

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 



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?

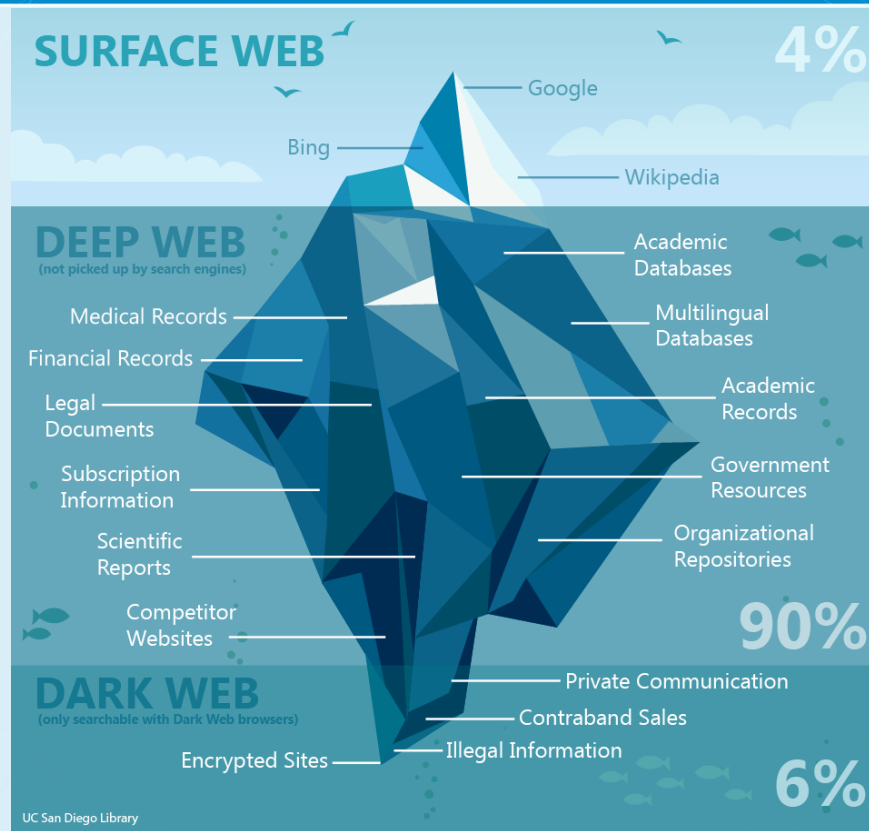
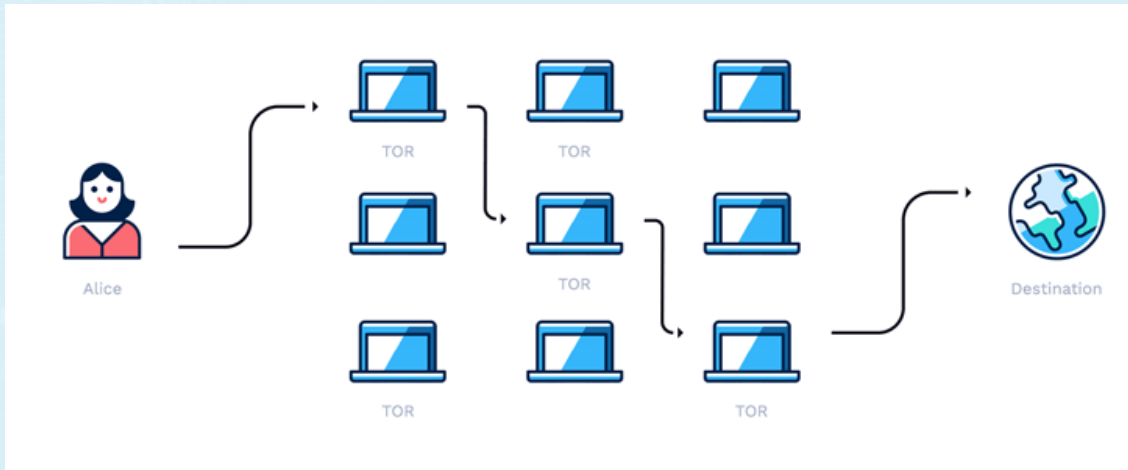
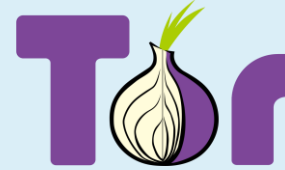


Image Source: UC San Diego Library

Accessing the Dark Web

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



Relevant site types?

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



Image Source: Intsignts

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**

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

Default - 4 days - USD + 0.00 / order

Purchase price: **USD 90.00**

Qty: **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, 2019 **Vendor Level 4** **Trust level 4**

Unlimited items available for auto-dispatch

Product Class	Features
Digital	Digital
Quantity Left	Unlimited
Ends In	Never

Private Message - 1 days - USD + 0.00 / order

Purchase price: **USD 9.99**

Qty: **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

Rent-A-Hacker

Experienced hacker offering his services (Illegal) Hacking and social engineering. I'm really good at hacking and I made a lot of money. I have worked for other people before.



USA Bank login Cracker Bruter
 banks: bruteforce 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

Product Class	Features
Digital	Digital
Quantity Left	Unlimited
Ends In	Never

default - 1 day - USD + 0.00

Purchase price: **USD 3.00**

Qty: **Buy Now** **Buy Now**

0.000319 BTC / 0.068368 LTC / 0.045537 XMR



VISA Virtual Card
 Valid only for use in the United states

DEBIT GIFT

VISA
 Visa® Virtual Account

Account Number: 4000 1234 5678 9010

Valid Thru: 12/23

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



Virtual MasterCard (USD)
 Valid Worldwide, All the World

PREPAID

5362 0588 8888 8888

Cardholder: 0000

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

[redacted]

Posts7

Threads4

JoinedAug 2020

Reputation53



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]

PM

Find

Why you should care?

H USA Hospital RDP For Sale - Больница США RDP на продажу

September 4 in Auctions



Paid registration

1

68 posts

Joined

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 signature]

+ Quote

3. Search engine tools for the Dark Web

Tools

- Katana
- OnionSearch
- Ahmia Search Engine
- DarkSearch



Katana

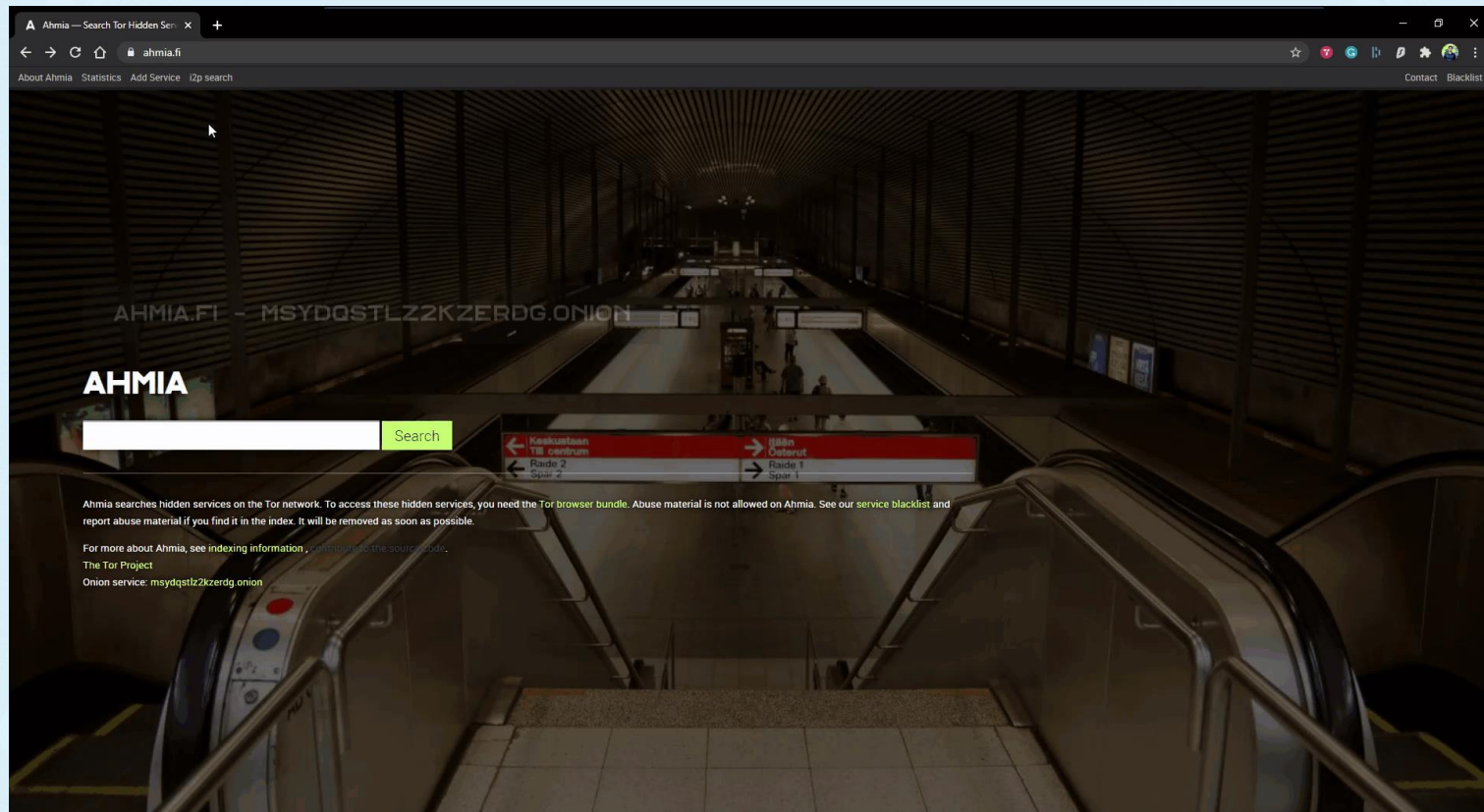


OnionSearch

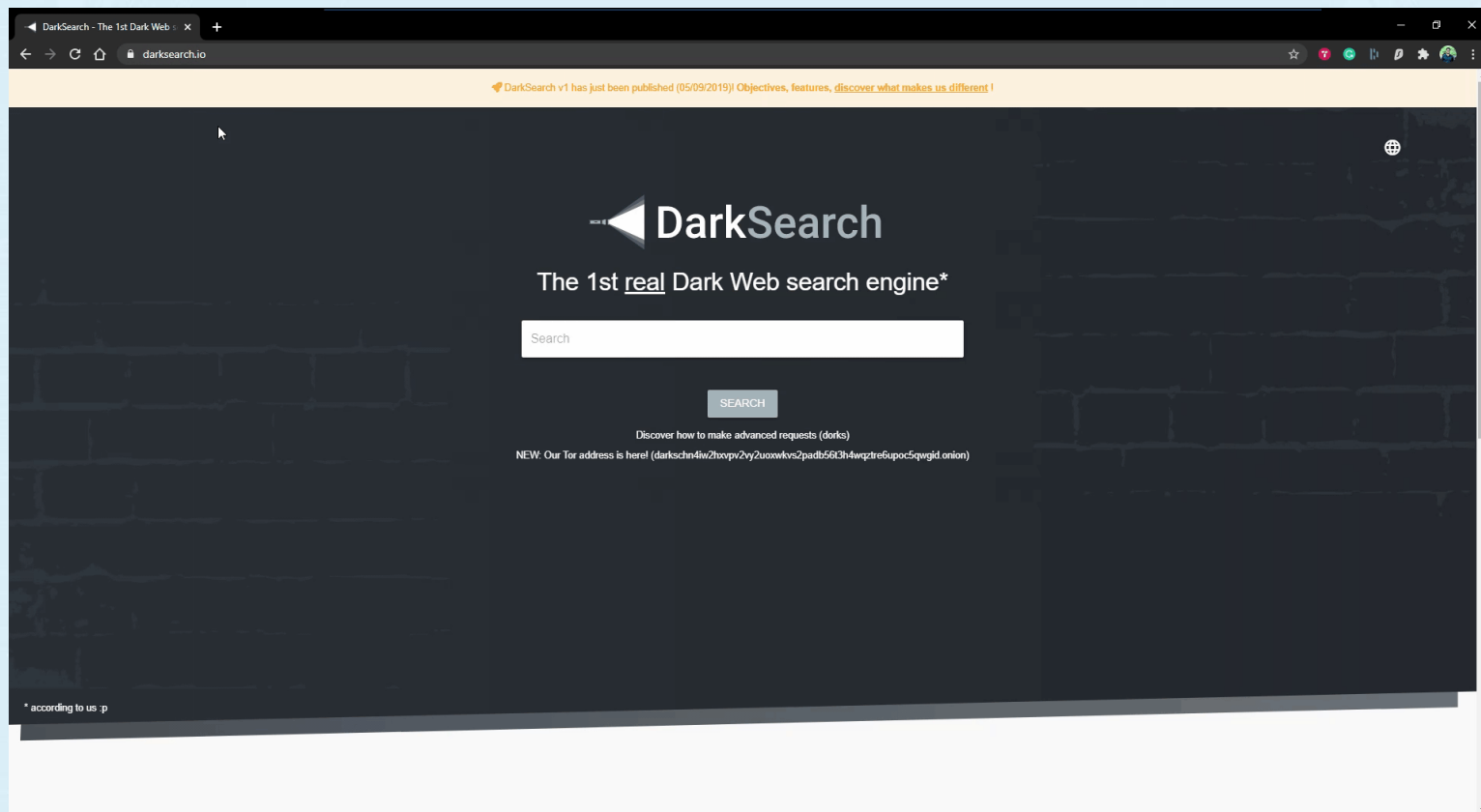


OnionSearch (Contd.)





DarkSearch



4. Tools to get onion links from the Dark Web

Tools

- Hunchly
- H-Indexer



SANS Summits

AutoSave

File Home Insert Page Layout Formulas Data Review View Help

Cut Copy Paste

Format Painter

Clipboard

Calibri 11

B I U

Font

General

Conditional Formatting

Format as Table

Number

Normal Bad Good Neutral

Calculation Check Cell Explanatory Input

Styles

Insert Delete Format

Cells

AutoSum

Fill

Clear

Editing

Sort & Filter

Find & Select

Analysis

Analyze Data

Sensitivity

Sensitivity

Comments

Share

Hidden Services - Excel

GA

Gautam, Apurv Singh

A1

fx

Last Contacted

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Last Contacted	Hidden Service	Language	HTTP Stati	Last Up	Title										
2	2021-01-09 23:59:18	epynixtbonx4odv34z4eqnlamnpuwfz6uwmsamcqd	N/A	503	2020-02-17 19:53:39											
3	2021-01-09 10:06:19	9de135hfvb961eefl.onion	N/A	503	Never											
4	2021-01-09 34:59:35	pegnetghuspr7nanuvncn5nt2vt65hhs6uauumdmtz225	N/A	503	2020-10-15 21:11:06											
5	2021-01-09 23:28:42	deepdotweb35vwmeydd5.onion	N/A	503	Never											
6	2021-01-09 15:39:27	chanyuyosmcristas.onion	N/A	503	Never											
7	2021-01-09 20:44:14	teamkden.crackedacct.onion	N/A	503	Never											
8	2021-01-09 05:12:42	hacker5quf443wrt4n7hi6m34kpcyasknjvhrb6pcba	N/A	503	2020-12-26 12:46:54											
9	2021-01-09 17:39:24	youdonefuckedupn.onion	N/A	503	Never											
10	2021-01-09 21:38:13	amazingd6g5ze7y.onionwikitorcjoweruxu.onion	N/A	503	Never											
11	2021-01-09 21:30:01	paoyu7gub72lykuk.onion	N/A	503	2021-01-08 22:55:56											
12	2021-01-09 10:35:00	wfflw5frtp5it4k.onion	N/A	503	2021-01-06 13:58:27											
13	2021-01-09 19:07:32	wbhkfwps2n33wde6lw3ki4njkfiesricqfcjshj6rdmxc	N/A	503	2020-04-01 23:19:20											
14	2021-01-09 30:39:36	prismsigadonepointone.onion	N/A	503	Never											
15	2021-01-09 17:09:42	6of3x4uhed5xqb4.onion	N/A	503	Never											
16	2021-01-09 04:06:37	adduser.3w2s7tpb5mc7ubsjnpz4oxvqupjeoycwzdwf	N/A	503	Never											
17	2021-01-09 11:02:59	shadow57vkjdjtx.onion	en	502	2019-07-11 00:21:24	502 - No server or forwarder data received (Privoxy@localhost)										
18	2021-01-09 15:06:34	rama.mayonaise.cabbage.tomatoes.onion	N/A	503	Never											
19	2021-01-09 09:31:14	3ubv4ppfed4o5kavu5uadp2rsjimm2lj2x4jbwktkwzbh	N/A	503	2019-04-23 12:20:21											
20	2021-01-09 11:55:41	xnwgk3hp7yne6kmlqpszsxz76ovysnjlrjrvyadjtr454y2	N/A	503	2020-04-04 13:21:57											
21	2021-01-09 21:21:17	qodv3evhcmffavuzjasokl6stmqsnjrbau2lskn4y2k7pkv	N/A	503	2019-08-01 14:11:44											
22	2021-01-09 22:50:04	raymoll13svsduhd7vwxvajagocfwps25nq67zyibaw	N/A	503	2020-10-26 18:02:14											
23	2021-01-09 12:01:03	bk4vffk2fazxhs3pvg74rgqv4puaj7hrcsalufullprkr2	N/A	503	2020-10-28 05:34:21											
24	2021-01-09 15:31:32	bv4saxirtmqmtqpt55bdsxle2brn46kv7gvnneh7qgs26	N/A	503	2019-06-05 23:23:25											
25	2021-01-09 09:22:01	zmlg6tgdentfcvazymakwsh7kzgdctlep72u44ktgjd5p	N/A	503	2020-09-22 10:55:01											
26	2021-01-09 20:29:09	sgeva4jy3ssklpd2kysvzvzeq3khy3x75qhyzw4og5zsr	N/A	503	2019-04-22 02:43:56											
27	2021-01-09 13:56:17	aqjsj4lyeleqdkxb5412bwbxlr7zsoe2xmema743msq7	N/A	503	2019-09-12 08:30:09											
28	2021-01-09 20:03:11	jafojztdgkjo7gcwq7wdip6eltx3vedt3ly3zuds6xhipd	N/A	503	2020-03-23 19:41:20											
29	2021-01-09 16:32:35	27Zdl54621eanrxcidfrance.onion	N/A	503	Never											
30	2021-01-09 16:14:38	smndqengabhaisv5t6j3jg3vubvfhds4vta4npvkgl46nl	N/A	503	Never											
31	2021-01-09 16:04:40	Rjkgbtinvdukcunbtrcintvctoy44dkhvc70ncdzcnk64dv	N/A	503	Never											
32	2021-01-09 16:22:51	yyjvt6hhwva44bgzpqbg4rrluas6u375mgkmf3maa6tjyf	N/A	503	2019-04-23 00:49:07											
33	2021-01-09 21:45:29	asfjasifadisfoasfscps.onion	N/A	503	Never											
34	2021-01-09 09:54:56	vy4ch3gie3sr6526t3u2ptbj5hw7ynklrfdmf6oq43ar37	N/A	503	2020-11-19 02:37:36											
35	2021-01-09 20:55:17	ukranian-services.onion	N/A	503	Never											
36	2021-01-09 19:28:53	4n5t65mv623abojfjr5wtit66lyxrrrstsquziuberhzoxxkr	N/A	503	2019-06-04 10:35:12											
37	2021-01-09 16:01:07	qxabu76bzgu5fd6jw7mx56lwmk5znnxzt5e4v2bflwu	N/A	503	2019-04-22 20:29:29											
38	2021-01-09 22:07:08	zphbuaiglb5bbhy4bpbk6bgbxzyhabr6io6vbcjrcxy4tvt	N/A	503	Never											

< >

New Today

Down

Up

+

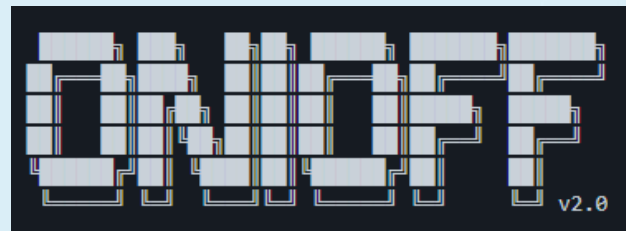
H-Indexer

"Last Contacted"	"Hidden Service"	Language	"HTTP Status"	Title			
"2021-01-23 13:48:57"	iwgpyxn6qv3b2twpwtzhi2sfvgnby2albbcotcyd5f7obrlwdbkyd.onion	en	200	"DrChronic - Weed straight from the source."			
"2021-01-23 12:12:26"	x57cqsirjuhgwxvx.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"	hlsf2cw74ydhcg6f.onion	en	200	"Premium Music Codes"			
"2021-01-23 11:31:05"	gcf42ph6vjzfmuez.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"	fc4booz5wmoq3knc63gf4sn7oisz45sc7zxtlgnqkeqb2pvzqow6ydyd.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



Onionscan



Onioff



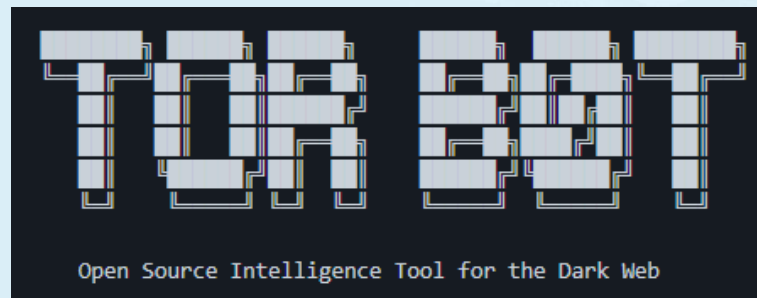
Onion-nmap



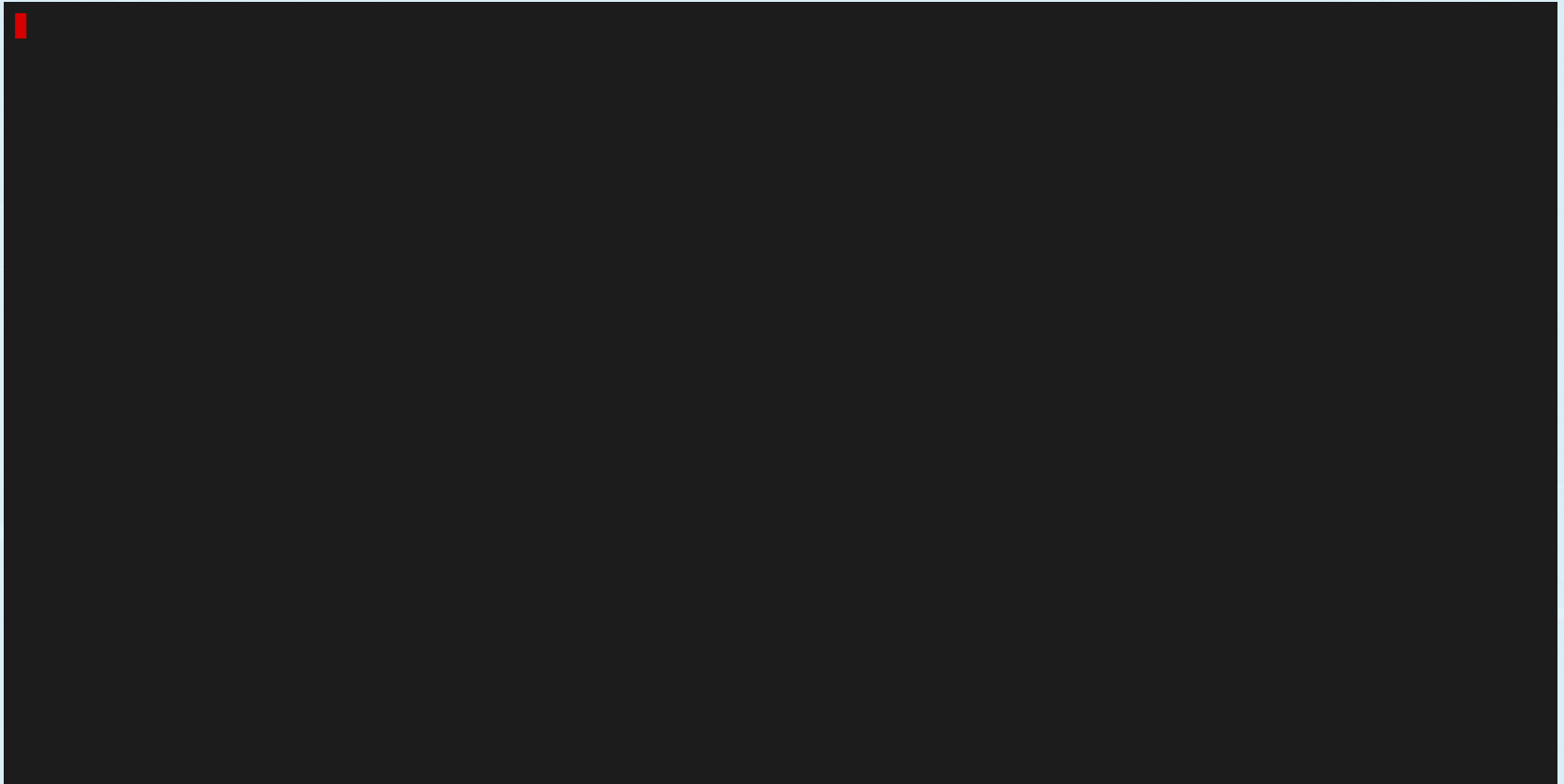
6. Tools to scrape data from the Dark Web

Tools

- TorBot
- TorCrawl
- OnionIngestor



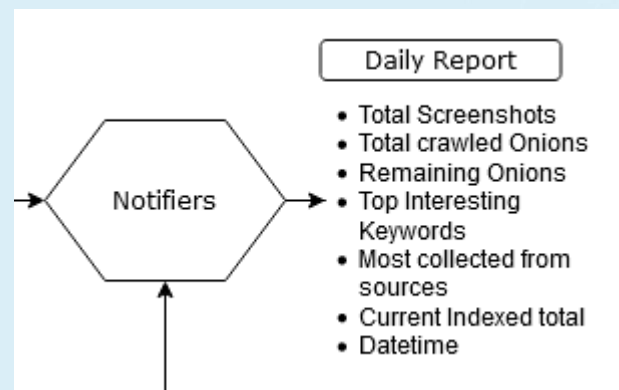
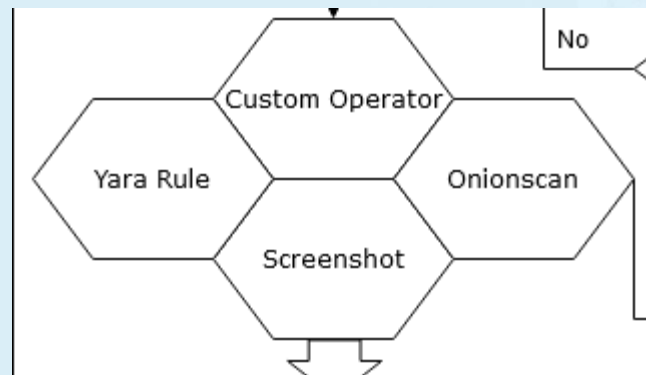
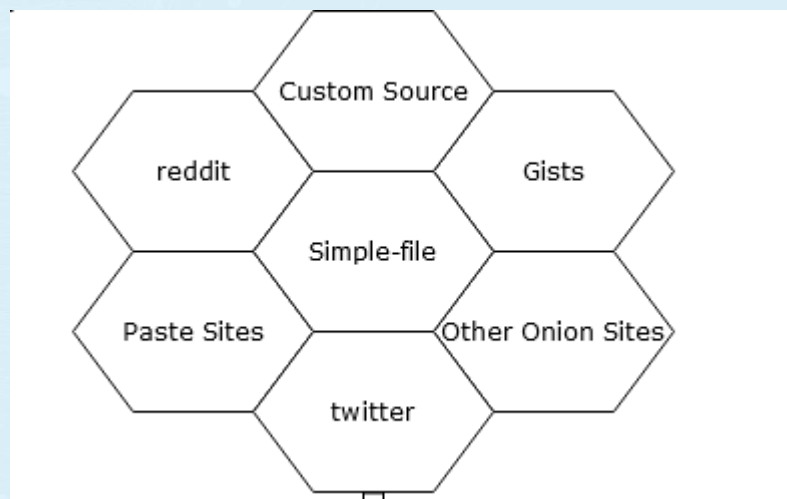
TorBot



TorCrawl



OnionIngestor



OnionIngester (Contd.)

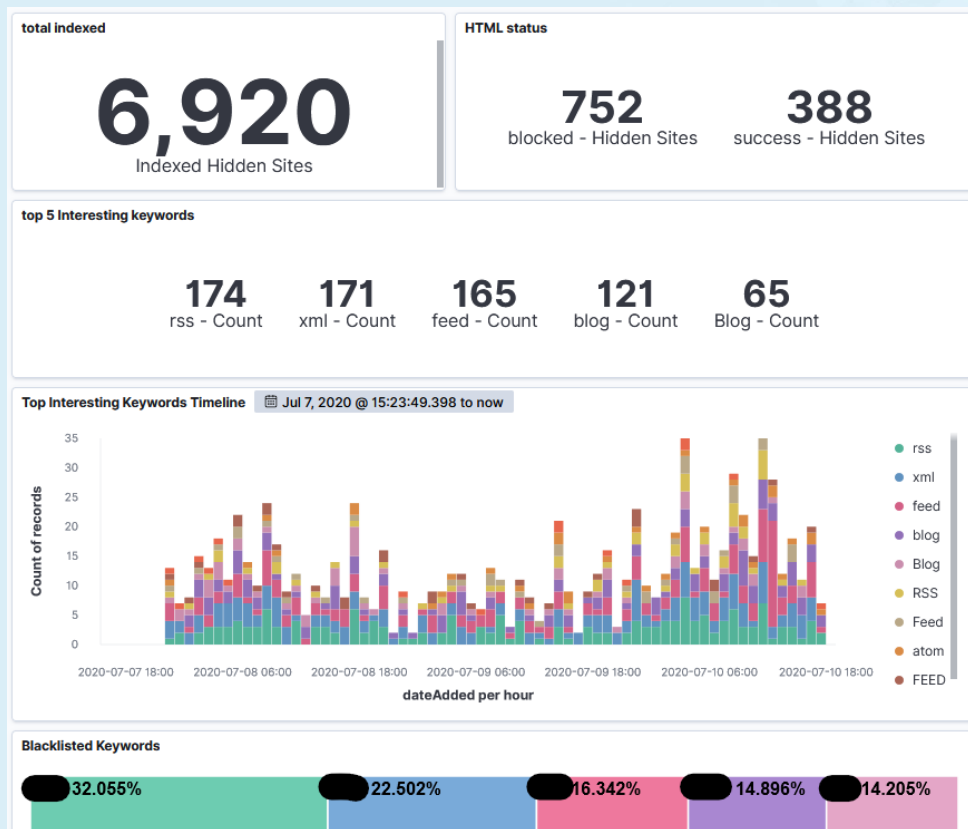
HiddenSite
[le7pkt4ghz62ncvl2dirxjoaixekjd2ivh5g](#)
[jdae3qs7igm2t5vpbad.onion](#)
 Source : simple-text-file
 Monitor : False
 Status : online

Blueteam Dark Web
 HiddenSite
[lchudify75on6rql.onion](#)
 Source : simple-text-file
 Monitor : False
 Status : offline

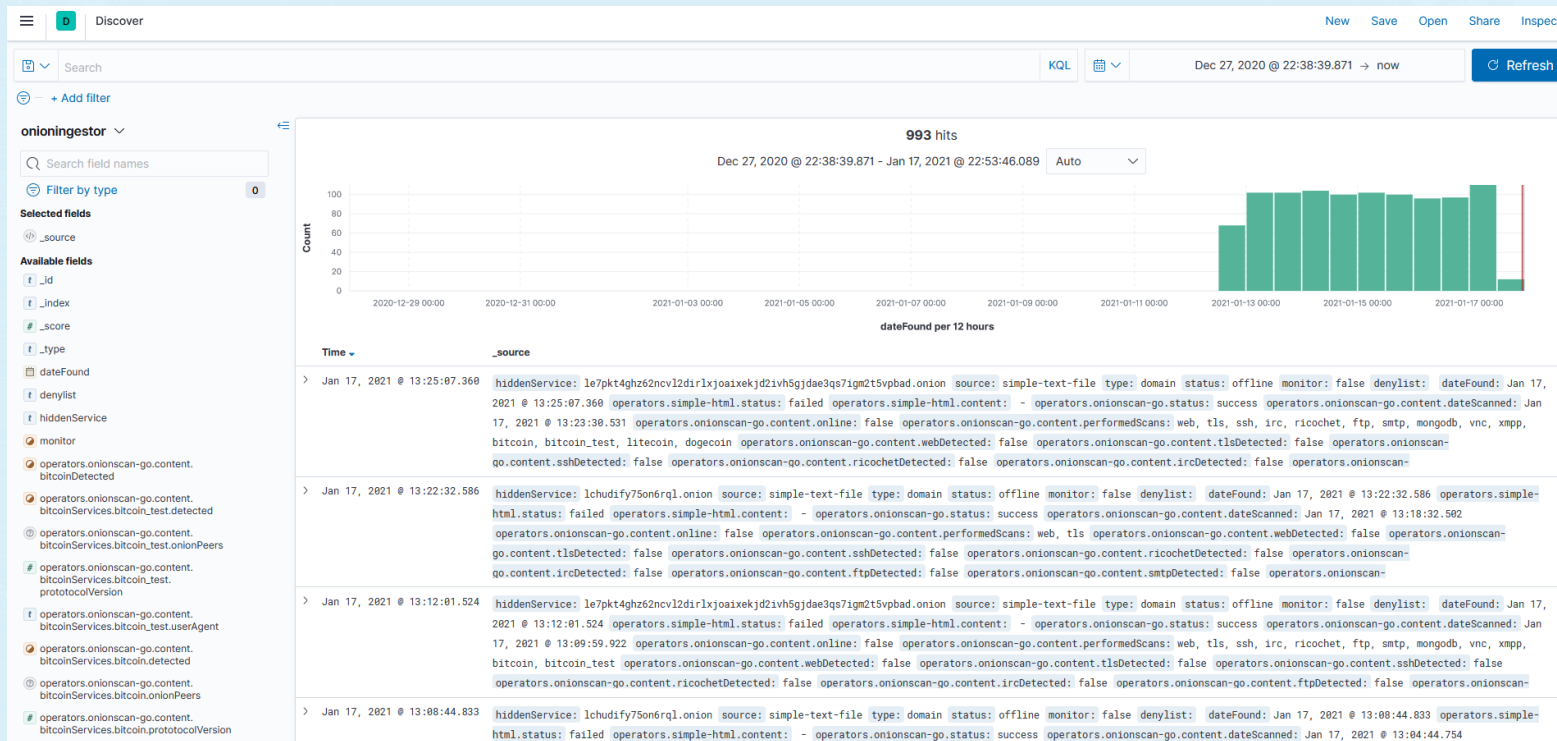
Blueteam Dark Web
 HiddenSite
[e3qs7igm2t5vpbad.onion](#)
 Source : crawled
 Monitor : False
 Status : offline

HiddenSite
[le7pkt4ghz62ncvl2dirxjoaixekjd2ivh5g](#)
[jdae3qs7igm2t5vpbad.onion](#)
 Source : simple-text-file
 Monitor : False
 Status : online

Blueteam Dark Web
 HiddenSite
[lchudify75on6rql.onion](#)



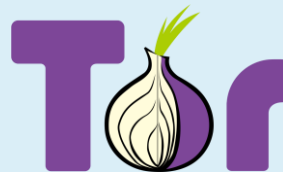
OnionIngestor (Contd.)



7. Tools to create data collection architecture

Tools

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



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
- Try searching for keywords in dark web search engines
- Analyze the results
- 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

- 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)

Thanks!

Any questions?

You can contact me at:

Twitter: @ASG_Sc0rpi0n

LinkedIn: /in/apurvsinghgautam

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

