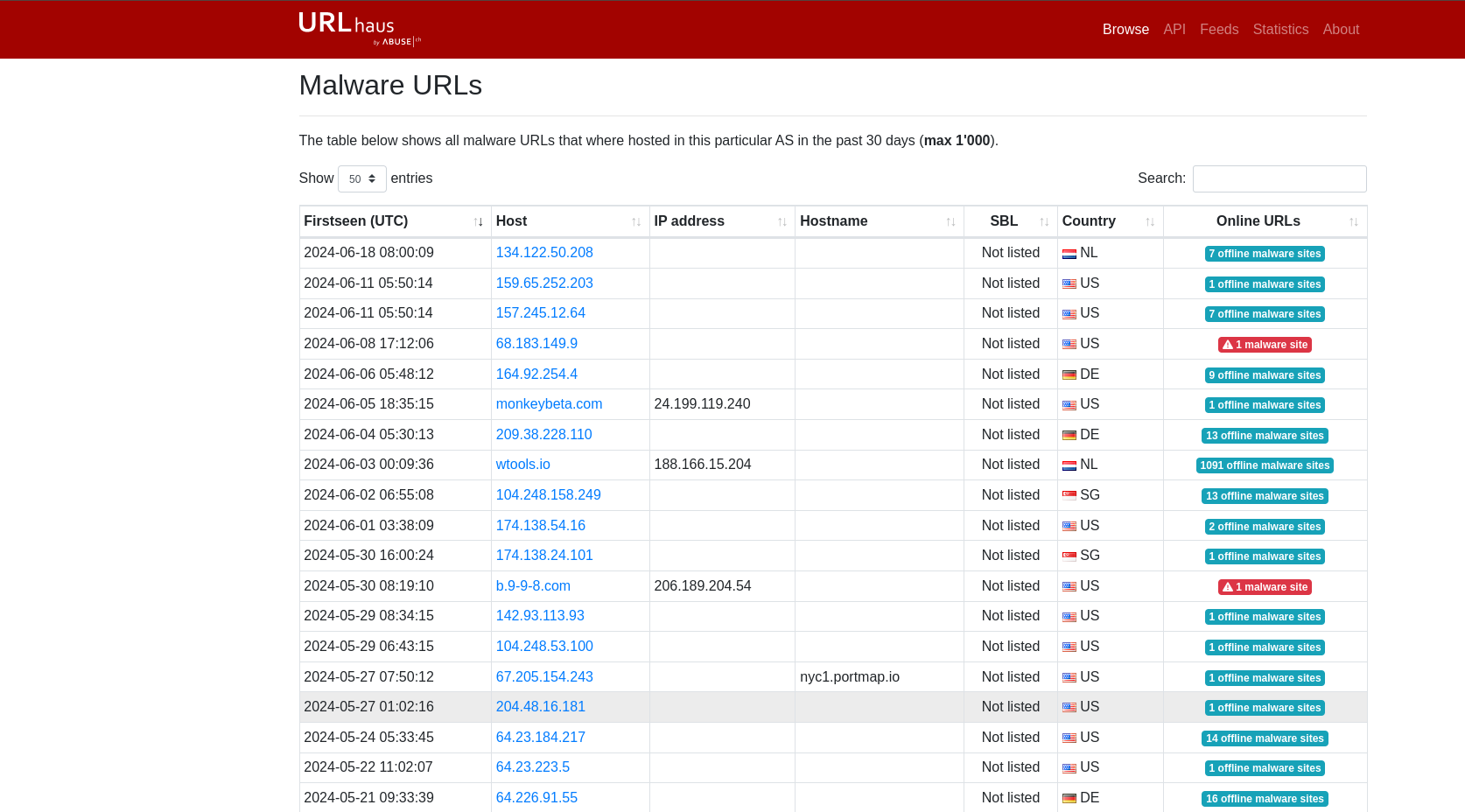
Here are the results:



The malware-hosting network with that ASN number is DIGITALOCEAN-ASN.

Further information on DIGITALOCEAN-ASN, including hosts that are online or offline:



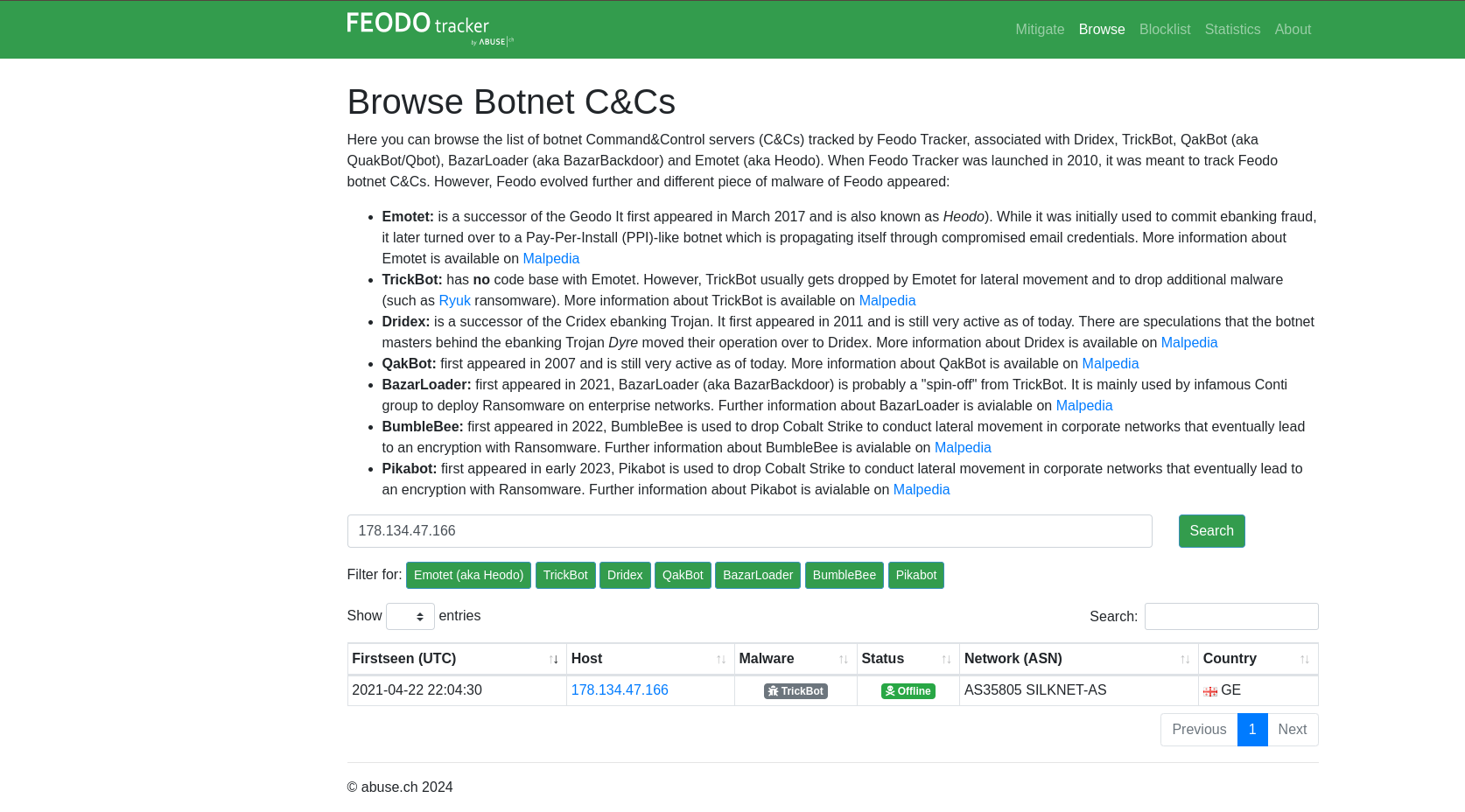


1. FeodoTracker

For sharing intelligence on botnet Command & Control (C&C) servers associated with Dridex, Emotes (aka Heodo), TrickBot, QakBot and BazarLoader/BazarBackdoor.

The task is to identify the country associated with a botnet IP **178.134.47.166**.

The country is Georgia



The botnet was last online in 2022.

