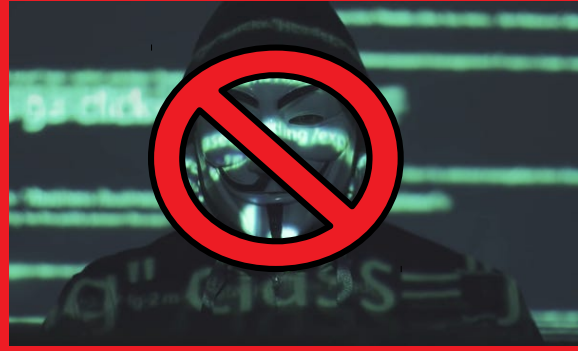
Becoming Anonymous

Part V - Action

@bugg

DISCLAIMER!!!



- This is not legal advice!
- This is a **FANTASY** BACKDROP for learning about Cybersecurity
- This has not been done IRL
- If you do this IRL you are committing a **CRIME**!

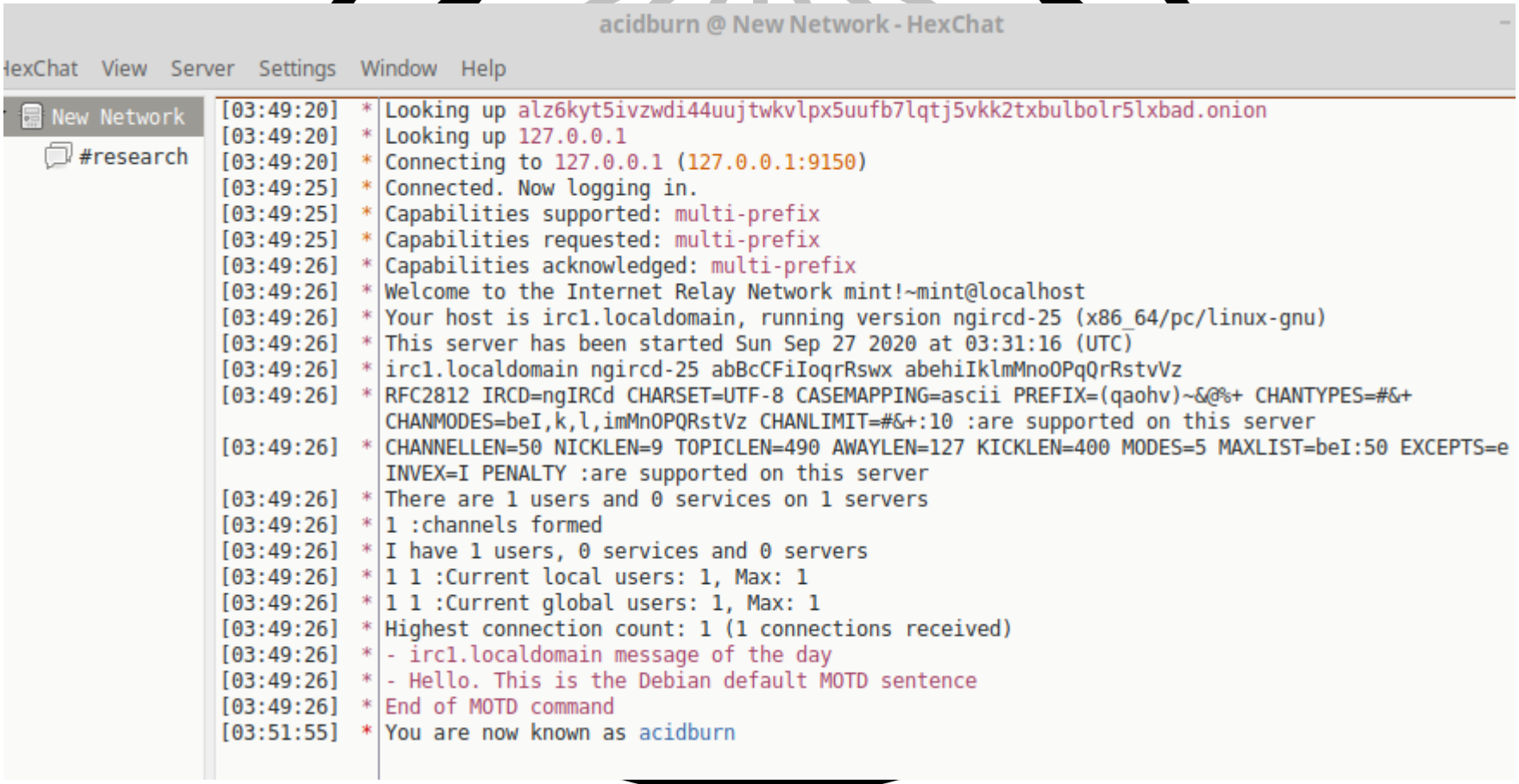
Series Overview

- Part I – Overview
- Part II – Intel
- Part III – Infrastructure
- Part IV – Recruiting
- Part V – Action

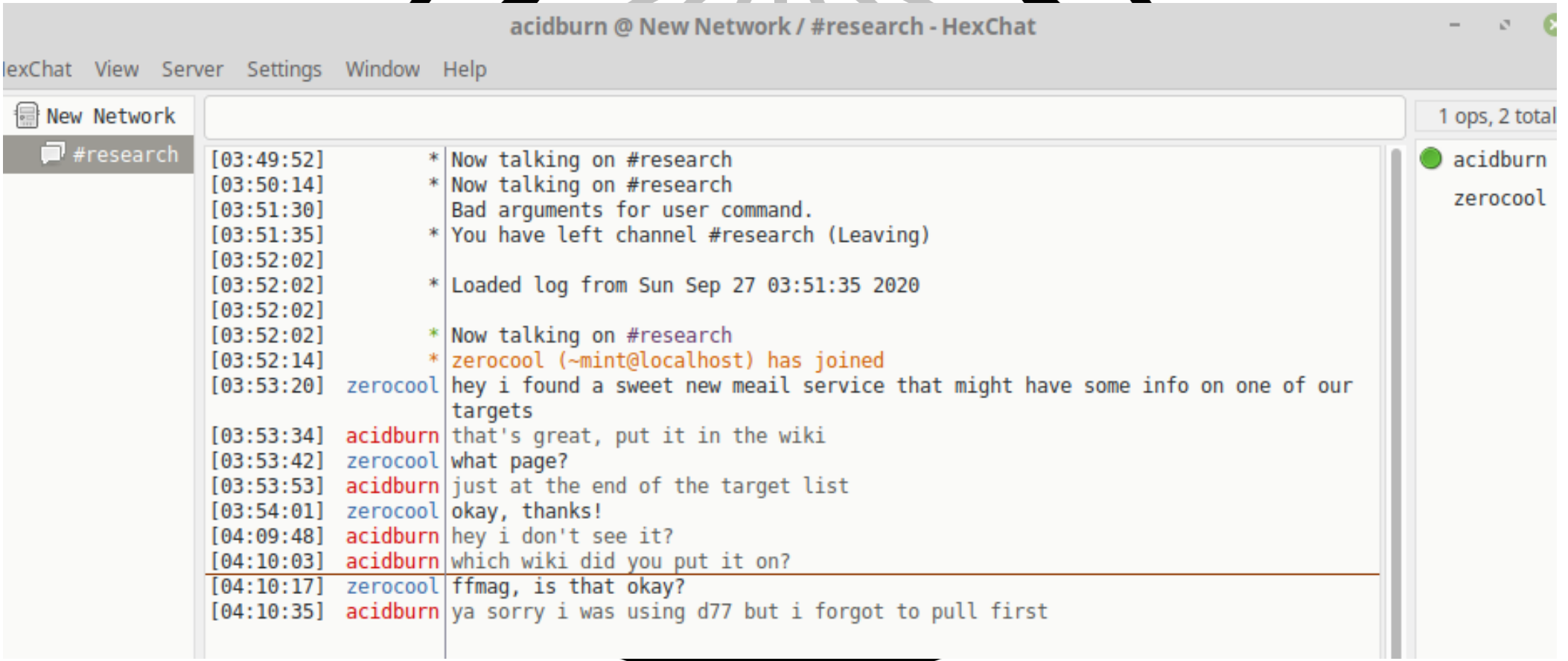
Action Overview

- Research
- OSINT
- Data Delivery

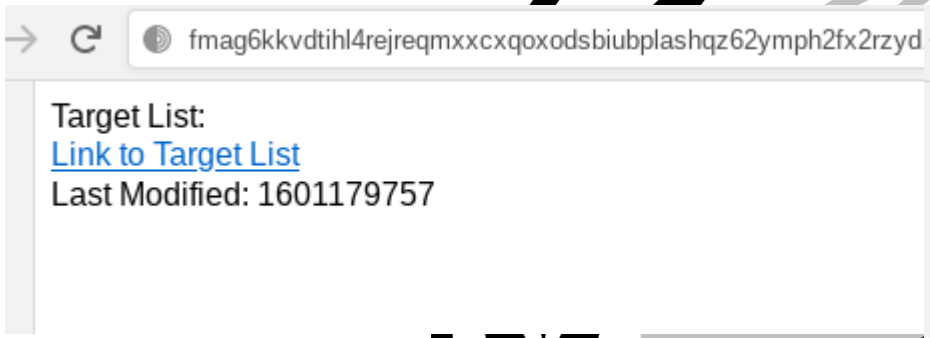
Research

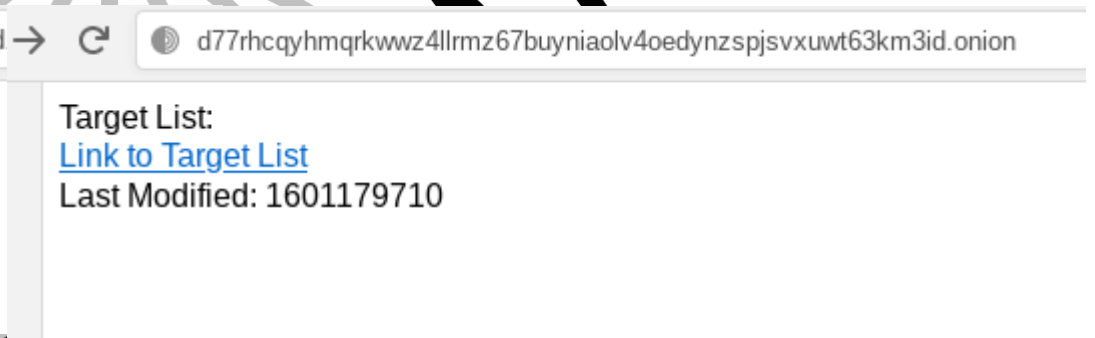

acidburn @ New Network - HexChat
HexChat View Server Settings Window Help
New Network
#research
[03:49:20] * Looking up alz6kyt5ivzwdi44uujtwkvlpx5uufb7lqtj5vkk2txbulbolr5lxbad.onion
[03:49:20] * Looking up 127.0.0.1
[03:49:20] * Connecting to 127.0.0.1 (127.0.0.1:9150)
[03:49:25] * Connected. Now logging in.
[03:49:25] * Capabilities supported: multi-prefix
[03:49:25] * Capabilities requested: multi-prefix
[03:49:26] * Capabilities acknowledged: multi-prefix
[03:49:26] * Welcome to the Internet Relay Network mint!~mint@localhost
[03:49:26] * Your host is irc1.localdomain, running version ngircd-25 (x86_64/pc/linux-gnu)
[03:49:26] * This server has been started Sun Sep 27 2020 at 03:31:16 (UTC)
[03:49:26] * irc1.localdomain ngircd-25 abBcCFiIoqrRswx abehiIklmMnoOPqQrRstvVz
[03:49:26] * RFC2812 IRCD=ngIRCd CHARSET=UTF-8 CASEMAPPING=ascii PREFIX=(qaohv)~&@%+ CHANTYPES=#&+
CHANMODES=beI,k,l,imMnOPQRstVz CHANLIMIT=#&+:10 :are supported on this server
[03:49:26] * CHANNELLEN=50 NICKLEN=9 TOPICLEN=490 AWAYLEN=127 KICKLEN=400 MODES=5 MAXLIST=beI:50 EXCEPTS=e
INVEX=I PENALTY :are supported on this server
[03:49:26] * There are 1 users and 0 services on 1 servers
[03:49:26] * 1 :channels formed
[03:49:26] * I have 1 users, 0 services and 0 servers
[03:49:26] * 1 1 :Current local users: 1, Max: 1
[03:49:26] * 1 1 :Current global users: 1, Max: 1
[03:49:26] * Highest connection count: 1 (1 connections received)
[03:49:26] * - irc1.localdomain message of the day
[03:49:26] * - Hello. This is the Debian default MOTD sentence
[03:49:26] * End of MOTD command
[03:51:55] * You are now known as acidburn

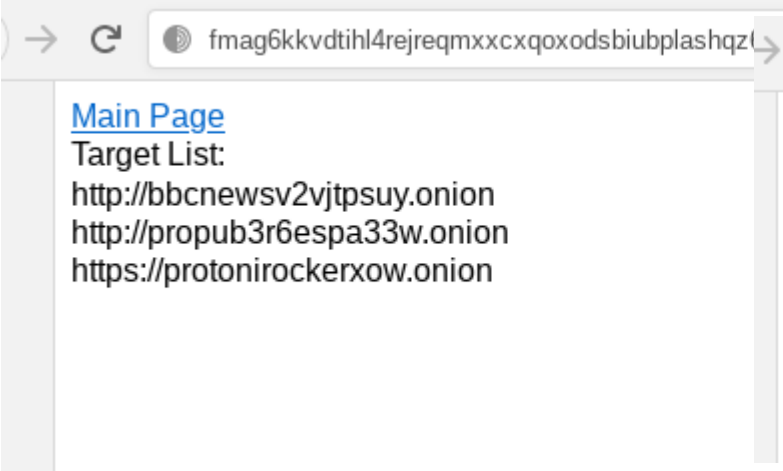
Research

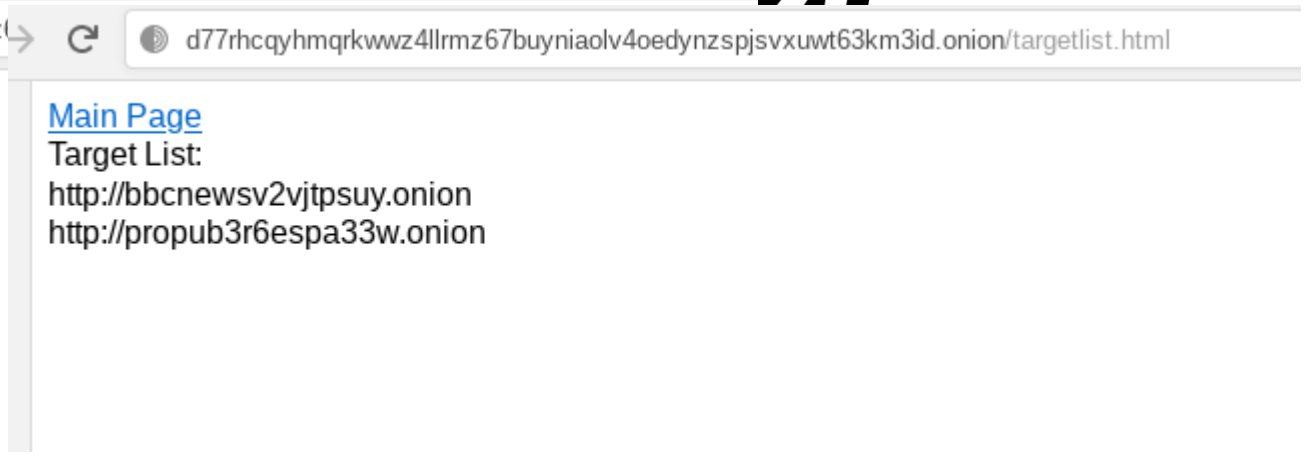

acidburn @ New Network / #research - HexChat
lexChat View Server Settings Window Help
New Network
#research
1 ops, 2 total
acidburn
zerocool
[03:49:52] * Now talking on #research
[03:50:14] * Now talking on #research
[03:51:30] Bad arguments for user command.
[03:51:35] * You have left channel #research (Leaving)
[03:52:02]
[03:52:02] * Loaded log from Sun Sep 27 03:51:35 2020
[03:52:02]
[03:52:02] * Now talking on #research
[03:52:14] * zerocool (~mint@localhost) has joined
[03:53:20] zerocool hey i found a sweet new meail service that might have some info on one of our targets
[03:53:34] acidburn that's great, put it in the wiki
[03:53:42] zerocool what page?
[03:53:53] acidburn just at the end of the target list
[03:54:01] zerocool okay, thanks!
[04:09:48] acidburn hey i don't see it?
[04:10:03] acidburn which wiki did you put it on?
[04:10:17] zerocool ffmag, is that okay?
[04:10:35] acidburn ya sorry i was using d77 but i forgot to pull first

Research

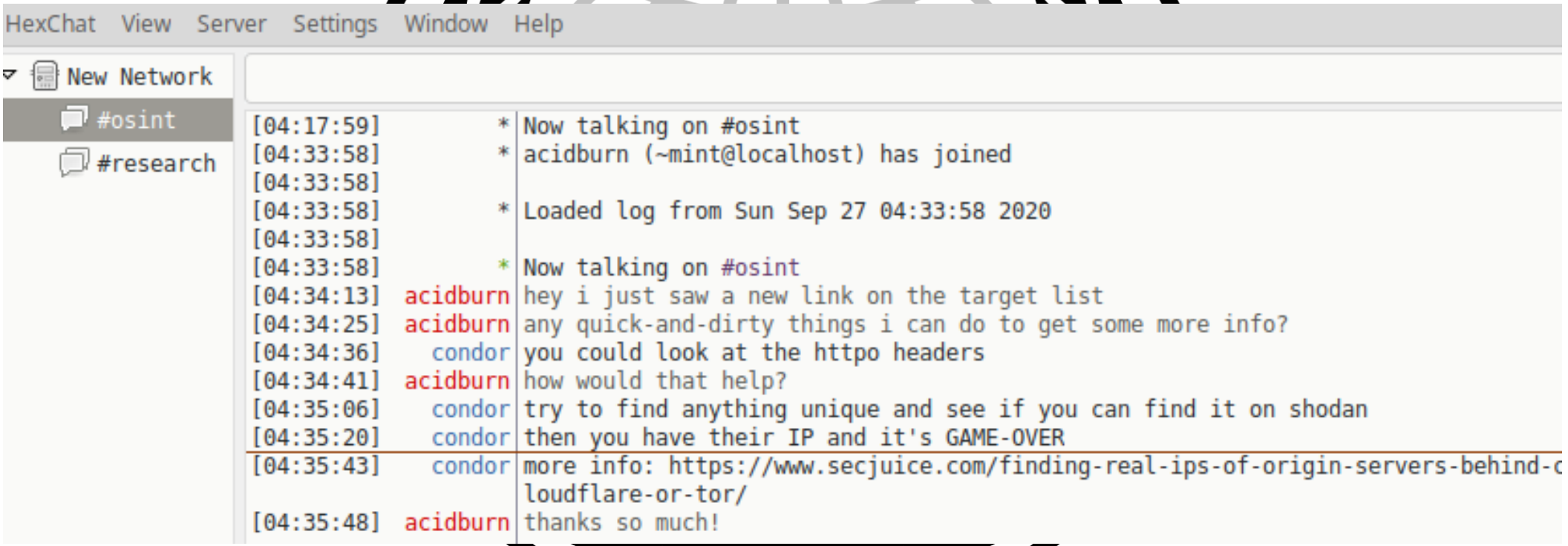

fmag6kkvdtihl4rejreqmxxcxqoxodsbiubplashqz62ymph2fx2rzyd
Target List:
Link to Target List
Last Modified: 1601179757


d77rhcqyhmqrkwwz4llrmz67buyniaolv4oedynzspjsvxuwt63km3id.onion
Target List:
Link to Target List
Last Modified: 1601179710


fmag6kkvdtihl4rejreqmxxcxqoxodsbiubplashqz
Main Page
Target List:
http://bbcnewsv2vjtpsuy.onion
http://propub3r6espa33w.onion
https://protonirockerxow.onion


d77rhcqyhmqrkwwz4llrmz67buyniaolv4oedynzspjsvxuwt63km3id.onion/targetlist.html
Main Page
Target List:
http://bbcnewsv2vjtpsuy.onion
http://propub3r6espa33w.onion

OSINT


HexChat View Server Settings Window Help
New Network
#osint
#research
[04:17:59] * Now talking on #osint
[04:33:58] * acidburn (~mint@localhost) has joined
[04:33:58]
[04:33:58] * Loaded log from Sun Sep 27 04:33:58 2020
[04:33:58]
[04:33:58] * Now talking on #osint
[04:34:13] acidburn hey i just saw a new link on the target list
[04:34:25] acidburn any quick-and-dirty things i can do to get some more info?
[04:34:36] condor you could look at the httpo headers
[04:34:41] acidburn how would that help?
[04:35:06] condor try to find anything unique and see if you can find it on shodan
[04:35:20] condor then you have their IP and it's GAME-OVER
[04:35:43] condor more info: https://www.secjuice.com/finding-real-ips-of-origin-servers-behind-c
loudflare-or-tor/
[04:35:48] acidburn thanks so much!

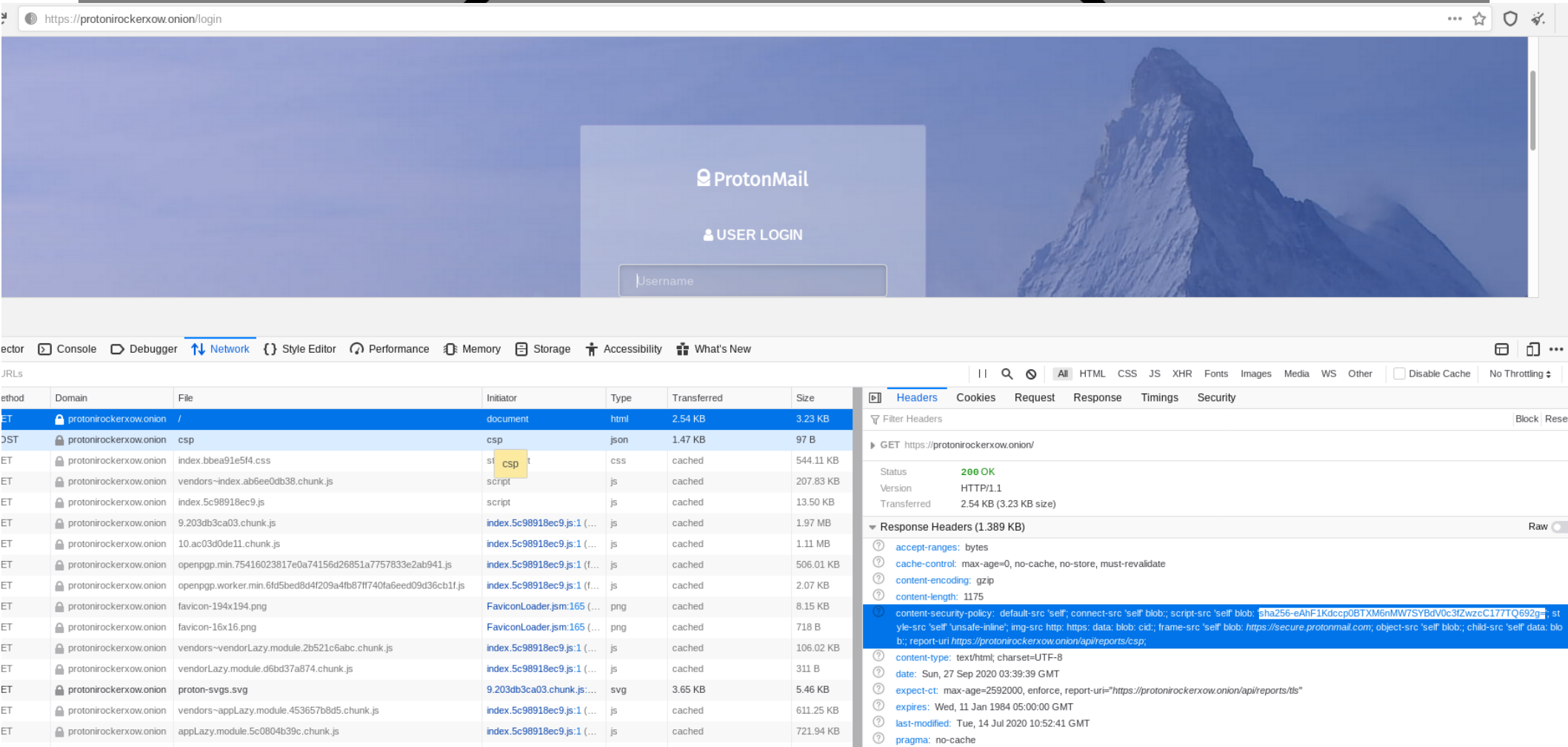
its own mail server on the same server and IP as the web server, the origin server IP will be in the MX records.

3. HTTP Headers

With data-driven platforms that let anyone do powerful searches across a huge amount of data, even finding origin servers by comparing HTTP headers is a possibility.

Especially when having a pretty unique server header with various software including subversions, finding you is getting much easier.
This is also not limited to a single parameter. As mentioned in **1.1**, you can combine search parameters on Censys. The **likelihood of being found** with this method is **increasing with every less common header key or value** you are sending.

OSINT


https://protonirockerxow.onion/login
ProtonMail
USER LOGIN
Username
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
What's New
csp
Headers
Cookies
Request
Response
Timings
Security
GET https://protonirockerxow.onion/
Status 200 OK
Version HTTP/1.1
Transferred 2.54 KB (3.23 KB size)
Response Headers (1.389 KB)
accept-ranges: bytes
cache-control: max-age=0, no-cache, no-store, must-revalidate
content-encoding: gzip
content-length: 1175
content-security-policy: default-src 'self'; connect-src 'self' blob:; script-src 'self' blob: sha256-eAhF1Kdccp0BTXM6nMW7SYBdV0c3fZwzcC177TQ692g=; style-src 'self' 'unsafe-inline'; img-src http: https: data: blob: cid:; frame-src 'self' blob: https://secure.protonmail.com; object-src 'self' blob:; child-src 'self' data: blob:; report-uri https://protonirockerxow.onion/api/reports/csp;
content-type: text/html; charset=UTF-8
date: Sun, 27 Sep 2020 03:39:39 GMT
expect-ct: max-age=2592000, enforce, report-uri="https://protonirockerxow.onion/api/reports/tls"
expires: Wed, 11 Jan 1984 05:00:00 GMT
last-modified: Tue, 14 Jul 2020 10:52:41 GMT
pragma: no-cache

OSINT

SHODAN | sha256-eAhF1Kdccp0BTXM6nMW7SYBdV0c3fZwz | Explore | Downloads | Reports | Pricing | Enterprise Access

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

5

TOP COUNTRIES

Switzerland	4
United States	1

TOP ORGANIZATIONS

Proton Technologies AG	4
Google Cloud	1

TOP PRODUCTS

nginx	1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Login - ProtonMail

185.70.40.151
185-70-40-151.protonmail.ch
Proton Technologies AG
Added on 2020-08-30 20:37:55 GMT
Switzerland

SSL Certificate

Issued By:
|- Common Name: SwissSign EV Gold CA 2014 - G22
|- Organization: SwissSign AG
Issued To:
|- Common Name: protonmail.com
|- Organization: Proton Technologies AG

Supported SSL Versions
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
date: Sun, 30 Aug 2020 20:37:55 GMT
last-modified: Mon, 17 Aug 2020 09:58:27 GMT
accept-ranges: bytes
content-length: 3309
vary: Accept-Encoding
cache-control: max-age=0, no-cache, no-store, must-revalidate
expires: Wed, 11 Jan 1984 05:00:00 GMT
set-cookie: Session-Id=X0wO...
```

Login - ProtonMail

185.70.41.133
185-70-41-133.protonmail.ch
Proton Technologies AG
Added on 2020-09-26 13:07:19 GMT
Switzerland

SSL Certificate

Issued By:
|- Common Name: SwissSign EV Gold CA 2014 - G22
|- Organization: SwissSign AG
Issued To:
|- Common Name: protonmail.com
|- Organization: Proton Technologies AG

Supported SSL Versions
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
date: Sat, 26 Sep 2020 13:07:19 GMT
last-modified: Mon, 17 Aug 2020 09:58:27 GMT
accept-ranges: bytes
content-length: 3309
vary: Accept-Encoding
cache-control: max-age=0, no-cache, no-store, must-revalidate
expires: Wed, 11 Jan 1984 05:00:00 GMT
set-cookie: Session-Id=X289...
```

Login - ProtonMail

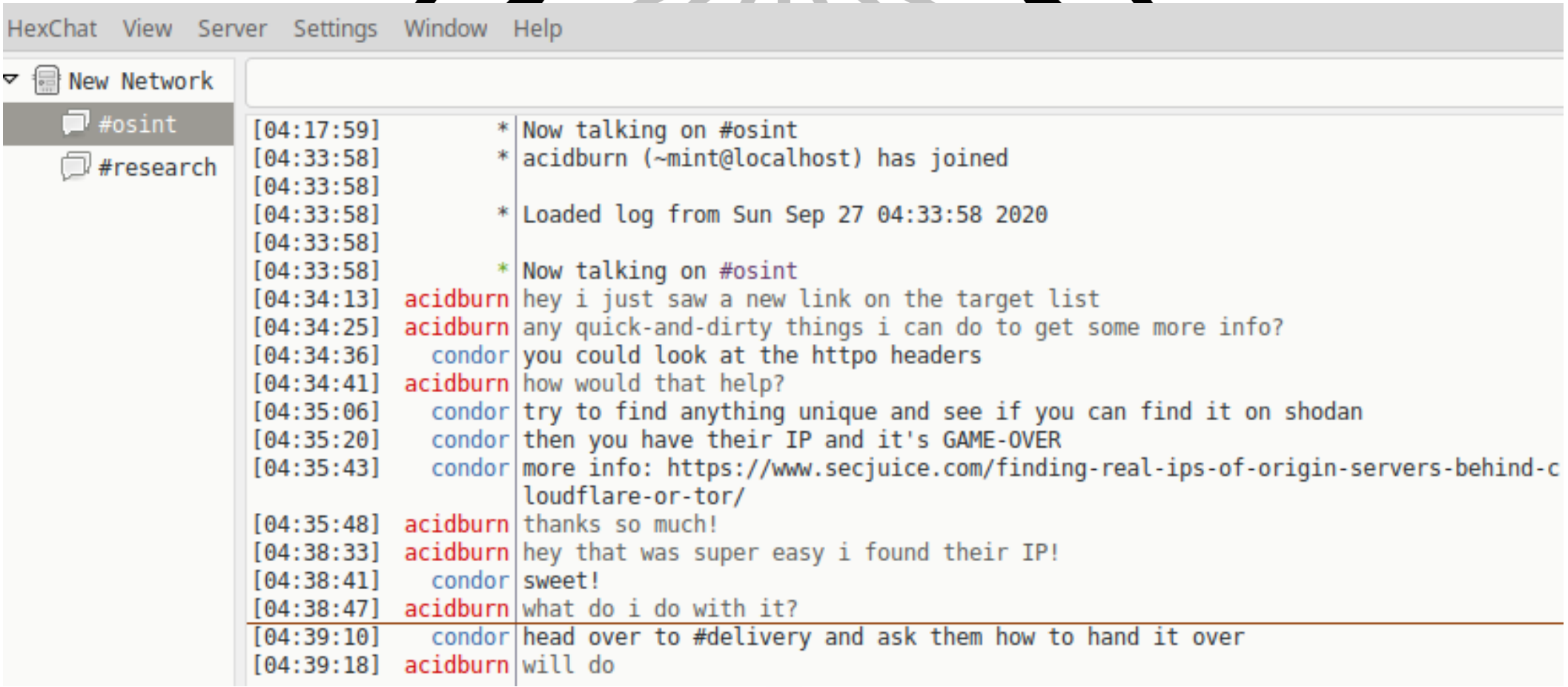
185.70.41.130
185-70-41-130.protonmail.ch
Proton Technologies AG

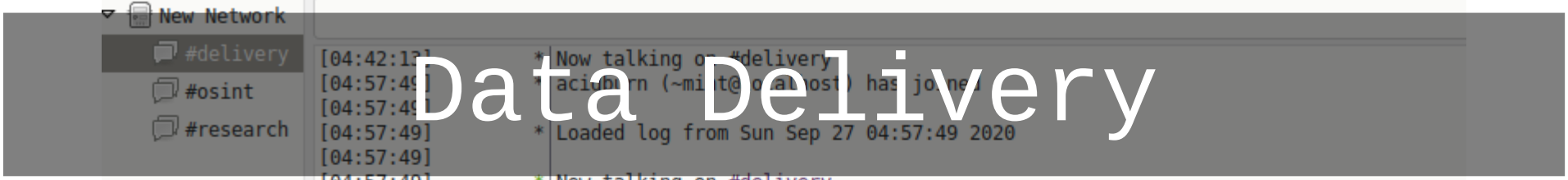
SSL Certificate

Issued By:

```
HTTP/1.1 200 OK
date: Wed, 23 Sep 2020 17:41:27 GMT
```

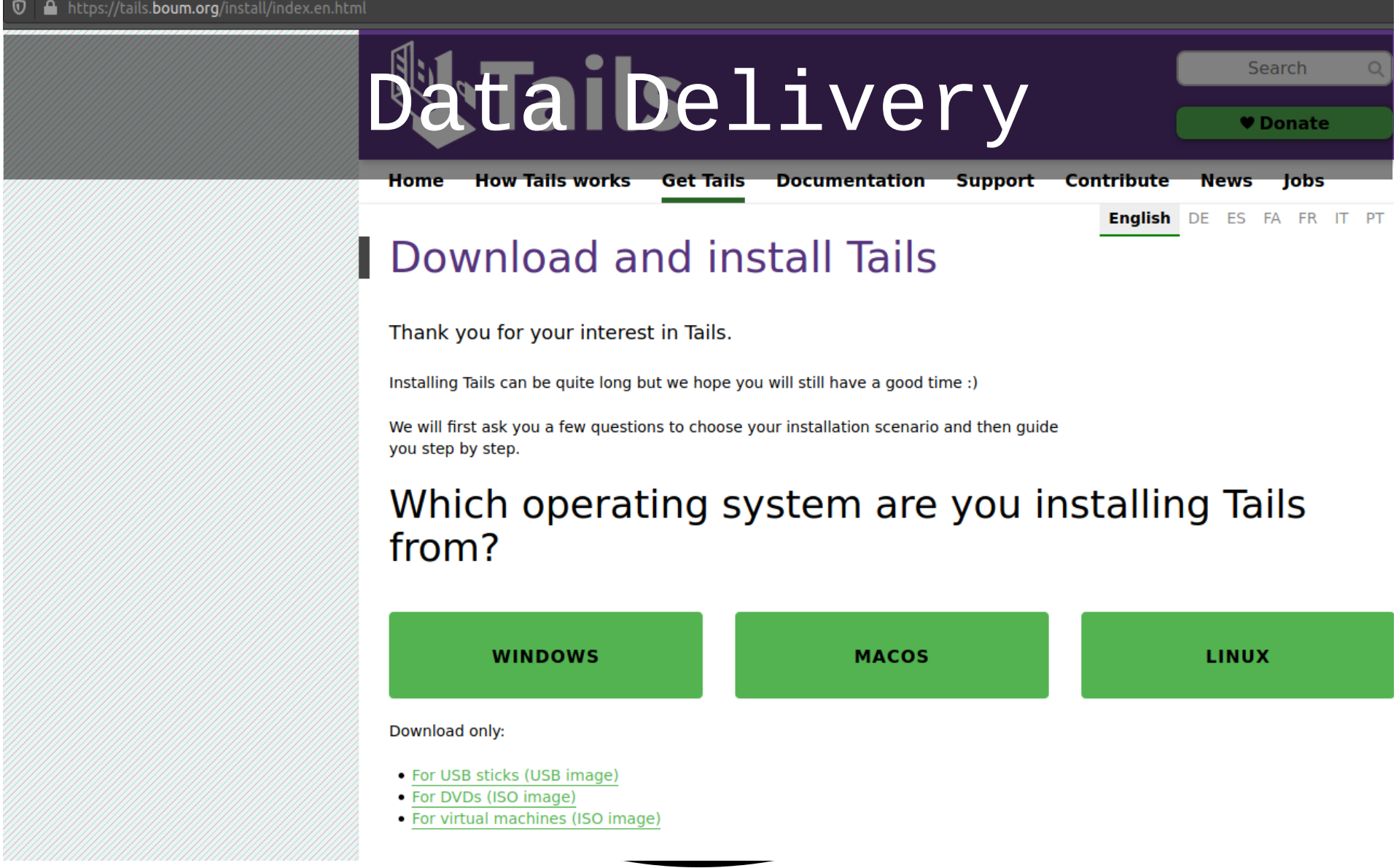
OSINT


HexChat View Server Settings Window Help
New Network
#osint
#research
[04:17:59] * Now talking on #osint
[04:33:58] * acidburn (~mint@localhost) has joined
[04:33:58]
[04:33:58] * Loaded log from Sun Sep 27 04:33:58 2020
[04:33:58]
[04:33:58] * Now talking on #osint
[04:34:13] acidburn hey i just saw a new link on the target list
[04:34:25] acidburn any quick-and-dirty things i can do to get some more info?
[04:34:36] condor you could look at the httpo headers
[04:34:41] acidburn how would that help?
[04:35:06] condor try to find anything unique and see if you can find it on shodan
[04:35:20] condor then you have their IP and it's GAME-OVER
[04:35:43] condor more info: https://www.secjuice.com/finding-real-ips-of-origin-servers-behind-c
loudflare-or-tor/
[04:35:48] acidburn thanks so much!
[04:38:33] acidburn hey that was super easy i found their IP!
[04:38:41] condor sweet!
[04:38:47] acidburn what do i do with it?
[04:39:10] condor head over to #delivery and ask them how to hand it over
[04:39:18] acidburn will do



New Network
#delivery
#osint
#research

[04:42:13] * Now talking on #delivery
[04:57:49] * acidburn (~mint@localhost) has joined
[04:57:49] * Now talking on #delivery
[04:57:49] * Loaded log from Sun Sep 27 04:57:49 2020
[04:57:49]
[04:57:49] * Now talking on #delivery
[04:58:15] acidburn hey! I found some info and was told to come here to figure out how to deliver it
[04:58:34] mendax that's great!
[04:58:42] mendax here's our standard rund-won:
[04:59:11] mendax - Decide exactly what detaisls you're giving
[04:59:20] mendax - Prune out anything that might identify our existence
[04:59:28] mendax -get Tails (tails.boum.org)
[04:59:38] mendax - write down athe info on a small piece of paper
[05:00:02] mendax - head out NEAR a local coffeshop/place with wifi
[05:00:11] mendax - DON"T GO IN THE PLACE for the next month
[05:00:28] mendax - Find a nice spot to sit with your lappy top for less than 30 min
[05:00:28] mendax - boot up tails
[05:00:37] mendax - go to 'https://report.cybertip.org'
[05:00:42] mendax enter your info
[05:00:44] mendax double-check it
[05:00:46] mendax -submit
[05:00:57] mendax -close down everything normally, allowing tails to wipe the RAM
[05:01:09] mendax - calmly collect your crap and head home
[05:01:14] mendax - DESTROY the paper
[05:01:17] mendax - celebrate!
[05:01:27] acidburn holy cow that's a lot of steps!
[05:01:35] acidburn how do i destroy the paper?
[05:01:45] mendax do you have cancles?
[05:01:52] mendax *candels
[05:02:00] acidburn yes, i burn it?
[05:02:09] mendax cut it up into thin strips and burn those
[05:02:29] mendax use twezers to hold it so you can actually burn it all without burning your hands
[05:02:36] acidburn that's super clever, thanks!
[05:02:47] mendax np, good luck!


https://tails.boum.org/install/index.en.html
Data Delivery
Search
Donate
Home
How Tails works
Get Tails
Documentation
Support
Contribute
News
Jobs
English
DE
ES
FA
FR
IT
PT
Download and install Tails
Thank you for your interest in Tails.
Installing Tails can be quite long but we hope you will still have a good time :)
We will first ask you a few questions to choose your installation scenario and then guide you step by step.
Which operating system are you installing Tails from?
WINDOWS
MACOS
LINUX
Download only:
For USB sticks (USB image)
For DVDs (ISO image)
For virtual machines (ISO image)

Data Delivery

https://report.cybertip.org

Report an incident

Information entered into this report will be made available to law enforcement for possible investigation. You can contact the National Center for Missing & Exploited Children 24 hours a day at 1-800-THE-LOST (1-800-843-5678).

0% complete

Incident Information Your Information:

What are you reporting?*

Select

Select a value...

Where did the incident occur?

Email

Select a value...

Please specify as many details as possible

Please describe the incident you are reporting

https://protonirockerxow.onion
185.70.40.151

Approximate Date and Time of Incident

Time Zone

Select

Report It

24-Hour HOTLINE

1-800-THE-LOST (1-800-843-5678)

If you think you have seen a missing child, contact the National Center for Missing & Exploited Children 24-hours a day, 7 days a week.

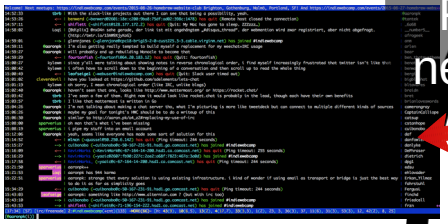
Report Child Sexual Exploitation

Use the CyberTipline to report child sexual exploitation. Reports may be made 24-hours a day, 7 days a week online at www.cybertipline.org

Learn more about CyberTipline

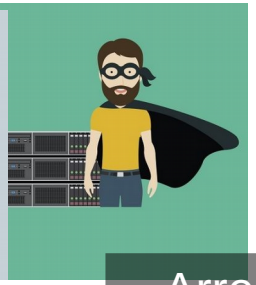
Celebrate!

The DATDA Collective (TDC)



Posts new link

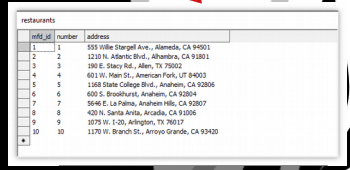
Finds Address



Arrests Site Operator

Puts link in Target List

Starts Targeting Site



Sends Address to POPO