OSINT Tools for diving deep into the Dark Web

Apurv Singh Gautam
@ASG_Sc0rpi0n

$whoami

- Apurv Singh Gautam (@ASG_Sc0rpi0n)
- Security Researcher, Threat Intel/Hunting
- Cybersecurity @ Georgia Tech (Go Jackets)

- Hobbies
  - Hiking 🚶
  - Lockpicking 🔐

n|u

CYBRARY

cybercademy

STATIONX

- Social
  - Twitter - @ASG_Sc0rpi0n
  - Website - apurvsinghgautam.me

Agenda

- Introduction to the Dark Web
- Why focusing on the Dark Web?
- Search engine tools for the Dark Web
- Tools to get onion links from the Dark Web
- Tools to scan onion links
- Tools to scrape data from the Dark Web
- Tools to create data collection architecture
- Conclusion

1. Introduction to the Dark Web

Clear Web? Deep Web? Dark Web?

SANS Summits

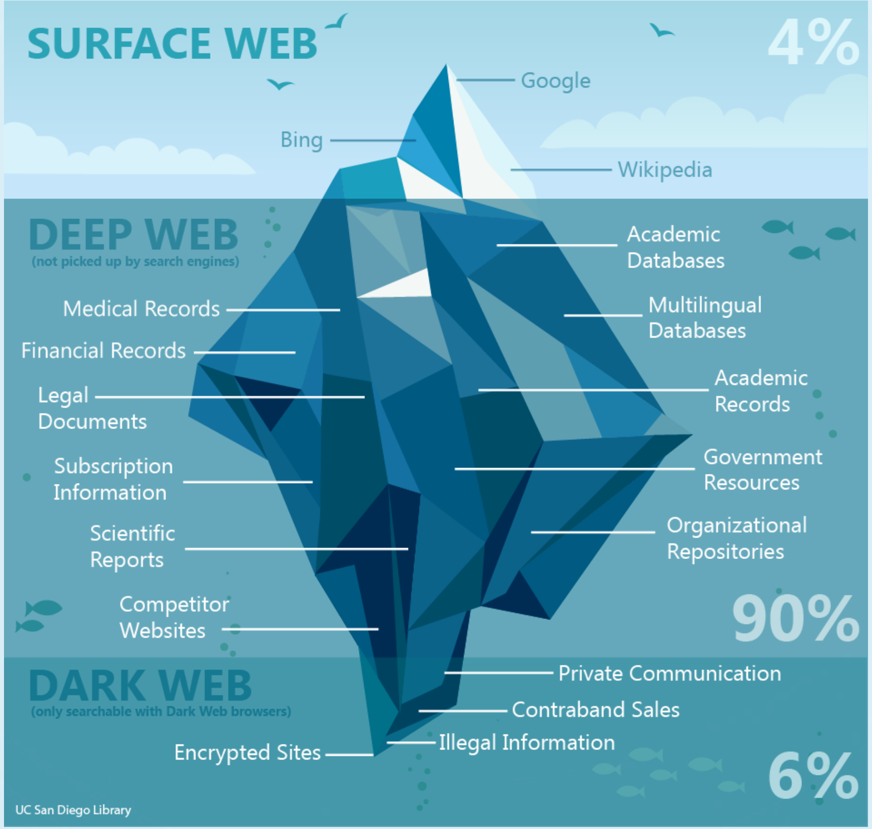
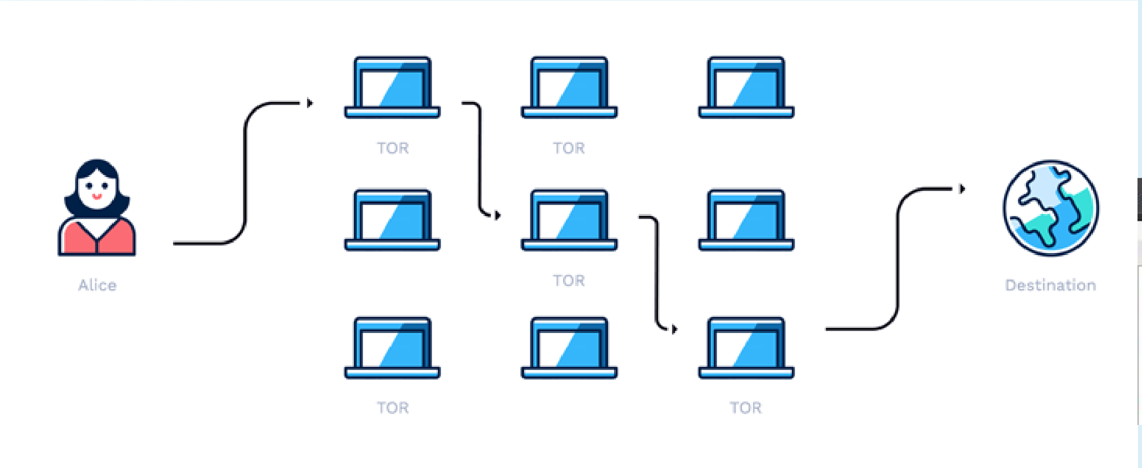


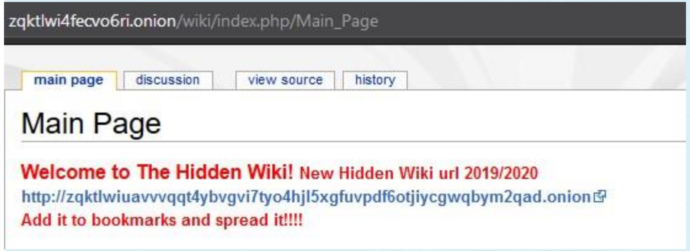
Image Source: UC San Diego Library

Accessing the Dark Web

- Tor /I2P/ZeroNet
- .onion domains/.i2p domains
- Traffic through relays

I2P




zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page

Main Page

Welcome to The Hidden Wiki! New Hidden Wiki url 2019/2020
http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion
Add it to bookmarks and spread it!!!!

Image Sources: Hotspot Shield, Tor Project, I2P Project, ZeroNet

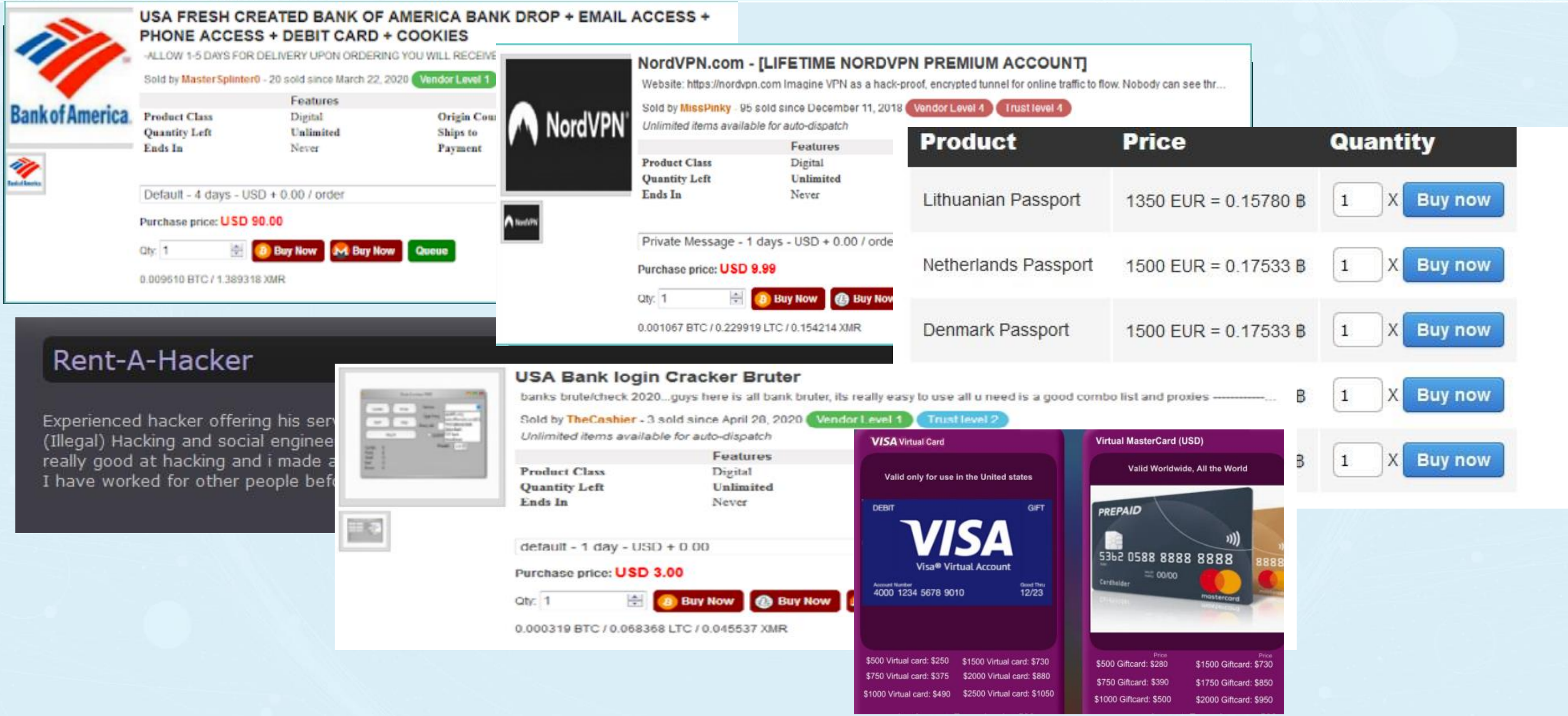
Relevant site types?

SANS Summits

- General Markets
- PII & PHI
- Credit Cards
- Digital identities
- Information Trading
- Remote Access
- Personal Documents
- Electronic Wallets
- Insider Threats

Image Source: Intsights

Product/Services Examples



USA FRESH CREATED BANK OF AMERICA BANK DROP + EMAIL ACCESS + PHONE ACCESS + DEBIT CARD + COOKIES

-ALLOW 1-5 DAYS FOR DELIVERY UPON ORDERING YOU WILL RECEIVE

Sold by MasterSplinter0 - 20 sold since March 22, 2020 Vendor Level 1

Features		
Product Class	Digital	Origin Cou
Quantity Left	Unlimited	Ships to
Ends In	Never	Payment

Default - 4 days - USD + 0.00 / order

Purchase price: USD 90.00

Qty: 1 Buy Now Buy Now Queue

0.009610 BTC / 1.389318 XMR

NordVPN.com - [LIFETIME NORDVPN PREMIUM ACCOUNT]

Website: https://nordvpn.com Imagine VPN as a hack-proof, encrypted tunnel for online traffic to flow. Nobody can see thr...

Sold by MissPinky - 95 sold since December 11, 2018 Vendor Level 4 Trust level 4

Unlimited items available for auto-dispatch

Features	
Product Class	Digital
Quantity Left	Unlimited
Ends In	Never

Private Message - 1 days - USD + 0.00 / orde

Purchase price: USD 9.99

Qty: 1 Buy Now Buy Now

0.001067 BTC / 0.229919 LTC / 0.154214 XMR

Product	Price	Quantity
Lithuanian Passport	1350 EUR = 0.15780 B	1 X Buy now
Netherlands Passport	1500 EUR = 0.17533 B	1 X Buy now
Denmark Passport	1500 EUR = 0.17533 B	1 X Buy now
	B	1 X Buy now
	B	1 X Buy now

Rent-A-Hacker

Experienced hacker offering his ser
(Illegal) Hacking and social enginee
really good at hacking and i made a
I have worked for other people bef

USA Bank login Cracker Bruter

banks brute/check 2020...guys here is all bank bruter, its really easy to use all u need is a good combo list and proxies -----------...

Sold by TheCashier - 3 sold since April 28, 2020 Vendor Level 1 Trust level 2

Unlimited items available for auto-dispatch

Features	
Product Class	Digital
Quantity Left	Unlimited
Ends In	Never

default - 1 day - USD + 0.00

Purchase price: USD 3.00

Qty: 1 Buy Now Buy Now

0.000319 BTC / 0.068368 LTC / 0.045537 XMR

VISA Virtual Card

Valid only for use in the United states

$500 Virtual card: $250	$1500 Virtual card: $730
$750 Virtual card: $375	$2000 Virtual card: $880
$1000 Virtual card: $490	$2500 Virtual card: $1050

Virtual MasterCard (USD)

Valid Worldwide, All the World

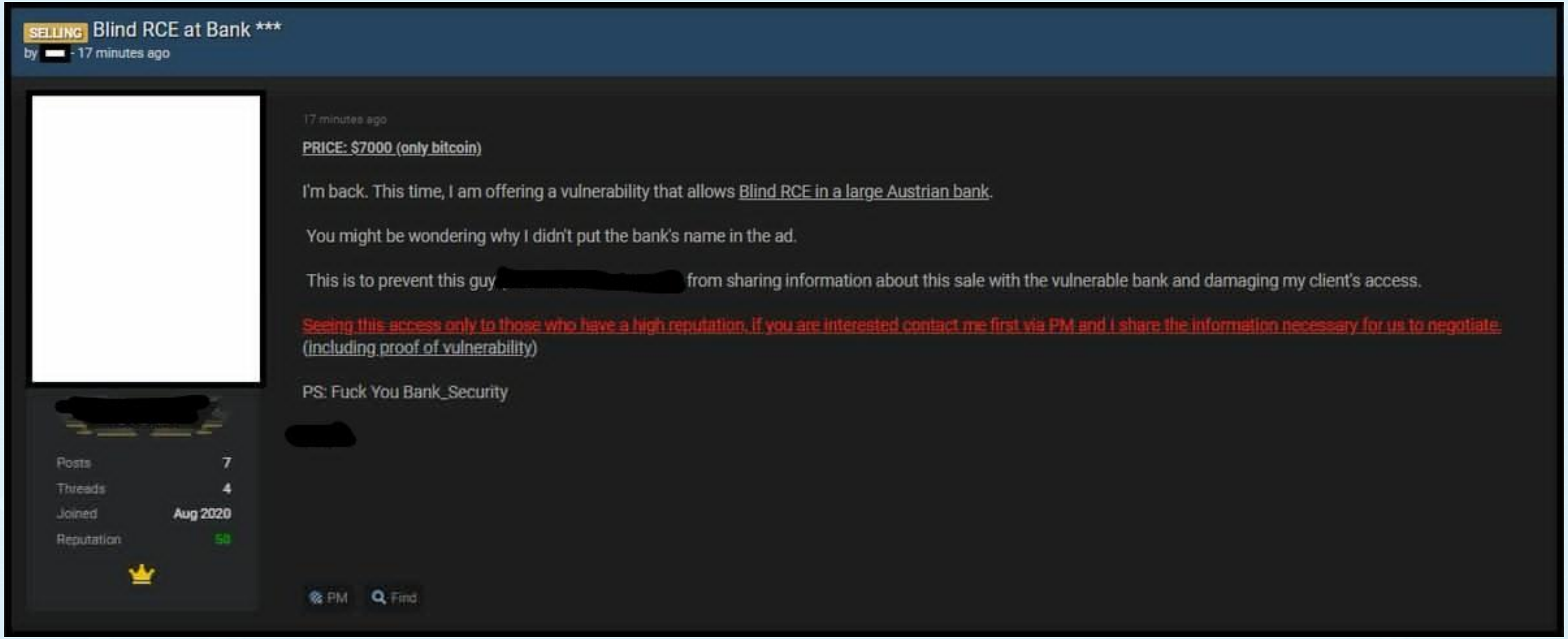
Price	Price
$500 Giftcard: $280	$1500 Giftcard: $730
$750 Giftcard: $390	$1750 Giftcard: $850
$1000 Giftcard: $500	$2000 Giftcard: $950

2. Why focusing on the Dark Web?

Why So Serious (Eh! Important)?

- Hacker forums, darknet markets, dump shops, etc.
- Criminals can learn, monetize, trade, and communicate
- Identification of compromised assets
- Can potentially identify attacks in earlier stages
- Direct impacts – PII (Personal Info), financial, EHRs (healthcare records), trade secrets
- Indirect impacts – reputation, revenue loss, legal penalties

Why you should care?



SELLING Blind RCE at Bank ***

by [redacted] - 17 minutes ago

17 minutes ago

PRICE: $7000 (only bitcoin)

I'm back. This time, I am offering a vulnerability that allows Blind RCE in a large Austrian bank.

You might be wondering why I didn't put the bank's name in the ad.

This is to prevent this guy [redacted] from sharing information about this sale with the vulnerable bank and damaging my client's access.

Seeing this access only to those who have a high reputation. If you are interested contact me first via PM and I share the information necessary for us to negotiate. (including proof of vulnerability)

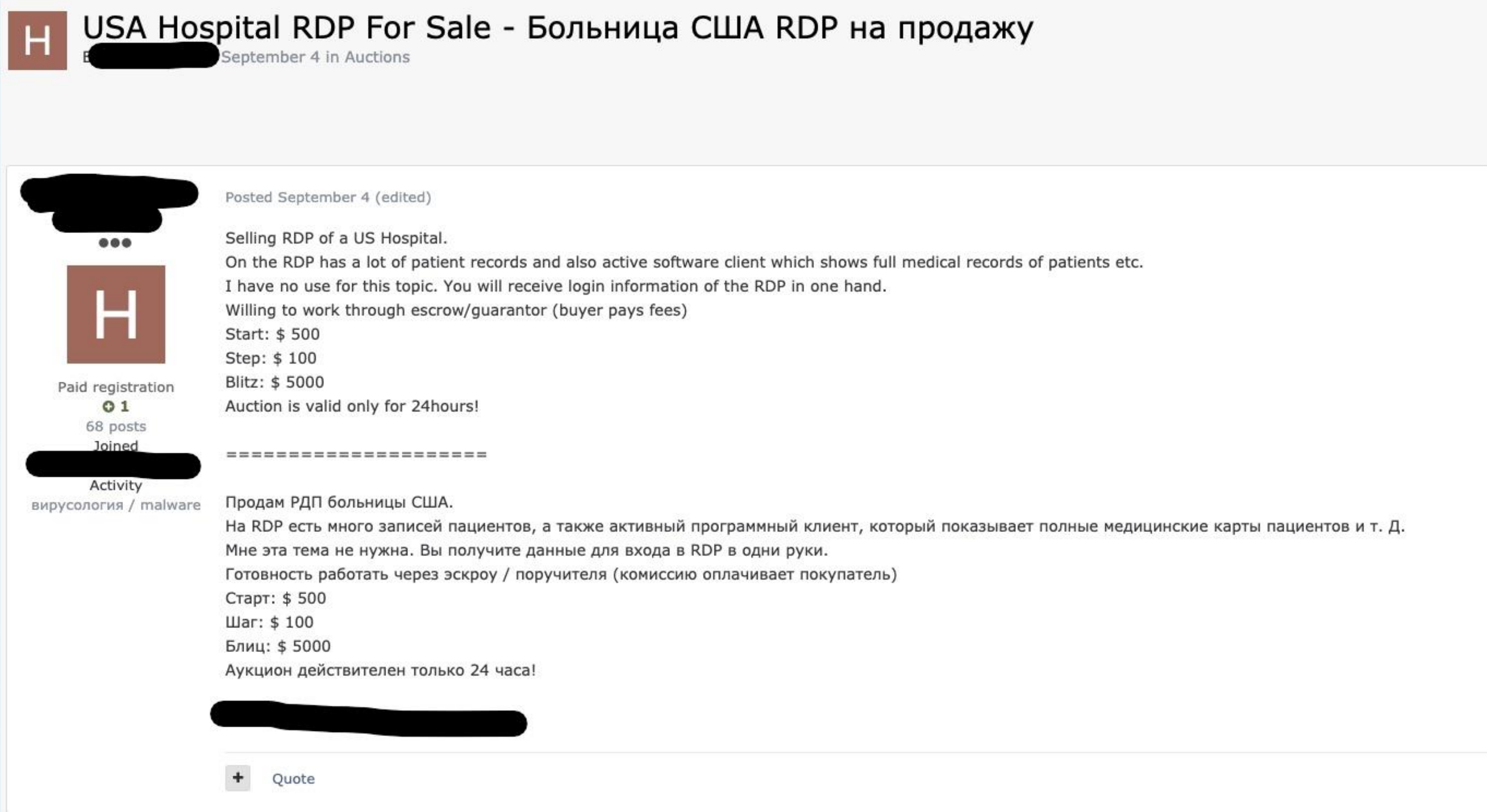
PS: Fuck You Bank_Security

[redacted]

[redacted]

Posts	7
Threads	4
Joined	Aug 2020
Reputation	50

Why you should care?



USA Hospital RDP For Sale - Больница США RDP на продажу

[redacted] September 4 in Auctions

[redacted]

●●●

H

Paid registration

⊕ 1

68 posts

Joined

[redacted]

Activity

вирусология / malware

Posted September 4 (edited)

Selling RDP of a US Hospital.
On the RDP has a lot of patient records and also active software client which shows full medical records of patients etc.
I have no use for this topic. You will receive login information of the RDP in one hand.
Willing to work through escrow/guarantor (buyer pays fees)
Start: $ 500
Step: $ 100
Blitz: $ 5000
Auction is valid only for 24hours!

=====================

Продам РДП больницы США.
На RDP есть много записей пациентов, а также активный программный клиент, который показывает полные медицинские карты пациентов и т. Д.
Мне эта тема не нужна. Вы получите данные для входа в RDP в одни руки.
Готовность работать через эскроу / поручителя (комиссию оплачивает покупатель)
Старт: $ 500
Шаг: $ 100
Блиц: $ 5000
Аукцион действителен только 24 часа!

[redacted]

3. Search engine tools for the Dark Web

Tools

- Katana
- OnionSearch
- Ahmia Search Engine
- DarkSearch

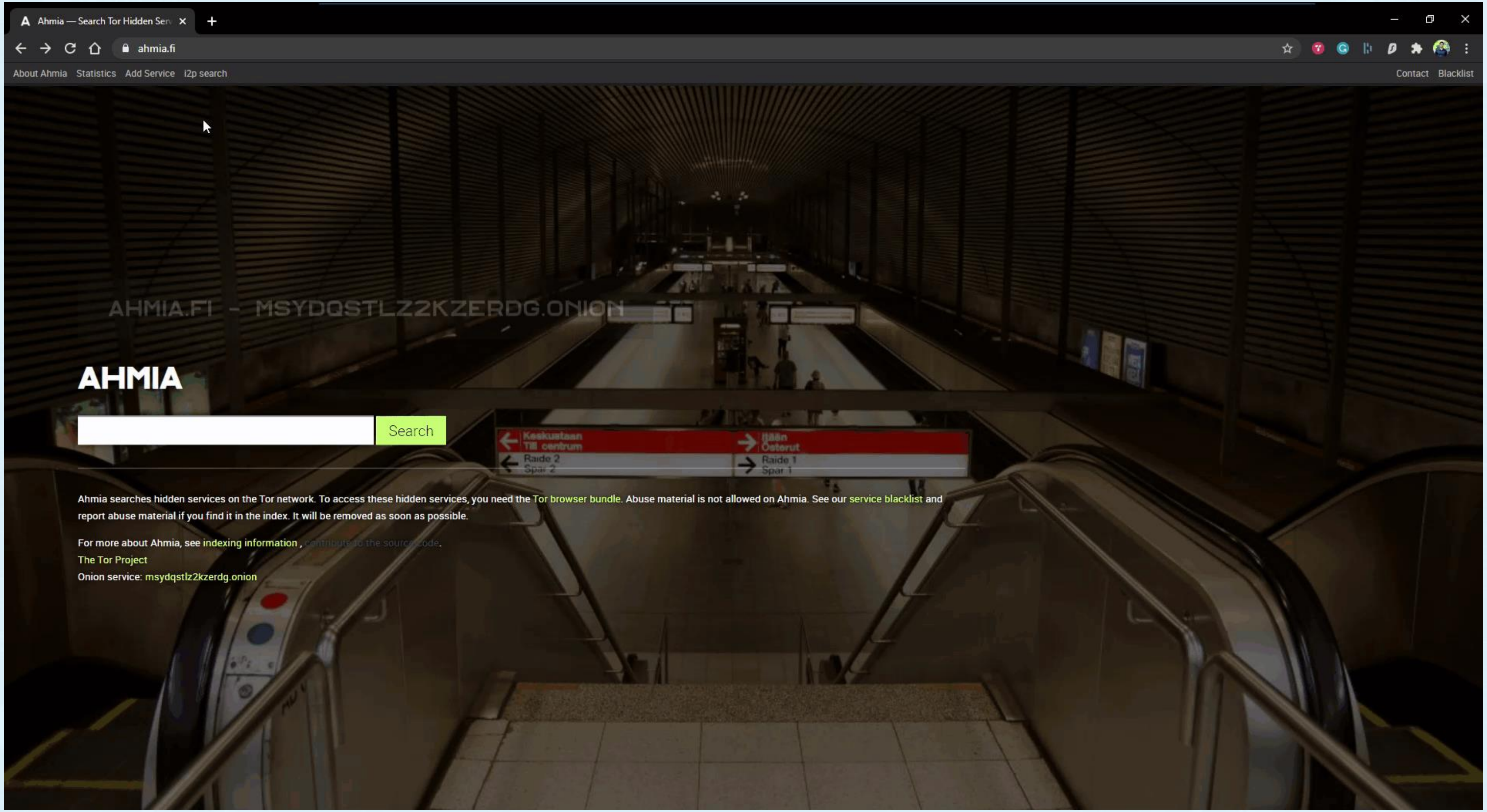
Image Sources: Katana, OnionSearch, Ahmia, DarkSearch

Katana

OnionSearch

OnionSearch (Contd.)

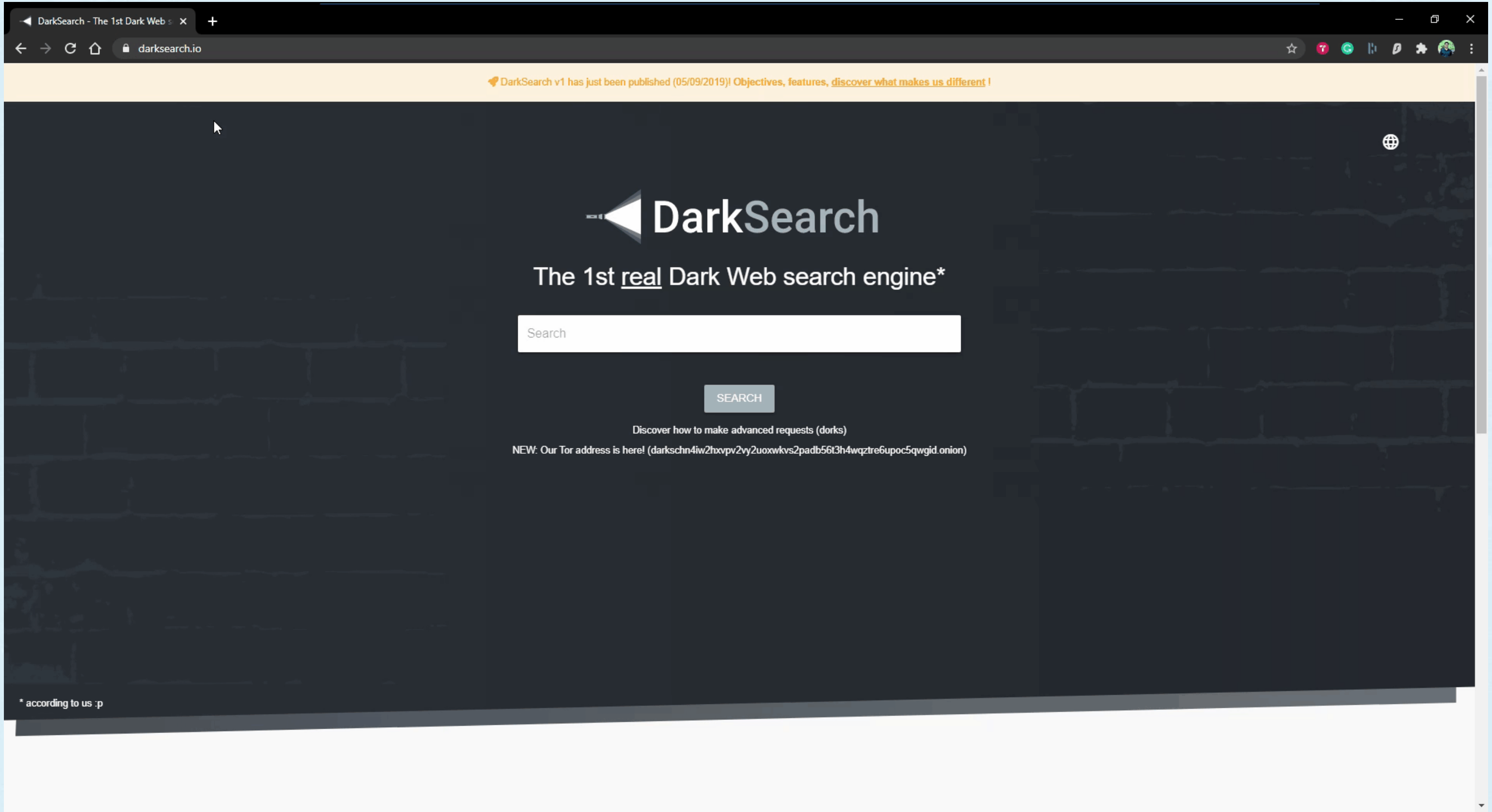
Ahmia



Ahmia searches hidden services on the Tor network. To access these hidden services, you need the Tor browser bundle. Abuse material is not allowed on Ahmia. See our service blacklist and report abuse material if you find it in the index. It will be removed as soon as possible.

For more about Ahmia, see indexing information , contribute to the source code.
The Tor Project
Onion service: msydqstlz2kzerdg.onion

DarkSearch



DarkSearch v1 has just been published (05/09/2019)! Objectives, features, discover what makes us different !

The 1st real Dark Web search engine*

Discover how to make advanced requests (dorks)

NEW: Our Tor address is here! (darkschn4iw2hxvpv2vy2uoxwkvs2padb56t3h4wqztre6upoc5qwgid.onion)

* according to us :p

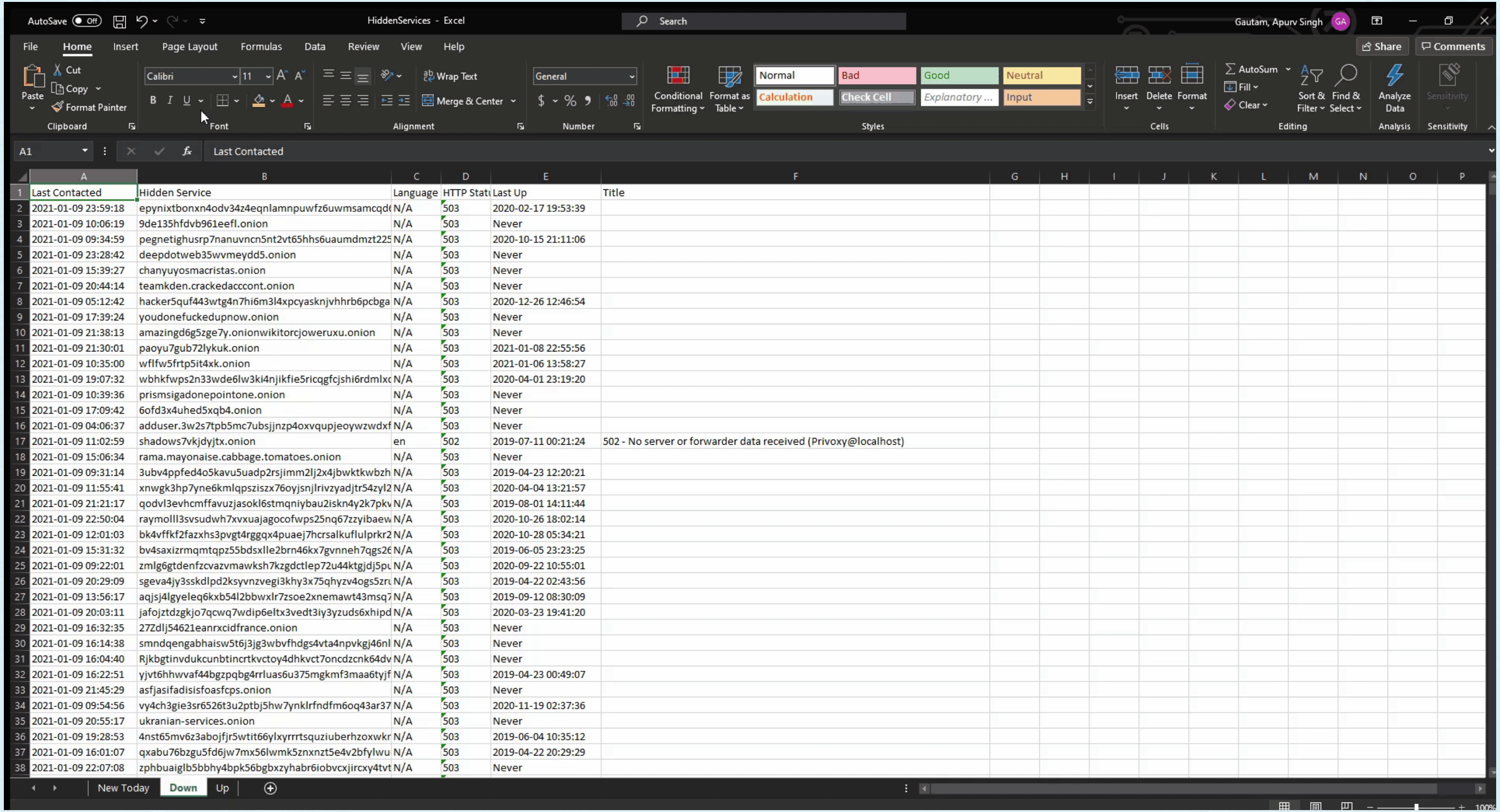
4. Tools to get onion links from the Dark Web

Tools

- Hunchly
- H-Indexer

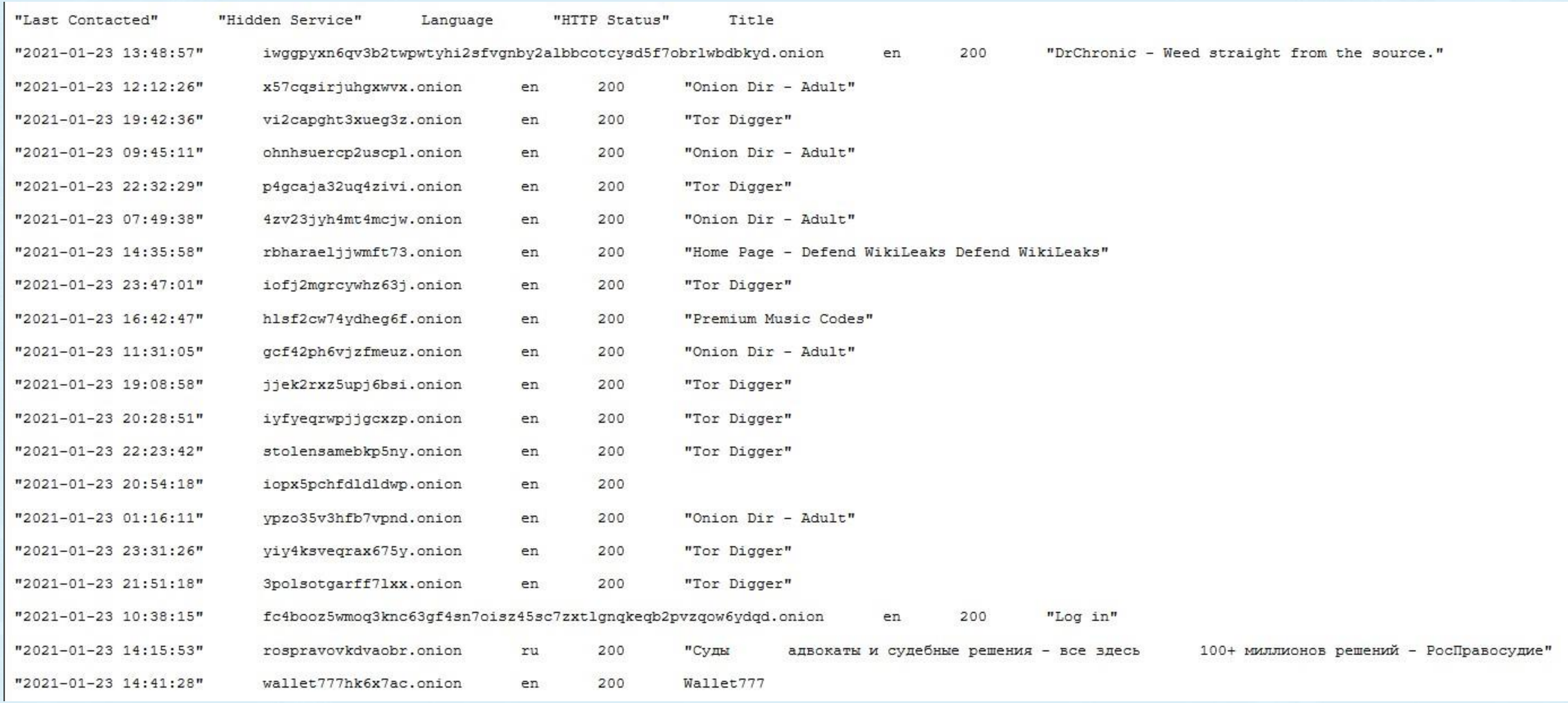
Image Sources: Hunchly

Hunchly



Last Contacted	Hidden Service	Language	HTTP Statu	Last Up	Title
2021-01-09 23:59:18	epynixtbonxn4odv34z4eqnlamnpuwfz6uwmsamcqd	N/A	503	2020-02-17 19:53:39	
2021-01-09 10:06:19	9de135hfdvb961eefl.onion	N/A	503	Never	
2021-01-09 09:34:59	pegnetighusrp7nanuvncn5nt2vt65hhs6uaumdmzt225	N/A	503	2020-10-15 21:11:06	
2021-01-09 23:28:42	deepdotweb35wvmeydd5.onion	N/A	503	Never	
2021-01-09 15:39:27	chanyuyosmacristas.onion	N/A	503	Never	
2021-01-09 20:44:14	teamkden.crackedacccont.onion	N/A	503	Never	
2021-01-09 05:12:42	hacker5quf443wtg4n7hi6m3l4xpcyasknjvhhrb6pcbga	N/A	503	2020-12-26 12:46:54	
2021-01-09 17:39:24	youdonefuckedupnow.onion	N/A	503	Never	
2021-01-09 21:38:13	amazingd6g5zge7y.onionwikitorcjoweruxu.onion	N/A	503	Never	
2021-01-09 21:30:01	paoyu7gub72lykuk.onion	N/A	503	2021-01-08 22:55:56	
2021-01-09 10:35:00	wflfw5frtp5it4xk.onion	N/A	503	2021-01-06 13:58:27	
2021-01-09 19:07:32	wbhkfwps2n33wde6lw3ki4njikfie5ricqgfcjshi6rdmlx	N/A	503	2020-04-01 23:19:20	
2021-01-09 10:39:36	prismsigadonepointone.onion	N/A	503	Never	
2021-01-09 17:09:42	6ofd3x4uhed5xqb4.onion	N/A	503	Never	
2021-01-09 04:06:37	adduser.3w2s7tpb5mc7ubsjjnzp4oxvqupjeoywzwdxf	N/A	503	Never	
2021-01-09 11:02:59	shadows7vkjdyjtx.onion	en	502	2019-07-11 00:21:24	502 - No server or forwarder data received (Privoxy@localhost)
2021-01-09 15:06:34	rama.mayonaise.cabbage.tomatoes.onion	N/A	503	Never	
2021-01-09 09:31:14	3ubv4ppfed4o5kavu5uadp2rsjimm2lj2x4jbwktkwbzh	N/A	503	2019-04-23 12:20:21	
2021-01-09 11:55:41	xnwgk3hp7yne6kmlqpsziszx76oyjsnjlrivzyadjtr54zyl2	N/A	503	2020-04-04 13:21:57	
2021-01-09 21:21:17	qodvl3evhcmffavuzjasokl6stmqniybau2iskn4y2k7pkv	N/A	503	2019-08-01 14:11:44	
2021-01-09 22:50:04	raymolll3svsudwh7xvxuajagocofwps25nq67zzyibaew	N/A	503	2020-10-26 18:02:14	
2021-01-09 12:01:03	bk4vffkf2fazxhs3pvgt4rggqx4puaej7hcrsalkuflulprkr2	N/A	503	2020-10-28 05:34:21	
2021-01-09 15:31:32	bv4saxizrmqmtqpz55bdsxlle2brn46kx7gvnneh7qgs26	N/A	503	2019-06-05 23:23:25	
2021-01-09 09:22:01	zmlg6gtdenfzcvazvmawksh7kzgdctlep72u44ktgjdj5pu	N/A	503	2020-09-22 10:55:01	
2021-01-09 20:29:09	sgeva4jy3sskdlpd2ksyvnzvegi3khy3x75qhyzv4ogs5zru	N/A	503	2019-04-22 02:43:56	
2021-01-09 13:56:17	aqjsj4lgyeleq6kxb54l2bbwxlr7zsoe2xnemawt43msq7	N/A	503	2019-09-12 08:30:09	
2021-01-09 20:03:11	jafojztdzgkjo7qcwq7wdip6eltx3vedt3iy3yzuds6xhipd	N/A	503	2020-03-23 19:41:20	
2021-01-09 16:32:35	27Zdlj54621eanrxcidfrance.onion	N/A	503	Never	
2021-01-09 16:14:38	smndqengabhaisw5t6j3jg3wbvfhdgs4vta4npvkgj46nl	N/A	503	Never	
2021-01-09 16:04:40	Rjkbgtinvdukcunbtincrtkvctoy4dhkvct7oncdzcnk64dv	N/A	503	Never	
2021-01-09 16:22:51	yjvt6hhwvaf44bgzpqbg4rrluas6u375mgkmf3maa6tyjf	N/A	503	2019-04-23 00:49:07	
2021-01-09 21:45:29	asfjasifadisisfoasfcps.onion	N/A	503	Never	
2021-01-09 09:54:56	vy4ch3gie3sr6526t3u2ptbj5hw7ynklrfndfm6oq43ar37	N/A	503	2020-11-19 02:37:36	
2021-01-09 20:55:17	ukranian-services.onion	N/A	503	Never	
2021-01-09 19:28:53	4nst65mv6z3abojfjr5wtit66ylxyrrrtsquziuberhzoxwkr	N/A	503	2019-06-04 10:35:12	
2021-01-09 16:01:07	qxabu76bzgu5fd6jw7mx56lwmk5znxnzt5e4v2bfylwu	N/A	503	2019-04-22 20:29:29	
2021-01-09 22:07:08	zphbuaiglb5bbhy4bpk56bgbxzyhabr6iobvcxjircxy4tvt	N/A	503	Never	

H-Indexer

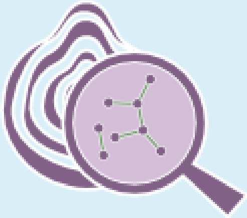


```
"Last Contacted"      "Hidden Service"      Language      "HTTP Status"      Title
"2021-01-23 13:48:57"      iwggpyxn6qv3b2twpwtyhi2sfvgnby2albbcotcysd5f7obrlwbdbkyd.onion      en      200      "DrChronic - Weed straight from the source."
"2021-01-23 12:12:26"      x57cqsirjuhgxwvx.onion      en      200      "Onion Dir - Adult"
"2021-01-23 19:42:36"      vi2capght3xueg3z.onion      en      200      "Tor Digger"
"2021-01-23 09:45:11"      ohnhsuercp2uscpl.onion      en      200      "Onion Dir - Adult"
"2021-01-23 22:32:29"      p4gcaja32uq4zivi.onion      en      200      "Tor Digger"
"2021-01-23 07:49:38"      4zv23jyh4mt4mcjw.onion      en      200      "Onion Dir - Adult"
"2021-01-23 14:35:58"      rbharaeljjwmft73.onion      en      200      "Home Page - Defend WikiLeaks Defend WikiLeaks"
"2021-01-23 23:47:01"      iofj2mgrcywhz63j.onion      en      200      "Tor Digger"
"2021-01-23 16:42:47"      hlsf2cw74ydheg6f.onion      en      200      "Premium Music Codes"
"2021-01-23 11:31:05"      gcf42ph6vjzfmeuz.onion      en      200      "Onion Dir - Adult"
"2021-01-23 19:08:58"      jjek2rxz5upj6bsi.onion      en      200      "Tor Digger"
"2021-01-23 20:28:51"      iyfyeqrwpjjgcxzp.onion      en      200      "Tor Digger"
"2021-01-23 22:23:42"      stolensamebkp5ny.onion      en      200      "Tor Digger"
"2021-01-23 20:54:18"      iopx5pchfdldldwp.onion      en      200
"2021-01-23 01:16:11"      ypzo35v3hfb7vpnd.onion      en      200      "Onion Dir - Adult"
"2021-01-23 23:31:26"      yiy4ksveqrax675y.onion      en      200      "Tor Digger"
"2021-01-23 21:51:18"      3polsotgarff7lxx.onion      en      200      "Tor Digger"
"2021-01-23 10:38:15"      fc4booz5wmoq3knc63gf4sn7oisz45sc7zxtlgnqkeqb2pvzqow6ydqd.onion      en      200      "Log in"
"2021-01-23 14:15:53"      rospravovkdvaobr.onion      ru      200      "Суды      адвокаты и судебные решения - все здесь      100+ миллионов решений - РосПравосудие"
"2021-01-23 14:41:28"      wallet777hk6x7ac.onion      en      200      Wallet777
```

5. Tools to scan onion links

Tools

- OnionScan
- Onioff
- Onion-nmap



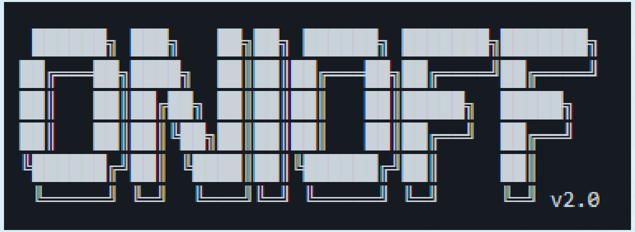


Image Sources: OnionScan, Onioff

Onionscan

Onioff

Onion-nmap

6. Tools to scrape data from the Dark Web

Tools

- TorBot
- TorCrawl
- OnionIngestor

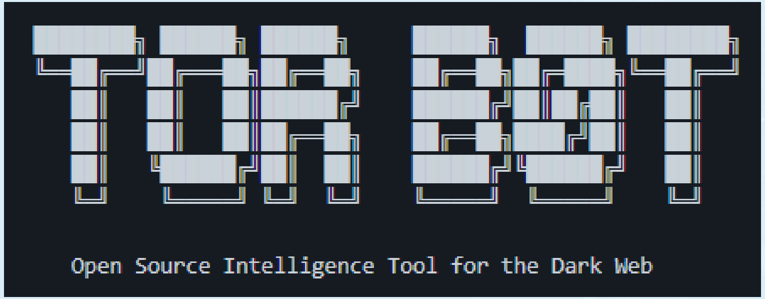
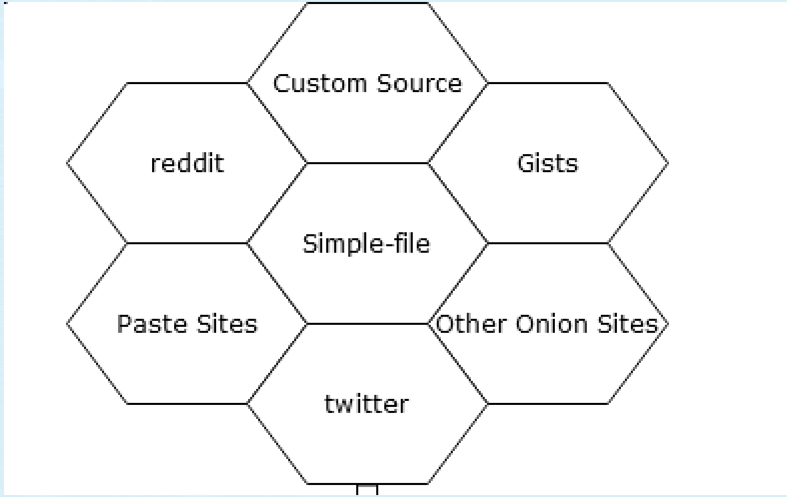


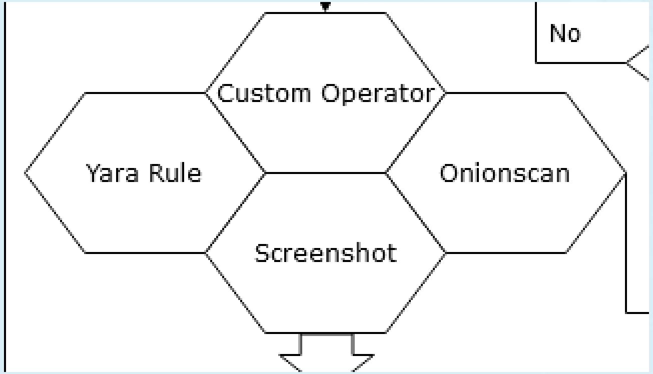
Image Sources: TorBot, OnionIngestor

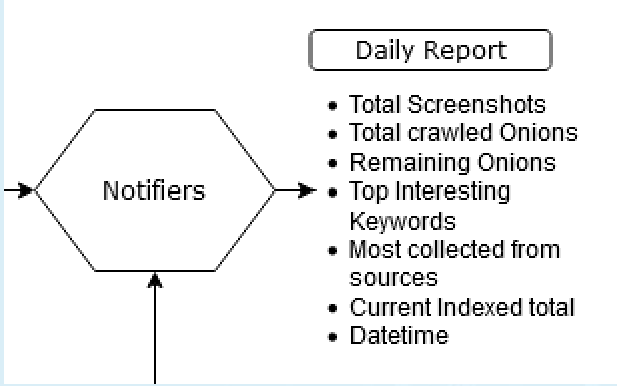
TorBot

TorCrawl

OnionIngestor

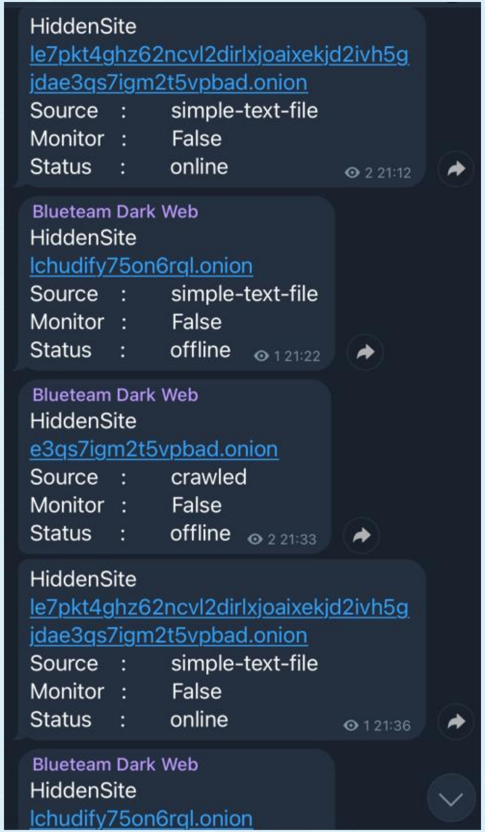






- Total Screenshots
- Total crawled Onions
- Remaining Onions
- Top Interesting Keywords
- Most collected from sources
- Current Indexed total
- Datetime

OnionIngestor (Contd.)



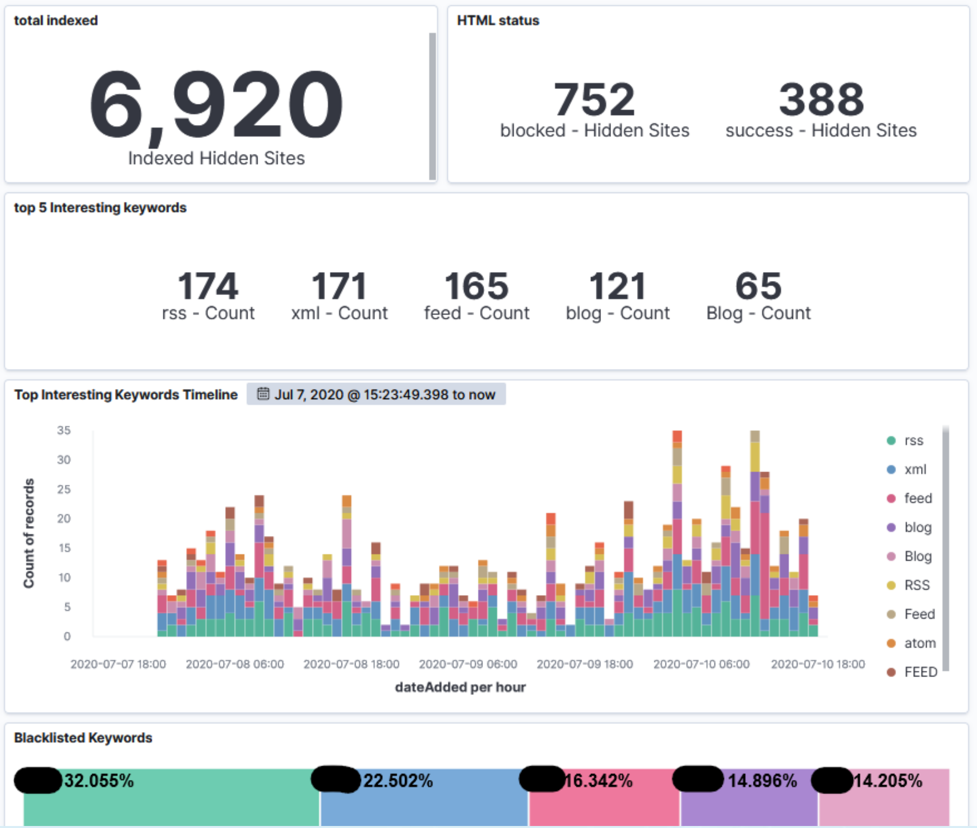
HiddenSite
le7pkt4ghz62ncvl2dirlxjoaixekjd2ivh5gjdae3qs7igm2t5vpbad.onion
Source : simple-text-file
Monitor : False
Status : online
2 21:12

Blueteam Dark Web
HiddenSite
lchudify75on6rql.onion
Source : simple-text-file
Monitor : False
Status : offline
1 21:22

Blueteam Dark Web
HiddenSite
e3qs7igm2t5vpbad.onion
Source : crawled
Monitor : False
Status : offline
2 21:33

HiddenSite
le7pkt4ghz62ncvl2dirlxjoaixekjd2ivh5gjdae3qs7igm2t5vpbad.onion
Source : simple-text-file
Monitor : False
Status : online
1 21:36

Blueteam Dark Web
HiddenSite
lchudify75on6rql.onion



total indexed

6,920
Indexed Hidden Sites

HTML status

752
blocked - Hidden Sites

388
success - Hidden Sites

top 5 Interesting keywords

174
rss - Count

171
xml - Count

165
feed - Count

121
blog - Count

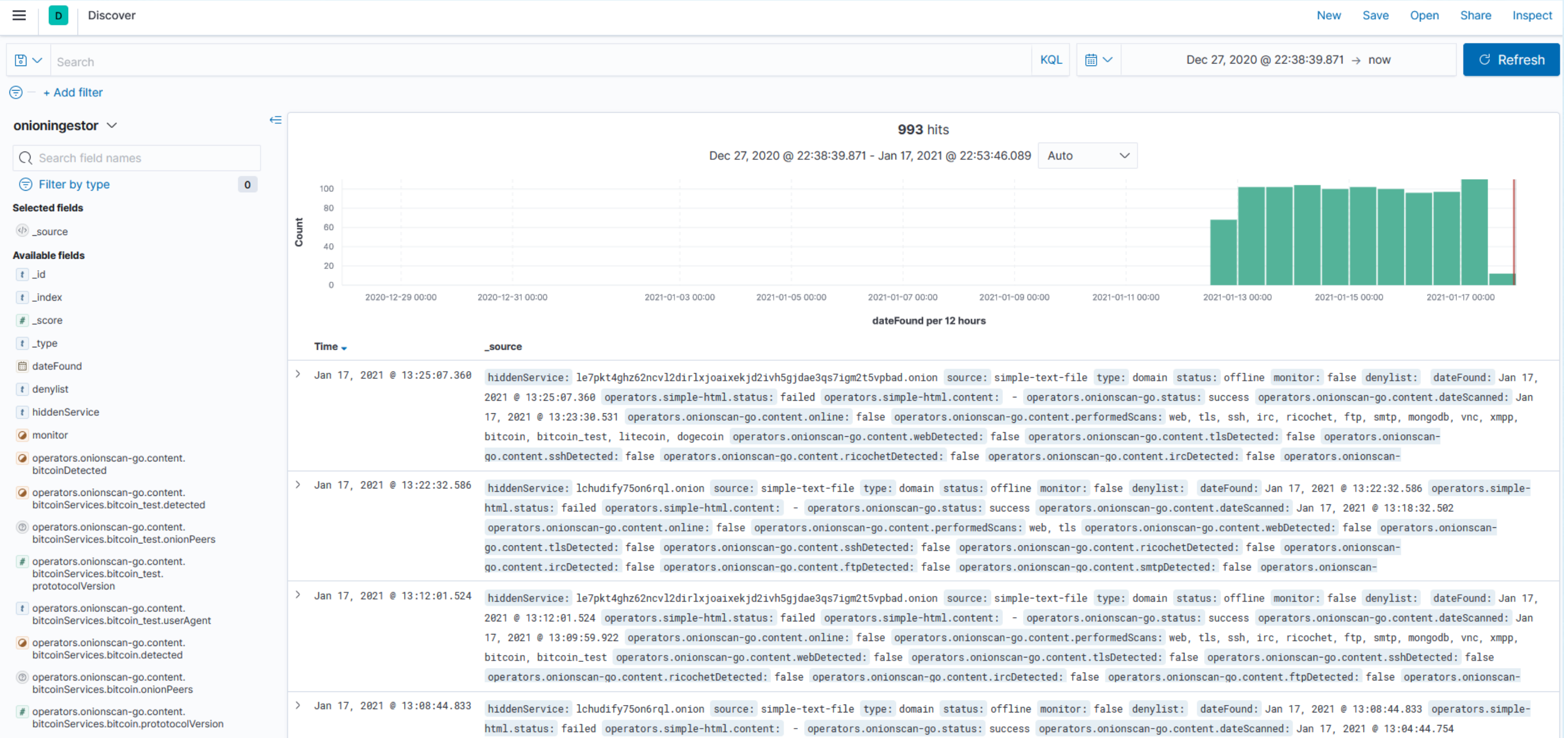
65
Blog - Count

Top Interesting Keywords Timeline Jul 7, 2020 @ 15:23:49.398 to now

Blacklisted Keywords

[redacted] 32.055%
[redacted] 22.502%
[redacted] 16.342%
[redacted] 14.896%
[redacted] 14.205%

OnionIngestor (Contd.)



Dec 27, 2020 @ 22:38:39.871 → now

onioningestor

Search field names

Filter by type 0

Selected fields

- _source

Available fields

- _id
- _index
- _score
- _type
- dateFound
- denylist
- hiddenService
- monitor
- operators.onionscan-go.content.bitcoinDetected
- operators.onionscan-go.content.bitcoinServices.bitcoin_test.detected
- operators.onionscan-go.content.bitcoinServices.bitcoin_test.onionPeers
- operators.onionscan-go.content.bitcoinServices.bitcoin_test.prototocolVersion
- operators.onionscan-go.content.bitcoinServices.bitcoin_test.userAgent
- operators.onionscan-go.content.bitcoinServices.bitcoin.detected
- operators.onionscan-go.content.bitcoinServices.bitcoin.onionPeers
- operators.onionscan-go.content.bitcoinServices.bitcoin.protocolVersion

993 hits

Dec 27, 2020 @ 22:38:39.871 - Jan 17, 2021 @ 22:53:46.089 Auto

```
Time      _source

Jan 17, 2021 @ 13:25:07.360  hiddenService: le7pkt4ghz62ncvl2dirlxjoaixekjd2ivh5gjdae3qs7igm2t5vpbad.onion source: simple-text-file type: domain status: offline monitor: false denylist:  dateFound: Jan 17,
2021 @ 13:25:07.360 operators.simple-html.status: failed operators.simple-html.content:  - operators.onionscan-go.status: success operators.onionscan-go.content.dateScanned: Jan
17, 2021 @ 13:23:30.531 operators.onionscan-go.content.online: false operators.onionscan-go.content.performedScans: web, tls, ssh, irc, ricochet, ftp, smtp, mongodb, vnc, xmpp,
bitcoin, bitcoin_test, litecoin, dogecoin operators.onionscan-go.content.webDetected: false operators.onionscan-go.content.tlsDetected: false operators.onionscan-
go.content.sshDetected: false operators.onionscan-go.content.ricochetDetected: false operators.onionscan-go.content.ircDetected: false operators.onionscan-

Jan 17, 2021 @ 13:22:32.586  hiddenService: lchudify75on6rql.onion source: simple-text-file type: domain status: offline monitor: false denylist:  dateFound: Jan 17, 2021 @ 13:22:32.586 operators.simple-
html.status: failed operators.simple-html.content:  - operators.onionscan-go.status: success operators.onionscan-go.content.dateScanned: Jan 17, 2021 @ 13:18:32.502
operators.onionscan-go.content.online: false operators.onionscan-go.content.performedScans: web, tls operators.onionscan-go.content.webDetected: false operators.onionscan-
go.content.tlsDetected: false operators.onionscan-go.content.sshDetected: false operators.onionscan-go.content.ricochetDetected: false operators.onionscan-
go.content.ircDetected: false operators.onionscan-go.content.ftpDetected: false operators.onionscan-go.content.smtpDetected: false operators.onionscan-

Jan 17, 2021 @ 13:12:01.524  hiddenService: le7pkt4ghz62ncvl2dirlxjoaixekjd2ivh5gjdae3qs7igm2t5vpbad.onion source: simple-text-file type: domain status: offline monitor: false denylist:  dateFound: Jan 17,
2021 @ 13:12:01.524 operators.simple-html.status: failed operators.simple-html.content:  - operators.onionscan-go.status: success operators.onionscan-go.content.dateScanned: Jan
17, 2021 @ 13:09:59.922 operators.onionscan-go.content.online: false operators.onionscan-go.content.performedScans: web, tls, ssh, irc, ricochet, ftp, smtp, mongodb, vnc, xmpp,
bitcoin, bitcoin_test operators.onionscan-go.content.webDetected: false operators.onionscan-go.content.tlsDetected: false operators.onionscan-go.content.sshDetected: false
operators.onionscan-go.content.ricochetDetected: false operators.onionscan-go.content.ircDetected: false operators.onionscan-go.content.ftpDetected: false operators.onionscan-

Jan 17, 2021 @ 13:08:44.833  hiddenService: lchudify75on6rql.onion source: simple-text-file type: domain status: offline monitor: false denylist:  dateFound: Jan 17, 2021 @ 13:08:44.833 operators.simple-
html.status: failed operators.simple-html.content:  - operators.onionscan-go.status: success operators.onionscan-go.content.dateScanned: Jan 17, 2021 @ 13:04:44.754
```

7. Tools to create data collection architecture

Tools

- Scrapy
- Tor
- OnionScan
- Privoxy
- Elastic
- Redis
- and many more…

Image Sources: Tor Project, OnionScan, Scrapy, Privoxy, Redis

8. Conclusion

What we discussed so far?

- Little about the Dark Web
- Dark Web forums/marketplaces
- OSINT tools (search engine, onion links, scan onions, crawl onions)
- Tools to create your own data collection architecture

Tips for getting started in this..

- Figure out your assets/motives/threat model
- Try searching for keywords in dark web search engines
- Analyze the result if found
- Try using other tools to scan and crawl the data
- Create your own tools if needed
- Do this on a monthly basis with different keywords
- Report to your team through intelligence briefing

Resources

SANS Summits

- OSINT Framework - https://osintframework.com/
- OSINT Combine Dark Web Searching - https://www.osintcombine.com/post/dark-web-searching
- Jake Creps Blog - https://jakecreps.com/2019/05/16/osint-tools-for-the-dark-web/
- Blogs & White papers by Recorded Future
- White papers by IntSights
- Blogs by Palo Alto's Unit 42
- White papers by Digital Shadows
- Automating Threat Hunting on the Dark Web and other nitty-gritty things talk by Apurv Singh Gautam
- Ambly the Smart Darknet Spider talk by Cytisus Eurydice (@levitannin)

SANS Summits

Thanks!

Any questions?

You can contact me at:
Twitter: @ASG_Sc0rpi0n
LinkedIn: /in/apurvsinghgautam

GitHub Repo: https://github.com/apurvsinghgautam/dark-web-osint-tools