Technisches Gutachten für die Telekom-Control-Kommission im Verfahren R 31/22

Gutachter:

Dipl.-Ing. Thomas Schreiber, LL.M. (WU)

Wien am 13. April 2023

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH)

Mariahilfer Straße 77–79
1060 WIEN, ÖSTERREICH
www.rtr.at

E: rtr@rtr.at
T: +43 1 58058-0
F: +43 1 58058-9191

FN 208312t, HG Wien
UID-Nr.: ATU43773001

Inhaltsverzeichnis

1 Einleitung

1.1 Gutachtensauftrag

Am 02.02.2023 hat die Telekom-Control-Kommission (TKK) im Verfahren R 31/22 folgenden Gutachtensauftrag erteilt[1]

„Gemäß § 52 AVG wird Dipl.-Ing. Thomas Schreiber, LL.M. (WU) zum Amtssachverständigen bestellt und mit der Erstellung eines Gutachtens bis zum 13.04.2023 zu folgenden Fragen beauftragt:

1. Was bewirkt aus technischer Sicht eine Sperre der IP-Adresse 190.115.18.20 durch einen Anbieter von Internetzugangsdiensten?

    a. Wie und wem gegenüber wirkt eine durch Anbieter von Internetzugangsdiensten eingerichtete IP-Sperre?
    b. Kann es aus technischer Sicht zu „Overblocking“ kommen, wenn eine IP-Sperre durch einen Internetzugangsdiensteanbieter umgesetzt wird?
    c. Kann ein Internetzugangsdiensteanbieter pro-aktiv abschließend und umfassend erkennen, ob im Falle einer konkreten IP-Sperre auch andere Dienste mitumfasst sind?

2. Wer ist Inhaber der IP-Adresse 190.115.18.20?

    a. Wem ist die IP-Adresse zugewiesen, wer kann aus technischer Sicht den unter einer IP-Adresse abrufbaren Inhalt bestimmen / verändern / steuern oder sonst über ihn verfügen?
    b. Wie ist die Zuordnung Hosting-Dienst bzw Content Delivery Network zur IP-Adresse?
    c. Welche verschiedenen Inhalte lassen sich unter dieser IP-Adresse abrufen? Wie kann dies aus technischer Sicht festgestellt werden?
    d. Ist es aus technischer Sicht möglich, alle unter einer IP-Adresse abrufbaren Inhalte aufzulisten? Ist es für einen Internetzugangsdiensteanbieter möglich, alle abrufbaren Inhalte zu erkennen?
    e. Sollte sich der Inhaber einer IP-Adresse verändern, wäre auch der neue Inhaber durch eine bestehende IP-Sperre betroffen?
    f. Sollte sich der unter der IP-Adresse bereitgestellte Inhalt verändern, wären auch Inhalte dieser neuen Angebote durch die bestehende IP-Sperre betroffen?

3. Wie effektiv ist die IP-Sperre der IP-Adresse 190.115.18.20 durch einen Anbieter von Internetzugangsdiensten?

    a. Verfügt ein Domaininhaber über technische Möglichkeiten, die Wirksamkeit einer IP-Sperre zu verringern?

[1] Aus Gründen der Referenzierbarkeit wurden die Gutachtensfragen nummeriert.

b. Welche praktischen Auswirkungen hat für Endnutzer der Wechsel einer IP-Adresse durch einen Domaininhaber? Wie häufig kann die einer Domain zugeordnete IP-Adresse geändert werden? Wie lange dauert es bei einem Wechsel der IP-Adresse, bis eine Domain für Internetnutzer wieder erreichbar ist?
c. Unterscheidet sich die Effektivität im Falle des Einsatzes von IPv6?
d. Gibt es für Endnutzer – aus technischer Sicht – Möglichkeiten, die Sperre der genannten IP-Adresse durch ihren Internetzugangsdiensteanbieter zu umgehen? Ist dies auch Endnutzer ohne ausgeprägtem IT-Know-How möglich? Unterscheidet sich dies im Vergleich zu einer DNS-Sperre? Was bewirkt der Einsatz von VPNs?“

1.2 Aufbau des Gutachtens

Im vorliegenden Gutachten werden in Abschnitt 2 zuerst die für das Verständnis notwendigen Grundlagen und Systeme des „Word Wide Web“ erklärt. Anschließend wird darauf eingegangen, wie sich aus technischer Sicht die Sperre einer IP-Adresse durch einen Anbieter von Internetzugangsdiensten auswirkt. In Abschnitt 3 wird versucht, zu ermitteln, welche Dienste unter der verfahrensgegenständlichen IP-Adresse 190.115.18.20 angeboten werden und darauf eingegangen, ob durch die Einrichtung einer IP-Sperre bestimmte Dienste zielgerichtet blockiert werden können. Abschnitt 4 behandelt schließlich die Frage, wie eine eingerichtete IP-Sperre sowohl durch Endnutzer:innen als auch durch Domaininhaber:innen umgangen werden kann. Dabei wird besonders auf s.g. VPNs eingegangen und es wird auf die Unterschiede in Bezug auf IPv6 hingewiesen. Abschnitt 5 fasst die wesentlichen Schlussfolgerungen zusammen.

2 Technische Grundlagen des WWW

Wenn vom „Internet“ gesprochen wird, ist tatsächlich meist die spezielle Anwendung des „World Wide Web“ gemeint. Diese setzt sich im Wesentlichen aus den folgenden Komponenten zusammen, die jeweils auf verschiedene Ebenen des OSI-Modells[2] agieren:

- Die Datenübertragung auf IP-Ebene („Internet Protocol“) durch das „Internet“ im engeren Sinne. Dieses ermöglicht die Übertragung von „IP-Paketen“, die durch Sender- und Empfänger-IP-Adressen bestimmt sind.
- Das Domain Name Service (DNS) zur Konvertierung von einfach merkbaren Internetadressen wie „orf.at“ in die aus technischer Sicht notwendigen IP-Adressen wie „194.232.104.3“ (IPv4) und „2a01:468:1000:9::150“ (IPv6).
- Das Hypertext Transfer Protokoll („HTTP“) für die strukturierte Übertragung von Inhalten
- Web-Technologien wie HTML, CSS und JavaScript für die Aufbereitung von Inhalten

Illustrieren lässt sich das etwa am Aufruf der URL „https://www.orf.at/“: Technisch beginnt dieser Prozess im Normalfall damit, dass der aufrufende Browser beim DNS-Resolver des Anbieters des Internetzugangsdienstes[3] in einer ersten Anfrage um die Zuordnung der Domain[4] „www.orf.at“ zu einer IP-Adresse anfragt. Werden vom DNS-Resolver auf diese Anfrage dann eine oder mehrere IP-Adressen zurückgegeben, baut der Browser (wie etwa Mozilla Firefox, Google Chrome, Microsoft Edge) eine Verbindung[5] zu einer zurückgegebenen IP-Adresse auf. Falls durch den DNS-Resolver mehrere IP-Adressen zu einer Domain zugeordnet werden, obliegt die Entscheidung der verwendeten IP-Adresse dem Browser.

Unter Verwendung dieser aufgebauten Verbindung kommuniziert der Browser über HTTP, um vom kontaktierten Server die Ressource „/“ (die Startseite) der Domain „www.orf.at“ abzurufen. Existiert diese, sendet der Server unter Verwendung eines in HTTP definierten Statuscodes – im Fall, dass die Ressource abrufbar ist „200“ – den entsprechenden HTML-Code, der anschließend vom Browser grafisch aufbereitet und dargestellt wird. Dieser gesamte Prozess ist in Abbildung 1 dargestellt.

Ein DNS-Request ist für eine Auflösung einer Domain notwendig. Kommt es im Zuge der weiteren Nutzung zum Aufruf unterschiedlicher Ressourcen derselben Domain (etwa „https://www.rtr.at/TKP/startseite.de.html“ und „https://www.rtr.at/TKP/wer_wir_sind/tkk/TKK.de.html“) erfolgt keine weitere DNS-Abfrage.

[2] ITU-T X.200 (07/1994).
[3] Die IP-Adresse dieses Dienstes ist durch das Dynamic Host Configuration Protocol („DHCP“) bekannt – je nach Netzwerkkonfiguration entweder dem aufrufenden Computer direkt, oder dem verwendeten Router.
[4] Im weiteren wird der „Fully Qualified Domain Name“ als „Domain“ bezeichnet – d.h. inklusive der Subdomains wie „www.orf.at“ anstatt der reinen Second-Level-Domain „orf.at“.
[5] Unter Verwendung des „Transmission Control Protocols“ (TCP) und einem vordefinierten „Port“, üblicherweise 443 bei verschlüsselten Verbindungen.

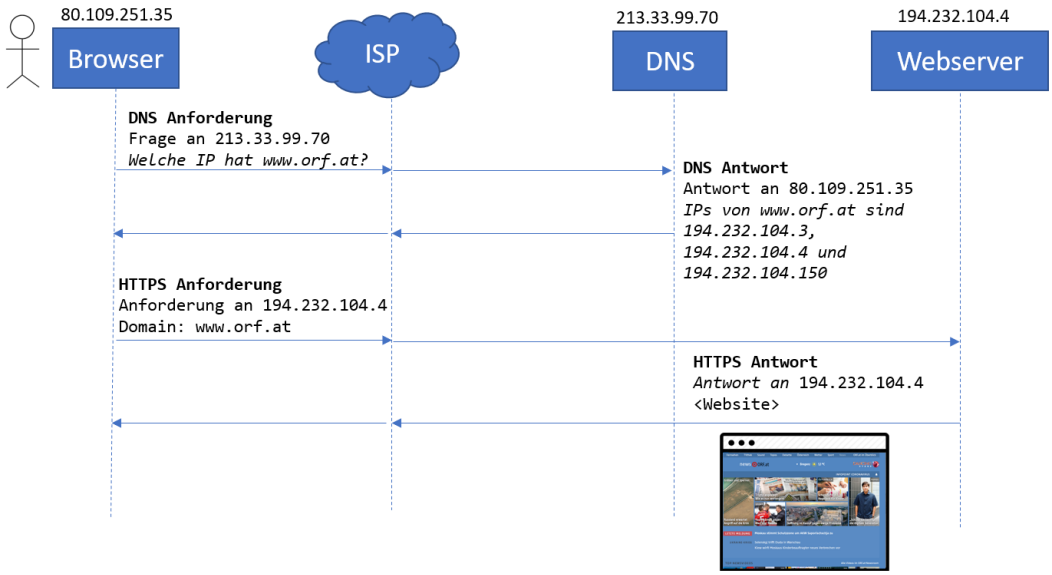

Abbildung 1: Ablauf beim Aufruf einer Website

Aus technischer Sicht ist hier zu beachten, dass zwischen IP-Adresse (wie „194.232.104.4“) und der Domain (wie „orf.at“) in keine Richtung eine eindeutige Beziehung besteht. Begründet ist dies darin, dass IP-Adresse und Domain jeweils Ausgestaltungen unterschiedlicher Komponenten des WWW sind. Weder ist es technisch notwendig, dass eine Domain genau einer IP-Adresse zugeordnet ist[6], noch ist es technisch notwendig, dass eine IP-Adresse genau zum Hosting einer einzelnen Domain verwendet wird. Dies ist auch praktisch im Beispiel erkennbar, durch den DNS-Resolver von „orf.at“ eine Liste an IP-Adressen zurückgegeben wird, wovon durch den Browser eine konkrete IP-Adresse für den Verbindungsaufbau ausgewählt wird.

Die technische Basis für eine Unterscheidung der angeforderten Domain durch einen Server bildet seit 1999 das Hypertext Transfer Protocol[7] (HTTP). Die gängigen Webserver wie „Apache“ und „nginx“ setzen diese Möglichkeit durch s.g. „Virtual Hosts“[8] bzw „Server Blocks“[9] um – es ist deshalb möglich, dass ein einzelner Server unter einer einzigen IP-Adresse eine praktisch unlimitierte Anzahl von verschiedenen Domains serviciert. Diese Domains müssen auch in keinem Zusammenhang stehen (wie etwa „orf.at“ und „news.orf.at“) – es gibt hier keine technischen Einschränkungen an die Art der Domains, die durch denselben Server bzw. dieselbe IP-Adresse bedient werden können.

Bedingt durch den oben beschriebenen Ablauf ist es für einen Dritten, etwa den Besucher einer Website, aber weder möglich, alle einer Domain zugeordneten IP-

[6] Technisch denkbar ist etwa, dass, je nach Region, unterschiedliche Server und IP-Adressen verwendet werden. Ebenfalls üblich ist, dass aus Redundanz- und Performance-Gründen ein Hostname auf mehrere IP-Adressen verteilt wird. Das ist auch im konkret gewählten Beispiel der Fall: Für die Domain “orf.at“ sind jeweils 8 IPv4-Adressen und 8 IPv6-Adressen hinterlegt. Es ist technisch aber nicht erforderlich, dass ein DNS-Server tatsächlich eine vollständige Liste der hinterlegten IP-Adressen zurücksendet.

[7] Dies ist im Standard IETF RFC 2616, 14.23 definiert: “*The Host field value MUST represent the naming authority of the origin server or gateway given by the original URL. This allows the origin server or gateway to differentiate between internally-ambiguous URLs, such as the root "/" URL of a server for multiple host names on a single IP address.*”

[8] https://httpd.apache.org/docs/2.4/de/vhosts/

[9] https://nginx.org/en/docs/http/server_names.html

Adressen aufzulisten, noch, alle unter einer IP-Adresse hinterlegten Domains abzurufen.

2.1 Wirkung einer IP-Sperre

Zur Gutachtensfrage 1.a *„Wie und wem gegenüber wirkt eine durch Anbieter von Internetzugangsdiensten eingerichtete IP-Sperre?“* lässt sich folgendes ausführen:

Wenn im Gutachtensauftrag von einer „IP-Sperre“ gesprochen wird, ist damit in diesem Kontext eine Sperre gemeint, die der Anbieter eines Internetzugangsdienstes im eigenen Netzwerk einrichtet. Grafisch ist die Position einer Sperre in Abbildung 2 dargestellt.

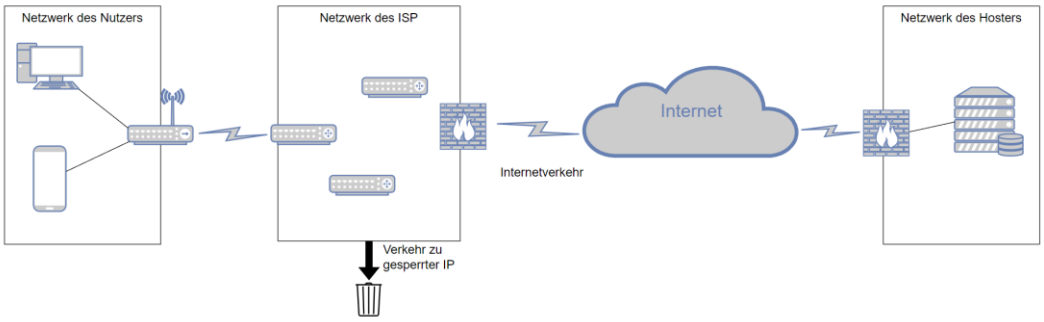

Abbildung 2: Verschiedene Netzwerke beim Aufruf einer Internetseite. Eine IP-Sperre wird im mit „Netzwerk des ISPs“ beschrifteten Segment eingerichtet, d.h. bevor der Verkehr an das öffentliche Internet übergeben wird.

Technisch wird eine IP-Sperre so umgesetzt, dass IP-Pakete, die die zu sperrende IP-Adresse als Zieladresse besitzen, vom Anbieter nicht weitergeleitet, sondern verworfen werden. Es kann deshalb keine Kommunikation mit der gesperrten Ziel-IP-Adresse aufgebaut werden.

Für Endnutzer:innen des sperrenden Anbieters bedeutet das, dass die gesperrte IP-Adresse für sie nicht mehr erreichbar ist. Auf Endnutzer:innen anderer Anbieter hat die Sperre der IP-Adresse keine Auswirkung.

Auch für die Inhaber:in der gesperrten IP-Adresse ist die ergriffene Sperre im Zweifel nicht erkennbar – die Seite hat schließlich weiterhin Besucher (anderer ISPs). Die Sperre kann deshalb für den Seiteninhaber deshalb nur indirekt daran erkannt werden, dass keine Verbindungen mehr von Nutzer:innen des sperrenden Anbieters – erkennbar am Ausbleiben von Verbindungen mit Quell-IP-Adressen aus dem Besitz des sperrenden Anbieters – eingehen.

Da sich die Sperre auf eine konkrete IP-Adresse bezieht, wirkt sie auf Ebene der IP-Verbindung. Sie ist damit nicht auf eine bestimmte Domain oder einen bestimmten Dienst beschränkt – deshalb sind alle unter dieser IP-Adresse abrufbaren Inhalte für die Endnutzer:innen des sperrenden Anbieters nicht mehr verfügbar, unabhängig davon, auf welche Art und Weise bzw. unter welcher Domain sie üblicherweise abrufbar sind. Da auf IP-Ebene blockiert wird, wirkt die Sperre grundsätzlich

gegenüber allen unter dieser IP-Adresse erreichbaren Services, d.h. neben Websites wäre etwa auch ein VoIP-Server oder ein E-Mail-Dienst geblockt.

Zur Gutachtensfrage 1.a: Eine durch einen Anbieter von Internetzugangsdiensten eingerichtete IP-Sperre wirkt gegenüber dessen Kund:innen. Verkehr zur gesperrten IP-Adresse wird nicht zugestellt.

2.2 Erfassung unter einer IP abrufbaren Inhalte

Zur Gutachtensfrage 1.c: „*Kann ein Internetzugangsdiensteanbieter pro-aktiv abschließend und umfassend erkennen, ob im Falle einer konkreten IP-Sperre auch andere Dienste mitumfasst sind?*“ ist folgendes auszuführen:

Da unter Zuhilfenahme der IP-Adresse als Adressierungselement eine Verbindung zu einem Server aufgebaut wird, entscheidet dessen Software darüber, wie mit einer eingehenden Anfrage umgegangen wird. Fungiert der Server als Webserver, kann je nach angefragter Ressource die entsprechende Datei in einer Antwort versendet werden. Läuft ein Mailserver, kann der Eingang eines Mails bestätigt werden. Läuft ein VoIP-Service, kann ein Anruf hergestellt werden. Je nach Service ist es auch möglich, dass der Server überhaupt ausschließlich dann reagiert, wenn er unter Übermittlung eines „shared secret“ aufgerufen wird.

Der Server kann auch abhängig von der IP-Adresse des Kommunikationspartners unterschiedliche Antworten versenden, und etwa Anfragen je nach geographischem Land der anfragenden IP-Adresse unterschiedlich beantworten oder in Form eines „Geoblocking“ aussperren. All diese Beispiele sollen illustrieren, dass es allein dem Server obliegt, ob und wie eine Anfrage beantwortet wird. Da der auf einem Server befindliche Programmcode bzw. die hinterlegten Regeln für Dritte nicht einsehbar ist, ist es aus technischer Sicht unmöglich, alle auf einem Server hinterlegten Funktionen aufzulisten.

Im Speziellen gilt das auch für den Fall eines Webservers: Aufgrund der Ausgestaltung von HTTP und DNS ist nicht möglich, alle unter einer IP-Adresse abrufbaren Inhalte aufzulisten. Weder ist es möglich, alle hinter einer Domain hinterlegten Inhalte abzurufen, noch ist es möglich, alle einer IP-Adressen zugeordneten Domains abzufragen. Diese Möglichkeit besteht weder für Endnutzer:innen, noch für Anbieter von Internetzugangsdiensten oder andere Dritte. Einzig der Administrator des Servers hat auch die Kontrolle und Übersicht über alle dort angebotenen Inhalte und Dienste.

Zur Gutachtensfrage 1.c: Es ist für einen Internetzugangsanbieter technisch nicht möglich, pro-aktiv abschließend und umfassend zu erkennen, ob im Fall einer konkreten IP-Sperre auch andere Dienste mitumfasst sind.

2.3 Gefahr von Overblocking bei IP-Sperren

Zur Gutachtensfrage 1.b: „*Kann es aus technischer Sicht zu „Overblocking“ kommen, wenn eine IP-Sperre durch einen Internetzugangsdiensteanbieter umgesetzt wird?*“ ist folgendes auszuführen:

Da, wie vorhin ausgeführt, nur dem Inhaber der IP-Adresse die unter dieser IP-Adresse abrufbaren Inhalte bekannt sind, kann es bei der Einrichtung einer IP-Sperre durch einen Internetzugangsdienstanbieter immer zu einem „Overblocking“ – also der Sperre von Inhalten, die nicht im Zusammenhang mit dem Grund und Inhalt der Sperre stehen – kommen. Das ist dadurch bedingt, dass es für Anbieter von Internetzugangsdiensten, wie für alle anderen Dritten, nicht möglich ist, die durch eine IP-Sperre betroffenen Inhalte vollständig zu erfassen. Insbesondere kann ein solcher Anbieter mit eigenen Mitteln nicht abschließend und umfassend erkennen, ob im Falle einer konkreten IP-Sperre auch andere Dienste umfasst sind.

Den Anbietern von Internetzugangsdiensten stehen, wie für alle anderen Nutzer:innen, nur heuristische und abschätzende Methoden zur Verfügung, um die auf einer IP-Adressen abrufbaren Inhalte zu ermitteln. Aus diesen technischen Gründen kann eine Vollständigkeit der so aufgelisteten Inhalte deshalb nie sichergestellt werden.

Zur Gutachtensfrage 1.b: Bei der Umsetzung einer IP-Sperre durch einen Internetzugangsanbieter kann es aus technischer Sicht immer zu einem „Overblocking“ kommen, da eine vollständige Ermittlung aller von einer Sperre umfassten Inhalte für einen Internetzugangsanbieter technisch nicht möglich ist.

3 Zur IP-Adresse 190.115.18.20

3.1 Inhaberschaft der IP-Adresse 190.115.18.20

Zu den Gutachtensfrage 2.a und 2.b: „*Wer ist Inhaber der IP-Adresse 190.115.18.20? Wem ist die IP-Adresse zugewiesen, wer kann aus technischer Sicht den unter einer IP-Adresse abrufbaren Inhalt bestimmen / verändern / steuern oder sonst über ihn verfügen? Wie ist die Zuordnung Hosting-Dienst bzw Content Delivery Network zur IP-Adresse?*“ lässt sich folgendes ausführen:

Die Verwaltung von IP-Adressen weltweit obliegt der „Internet Assigned Numbers Authority“ (IANA). Dazu greift sie auf regionale Organisationen zurück, in Europa etwa die RIPE NCC[10]. Auf der von der IANA veröffentlichten Zuteilungsliste[11] ist sichtbar, dass für den IP-Adressraum von 190.X.X.X seit 1995 die regionale Organisation „Latin America and Caribbean Network Information Centre“ (LACNIC) zuständig ist, siehe Abbildung 3.

188/8	Administered by RIPE NCC	1993-05	whois.ripe.net	https://rdap.db.ripe.net/	LEGACY
189/8	LACNIC	1995-06	whois.lacnic.net	https://rdap.lacnic.net/rdap/	ALLOCATED
190/8	LACNIC	1995-06	whois.lacnic.net	https://rdap.lacnic.net/rdap/	ALLOCATED
191/8	Administered by LACNIC	1993-05	whois.lacnic.net	https://rdap.lacnic.net/rdap/	LEGACY

Abbildung 3: Screenshot der Zuteilungsliste der IANA

Eine Abfrage beim WHOIS-Service[12] der LACNIC zeigt, dass der IP-Adressbereich von 190.115.16.0 bis 190.115.31.255, der auch die verfahrensgegenständliche IP-Adresse 190.115.18.20 beinhaltet, dem Content Delivery Network und Hosting-Dienstleister „DDoS-Guard“ zugeordnet ist, siehe unten:

```
whois 190.115.18.20
% IP Client: 213.47.207.178

% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2023-02-17 06:45:33 (-03 -03:00)

inetnum:     190.115.16.0/20
status:      allocated
aut-num:     AS262254
owner:       DDOS-GUARD CORP.
ownerid:     BZ-DALT-LACNIC
responsible: Evgeniy Marchenko
```

[10] https://www.ripe.net/
[11] http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml
[12] https://query.milacnic.lacnic.net/search?id=190.115.18.20

```
address:     Suite 102, Ground Floor, Blake Building, Corner Eyre
     Hutson Streets, 0, -
address:     - - Belize - BZ
country:     BZ
phone:       +7  9282797045 [0000]
owner-c:     EVM3
tech-c:      EVM3
abuse-c:     EVM3
inetrev:     190.115.16.0/24
nserver:     NS1.DDOS-GUARD.NET
nsstat:      20230212 AA
nslastaa:    20230212
                              […][13]
nserver:     NS5.DDOS-GUARD.NET
nsstat:      20230216 AA
nslastaa:    20230216
created:     20130627
changed:     20210202

nic-hdl:     EVM3
person:      Evgeniy Marchenko
e-mail:      e.marchenko@ddos-guard.net
address:     1 2 Miles Northern Highway Belize City Belize, 12, -
address:     0000 - Belize -
country:     BZ
phone:       +55 11 46733474 [0000]
created:     20121102
changed:     20220320

% whois.lacnic.net accepts only direct match queries.
% Types of queries are: POCs, ownerid, CIDR blocks, IP
% and AS numbers.
```

Eine WHOIS-Abfrage der „Autonomous System Number“ (ASN, in der obigen Ausgabe „aut-num“) von DDoS-Guard zeigt den weiteren zugeteilten IPv4-Bereich 186.2.160.1 - 186.2.175.254 sowie den IPv6-Bereich 2803:f900:0000:0000:0000:0000:0000:0000 - 2803:f900:ffff:ffff:ffff:ffff:ffff:ffff.

```
whois AS262254
% IP Client: 213.47.207.178

% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2023-03-15 10:28:20 (-03 -03:00)
```

[13] Antwort um Auflistung von Nameservern gekürzt.

```
aut-num:     AS262254
owner:       DDOS-GUARD CORP.
ownerid:     BZ-DALT-LACNIC
responsible: Evgeniy Marchenko
address:      Suite 102, Ground Floor, Blake Building, Corner Eyre
     Hutson Streets, 0, -
address:     - - Belize - BZ
country:     BZ
phone:       +7  9282797045 [0000]
owner-c:     EVM3
routing-c:   EVM3
abuse-c:     EVM3
created:     20121205
changed:     20210202
inetnum:     190.115.16.0/20
inetnum:     2803:f900::/32
inetnum:     186.2.160.0/20

nic-hdl:     EVM3
person:      Evgeniy Marchenko
e-mail:      e.marchenko@ddos-guard.net
address:     1 2 Miles Northern Highway Belize City Belize, 12, -
address:     0000 - Belize -
country:     BZ
phone:       +55 11 46733474 [0000]
created:     20121102
changed:     20220320

% whois.lacnic.net accepts only direct match queries.
% Types of queries are: POCs, ownerid, CIDR blocks, IP
% and AS numbers.
```

Die IP-Adresse 190.115.18.20 ist bei der LANIC demnach dem Hosting-Dienst „DDoS-Guard“ zugewiesen. Die Steuerung des Inhalts unter der IP-Adresse 190.115.18.20 ist damit technisch gesehen nur für DDoS-Guard möglich. Es ist aber anzunehmen, dass DDoS-Guard hier als Hosting-Anbieter agiert und Inhalte im Auftrag seiner Kunden speichert bzw. zur Verfügung stellt. Der abrufbare Inhalt wird dabei durch einen Kunden von DDoS-Guard bereitgestellt, ohne dass der Kunde selbst bei der LANIC als Inhaber der IP-Adresse eingetragen wird.

Dieses bei Hosting-Dienstleistern übliche Vorgehen verfolgen auch österreichische Hoster wie easyname, world4you, hosttech, und Cloud-Anbieter wie Azure, AWS, Cloudflare und Akamai. Die faktische Verfügungsgewalt über die unter der IP-Adresse abrufbaren Inhalte hat demnach wahrscheinlich ein (nicht offengelegte) Kunde von DDoS-Guard. Es ist auch möglich, dass sich mehrere verschiedene Kunden eine einzelne IP-Adresse teilen. Trotz diese Kundenbeziehung bleibt DDoS-Guard aus technischer Sicht Inhaber der IP-Adresse und könnte die Kundenzuordnung jederzeit ändern oder kündigen.

Zu den Gutachtensfrage 2.a und 2.b: Die IP-Adresse 190.115.18.20 ist dem Hosting-Dienst bzw Content Delivery Network „DDoS-Guard“ zugewiesen. DDoS-Guard, bzw.

dessen Kunde, kann aus technischer Sicht den unter dieser IP-Adresse abrufbaren Inhalt bestimmen/verändern/steuern.

3.2 Inhalte der IP-Adresse 190.115.18.20

Zu den miteinander in Verbindung stehenden Gutachtensfrage 2.c *„Welche verschiedenen Inhalte lassen sich unter dieser IP-Adresse abrufen? Wie kann dies aus technischer Sicht festgestellt werden?*“, 2.d *„Ist es aus technischer Sicht möglich, alle unter einer IP-Adresse abrufbaren Inhalte aufzulisten? Ist es für einen Internetzugangsdiensteanbieter möglich, alle abrufbaren Inhalte zu erkennen?*“, 2.e *„Sollte sich der Inhaber einer IP-Adresse verändern, wäre auch der neue Inhaber durch eine bestehende IP-Sperre betroffen?*“ und 2.f *„Sollte sich der unter der IP-Adresse bereitgestellte Inhalt verändern, wären auch Inhalte dieser neuen Angebote durch die bestehende IP-Sperre betroffen?*“ kann folgendes erörtert werden:

Wie oben angeführt, hat lediglich der Inhaber der IP-Adresse, DDoS-Guard, bzw., dessen Kunde, eine vollständige Übersicht und Kontrolle über die unter der IP-Adresse bereitgestellten Inhalte. Für dieses Gutachten kann deshalb nur auf Hilfsmittel zurückgegriffen werden, die eine überblicksmäßige Auflistung der Inhalte ermöglichen, aber aus technischer Sicht keine Vollständigkeit sicherstellen können.

Zur Methodik sei angeführt, dass alle Abfragen unter Verwendung eines Virtual Private Network („VPN“, siehe Kapitel 4.2) durchgeführt wurden. Damit kann ausgeschlossen werden, dass etwaig in Österreich eingerichtete IP-Sperren die Abfrageergebnisse verzerren. Als VPN-Anbieter wurde der VPN-Dienst des Browser-Herstellers „Mozilla“ verwendet.[14]

Bei einem Aufruf der IP-Adresse wird folgende Website angezeigt:

[14] https://www.mozilla.org/de/products/vpn/

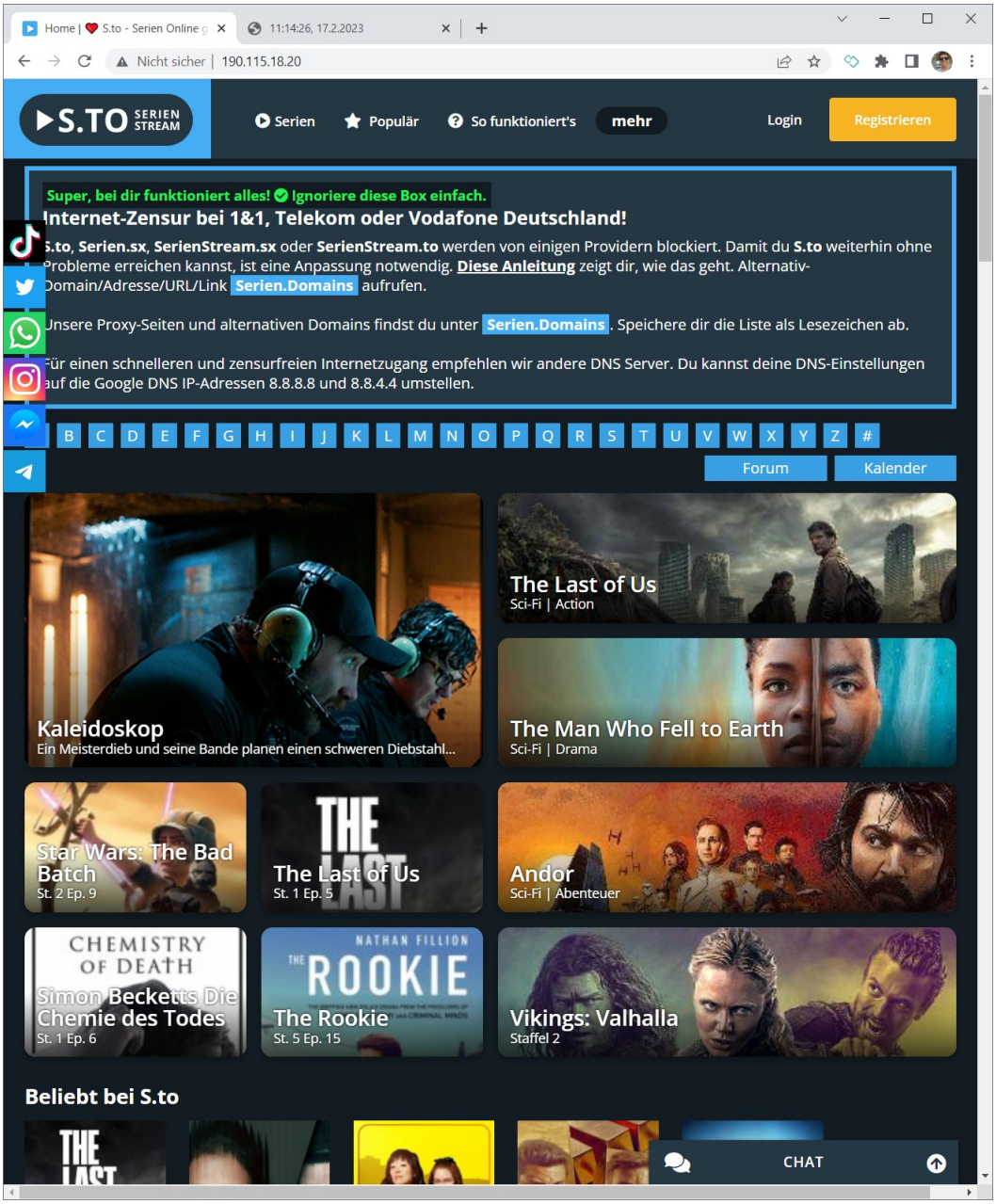

Abbildung 4: Direktaufruf der IP-Adresse 190.115.18.20

Die Website wurde am 17.2.2023 um 11:14 Uhr abgerufen. Die Metainformationen der HTTP-Antwort des Servers wurden mittels der Standard-Software „cURL“[15] abgefragt und sind unten angeführt.

```
curl -vv --head -L http://190.115.18.20/


*   Trying 190.115.18.20:80...
* TCP_NODELAY set
* Connected to 190.115.18.20 (190.115.18.20) port 80 (#0)
> HEAD / HTTP/1.1
> Host: 190.115.18.20
```

[15] https://github.com/curl/curl

```
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
HTTP/1.1 200 OK
< Server: ddos-guard
Server: ddos-guard
< Connection: keep-alive
Connection: keep-alive
< Keep-Alive: timeout=60
Keep-Alive: timeout=60
<    Set-Cookie:    __ddg1_=wF5CQsL7bc9f2fmWhOpl;    Domain=.18.20;
     HttpOnly; Path=/; Expires=Sat, 17-Feb-2024 10:16:43 GMT
Set-Cookie: __ddg1_=wF5CQsL7bc9f2fmWhOpl; Domain=.18.20; HttpOnly;
     Path=/; Expires=Sat, 17-Feb-2024 10:16:43 GMT
< Date: Fri, 17 Feb 2023 10:16:43 GMT
Date: Fri, 17 Feb 2023 10:16:43 GMT
< Content-Type: text/html; charset=UTF-8
Content-Type: text/html; charset=UTF-8
< Vary: Accept-Encoding
Vary: Accept-Encoding
< Vary: Accept-Encoding
Vary: Accept-Encoding
< Set-Cookie: PHPSESSID=bp32iape8h28pmnqh702tsrouo; path=/
Set-Cookie: PHPSESSID=bp32iape8h28pmnqh702tsrouo; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-store, no-cache, must-revalidate
< Pragma: no-cache
Pragma: no-cache
```

Auch dieser Aufruf legt nahe, dass der Server selbst von DDoS-Guard betrieben wird. Ersichtlich ist dies aus dem „Server“-HTTP-Header, der mit „ddos-guard“ ausgefüllt wird.

Ansonsten gibt es weder aus der Antwort noch aus der Website selbst direkte Verweise auf andere unter dieser IP-Adresse gehostete Inhalte. Die abgerufene Website selbst bezeichnet sich als „s.to“ und verweist auch auf „serien.domains“. Beide dieser Domains verweisen allerdings auf andere IP-Adressen. Aus technischer Sicht anzumerken ist, dass, zumindest stichprobenweise, abrufbare Videos nicht unmittelbar von der IP-Adresse bereitgestellt werden, sondern die Website hier auf die Dienste von Videostreaming-Anbietern zurückgreift. Die Website selbst weist pro verfügbarem Stream unterschiedliche Anbieter aus (s. Abbildung 5). Die exemplarisch hier angeführten Anbieter sind voe.sx, dood.la, vidoza.net und streamtape.com. Der eigentliche Stream erfolgt dann von deren Servern, ist aber mittels eines „iFrames“ in die verfahrensgegenständliche Seite integriert.

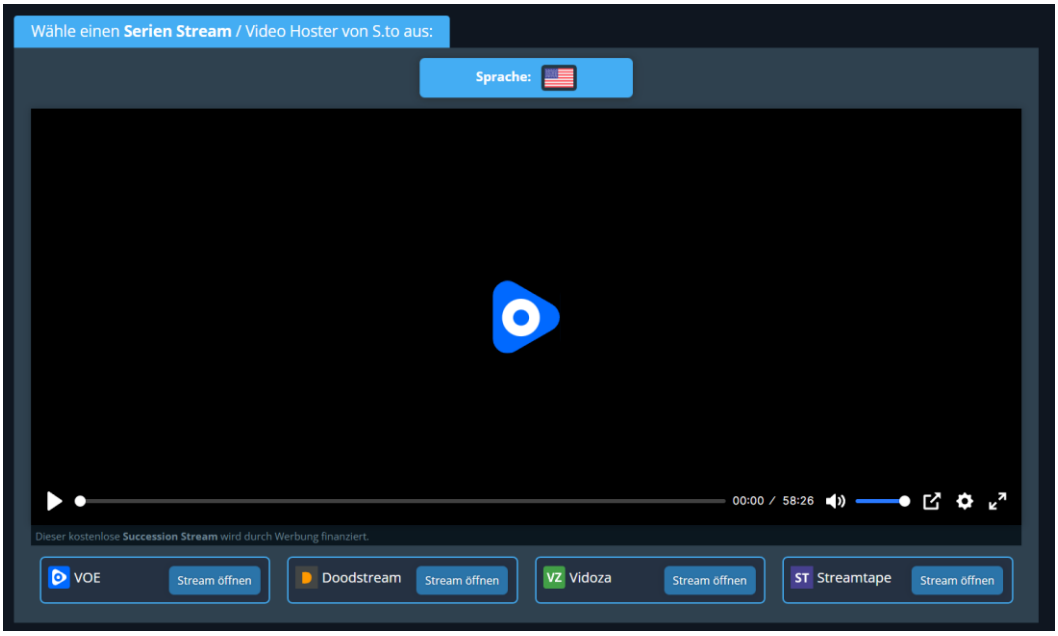

Abbildung 5: "Anbieterauswahl" eines exemplarischen Streams.

Eine DNS-Abfrage der angeführten Domains („s.to“ und „serien.domains“) ergibt für „s.to“:

```
dig s.to

; <<>> DiG 9.16.1-Ubuntu <<>> s.to
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57554
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL:
     1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 89ff3ef8ebb89f8e01ea49a063ef5749c7a8bddb10040105 (good)
;; QUESTION SECTION:
;s.to.                          IN      A

;; ANSWER SECTION:
s.to.                   143     IN      A       186.2.163.237

;; AUTHORITY SECTION:
s.to.                36792   IN      NS      jack.ns.cloudflare.com.
s.to.                36792   IN      NS      megan.ns.cloudflare.com.

;; Query time: 8 msec
;; SERVER: 10.64.0.1#53(10.64.0.1)
;; WHEN: Fri Feb 17 11:30:31 CET 2023
;; MSG SIZE  rcvd: 133
```

Die zugehörige „cURL“-Abfrage für „s.to“ ergibt:

```
curl -vv --head -L s.to
```

```
*   Trying 186.2.163.237:80...
* TCP_NODELAY set
* Connected to s.to (186.2.163.237) port 80 (#0)
> HEAD / HTTP/1.1
> Host: s.to
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 301 Moved Permanently
HTTP/1.1 301 Moved Permanently
< Server: ddos-guard
Server: ddos-guard
< Date: Fri, 17 Feb 2023 10:31:16 GMT
Date: Fri, 17 Feb 2023 10:31:16 GMT
< Connection: keep-alive
Connection: keep-alive
< Keep-Alive: timeout=60
Keep-Alive: timeout=60
< Location: https://s.to/
Location: https://s.to/

<
* Connection #0 to host s.to left intact
* Clear auth, redirects to port from 80 to 443Issue another request
     to this URL: 'https://s.to/'
*   Trying 186.2.163.237:443...
* TCP_NODELAY set
* Connected to s.to (186.2.163.237) port 443 (#1)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: /etc/ssl/certs
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_128_GCM_SHA256
* ALPN, server accepted to use h2
* Server certificate:
*  subject: CN=s.to
*  start date: Jan 31 19:42:06 2023 GMT
*  expire date: May  1 19:42:05 2023 GMT
*  subjectAltName: host "s.to" matched cert's "s.to"
*  issuer: C=US; O=Let's Encrypt; CN=R3
*  SSL certificate verify ok.
* Using HTTP2, server supports multi-use
* Connection state changed (HTTP/2 confirmed)
* Copying HTTP/2 data in stream buffer to connection buffer after
     upgrade: len=0
* Using Stream ID: 1 (easy handle 0x7fffe72f18c0)
> HEAD / HTTP/2
> Host: s.to
```

```
> user-agent: curl/7.68.0
> accept: */*
>
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* old SSL session ID is stale, removing
* Connection state changed (MAX_CONCURRENT_STREAMS == 8)!
< HTTP/2 200
HTTP/2 200
< server: ddos-guard
server: ddos-guard
< strict-transport-security: max-age=31536000
strict-transport-security: max-age=31536000
< content-security-policy: upgrade-insecure-requests;
content-security-policy: upgrade-insecure-requests;
< set-cookie: __ddg1_=XoCmXhpJqwLnC4P7z6JI; Domain=.s.to; HttpOnly;
     Path=/; Expires=Sat, 17-Feb-2024 10:31:16 GMT
set-cookie:  __ddg1_=XoCmXhpJqwLnC4P7z6JI;  Domain=.s.to;  HttpOnly;
     Path=/; Expires=Sat, 17-Feb-2024 10:31:16 GMT
< date: Fri, 17 Feb 2023 10:31:16 GMT
date: Fri, 17 Feb 2023 10:31:16 GMT
< content-type: text/html; charset=UTF-8
content-type: text/html; charset=UTF-8
< vary: Accept-Encoding
vary: Accept-Encoding
< set-cookie: PHPSESSID=vds2bmtt01msrap4v75uch5cba; path=/
set-cookie: PHPSESSID=vds2bmtt01msrap4v75uch5cba; path=/
< expires: Thu, 19 Nov 1981 08:52:00 GMT
expires: Thu, 19 Nov 1981 08:52:00 GMT
< cache-control: no-store, no-cache, must-revalidate
cache-control: no-store, no-cache, must-revalidate
< pragma: no-cache
pragma: no-cache
```

Für „serien.domains”:

```
dig A serien.domains

; <<>> DiG 9.16.1-Ubuntu <<>> A serien.domains
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48039
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL:
     7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 0890402486c50746bfa197f263ef57b2558ae7cfaf57fef0 (good)
;; QUESTION SECTION:
;serien.domains.                        IN      A

;; ANSWER SECTION:
serien.domains.         46      IN      A       104.21.94.207
serien.domains.         46      IN      A       172.67.140.12

;; AUTHORITY SECTION:
```

```
serien.domains.        2383    IN      NS      jim.ns.cloudflare.com.
serien.domains.       2383    IN      NS      rayne.ns.cloudflare.com.

;; ADDITIONAL SECTION:
jim.ns.cloudflare.com.  1235    IN      A       172.64.33.125
jim.ns.cloudflare.com.  1235    IN      A       173.245.59.125
jim.ns.cloudflare.com.  1235    IN      A       108.162.193.125
jim.ns.cloudflare.com.      1235            IN                  AAAA
     2a06:98c1:50::ac40:217d
jim.ns.cloudflare.com.      1235            IN                  AAAA
     2606:4700:58::adf5:3b7d
jim.ns.cloudflare.com.      1235            IN                  AAAA
     2803:f800:50::6ca2:c17d
```

Die zugehörige “cURL“-Abfrage für „serien.domains“:

```
curl -vv --head -L serien.domains
*   Trying 172.67.140.12:80...
* TCP_NODELAY set
* Connected to serien.domains (172.67.140.12) port 80 (#0)
> HEAD / HTTP/1.1
> Host: serien.domains
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
HTTP/1.1 200 OK
< Date: Fri, 17 Feb 2023 10:31:55 GMT
Date: Fri, 17 Feb 2023 10:31:55 GMT
< Content-Type: text/html
Content-Type: text/html
< Connection: keep-alive
Connection: keep-alive
< Last-Modified: Sat, 15 Oct 2022 12:45:36 GMT
Last-Modified: Sat, 15 Oct 2022 12:45:36 GMT
< Vary: Accept-Encoding
Vary: Accept-Encoding
< Expires: Fri, 17 Feb 2023 14:12:42 GMT
Expires: Fri, 17 Feb 2023 14:12:42 GMT
< Cache-Control: max-age=21600
Cache-Control: max-age=21600
< CF-Cache-Status: HIT
CF-Cache-Status: HIT
< Age: 8353
Age: 8353
<                                                       Report-To:
     {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\
     /v3?s=uK8PKGzK%2B%2FU4dhatylFZ6GGpAndnxgnArsq%2BwMmlbvukA1VVC
     m9p2%2F9D7f3l5r1kWC7l3xiFZSXpoaeAThiuns3yjyiJVO5IRFRi0diqFMAk
     ZSdQhNlBMf41moYkjfhvpw%3D%3D"}],"group":"cf-
     nel","max_age":604800}
Report-To:
     {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\
     /v3?s=uK8PKGzK%2B%2FU4dhatylFZ6GGpAndnxgnArsq%2BwMmlbvukA1VVC
     m9p2%2F9D7f3l5r1kWC7l3xiFZSXpoaeAThiuns3yjyiJVO5IRFRi0diqFMAk
```

```
     ZSdQhNlBMf41moYkjfhvpw%3D%3D"}],"group":"cf-
     nel","max_age":604800}
<            NEL:           {"success_fraction":0,"report_to":"cf-
     nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
< Server: cloudflare
Server: cloudflare
< CF-RAY: 79addb2a9f027809-VIE
CF-RAY: 79addb2a9f027809-VIE
< alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
```

Es zeigt sich demnach, dass „s.to“ selbst auf einer anderen IP-Adresse abrufbar ist (186.2.163.237, Abbildung 6). Diese wird ebenfalls von DDoS-Guard betrieben, wie aus der Serverantwort ersichtlich ist (Abbildung 7). Was dabei beachtenswert scheint ist, dass bei einem Direktaufruf dieser IP-Adresse eine Fehlermeldung von DDoS-Guard zurückgegeben wird. Dies unterscheidet sich von der verfahrensgegenständlichen IP-Adresse 190.115.18.20, die unmittelbar auch bei einem Direktaufruf einen Inhalt zurückliefert.

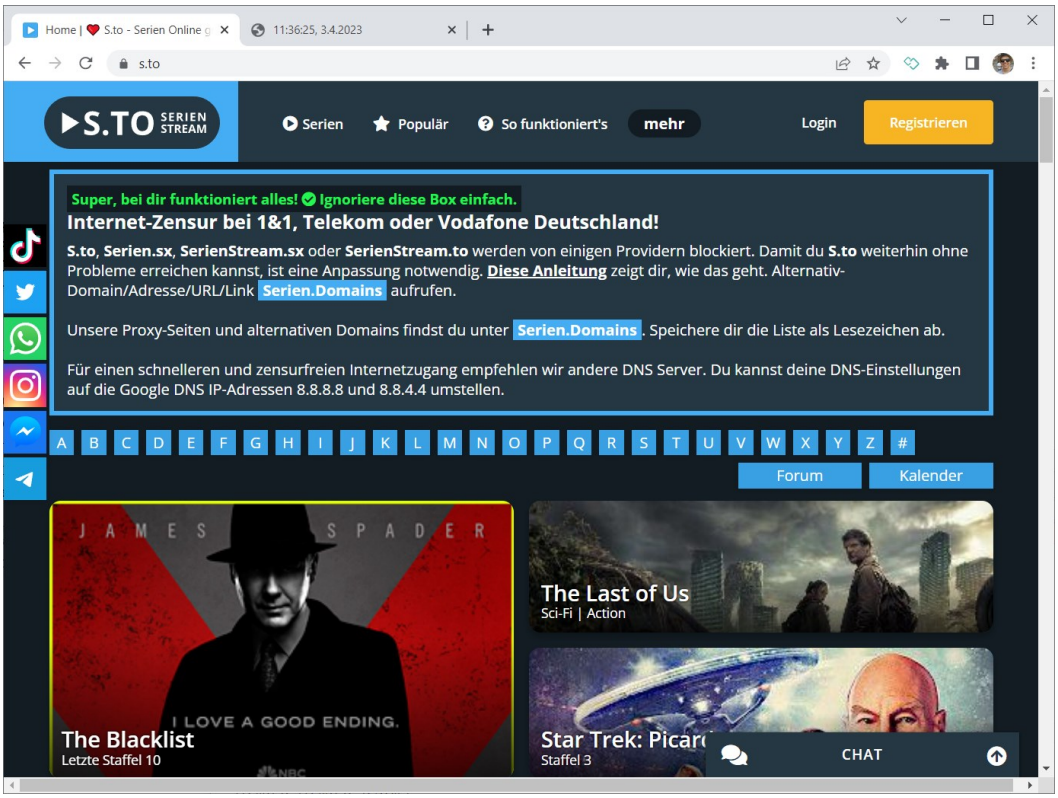

Abbildung 6: s.to unter der IP-Adresse 186.2.163.237

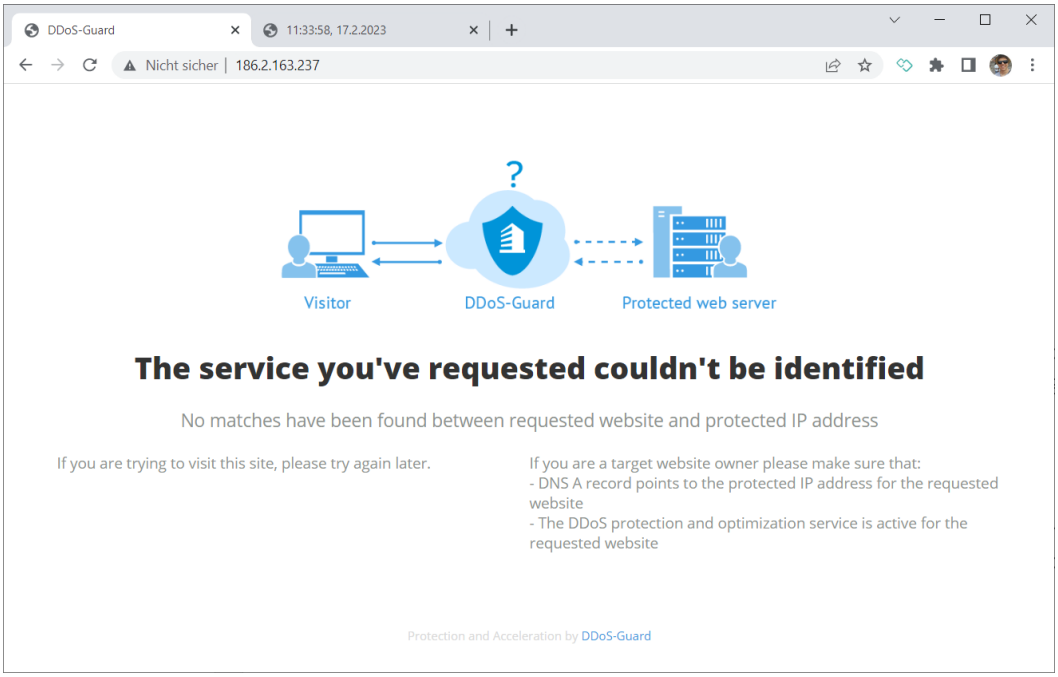

Abbildung 7: s.to IP-Adresse

DDoS-Guard bietet als Hosting-Anbieter eine breite Produktpalette an. So enthält beispielsweise das Produkt „Website DDoS Protection“[16] verschieden teure Abo-Modelle, die sich in der Anzahl der verwaltbaren Domains als auch in der Zuweisung einer dedizierten IP-Adresse unterscheiden. Abgesehen vom billigsten Paket werben alle mit einer dedizierten IP-Adresse. Neben diesem Produkt bietet DDoS-Guard auch verschiedene Hosting- und Server-Produkte an, die zum Teil mit dezidierten IP-Adressen werben (siehe Abbildung 8). Die verschiedene Antwort bei Direktaufruf von IP-Adressen von DDoS-Guard (186.2.163.237, 190.115.18.20) könnte deshalb in unterschiedlichen zu Grunde liegenden Produkten begründet sein. Eine Zuordnung ist aber im Rahmen dieses Gutachtens nicht möglich.

[16] https://ddos-guard.net/en/store/web

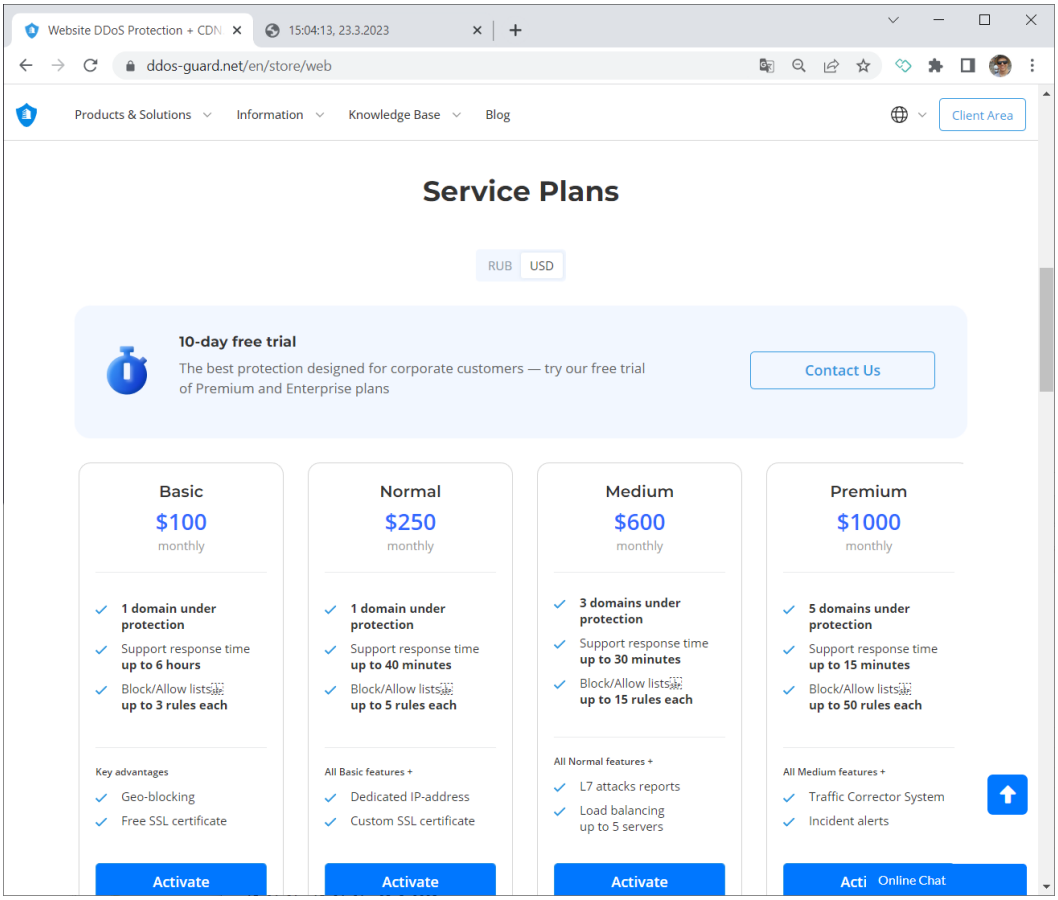

Abbildung 8: Verschiedene von DDoS-Guard angebotene Tarifpakete.

Die Tatsache, dass die DNS-Konfiguration (ersichtlich am „Nameserver“-Eintrag von s.to und serien.domains) selbst vom CDN-Anbieter „Cloudflare“ betrieben wird, erscheint beachtenswert und deutet darauf hin, dass unter Umständen ein Wechsel zu oder von Cloudflare stattgefunden hat. Die verlinkte Seite „serien.domains“ selbst wird auch bei Cloudflare gehostet, wie an der oben angeführten „cURL“-Abfrage ersichtlich ist.

Zurückkommend zur verfahrensgegenständlichen IP-Adresse 190.115.18.20 existieren noch weitere Methoden, um Inhalte einer Domain zuzuordnen. Eine solche Methode, IP-Adressen einer Domain zuzuordnen, ist für die IP-Adresse einen „Pointer“-Eintrag für Reverse-DNS-Abfragen zu hinterlegen, der eine solche Abfrage ermöglicht. Diese Möglichkeit hat jeweils der über die IP-Adresse Verfügende. Für die Abfrage besteht die „in-addr.arpa“-Zone, als deren Subdomains die gewünschte IP-Adresse in umgekehrter Reihenfolge vorangestellt wird.

Dies kann grundsätzlich etwa für die Domain „www.rtr.at“ veranschaulicht werden: Für die IP von „www.rtr.at“, 81.16.157.3, wäre das demnach etwa 3.157.16.81.in-addr.arpa. Unten angeführt ist dann etwa sichtbar, dass als Domain der IP-Adresse der „PTR“ „www.rtr.at“ hinterlegt ist.

```
dig 3.157.16.81.in-addr.arpa PTR

; <<>> DiG 9.16.1-Ubuntu <<>> 3.157.16.81.in-addr.arpa PTR
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45813
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL:
     1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: be437f71d564fb9cd8ada66463ef7b069fc4f53ea4d3b4ec (good)
;; QUESTION SECTION:
;3.157.16.81.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
3.157.16.81.in-addr.arpa. 172256 IN     PTR     www.rtr.at.

;; AUTHORITY SECTION:
157.16.81.in-addr.arpa. 85856   IN      NS      ns5.rtr.at.
157.16.81.in-addr.arpa. 85856   IN      NS      ns1.rtr.at.

;; Query time: 8 msec
;; SERVER: 10.64.0.1#53(10.64.0.1)
;; WHEN: Fri Feb 17 14:03:00 CET 2023
;; MSG SIZE  rcvd: 141
```

Angewandt auf die gegenständliche IP-Adresse 190.115.18.20 führt dies zu folgendem Ergebnis:

```
dig 20.18.115.190.in-addr.arpa PTR

; <<>> DiG 9.16.1-Ubuntu <<>> 20.18.115.190.in-addr.arpa PTR
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58858
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL:
     1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7fb05c8b7ec52d66fe56c12863ef7beb3125f027c4388354 (good)
;; QUESTION SECTION:
;20.18.115.190.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
20.18.115.190.in-addr.arpa. 3591 IN     PTR     mail.ico-capital.io.

;; AUTHORITY SECTION:
18.115.190.in-addr.arpa. 77797  IN      NS      NS4.DDOS-GUARD.NET.
18.115.190.in-addr.arpa. 77797  IN      NS      NS1.DDOS-GUARD.NET.
18.115.190.in-addr.arpa. 77797  IN      NS      NS5.DDOS-GUARD.NET.
18.115.190.in-addr.arpa. 77797  IN      NS      NS3.DDOS-GUARD.NET.
18.115.190.in-addr.arpa. 77797  IN      NS      NS2.DDOS-GUARD.NET.

;; Query time: 12 msec
```

```
;; SERVER: 10.64.0.1#53(10.64.0.1)
;; WHEN: Fri Feb 17 14:06:49 CET 2023
;; MSG SIZE  rcvd: 220
```

Diese Abfrage liefert demnach, dass die Domain „mail.ico-capital.io“ der IP-Adresse zugeordnet sei. Gleichzeitig zeigt sich allerdings, dass die Domain „ico-capital.io“ nicht vergeben ist und vielmehr aktuell zum Verkauf stehe, wie unterhalb in der „whois“-Abfrage und exemplarisch im Screenshot eines Domainhändlers (Abbildung 9) abgebildet.

```
whois ico-capital.io
Domain not found.
>>> Last update of WHOIS database: 2023-02-17T13:09:13Z <<<
```

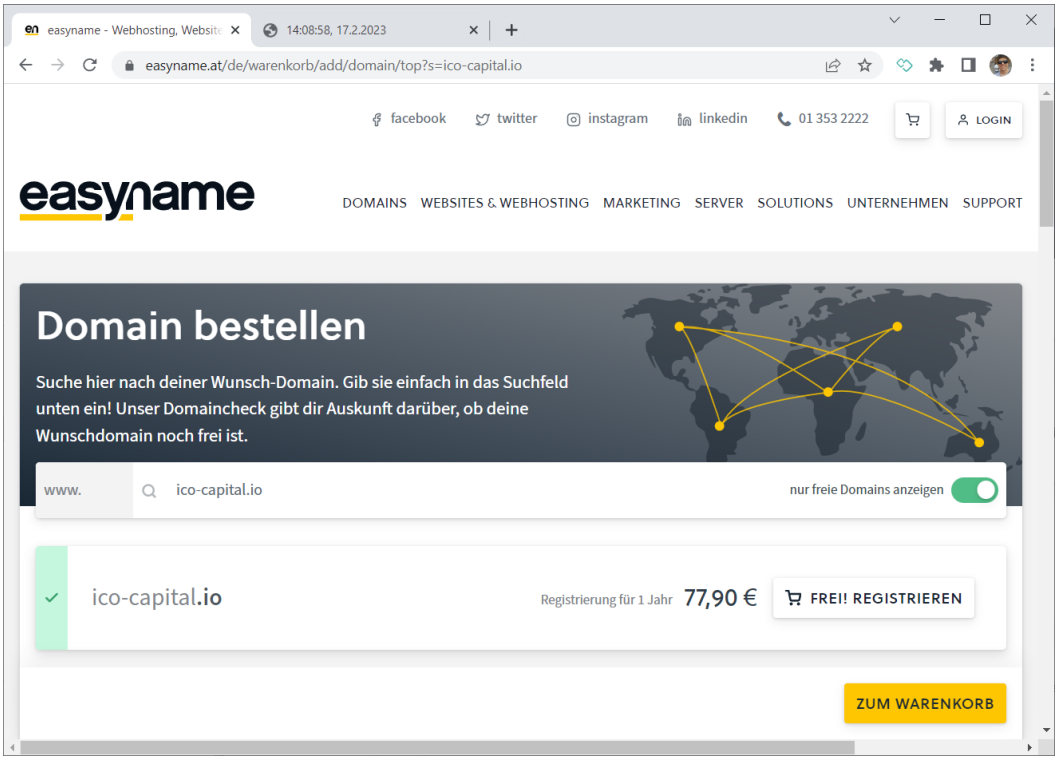

Abbildung 9: Ein Domainhändler weist die Domain ico-capital.io als verfügbar aus.

Während der „PTR“-Record dementsprechend keine weiteren Hinweise auf andere gehostete Inhalte liefert, scheint er als Indiz, dass die IP-Adresse historisch zum Hosting von anderen Inhalten verwendet wurde, oder, dass der PTR-Record vom Inhaber der IP, DDoS-Guard, falsch konfiguriert wurde.

Eine weitere Möglichkeit zur heuristischen Auflistung der unter der IP-Adresse abrufbaren Inhalte ist es, auf Webdienste zurückzugreifen. So existieren Dienste, die in regelmäßigen Abständen das Internet durchsuchen („crawlen“) und die aufgefundenen Domains zu den verbundenen IP-Adressen auflösen und diese Zuordnung speichern. Diese im Laufe der Zeit zusammengetragene Datenbasis wird anschließend als Dienstleistung verkauft. Diese Methode bedingt, dass es nie möglich

ist, tatsächlich alle unter einer IP-Adresse abrufbaren Inhalte aufzulisten, da nur Domains abgebildet werden, die im Zuge eines Crawlings aufgefunden werden. Insbesondere hinsichtlich neuer Domains und wenig verbreiteten bzw. verlinkten Websites liefert sie deshalb unvollständige Ergebnisse. Aber sie bietet einen gewissen Überblick.

Ein „Reverse IP Lookup“ der IP-Adresse beim Dienstleister „DomainTools“ (Abbildung 10, https://reverseip.domaintools.com/search/?q=190.115.18.20) listet „internet-lexikon.biz“ sowie „tradinginsight.ai“ als auf derselben IP befindlich auf.

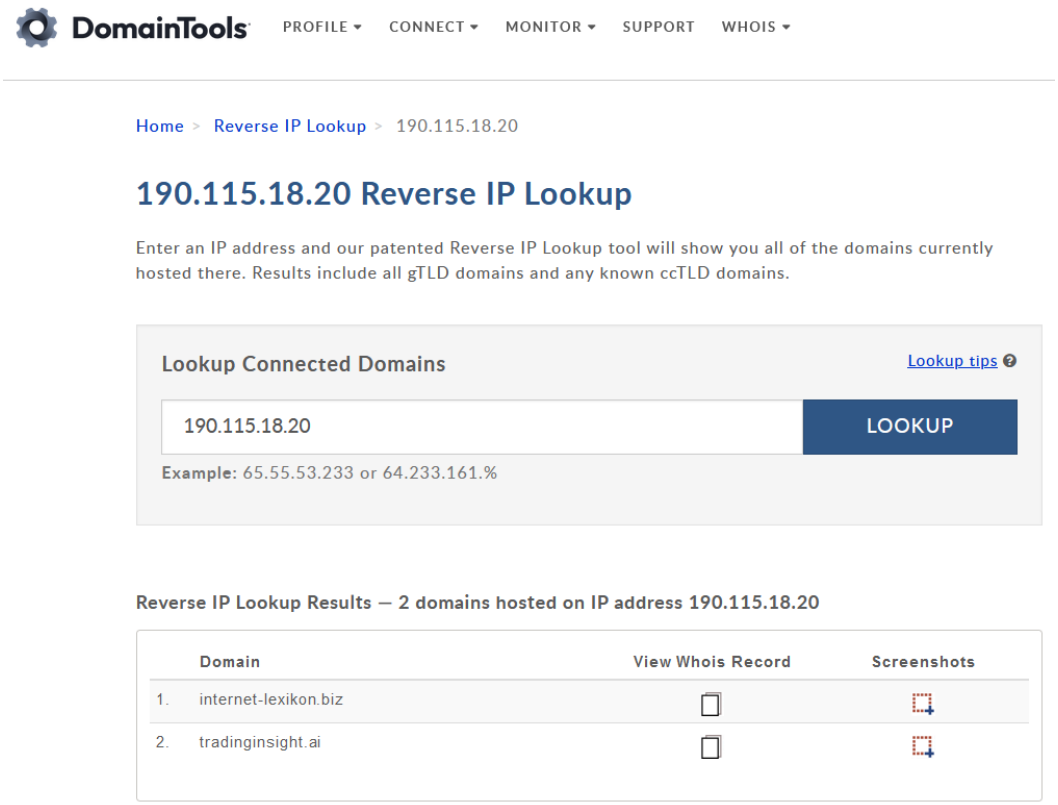

Abbildung 10 Reverse IP Lookup bei DomainTools

Beides kann auch mit einer DNS-Abfrage verifiziert werden. Sowohl für „internet-lexikon.biz“:

```
dig internet-lexikon.biz A

; <<>> DiG 9.16.1-Ubuntu <<>> internet-lexikon.biz A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17647
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL:
     1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
```

```
; COOKIE: cd3749e8a3c4a6daf64fc45b63ef8192ed6e8cb75e15c039 (good)
;; QUESTION SECTION:
;internet-lexikon.biz.          IN      A

;; ANSWER SECTION:
internet-lexikon.biz.   1799    IN      A       190.115.18.20

;; AUTHORITY SECTION:
internet-lexikon.biz.    3600     IN       NS       dns2.registrar-
     servers.com.
internet-lexikon.biz.    3600     IN       NS       dns1.registrar-
     servers.com.

;; Query time: 200 msec
;; SERVER: 10.64.0.1#53(10.64.0.1)
;; WHEN: Fri Feb 17 14:30:57 CET 2023
;; MSG SIZE  rcvd: 152
```

Als auch für „tradinginsight.ai“:

```
dig tradinginsight.ai A

; <<>> DiG 9.16.1-Ubuntu <<>> tradinginsight.ai A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46377
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL:
     1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d0278eced986fcfbb071eb2363ef81deb6f5996d6edf4bc8 (good)
;; QUESTION SECTION:
;tradinginsight.ai.             IN      A

;; ANSWER SECTION:
tradinginsight.ai.      1799    IN      A       190.115.18.20

;; AUTHORITY SECTION:
tradinginsight.ai.       86400    IN       NS       dns1.registrar-
     servers.com.
tradinginsight.ai.       86400    IN       NS       dns2.registrar-
     servers.com.

;; Query time: 37 msec
;; SERVER: 10.64.0.1#53(10.64.0.1)
;; WHEN: Fri Feb 17 14:32:13 CET 2023
;; MSG SIZE  rcvd: 149
```

Die WHOIS-Auskünfte beider Domains liefern keine weiteren Informationen zum Inhaber. Sie sind nachfolgend für beide der Domains angeführt.

```
> whois tradinginsight.ai
Domain Name: tradinginsight.ai
```

```
Registry Domain ID: 1164796_nic_ai
Registry WHOIS Server: whois.nic.ai
Creation Date: 2021-03-05T12:11:38.322Z
Registrar: Namecheap
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Registry RegistrantID: 8thXc-hrs6V
RegistrantName: Redacted for Privacy
RegistrantOrganization: Privacy service provided by Withheld for
     Privacy ehf
RegistrantStreet: Kalkofnsvegur 2
RegistrantCity: Reykjavik
RegistrantState/Province: Capital Region
RegistrantPostal Code: 101
RegistrantCountry: IS
RegistrantPhone: +354.4212434
RegistrantEmail:
     c45fb3e1ea3344c49f8eda3ffb6e25d3.protect@withheldforprivacy.c
     om
Registry AdminID: EWu4j-jTvTl
AdminName: Redacted for Privacy
AdminOrganization: Privacy service provided by Withheld for Privacy
     ehf
AdminStreet: Kalkofnsvegur 2
AdminCity: Reykjavik
AdminState/Province: Capital Region
AdminPostal Code: 101
AdminCountry: IS
AdminPhone: +354.4212434
AdminEmail:
     c45fb3e1ea3344c49f8eda3ffb6e25d3.protect@withheldforprivacy.c
     om
Registry TechID: tMNQY-Dhe4A
TechName: Redacted for Privacy
TechOrganization: Privacy service provided by Withheld for Privacy
     ehf
TechStreet: Kalkofnsvegur 2
TechCity: Reykjavik
TechState/Province: Capital Region
TechPostal Code: 101
TechCountry: IS
TechPhone: +354.4212434
TechEmail:
     c45fb3e1ea3344c49f8eda3ffb6e25d3.protect@withheldforprivacy.c
     om
Registry BillingID: Bg55y-29pvn
BillingName: Redacted for Privacy
BillingOrganization: Privacy service provided by Withheld for
     Privacy ehf
BillingStreet: Kalkofnsvegur 2
BillingCity: Reykjavik
BillingState/Province: Capital Region
BillingPostal Code: 101
BillingCountry: IS
BillingPhone: +354.4212434
BillingEmail:
     c45fb3e1ea3344c49f8eda3ffb6e25d3.protect@withheldforprivacy.c
     om
```

```
Name Server: dns1.registrar-servers.com
Name Server: dns2.registrar-servers.com
DNSSEC: unsigned
>>> Last update of WHOIS database: 2023-02-17T13:33:16.418Z <<<
```

[…][17]

```
> whois internet-lexikon.biz
Domain Name: internet-lexikon.biz
Registry Domain ID: D02E3743883FD44F79540253B4A7FFA23-GDREG
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2022-09-04T20:57:37Z
Creation Date: 2022-08-30T20:57:37Z
Registry Expiry Date: 2023-08-30T20:57:37Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain               Status:              clientTransferProhibited
     https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Privacy service provided by Withheld for
     Privacy ehf
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Capital Region
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IS
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of
     Record identified in this output for information on how to
     contact the Registrant, Admin, or Tech contact of the queried
     domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of
     Record identified in this output for information on how to
```

[17] WHOIS-Abfrage um Informationen zu Nutzungsbedingungen von ICANN gekürzt.

```
     contact the Registrant, Admin, or Tech contact of the queried
     domain name.
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please query the RDDS service of the Registrar of Record
     identified in this output for information on how to contact
     the Registrant, Admin, or Tech contact of the queried domain
     name.
Name Server: dns1.registrar-servers.com
Name Server: dns2.registrar-servers.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form:
     https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-02-17T13:35:26Z <<<
```

[…][18]

Beide Domains sind demnach bei „Namecheap“ registriert, es wird der Dienst „WithheldforPrivacy“ verwendet[19] um den tatsächlichen Inhaber zu anonymisieren. Namecheap verfügt über Regeln, die festlegen, unter welchen Umständen WHOIS-Daten dennoch offengelegt werden[20].

Ein zweiter Dienst, „urlscan.io“ (Abbildung 11, https://urlscan.io/ip/190.115.18.20) liefert ebenfalls „tradinginsight.ai“ als auf der IP-Adresse gehosteten Dienst.

[18] WHOIS-Abfrage um Informationen zu Nutzungsbedingungen von ICANN gekürzt.
[19] https://withheldforprivacy.com/, siehe https://www.namecheap.com/blog/domain-privacy-is-changing-at-namecheap/.
[20] https://www.namecheap.com/legal/

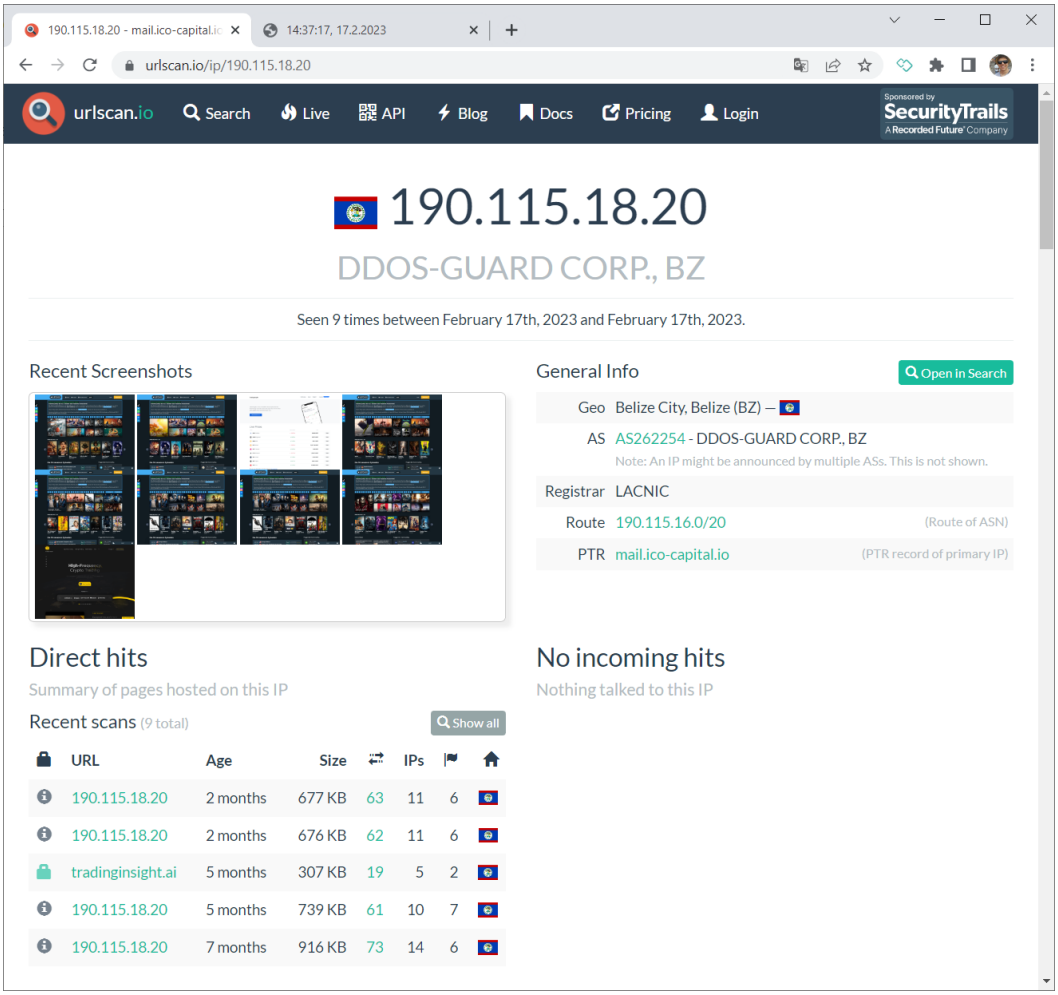

Abbildung 11: Auflistung der Inhalte der IP durch urlscan.io – an den Screenshots lässt sich ein kurzzeitiger Wechsel des Inhalts erkennen.

Bei einem Direktaufruf von „internet-lexikon.biz“ wird mit einem HTTP-Statuscode 302 („moved temporarily“) auf einen Direktaufruf der IP-Adresse 190.115.18.20 verwiesen. Das bedeutet, dass bei einem Aufruf von „internet-lexikon.biz“ wieder die in Abbildung 4 abgebildete Website angezeigt wird.

```
curl -L -vv --head internet-lexikon.biz
*   Trying 190.115.18.20:80...
* TCP_NODELAY set
* Connected to internet-lexikon.biz (190.115.18.20) port 80 (#0)
> HEAD / HTTP/1.1
> Host: internet-lexikon.biz
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 302 Moved Temporarily
HTTP/1.1 302 Moved Temporarily
< Server: ddos-guard
Server: ddos-guard
< Connection: keep-alive
Connection: keep-alive
< Keep-Alive: timeout=60
```

```
Keep-Alive: timeout=60
<   Set-Cookie:   __ddg1_=AxLykjVXJfDFjaLtKzSd;   Domain=.internet-
     lexikon.biz;   HttpOnly;   Path=/;   Expires=Sat,   17-Feb-2024
     13:38:50 GMT
Set-Cookie:     __ddg1_=AxLykjVXJfDFjaLtKzSd;     Domain=.internet-
     lexikon.biz;   HttpOnly;   Path=/;   Expires=Sat,   17-Feb-2024
     13:38:50 GMT
< Date: Fri, 17 Feb 2023 13:38:50 GMT
Date: Fri, 17 Feb 2023 13:38:50 GMT
< Content-Type: text/html
Content-Type: text/html
< Content-Length: 138
Content-Length: 138
< Location: http://190.115.18.20/
Location: http://190.115.18.20/

<
* Connection #0 to host internet-lexikon.biz left intact
* Issue another request to this URL: 'http://190.115.18.20/'
*   Trying 190.115.18.20:80...
* TCP_NODELAY set
* Connected to 190.115.18.20 (190.115.18.20) port 80 (#1)
> HEAD / HTTP/1.1
> Host: 190.115.18.20
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
HTTP/1.1 200 OK
< Server: ddos-guard
Server: ddos-guard
< Connection: keep-alive
Connection: keep-alive
< Keep-Alive: timeout=60
Keep-Alive: timeout=60
<    Set-Cookie:    __ddg1_=Ls1nrSyonhCErPPwLcYI;    Domain=.18.20;
     HttpOnly; Path=/; Expires=Sat, 17-Feb-2024 13:38:50 GMT
Set-Cookie: __ddg1_=Ls1nrSyonhCErPPwLcYI; Domain=.18.20; HttpOnly;
     Path=/; Expires=Sat, 17-Feb-2024 13:38:50 GMT
< Date: Fri, 17 Feb 2023 13:38:50 GMT
Date: Fri, 17 Feb 2023 13:38:50 GMT
< Content-Type: text/html; charset=UTF-8
Content-Type: text/html; charset=UTF-8
< Vary: Accept-Encoding
Vary: Accept-Encoding
< Vary: Accept-Encoding
Vary: Accept-Encoding
< Set-Cookie: PHPSESSID=btlaq6grs9nbpor9qak083h9ct; path=/
Set-Cookie: PHPSESSID=btlaq6grs9nbpor9qak083h9ct; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-store, no-cache, must-revalidate
< Pragma: no-cache
Pragma: no-cache
```

Bei einem direkten Aufruf von „tradinginsight.ai“ wird ein Inhalt zurückgegeben, der eine vom Videoportal gänzlich unabhängige Website zu sein scheint. Die dort gehostete Website scheint dem Open Source-Projekt „trading-charts“[21] zu entsprechen und Informationen zu Kryptowährungen bereitzustellen. Der cURL-Aufruf ist unten abgedruckt. Die sichtbare Website ist in Abbildung 12 abgebildet.

```
curl -L -vv --head tradinginsight.ai
*   Trying 190.115.18.20:80...
* TCP_NODELAY set
* Connected to tradinginsight.ai (190.115.18.20) port 80 (#0)
> HEAD / HTTP/1.1
> Host: tradinginsight.ai
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
HTTP/1.1 200 OK
< Server: ddos-guard
Server: ddos-guard
< Connection: keep-alive
Connection: keep-alive
< Keep-Alive: timeout=60
Keep-Alive: timeout=60
<             Set-Cookie:             __ddg1_=1j5CddDZ5qRxhPpNjhy0;
     Domain=.tradinginsight.ai; HttpOnly; Path=/; Expires=Sat, 17-
     Feb-2024 13:43:50 GMT
Set-Cookie:                          __ddg1_=1j5CddDZ5qRxhPpNjhy0;
     Domain=.tradinginsight.ai; HttpOnly; Path=/; Expires=Sat, 17-
     Feb-2024 13:43:50 GMT
< Date: Fri, 17 Feb 2023 13:43:50 GMT
Date: Fri, 17 Feb 2023 13:43:50 GMT
< Content-Type: text/html
Content-Type: text/html
< Content-Length: 2907
Content-Length: 2907
< Vary: Accept-Encoding
Vary: Accept-Encoding
< Last-Modified: Tue, 30 Aug 2022 22:27:10 GMT
Last-Modified: Tue, 30 Aug 2022 22:27:10 GMT
< Vary: Accept-Encoding
Vary: Accept-Encoding
< ETag: "630e8ebe-b5b"
ETag: "630e8ebe-b5b"
< Expires: Fri, 17 Feb 2023 19:43:50 GMT
Expires: Fri, 17 Feb 2023 19:43:50 GMT
< Cache-Control: max-age=21600
Cache-Control: max-age=21600
< Accept-Ranges: bytes
Accept-Ranges: bytes
```

[21] https://adrianmanchev.github.io/trading-charts/

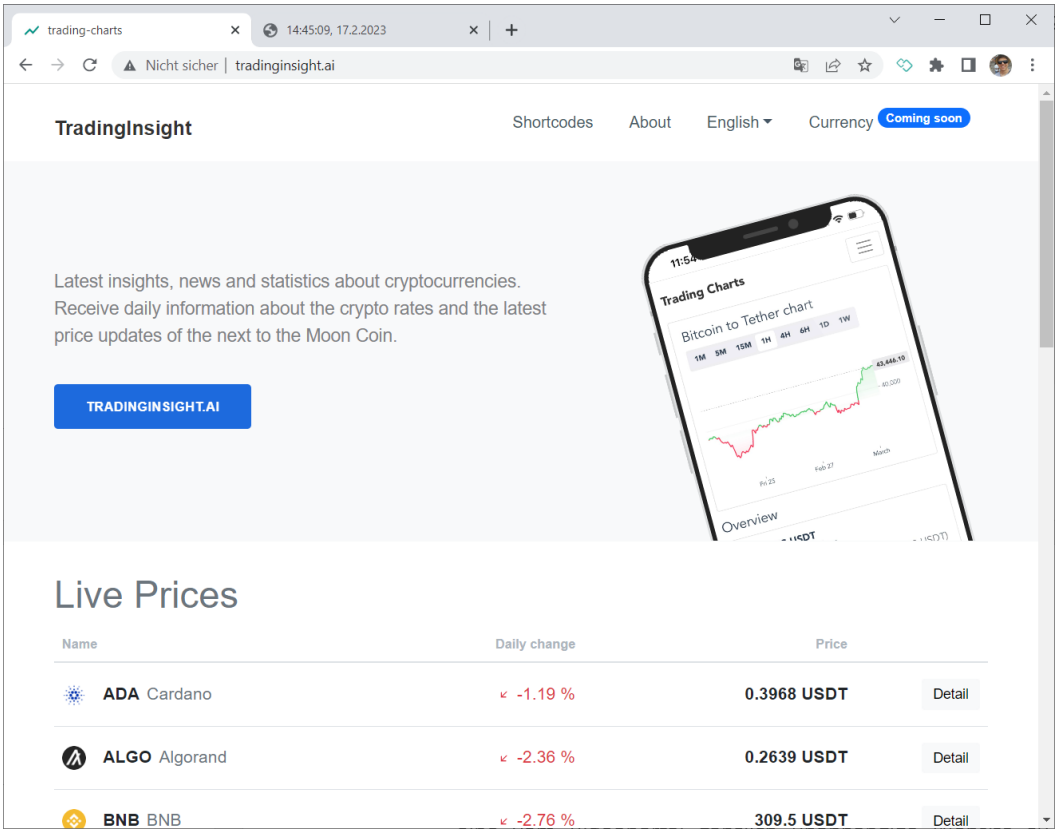

Abbildung 12: Aufruf von "tradinginsight.ai" am 17.2.2023

Zusammenfassend lässt sich damit zur IP-Adresse 190.115.18.20 festhalten, dass ein Direktaufruf ein mit „s.to“ benanntes Portal zeigt. Unter derselben IP-Adresse waren zum Abfragezeitpunkt auch weitere Inhalte, in diesem Fall „tradinginsight.ai“ gehostet.

Da diese Inhalte wie vorangehend angeführt nur durch die Nutzung von Online-Diensten gefunden werden konnten, wird illustriert, wie es technisch nicht feststellbar ist, ob sich noch weitere Inhalte unter dieser IP-Adresse abrufbar ist.

Da die IP-Adresse dem Webhoster „DDoS-Guard“ zugeordnet ist, ist es jederzeit möglich, dass sich der auf dieser IP-Adresse dargestellte Inhalt einfach ändern kann, indem etwa die IP-Adresse einem neuen Kundenkonto zugeordnet wird.

Da sich eine Sperre der IP-Adresse aus technischer Sicht nur auf die Adresse, aber nicht auf einen Inhalt, beschränkt, würde eine gesetzte Sperre auch gegenüber allen anderen Inhalten wirken. In diesem Fall wären auch neue Inhalte von neuen Inhabern für Endnutzer:innen der Internetanbieter, die eine Sperre gesetzt haben, nicht abrufbar. Aus dem gleichen Grund wirkt die Sperre auch weiter, wenn es unter demselben Inhaber zur Zurverfügungstellung neuer Inhalte kommt – durch eine IP-Sperre sind aus technischer Sicht jedenfalls immer sämtliche Inhalte einer IP-Adresse gesperrt, unabhängig von deren Erstellungsdatum, Änderungsdatum oder des Verfügungsberechtigten.

Während des Zeitraums der Gutachtenserstellung hat sich die Abfrage für tradinginsight.ai weiter verändert. Löste eine DNS-Abfrage am 17.2.2023 für tradinginsight.ai noch auf 190.115.18.20 auf, wie oben angeführt, lieferte sie am 15.3.2023 bereits mit „NXDOMAIN“ einen Hinweis darauf, dass diese Domain nicht mehr bespielt wird.

```
> dig tradinginsight.ai A

; <<>> DiG 9.16.1-Ubuntu <<>> tradinginsight.ai A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 27386
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL:
     1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;tradinginsight.ai.             IN      A

;; AUTHORITY SECTION:
ai.                        86193   IN      SOA     pch.whois.ai.
     vince.offshore.ai. 2023031505 21600 3600 86400 86400

;; Query time: 13 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Mar 15 14:15:59 CET 2023
;; MSG SIZE  rcvd: 107
```

Der „whois“-Eintrag ist weiterhin unverändert, so dass zu diesem Zeitpunkt keine Rückschlüsse darüber getätigt werden können, ob es sich um eine temporäre oder dauerhafte Nicht-Auflösung handelt.

```
whois tradinginsight.ai
Domain Name: tradinginsight.ai
Registry Domain ID: 1164796_nic_ai
Registry WHOIS Server: whois.nic.ai
Creation Date: 2021-03-05T12:11:38.322Z
Registrar: Namecheap
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Registry RegistrantID: ONP4h-wUZ8M
RegistrantName: Redacted for Privacy
RegistrantOrganization: Privacy service provided by Withheld for
     Privacy ehf
RegistrantStreet: Kalkofnsvegur 2
RegistrantCity: Reykjavik
RegistrantState/Province: Capital Region
RegistrantPostal Code: 101
RegistrantCountry: IS
RegistrantPhone: +354.4212434
RegistrantEmail:
     c45fb3e1ea3344c49f8eda3ffb6e25d3.protect@withheldforprivacy.c
     om
Registry AdminID: DJZcq-yTvYq
```

```
AdminName: Redacted for Privacy
AdminOrganization: Privacy service provided by Withheld for Privacy
     ehf
AdminStreet: Kalkofnsvegur 2
AdminCity: Reykjavik
AdminState/Province: Capital Region
AdminPostal Code: 101
AdminCountry: IS
AdminPhone: +354.4212434
AdminEmail:
     c45fb3e1ea3344c49f8eda3ffb6e25d3.protect@withheldforprivacy.c
     om
Registry TechID: 5B45k-BWWkw
TechName: Redacted for Privacy
TechOrganization: Privacy service provided by Withheld for Privacy
     ehf
TechStreet: Kalkofnsvegur 2
TechCity: Reykjavik
TechState/Province: Capital Region
TechPostal Code: 101
TechCountry: IS
TechPhone: +354.4212434
TechEmail:
     c45fb3e1ea3344c49f8eda3ffb6e25d3.protect@withheldforprivacy.c
     om
Registry BillingID: OLR9u-5HeKZ
BillingName: Redacted for Privacy
BillingOrganization: Privacy service provided by Withheld for
     Privacy ehf
BillingStreet: Kalkofnsvegur 2
BillingCity: Reykjavik
BillingState/Province: Capital Region
BillingPostal Code: 101
BillingCountry: IS
BillingPhone: +354.4212434
BillingEmail:
     c45fb3e1ea3344c49f8eda3ffb6e25d3.protect@withheldforprivacy.c
     om
Name Server: dns101.registrar-servers.com
Name Server: dns102.registrar-servers.com
DNSSEC: unsigned
>>> Last update of WHOIS database: 2023-03-15T13:18:20.138Z <<<
```

[…][22]

Das Beispiel der Änderung des Inhalts für tradinginsight.ai innerhalb des Gutachtenszeitraums illustriert, wie kurzlebig Inhalte im Internet sein können.

Zur Gutachtensfrage 2.c: Unter der IP-Adresse 190.115.18.20 konnten im Gutachtenszeitraum eine sich als „s.to“ bezeichnende Videostreamingseite, sowie zeitweise eine unter der Domain „tradinginsight.ai“ verfügbare Website zu Kryptowährungen abgerufen werden. Zudem verweist die Domain „internet-lexikon.biz“ auf die IP-Adresse, leitet aber auf die sich als „s.to“ bezeichnende Seite

[22] WHOIS-Abfrage um Informationen zu Nutzungsbedingungen von ICANN gekürzt.

um. Aus technischer Sicht wurde zur Feststellung auf frei verfügbare Datenbanken zurückgegriffen, die durch Crawling eine historische Zuordnung von Domains zu IP-Adressen ermöglichen.

Zur Gutachtensfrage 2.d: Es ist aus technischer Sicht nicht möglich, alle unter einer IP-Adresse abrufbaren Inhalte aufzulisten. Dies ist auch für einen Internetzugangsdiensteanbieter nicht möglich.

Zu den Gutachtensfragen 2.e und 2.f: Eine eingerichtete IP-Sperre wirkt auf technischer Ebene zu sämtlichem Verkehr einer IP-Adresse. Sollte sich der Inhaber einer IP-Adresse verändern, wäre auch der neue Inhaber durch eine bestehende IP-Sperre betroffen. Sollte sich der unter der IP-Adresse bereitgestellte Inhalt verändern, wären auch Inhalte dieser neuen Angebote durch eine bestehende IP-Sperre betroffen.

4 Effektivität einer IP-Sperre

4.1 Umgehungsmöglichkeiten für Domain-Inhaber

Zu den Gutachtensfrage 3.a *„Wie effektiv ist die IP-Sperre der IP-Adresse 190.115.18.20 durch einen Anbieter von Internetzugangsdiensten? Verfügt ein Domaininhaber über technische Möglichkeiten, die Wirksamkeit einer IP-Sperre zu verringern?“* und 3.b *„Welche praktischen Auswirkungen hat für Endnutzer der Wechsel einer IP-Adresse durch einen Domaininhaber? Wie häufig kann die einer Domain zugeordnete IP-Adresse geändert werden? Wie lange dauert es bei einem Wechsel der IP-Adresse, bis eine Domain für Internetnutzer wieder erreichbar ist?“* kann folgendes ausgeführt werden:

Üblicherweise wird im Internet in der Interaktion mit Endnutzer:innen mit Domains gearbeitet – die Tatsache, dass im Hintergrund auf technischer Ebene IP-Adressen verwendet werden, ist für den Großteil der Nutzer:innen ein scheinbar rein technisches Detail, das nicht wahrgenommen wird.[23] Da nur die Domain das wesentliche Merkmal eines Dienstes ist, kommt der konkreten IP-Adresse in der Praxis keine große weitere Bedeutung zu.

Wird die IP-Adresse eines Diensteanbieters demnach gesperrt und möchte der Diensteanbieter diese Sperre umgehen, ist es aus technischer Sicht trivial, die IP-Adresse zu wechseln. Dafür ist lediglich die Änderung des „A-Record“ im DNS-Nameserver der Domain notwendig. Aus Effizienzgründen werden eingetragene Adressen eine Zeit lang zwischengespeichert, so dass die Propagierung der Änderung der IP-Adresse einige Sekunden bis zu wenigen Stunden dauern kann, bis sie bei abfragenden Nutzern auch aufscheint. Von Endnutzer:innen wird eine solche Änderung der IP-Adresse nicht wahrgenommen – da die angesurfte Domain gleichbleibt, werden sie eine Änderung der IP-Adresse nicht bemerken.

Wie lange die Umstellung auf eine neue IP-Adresse dauert, liegt in der Konzeption unter der Kontrolle des Inhabers der Domain. So wird im „A-Record“ einer Domain neben der Ziel-IP-Adresse auch die Caching-Zeitdauer in Sekunden hinterlegt, die ein abfragender Client abwarten kann, bevor erneut eine Abfrage gestellt wird.[24] Dieser Wert kann sich im Bereich einiger Sekunden befinden. Kommt es zu einem geplanten Wechsel der IP-Adresse, lässt sich ein solcher deshalb faktisch ohne Ausfall des angebotenen Services vollziehen – entweder durch einen Parallelbetrieb beider IP-Adressen über einen kurzen Zeitraum, oder durch einen kurzen Caching-Wert, so dass ein Wechsel der IP-Adresse annähernd sofort wirksam wird.

Voraussetzung für den Wechsel der IP-Adresse ist dann lediglich die Möglichkeit, über eine andere IP-Adresse zu verfügen. Je nach Hoster kann dies entweder einfach direkt über ein Online-Interface möglich sein, oder aber den Umzug auf ein anderes Kundenkonto bzw Wechsel des Hosters erfordern. Auch das ist für Endnutzer:innen

[23] Mit höchstens der Ausnahme der absichtlich einfach merkbaren IP-Adressen von DNS-Resolvern, die diese Umwandlung ermöglichen, wie 1.1.1.1, 8.8.8.8, 9.9.9.9
[24] IETF RFC 1035, 4.1.3.

nicht bemerkbar. Aus technischer Sicht gibt es kein relevantes zahlenmäßiges Limit der Häufigkeit eines Wechsels der IP-Adresse.

Zur Gutachtensfrage 3.a: Ein Domaininhaber verfügt mit der Maßnahme des Wechsels der IP-Adresse über die technische Möglichkeit, die Wirksamkeit einer IP-Sperre zu verringern bzw. diese unwirksam werden zu lassen.

Zur Gutachtensfrage 3.b: Ein Wechsel der IP-Adresse (z.B. von 1.2.3.4 auf 1.2.3.5) durch einen Domaininhaber hat für Endnutzer in der Regel keine praktischen Auswirkungen. Es kommt zu keiner Unterbrechung der Erreichbarkeit des Services. Im Gegensatz zu einem Wechsel der Domain geht ein Wechsel der IP-Adressen auch mit keinem Problem der Reichweite einher, da die (bei den Endnutzer:innen bekannte) Domain (z.B. www.rtr.at) ident bleibt.

Es gibt kein technisches Limit in der Anzahl der möglichen Wechsel der IP-Adresse.

4.2 Umgehungsmöglichkeiten für Endnutzer:innen

Hinsichtlich Gutachtensfrage 3.d *„Gibt es für Endnutzer – aus technischer Sicht – Möglichkeiten, die Sperre der genannten IP-Adresse durch ihren Internetzugangsdiensteanbieter zu umgehen? Ist dies auch Endnutzer ohne ausgeprägtem IT-Know-How möglich? Unterscheidet sich dies im Vergleich zu einer DNS-Sperre? Was bewirkt der Einsatz von VPNs?“* kann folgendes ausgeführt werden:

Auch wenn es zu keinem Wechsel der IP-Adresse durch den Anbieter kommt, gibt es für Endnutzer:innen technische Möglichkeiten, eine IP-Sperre des Anbieters eines Internetzugangsdienstes zu umgehen. Viele davon erfordern auch kein ausgeprägtes IT-Know-How der Endnutzer:innen.

Die bestehenden Umgehungsmöglichkeiten für Endnutzer:innen unterscheiden sich etwas im Vergleich zur Einrichtung von DNS-Sperren[25]. Kann bei einer DNS-Sperre mit ein wenig technischer Expertise eine Umgehung der Sperre durch eine Änderung des DNS-Resolvers auf einen alternativen Resolver[26] herbeigeführt werden, besteht diese Möglichkeit bei einer IP-Sperre nicht. Andere Umgehungsmöglichkeiten, die sowohl zur Umgehung von DNS-Sperren als auch IP-Sperren möglich sind, bestehen weiterhin und bedürfen wenig technischen Expertise.

Einsatz von VPN-Clients

Sogenannte „Virtual Private Networks“ (VPN) erlauben es Nutzern, sich durch Aufbau einer verschlüsselten Verbindung über das Internet in bestehende Netzwerke

[25] In diesem Fall wird bei der Auflösung einer Domain durch den Resolver des Internetzugangsdiensteanbieters auf die IP-Adresse einer Seite mit einem Sperrhinweis ausgelöst.
[26] Entweder durch eine Änderung in den Einstellungen des Betriebssystems, oder einer Änderung der Einstellungen in Browsern wie Mozilla Firefox oder Google Chrome.

einzuwählen. Dies ermöglicht es etwa Unternehmen, ihren Mitarbeiter auch von außerhalb des Firmennetzwerks Zugriff auf interne Ressourcen zu ermöglichen.

Außerhalb des verbreiteten Anwendungsgebiets für Firmennetzwerke sind werden VPN-Dienste auch für private Nutzer angeboten. Anbieter solcher VPN-Dienste sind zahlreich, VPN-Produkte sind zu niedrigen Preisen verfügbar. Diese ermöglichen, sämtlichen Internetdatenverkehr über eine clientseitig verschlüsselte Internetverbindung zum Anbieter des VPNs zu senden, und die eigentlich angesteuerten Dienste dann erst durch diesen aufzurufen. Dadurch werden alle Steuerungs- oder Beobachtungsmöglichkeit des Anbieters des Internetzugangsdiensts unterbunden. Für den eigentlichen Anbieter des Internetzugangsdienstes sichtbar ist deshalb nur die Verbindung der Endnutzer:in zum Anbieter des VPN. Umgekehrt ist für den aufgerufenen Dienst ebenfalls nur die IP-Adresse des VPN-Anbieters sichtbar, nicht jedoch die der aufrufenden Endnutzer:in. Dieser Vorgang ist in Abbildung 13 und Abbildung 14 dargestellt.

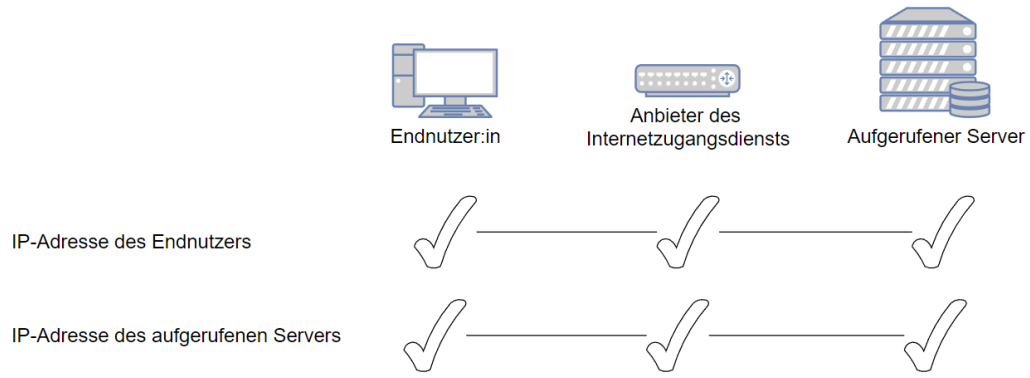

Abbildung 13: Aufruf eines Services ohne VPN: Quell- und Ziel-IP-Adresse sind für alle Akteure sichtbar.

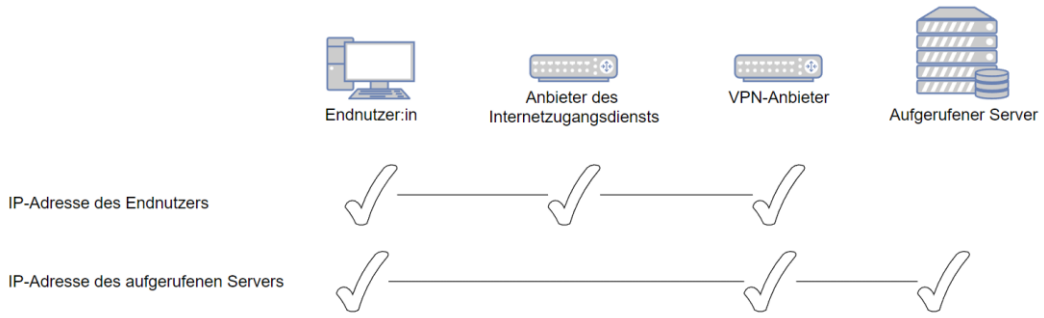

Abbildung 14: Aufruf eines Services mit VPN: Die Quell-IP-Adresse ist für den Serviceanbieter nicht sichtbar, die aufgerufene IP-Adresse ist für den Anbieter des Internetzugangsdiensts nicht sichtbar.

Aus diesem Grund greift auch eine durch den Anbieter des Internetzugangsdienstes eingerichtete IP-Sperre nicht, wenn ein VPN zum Einsatz kommt. Anders als bei Tor (s.u.) gibt es hier auch keine Einschränkungen bei der Nutzung von Videostreaming-

Services, da die von VPN-Diensten angebotene Geschwindigkeit in der Regel für die Nutzung von Videostreaming ausreichend ist[27].

VPN-Dienste werden in der Regel kostenpflichtig angeboten, wobei die streamingtauglichen Angebote etwa 2,50 € bis 5 € brutto pro Monat für die Nutzung des Dienstes verrechnen.[28] Auch der oben verwendete VPN-Dienst des Herstellers Mozilla wird mit 5 € brutto p.m. verrechnet. Den VPN-Diensten gemein ist eine einfache Installation, die mit wenigen Klicks auch für technische Laien möglich ist. Dies ist etwa in Abbildung 15 ersichtlich, wo sich die gesamte Benutzeroberfläche auf eine Möglichkeit der Aktivierung und Deaktivierung des VPN-Dienstes beschränkt sowie eine Auswahl des Landes des VPN-Servers möglich ist.

Abbildung 15: Beispiel der Benutzeroberfläche eines VPN-Anbieters am Beispiel „Mozilla VPN“

Alternativ zum Einsatz eines kommerziellen VPN-Anbieters ist auch die Einrichtung eines eigenen VPN-Dienstes möglich. Hierzu wird lediglich ein virtueller Server eines Hosting-Betreibers benötigt. Diese verursachen ähnliche monatliche Kosten wie ein kommerzieller VPN-Anbieter, erfordern zur Einrichtung jedoch zumindest grundlegende technische Fachkenntnisse.

Einsatz von Tor

Etwas langsam, aber kostenlos und ebenfalls einfach in der Bedienung ist der Einsatz des „Tor“-Netzwerks, etwa durch den kostenlosen „Tor Browser“. Im konkreten Fall

[27] Was zT auch Bestandteil der Produktpositionierung ist – VPN-Anbieter versprechen, durch die Nutzungsmöglichkeit von VPN-Servern in verschiedenen geographischen Regionen die bei Videostreaming anzugreffenden Geo-Blocks umgehen zu können.

[28] https://www.heise.de/download/specials/Anonym-surfen-mit-VPN-Die-besten-VPN-Anbieter-im-Vergleich-3798036

ist der geringe Datendurchsatz von Tor auch kein praktisches Problem, da durch das mit „s.to“ benannte Portal der IP-Adresse kein Hosting der Videostreams erfolgt[29]. Der Stream selbst kann dann außerhalb von Tor – in üblicher Internetgeschwindigkeit – aufgerufen werden.

Die Einrichtung ist ohne weiterer technischer Fachkenntnisse möglich – der Tor-Browser kann mittels Downloads von der offiziellen Seite „torproject.org“ heruntergeladen werden und ist sofort ausführbar. Eine App für Android-Geräte kann auch von Googles Playstore heruntergeladen werden[30].

Einsatz von Apple Private Relay

Ein für Apple-Nutzer verfügbarer VPN-Dienst ist Apples eigenes „Apple Private Relay“.[31] Dieser Dienst baut technisch ein VPN auf – d.h. sämtlicher Verkehr der Endnutzer:in wird zuerst zu Apples eigenen Server geleitet, die Ziel-IP-Adresse des aufgerufenen Diensts ist deshalb für den Anbieter des Internetzugangsdienstes nicht sichtbar. Sämtliche von diesen eingerichteten IP-Sperren sind deshalb unwirksam.

Apple Private Relay ist Bestandteil des „iCloud+“-Abonnements, und somit für viele Apple-Kunden ohne spezifische weitere Kosten auf MacBooks, iPhone und iPads verfügbar.[32] Die Kosten für ein „iCloud+“-Abonnement, in dem nebst Speicherplatz für Fotos auch „Apple Private Relay“ enthalten ist, belaufen sich ansonsten auf € 0,99 monatlich.[33]

HTTP-Proxy-Server

Da es sich beim gegenständlich angebotenen Dienst um eine Website handelt, ist eine Umgehung auch durch den Einsatz eines HTTP-Proxy-Servers möglich. Dies ist technisch gleich wie beim Einsatz eines VPN-Dienstes: Der Verkehr wird über einen zwischengeschalteten Server geroutet. Im Gegensatz zum VPN-Dienst beschränkt sich dieser auf Websites. Da mit VPN-Diensten eine umfassendere technische Lösung zur Verfügung steht, wird die Möglichkeit des Einsatzes von HTTP-Proxy-Servern hier zwar genannt, aber nicht genauer darauf eingegangen.

Zur Gutachtensfrage 3.d: Es gibt für Endnutzer aus technischer Sicht mehrere Möglichkeiten, die Sperre einer IP-Adresse durch ihren Internetzugangsdienste-anbieter zu umgehen. Das ist auch für Endnutzer ohne ausgeprägtem IT-Know-How möglich. Solche einfachen Umgehungsmöglichkeiten bieten etwa die Nutzung von Tor, oder der Einsatz eines VPNs.

[29] Siehe Kapitel 3.2.
[30] https://play.google.com/store/apps/details?id=org.torproject.torbrowser
[31] https://developer.apple.com/support/prepare-your-network-for-icloud-private-relay/
[32] https://support.apple.com/de-at/HT212614
[33] https://www.apple.com/at/icloud/ abgefragt am 5. April 2023.

Im Vergleich zu einer DNS-Sperre ist eine Umgehung einer eingerichteten Sperre einer IP-Adresse nicht durch den Wechsel des DNS-Resolvers möglich. Die anderen Umgehungsmöglichkeiten gelten sowohl für IP-Sperren als auch für DNS-Sperren.

4.2.1 Auswirkungen von IPv6

Zur Gutachtensfrage 3.c „*Unterscheidet sich die Effektivität im Falle des Einsatzes von IPv6?*“ kann folgendes ausgeführt werden:

Aufgrund der begrenzten Anzahl von Adressen im Internetprotokoll („IP“) der Version 4 („IPv4“) erfolgt seit Jahren eine schrittweise Umstellung auf das Nachfolgeprotokoll der Version 6 („IPv6“). Durch eine deutliche längere Adresslänge – mit 128 Bit statt 32 Bit Länge – gibt es dabei statt ca 4,3 Mrd Adressen bei IPv4 in IPv6 rechnerische 3,4 x 10^{38} Adressen. Praktisch ist das auch dadurch bemerkbar, dass die Notation der Adressen deutlich länger ist. Löst „rtr.at“ etwa auf die IPv4-Adresse „81.16.157.3“ auf, ist die zugehörige IPv6-Adresse „2a01:190:15fd:1c00::3“ trotz der hexadezimalen Notation augenscheinlich deutlich länger.

Gerade bei Cloud-Anbietern ist es zwischenzeitlich üblich, dass Kundenservices mittlerweile im „Dual Stack“ unter einer IPv4- und einer IPv6-Adresse erreichbar sind. Soll durch die Ergreifung einer IP-Sperre ein bestimmter Inhalt gesperrt werden, ist deshalb wichtig, dass die Sperre bei einer Dual-Stack-Erreichbarkeit sowohl IPv4 als auch IPv6 umfasst. Die Sperre einer IPv4-Adresse lässt den Zugriff über IPv6 offen und umgekehrt. Für Dritte ist es jedoch nicht möglich, auszulesen, ob ein mit einer bestimmten IPv4-Adresse adressierbarer Server auch über IPv6-Konnektivität verfügt. Auch dies ist nur heuristisch möglich, etwa, indem durch DNS-Abfragen bei Domains, die auf eine IPv4-Adresse zeigen, auch für IPv6 durchgeführt werden.

Wie oben angeführt, sind aus den Recherchen zwei Domains bekannt, die auf die gegenständliche IP-Adresse zeigen, nämlich tradinginsight.ai und internet-lexikon.biz. Beide Domains lösen, wie oben angeführt, zwar auf eine IPv4-Adresse auf, eine Abfrage des für IPv6-Adressen vorgesehenen „AAAA-Records“ zeigt aber keine zugeordneten Adressen. Es scheint deshalb keine IPv6-Konnektivität vorzuliegen.

Während internet-lexikon.biz zwar einen A-Record besitzt, liegt ein AAAA-Record nicht vor:

```
dig internet-lexikon.biz A

; <<>> DiG 9.16.1-Ubuntu <<>> internet-lexikon.biz A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21976
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
     1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
```

```
;internet-lexikon.biz.          IN      A

;; ANSWER SECTION:
internet-lexikon.biz.   1304    IN      A       190.115.18.20

;; Query time: 0 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Mar 15 14:21:31 CET 2023
;; MSG SIZE  rcvd: 65
```

```
dig internet-lexikon.biz AAAA

; <<>> DiG 9.16.1-Ubuntu <<>> internet-lexikon.biz AAAA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40819
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL:
     1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;internet-lexikon.biz.          IN      AAAA

;; AUTHORITY SECTION:
internet-lexikon.biz.    3601     IN       SOA      dns1.registrar-
     servers.com.   hostmaster.registrar-servers.com.   1661893212
     43200 3600 604800 3601

;; Query time: 25 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Mar 15 14:22:10 CET 2023
;; MSG SIZE  rcvd: 122
```

Da es aber aus technischer Sicht keine Möglichkeit gibt, eine IPv6-Konnektivität basierend auf einer IPv4-Adresse festzustellen, handelt es sich dabei nur um ein Indiz. Ein Gegenargument, dass es zu der IPv4-Adresse auch eine passende IPv6-Adresse gibt, wäre, dass der Hoster DDoS-Guard über einen großen zugeteilten IPv6-Adressbereich verfügt, wie oben in Abschnitt 3 festgestellt.

Zur Gutachtensfrage 3.c: Die Effektivität einer Sperre unterscheidet sich nicht im Falle des Einsatzes von IPv6. Bei einer s.g. Dual-Stack-Erreichbarkeit bewirkt die Sperre von nur ausschließlich der IPv4 bzw. ausschließlich der IPv6-Adresse, dass die angebotenen Inhalte über die jeweils andere Adresse weiterhin erreichbar bleiben. Im konkreten Fall der IP-Adresse 190.115.18.20 konnte keine zugehörige IPv6-Adresse ermittelt werden.

Zusammenfassend lässt sich festhalten, dass es sowohl für Inhaber von Domains, als auch für Endnutzer:innen einfach möglich ist, durch Anbieter von Internetzugangs-

dienste eingerichtete IP-Sperren zu umgehen. Die Umgehungsmöglichkeiten erfordern keine kein ausgeprägtes IT-Know-How der Endnutzer:innen und sind teilweise auch kostenlos verfügbar.

5 Zusammenfassung

In den vorangegangenen Kapiteln wurden die für die Beantwortung der Gutachtensfragen notwendigen Grundlagen erörtert sowie die notwendigen Informationen erhoben. Dabei konnten die Gutachtensfragen wie folgt beantwortet werden:

1. *Was bewirkt aus technischer Sicht eine Sperre der IP-Adresse 190.115.18.20 durch einen Anbieter von Internetzugangsdiensten?*

    a. *Wie und wem gegenüber wirkt eine durch Anbieter von Internetzugangsdiensten eingerichtete IP-Sperre?*

Eine durch einen Anbieter von Internetzugangsdiensten eingerichtete IP-Sperre wirkt gegenüber dessen Kund:innen. Verkehr zur gesperrten IP-Adresse wird nicht zugestellt.

    b. *Kann es aus technischer Sicht zu „Overblocking" kommen, wenn eine IP-Sperre durch einen Internetzugangsdiensteanbieter umgesetzt wird?*

Bei der Umsetzung einer IP-Sperre durch einen Internetzugangsanbieter kann es aus technischer Sicht immer zu einem „Overblocking" kommen, da eine vollständige Ermittlung aller von einer Sperre umfassten Inhalte für einen Internetzugangsanbieter technisch nicht möglich ist.

    c. *Kann ein Internetzugangsdiensteanbieter pro-aktiv abschließend und umfassend erkennen, ob im Falle einer konkreten IP-Sperre auch andere Dienste mitumfasst sind?*

Es ist für einen Internetzugangsanbieter technisch nicht möglich, pro-aktiv abschließend und umfassend zu erkennen, ob im Fall einer konkreten IP-Sperre auch andere Dienste mitumfasst sind.

2. *Wer ist Inhaber der IP-Adresse 190.115.18.20?*

    a. *Wem ist die IP-Adresse zugewiesen, wer kann aus technischer Sicht den unter einer IP-Adresse abrufbaren Inhalt bestimmen / verändern / steuern oder sonst über ihn verfügen?*
    b. *Wie ist die Zuordnung Hosting-Dienst bzw Content Delivery Network zur IP-Adresse?*

IP-Adresse 190.115.18.20 ist dem Hosting-Dienst bzw Content Delivery Network „DDoS-Guard" zugewiesen. DDoS-Guard, bzw. dessen Kunde, kann aus technischer Sicht den unter dieser IP-Adresse abrufbaren Inhalt bestimmen/verändern/steuern.

c. *Welche verschiedenen Inhalte lassen sich unter dieser IP-Adresse abrufen? Wie kann dies aus technischer Sicht festgestellt werden?*

Unter der IP-Adresse 190.115.18.20 konnten im Gutachtenszeitraum eine sich als „s.to“ bezeichnende Videostreamingseite, sowie zeitweise eine unter der Domain „tradinginsight.ai“ verfügbare Website zu Kryptowährungen abgerufen werden. Zudem verweist die Domain „internet-lexikon.biz“ auf die IP-Adresse, leitet aber auf die sich als „s.to“ bezeichnende Seite um. Aus technischer Sicht wurde zur Feststellung auf frei verfügbare Datenbanken zurückgegriffen, die durch Crawling eine historische Zuordnung von Domains zu IP-Adressen ermöglichen.

d. *Ist es aus technischer Sicht möglich, alle unter einer IP-Adresse abrufbaren Inhalte aufzulisten? Ist es für einen Internetzugangsdiensteanbieter möglich, alle abrufbaren Inhalte zu erkennen?*

Es ist aus technischer Sicht nicht möglich, alle unter einer IP-Adresse abrufbaren Inhalte aufzulisten. Dies ist auch für einen Internetzugangsdiensteanbieter nicht möglich.

e. *Sollte sich der Inhaber einer IP-Adresse verändern, wäre auch der neue Inhaber durch eine bestehende IP-Sperre betroffen?*
f. *Sollte sich der unter der IP-Adresse bereitgestellte Inhalt verändern, wären auch Inhalte dieser neuen Angebote durch die bestehende IP-Sperre betroffen?*

Eine eingerichtete IP-Sperre wirkt auf technischer Ebene zu sämtlichem Verkehr einer IP-Adresse. Sollte sich der Inhaber einer IP-Adresse verändern, wäre auch der neue Inhaber durch eine bestehende IP-Sperre betroffen. Sollte sich der unter der IP-Adresse bereitgestellte Inhalt verändern, wären auch Inhalte dieser neuen Angebote durch eine bestehende IP-Sperre betroffen.

3. *Wie effektiv ist die IP-Sperre der IP-Adresse 190.115.18.20 durch einen Anbieter von Internetzugangsdiensten?*

a. *Verfügt ein Domaininhaber über technische Möglichkeiten, die Wirksamkeit einer IP-Sperre zu verringern?*

Ein Domaininhaber verfügt mit der Maßnahme des Wechsels der IP-Adresse über die technische Möglichkeit, die Wirksamkeit einer IP-Sperre zu verringern bzw. diese unwirksam werden zu lassen.

b. *Welche praktischen Auswirkungen hat für Endnutzer der Wechsel einer IP-Adresse durch einen Domaininhaber? Wie häufig kann die einer Domain zugeordnete IP-Adresse geändert werden? Wie lange dauert es bei einem Wechsel der IP-Adresse, bis eine Domain für Internetnutzer wieder erreichbar ist?*

Ein Wechsel der IP-Adresse (z.B. von 1.2.3.4 auf 1.2.3.5) durch einen Domaininhaber hat für Endnutzer in der Regel keine praktischen Auswirkungen. Es kommt zu keiner Unterbrechung der Erreichbarkeit des Services. Im Gegensatz zu einem Wechsel der Domain geht ein Wechsel der IP-Adressen auch mit keinem Problem der Reichweite einher, da die (bei den Endnutzer:innen bekannte) Domain (z.B. www.rtr.at) ident bleibt.

Es gibt kein technisches Limit in der Anzahl der möglichen Wechsel der IP-Adresse.

c. *Unterscheidet sich die Effektivität im Falle des Einsatzes von IPv6?*

Die Effektivität einer Sperre unterscheidet sich nicht im Falle des Einsatzes von IPv6. Bei einer s.g. Dual-Stack-Erreichbarkeit bewirkt die Sperre von nur ausschließlich der IPv4 bzw. ausschließlich der IPv6-Adresse, dass die angebotenen Inhalte über die jeweils andere Adresse weiterhin erreichbar bleiben. Im konkreten Fall der IP-Adresse 190.115.18.20 konnte keine zugehörige IPv6-Adresse ermittelt werden.

d. *Gibt es für Endnutzer – aus technischer Sicht – Möglichkeiten, die Sperre der genannten IP-Adresse durch ihren Internetzugangsdiensteanbieter zu umgehen? Ist dies auch Endnutzer ohne ausgeprägtem IT-Know-How möglich? Unterscheidet sich dies im Vergleich zu einer DNS-Sperre? Was bewirkt der Einsatz von VPNs?*

Es gibt für Endnutzer aus technischer Sicht mehrere Möglichkeiten, die Sperre einer IP-Adresse durch ihren Internetzugangsdiensteanbieter zu umgehen. Das ist auch für Endnutzer ohne ausgeprägtem IT-Know-How möglich. Solche einfachen Umgehungsmöglichkeiten bieten etwa die Nutzung von Tor, oder der Einsatz eines VPNs.

6 Schlussbemerkungen

Ich versichere, das Gutachten nach bestem Wissen und Gewissen und aufgrund sorgfältiger Untersuchungen sowie den mir zur Verfügung gestellten Unterlagen und erteilten Auskünften erstellt zu haben:

Wien, am 13. April 2023

Dipl.-Ing. Thomas Schreiber, LL.M. (WU)

Abbildungsverzeichnis

Abkürzungsverzeichnis

CSS	Cascading Style Sheets
cURL	curl URL Request Library
DNS	Domain Name Service
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IPv4	Internet Protocol, Version 4
IPv6	Internet Protocol, Version 6
ISP	Internet Service Provider
URL	Uniform Resource Locator
VoIP	Voice over IP
VPN	Virtual Private Network
WWW	World Wide Web