Dark Web Monitoring: Everything you need to know

$whoami

- Apurv Singh Gautam (@ASG_Sc0rpi0n)
- Threat Researcher @ CYBLE
- Cybersecurity @ Georgia Tech (Go Jackets)
- Presented at conferences

- Hobbies
  - Hiking
  - Lockpicking
  - Gaming/Streaming

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

Agenda

- Introduction to the Dark Web
- Why focusing on the Dark Web?
- Methodology and Skills
- People Skills
- Technology Skills
- OpSec? What’s that?
- Case Study
- Conclusion

1.

Introduction to the Dark Web

Clear Web? Deep Web? Dark Web?

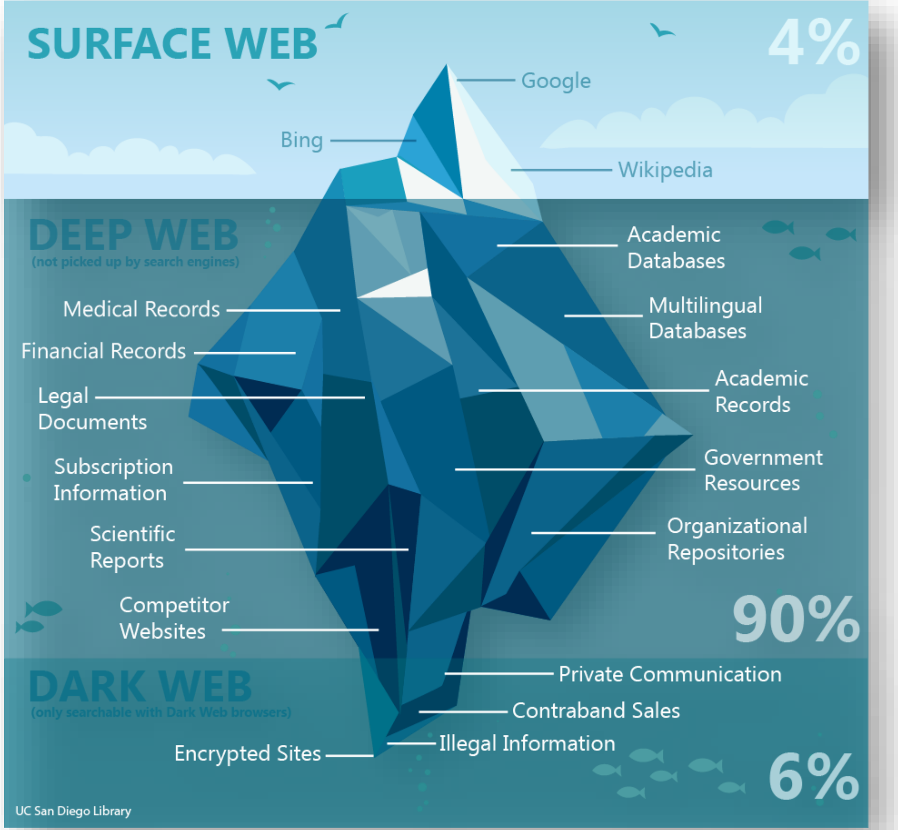
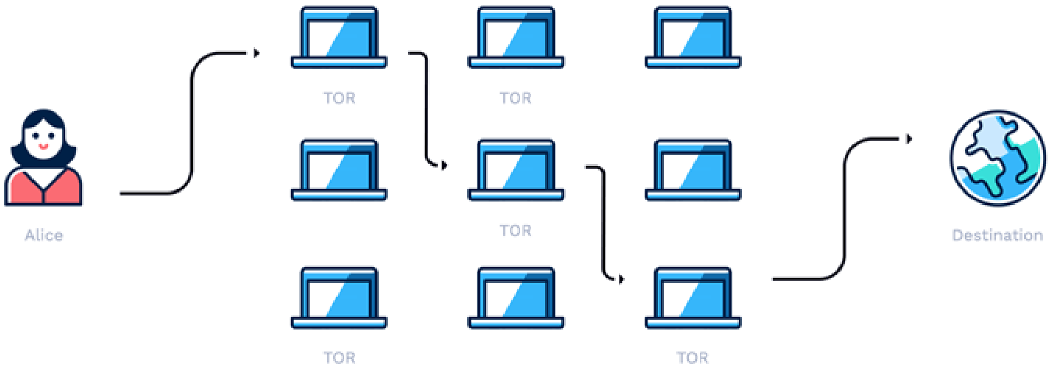
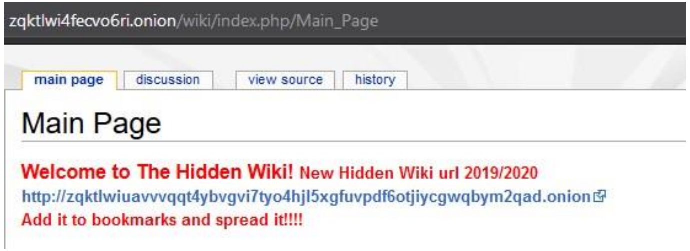


Image Source: UC San Diego Library

Accessing the Dark Web

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





zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page

Main Page

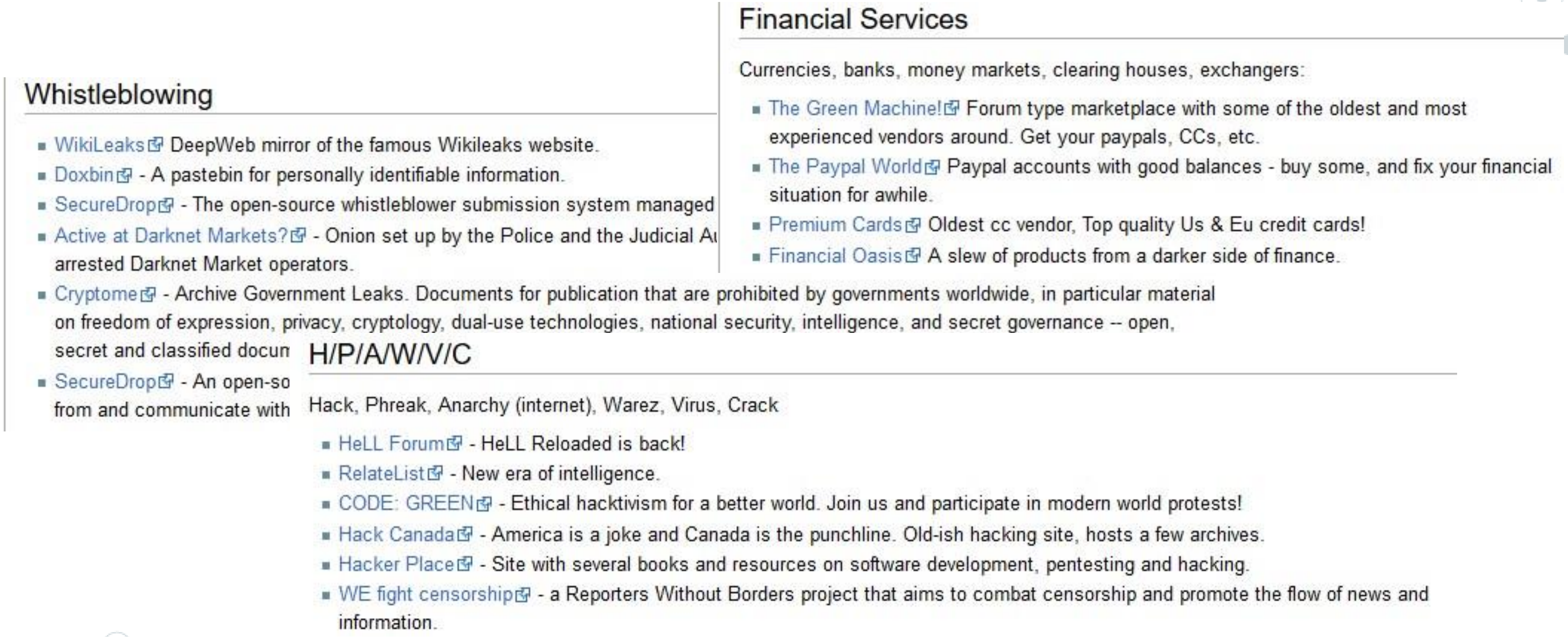
Welcome to The Hidden Wiki! New Hidden Wiki url 2019/2020
http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion
Add it to bookmarks and spread it!!!!

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

What’s all the Hype? Good..Bad..

- Hype
  - Vast and mysterious part of the Internet
  - Place for cybercriminals only
  - Illegal to access the Dark Web
- Reality
  - Few reachable onion domains
  - Uptime isn’t ideal
  - Useful for free expression in few countries
  - Popular sites like Facebook, NYTimes, etc.
  - Legal to access the Dark Web

Sites Examples



Financial Services

Currencies, banks, money markets, clearing houses, exchangers:

- The Green Machine! Forum type marketplace with some of the oldest and most experienced vendors around. Get your paypals, CCs, etc.
- The Paypal World Paypal accounts with good balances - buy some, and fix your financial situation for awhile.
- Premium Cards Oldest cc vendor, Top quality Us & Eu credit cards!
- Financial Oasis A slew of products from a darker side of finance.

Whistleblowing

- WikiLeaks DeepWeb mirror of the famous Wikileaks website.
- Doxbin - A pastebin for personally identifiable information.
- SecureDrop - The open-source whistleblower submission system managed
- Active at Darknet Markets? - Onion set up by the Police and the Judicial Au arrested Darknet Market operators.
- Cryptome - Archive Government Leaks. Documents for publication that are prohibited by governments worldwide, in particular material on freedom of expression, privacy, cryptology, dual-use technologies, national security, intelligence, and secret governance -- open, secret and classified docun
- SecureDrop - An open-so from and communicate with

H/P/A/W/V/C

Hack, Phreak, Anarchy (internet), Warez, Virus, Crack

- HeLL Forum - HeLL Reloaded is back!
- RelateList - New era of intelligence.
- CODE: GREEN - Ethical hacktivism for a better world. Join us and participate in modern world protests!
- Hack Canada - America is a joke and Canada is the punchline. Old-ish hacking site, hosts a few archives.
- Hacker Place - Site with several books and resources on software development, pentesting and hacking.
- WE fight censorship - a Reporters Without Borders project that aims to combat censorship and promote the flow of news and information.

Types of Information Sold?

- Personal health Records (PHI)
- Social Security Numbers (SSNs)
- Exposed codebases
- Personally Identifiable Information (PII)
- Email Password details
- Financial data like credit cards, accounts

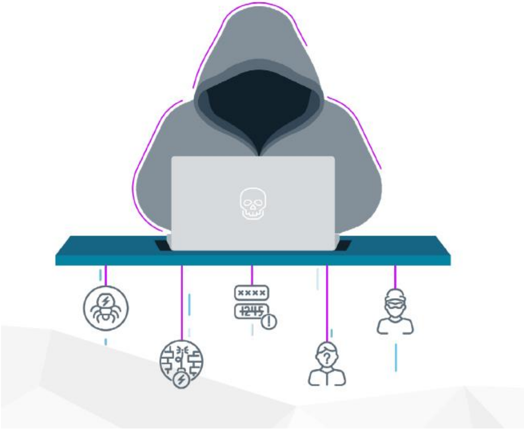


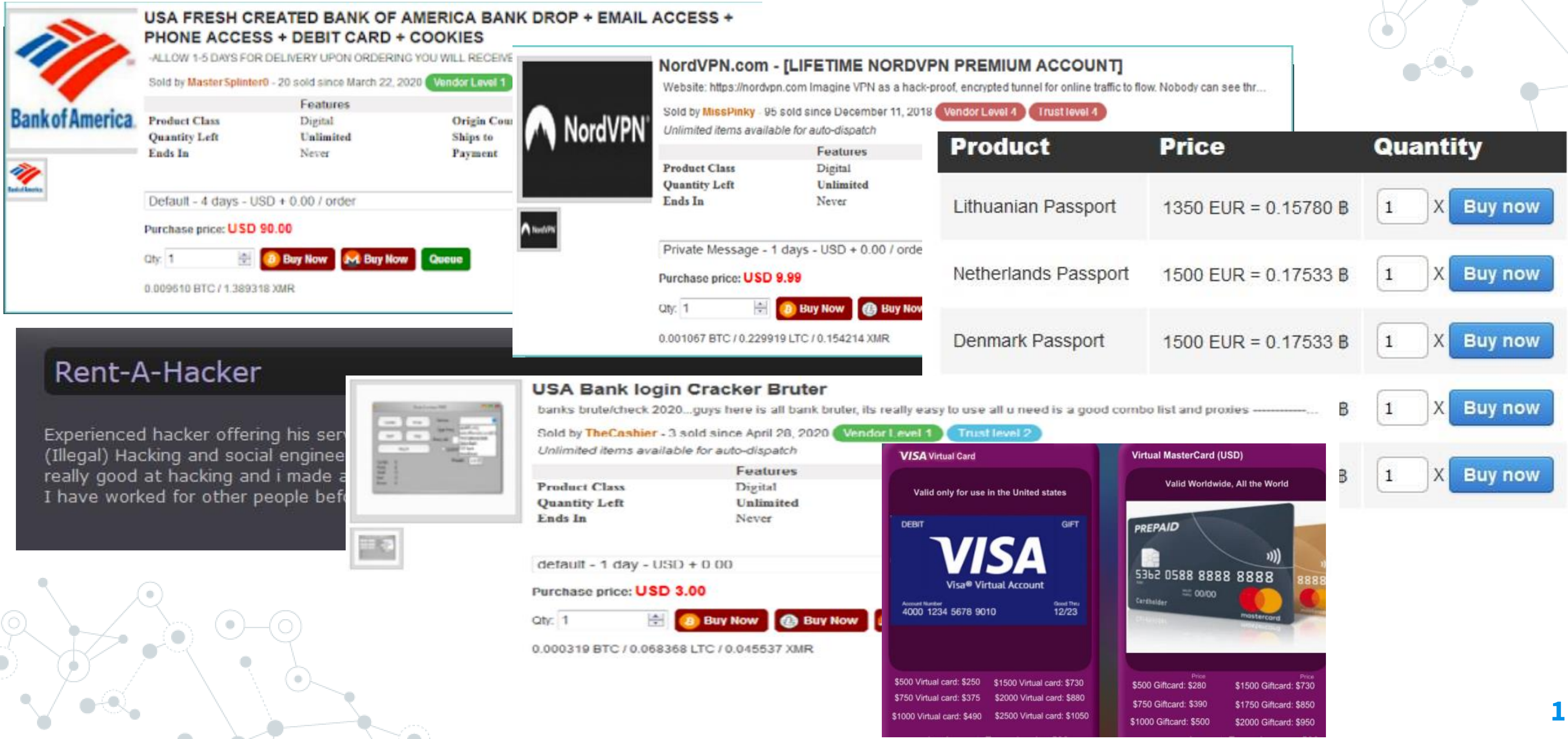
Image Source: Intsights

Cost of products?

- SSN - $2
- DDoS Service - $7/hr
- Rent a Hacker - $12/hr
- Credit Card - $25+
- FB Account- $65+
- Crypto Accounts - $300+
- License/Passport - $100 - $7000
- Bank Details - $1000+
- Exploits or 0-days - $150,000+
- Critical databases - $300,000+

Source: https://www.privacyaffairs.com/dark-web-price-index-2021

Product/Service 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

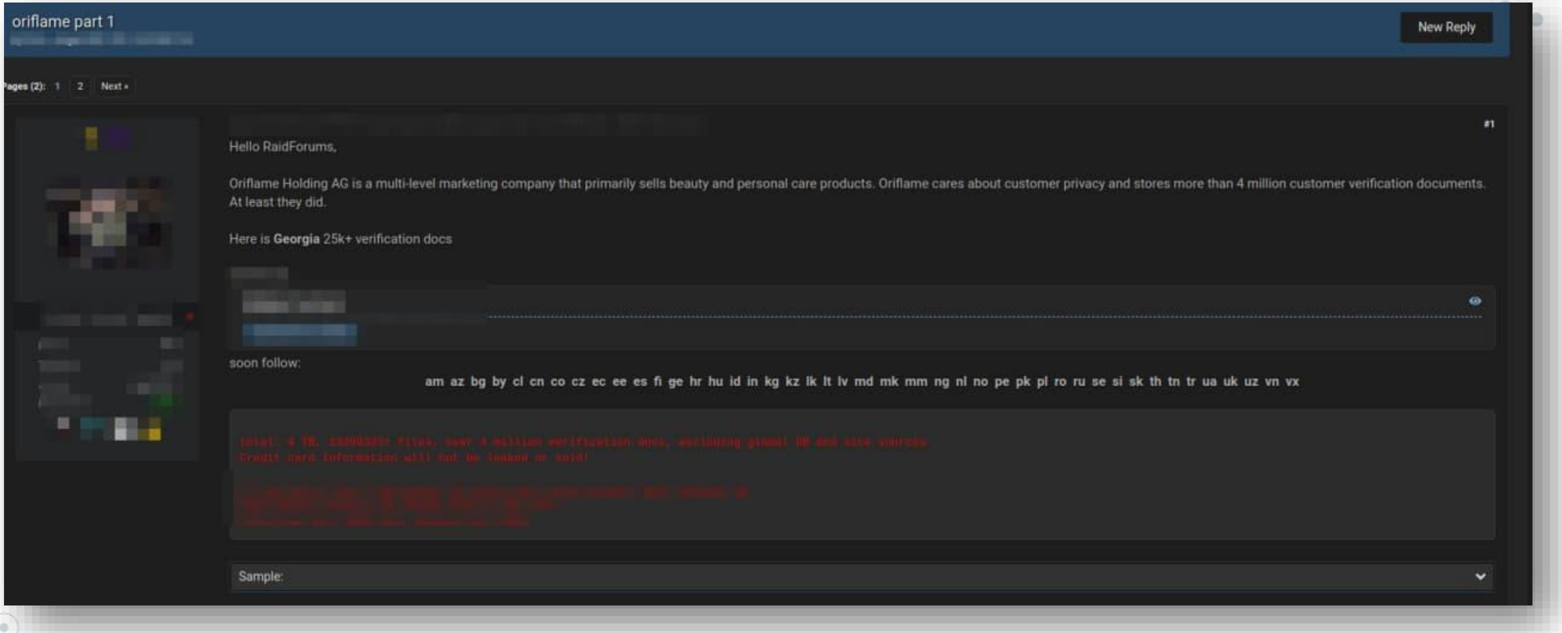
2.

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 should you care?



oriflame part 1

[redacted]

[redacted]

Hello RaidForums,

Oriflame Holding AG is a multi-level marketing company that primarily sells beauty and personal care products. Oriflame cares about customer privacy and stores more than 4 million customer verification documents. At least they did.

Here is **Georgia** 25k+ verification docs

[redacted]

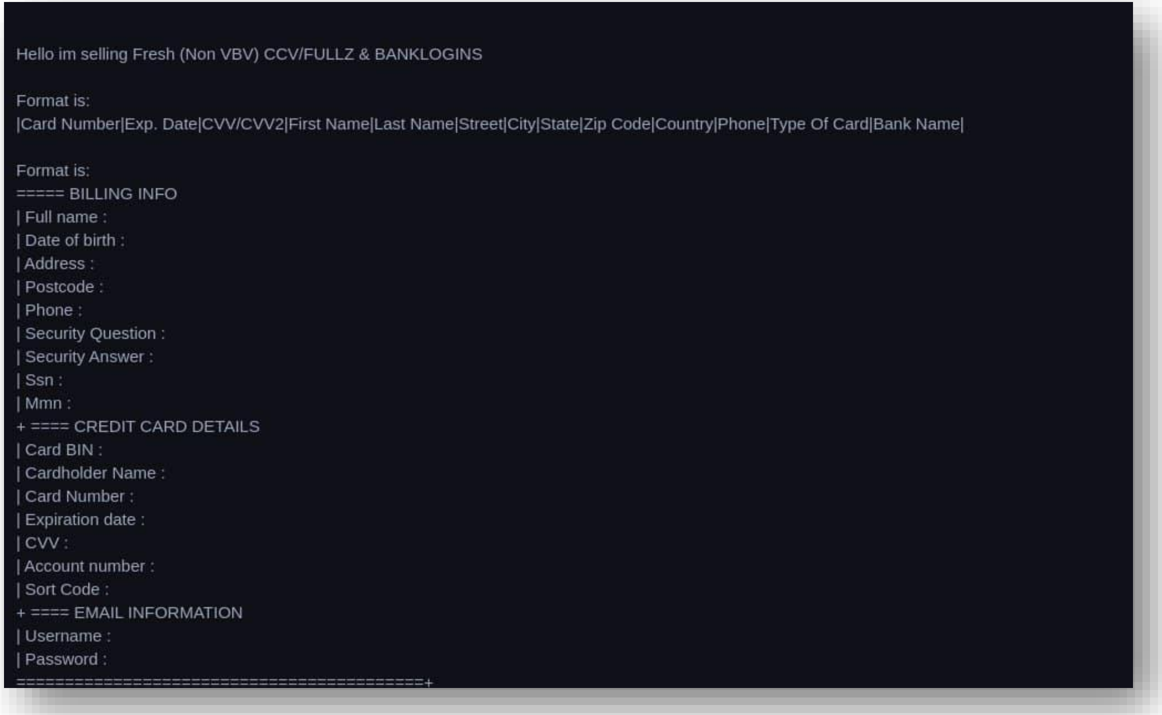
soon follow:

am az bg by cl cn co cz ec ee es fi ge hr hu id in kg kz lk lt lv md mk mm ng nl no pe pk pl ro ru se si sk th tn tr ua uk uz vn vx

```
Total: 4 TB, 15000000+ files, over 4 million verification docs, excluding global DB and site sources
Credit card information will not be leaked or sold!
```

[redacted]

Why should you care?

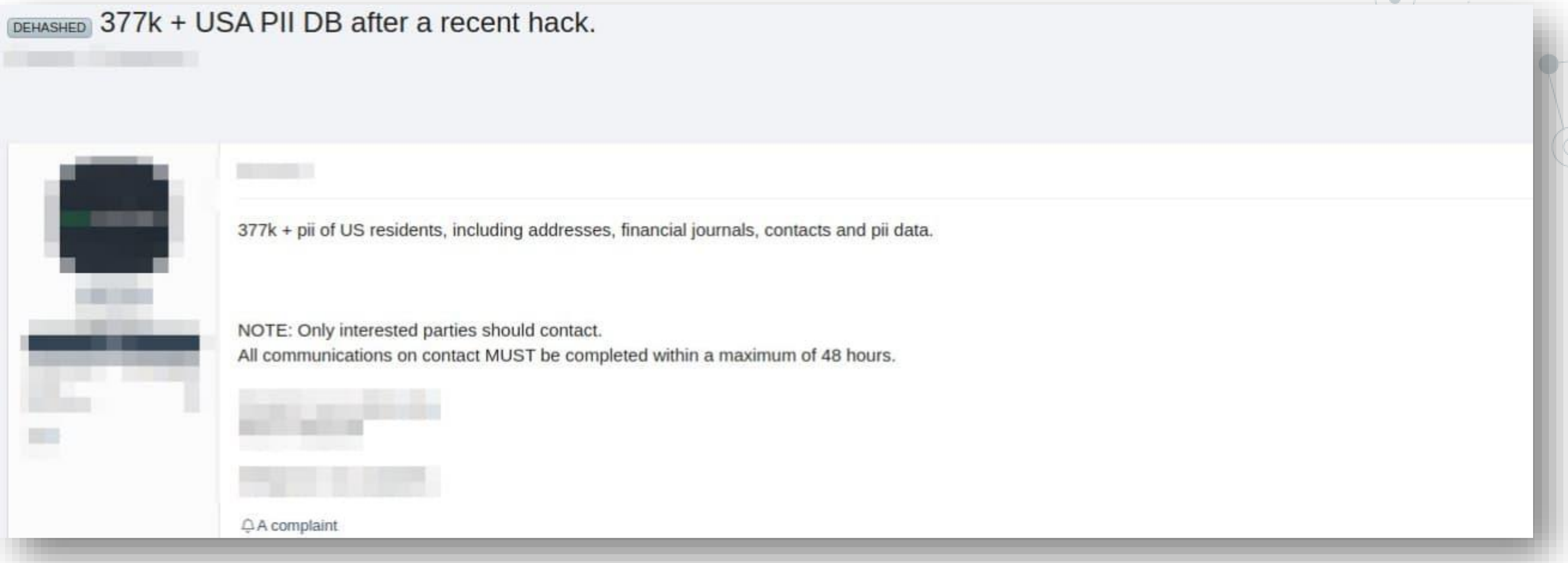


```
Hello im selling Fresh (Non VBV) CCV/FULLZ & BANKLOGINS

Format is:
|Card Number|Exp. Date|CVV/CVV2|First Name|Last Name|Street|City|State|Zip Code|Country|Phone|Type Of Card|Bank Name|

Format is:
===== BILLING INFO
| Full name :
| Date of birth :
| Address :
| Postcode :
| Phone :
| Security Question :
| Security Answer :
| Ssn :
| Mmn :
+ ==== CREDIT CARD DETAILS
| Card BIN :
| Cardholder Name :
| Card Number :
| Expiration date :
| CVV :
| Account number :
| Sort Code :
+ ==== EMAIL INFORMATION
| Username :
| Password :
==========================================+
```

Why should you care?



DEHASHED 377k + USA PII DB after a recent hack.

[redacted]

[redacted]

377k + pii of US residents, including addresses, financial journals, contacts and pii data.

NOTE: Only interested parties should contact.
All communications on contact MUST be completed within a maximum of 48 hours.

[redacted]

3.

Methodology and Skills

What skills you need?

- People Skills
  - Understanding people
  - Soft Skills
  - Knowledge of different languages
  - Research mindset

- Technology Skills
  - Scripting (Python, Go)
  - Knowledge of databases (SQL, ES, Mongo)
  - Knowledge of VMs, Cloud instances

4.

People Skills

OSINT

- Open-Source Intelligence
- Starter to any intelligence research
- All public surface web data
- Easy to find
- Basic information gathering
- Has good and bad parts
- Information on threat actors

Image Source: ACFCS

HUMINT

- Human Intelligence
- Most dangerous and difficult form
- Most valuable source
- Infiltrating forums, markets, etc.
- Become one of them
- How threat actors think
- Profiling actors
- Can be very risky
- Time consuming

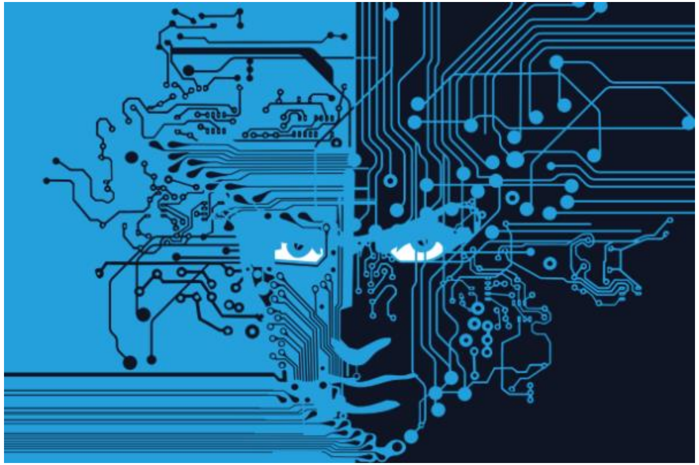


Image Source: Intsights

5.

Technology Skills

Setting up a Lab

- Lab/VM
- Physical or Cloud
- Isolate the network
- Install relevant tools
  - Go
  - Scrapy
  - Privoxy
  - Tor
  - ELK
  - Go libraries
  - Python libraries

Image Source: Hayden James

Readily Available Tools

- Search Engine tools
- Onion Link Collection tools
- Onion Link Scan tools
- Onion Link Scraping tools

All tools available at:
https://github.com/apurvsinghgautam/dark-web-osint-tools

Search Engine Tools

- Katana
- Onionsearch
- Ahmia Search Engine
- Darksearch

Image Sources: Katana, OnionSearch, Ahmia, DarkSearch

Onionsearch

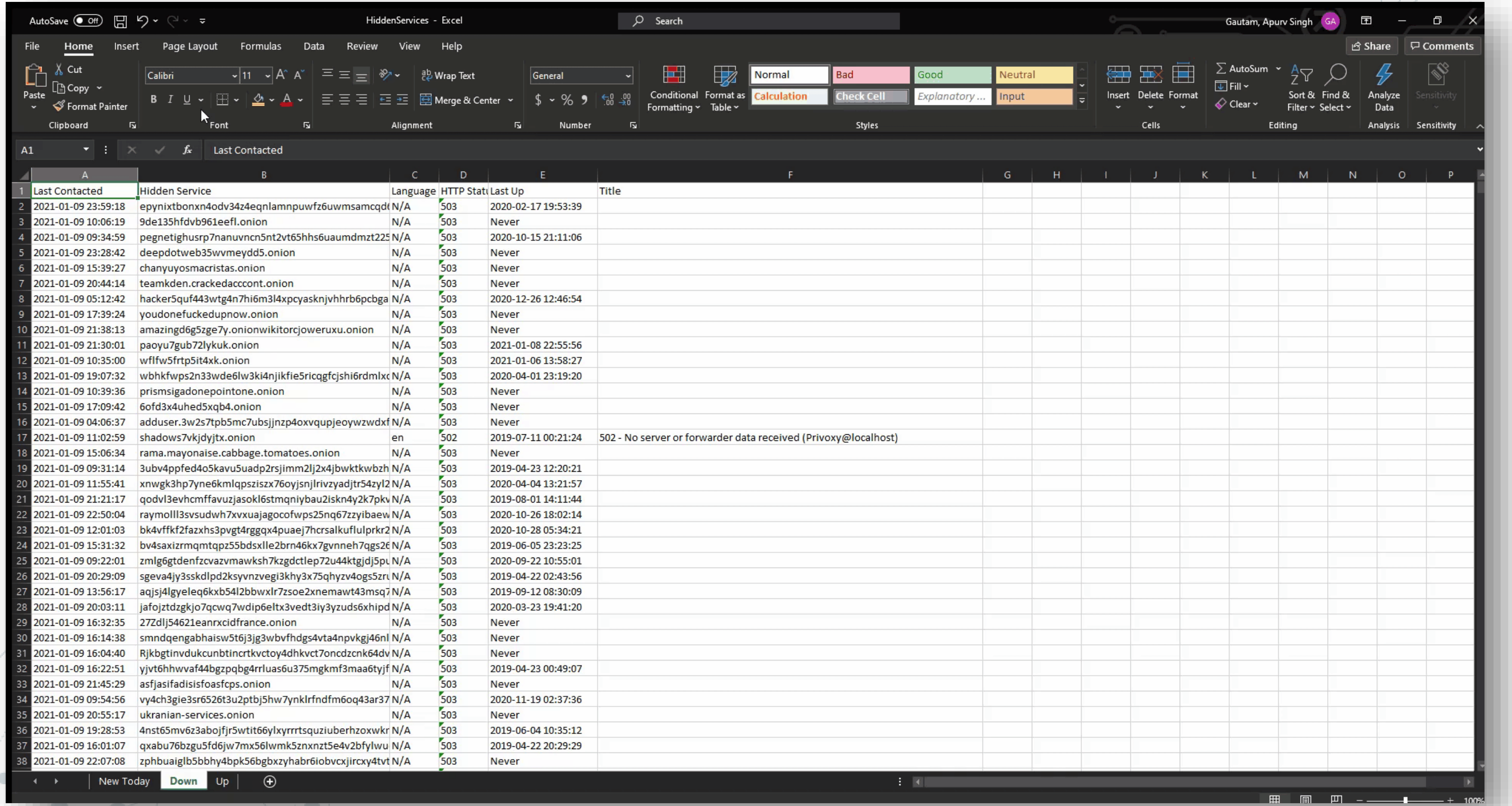
Onionsearch (Contd.)

Onion Link Collection Tools

- Hunchly
- H-Indexer
- Tor66
- r/onions

Image Sources: Hunchly

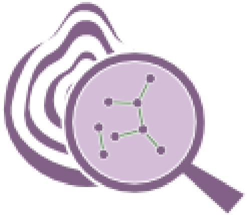
Hunchly



	A	B	C	D	E	F
1	Last Contacted	Hidden Service	Language	HTTP Statu	Last Up	Title
2	2021-01-09 23:59:18	epynixtbonxn4odv34z4eqnlamnpuwfz6uwmsamcqd	N/A	503	2020-02-17 19:53:39	
3	2021-01-09 10:06:19	9de135hfdvb961eefl.onion	N/A	503	Never	
4	2021-01-09 09:34:59	pegnetighusrp7nanuvncn5nt2vt65hhs6uaumdmzt225	N/A	503	2020-10-15 21:11:06	
5	2021-01-09 23:28:42	deepdotweb35wvmeydd5.onion	N/A	503	Never	
6	2021-01-09 15:39:27	chanyuyosmacristas.onion	N/A	503	Never	
7	2021-01-09 20:44:14	teamkden.crackedacccont.onion	N/A	503	Never	
8	2021-01-09 05:12:42	hacker5quf443wtg4n7hi6m3l4xpcyasknjvhhrb6pcbga	N/A	503	2020-12-26 12:46:54	
9	2021-01-09 17:39:24	youdonefuckedupnow.onion	N/A	503	Never	
10	2021-01-09 21:38:13	amazingd6g5zge7y.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	wflfw5frtp5it4xk.onion	N/A	503	2021-01-06 13:58:27	
13	2021-01-09 19:07:32	wbhkfwps2n33wde6lw3ki4njikfie5ricqgfcjshi6rdmlx	N/A	503	2020-04-01 23:19:20	
14	2021-01-09 10:39:36	prismsigadonepointone.onion	N/A	503	Never	
15	2021-01-09 17:09:42	6ofd3x4uhed5xqb4.onion	N/A	503	Never	
16	2021-01-09 04:06:37	adduser.3w2s7tpb5mc7ubsjjnzp4oxvqupjeoywzwdxf	N/A	503	Never	
17	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)
18	2021-01-09 15:06:34	rama.mayonaise.cabbage.tomatoes.onion	N/A	503	Never	
19	2021-01-09 09:31:14	3ubv4ppfed4o5kavu5uadp2rsjimm2lj2x4jbwktkwbzh	N/A	503	2019-04-23 12:20:21	
20	2021-01-09 11:55:41	xnwgk3hp7yne6kmlqpsziszx76oyjsnjlrivzyadjtr54zyl2	N/A	503	2020-04-04 13:21:57	
21	2021-01-09 21:21:17	qodvl3evhcmffavuzjasokl6stmqniybau2iskn4y2k7pkv	N/A	503	2019-08-01 14:11:44	
22	2021-01-09 22:50:04	raymolll3svsudwh7xvxuajagocofwps25nq67zzyibaew	N/A	503	2020-10-26 18:02:14	
23	2021-01-09 12:01:03	bk4vffkf2fazxhs3pvgt4rggqx4puaej7hcrsalkuflulprkr2	N/A	503	2020-10-28 05:34:21	
24	2021-01-09 15:31:32	bv4saxizrmqmtqpz55bdsxlle2brn46kx7gvnneh7qgs26	N/A	503	2019-06-05 23:23:25	
25	2021-01-09 09:22:01	zmlg6gtdenfzcvazvmawksh7kzgdctlep72u44ktgjdj5pu	N/A	503	2020-09-22 10:55:01	
26	2021-01-09 20:29:09	sgeva4jy3sskdlpd2ksyvnzvegi3khy3x75qhyzv4ogs5zru	N/A	503	2019-04-22 02:43:56	
27	2021-01-09 13:56:17	aqjsj4lgyeleq6kxb54l2bbwxlr7zsoe2xnemawt43msq7	N/A	503	2019-09-12 08:30:09	
28	2021-01-09 20:03:11	jafojztdzgkjo7qcwq7wdip6eltx3vedt3iy3yzuds6xhipd	N/A	503	2020-03-23 19:41:20	
29	2021-01-09 16:32:35	27Zdlj54621eanrxcidfrance.onion	N/A	503	Never	
30	2021-01-09 16:14:38	smndqengabhaisw5t6j3jg3wbvfhdgs4vta4npvkgj46nl	N/A	503	Never	
31	2021-01-09 16:04:40	Rjkbgtinvdukcunbtincrtkvctoy4dhkvct7oncdzcnk64dv	N/A	503	Never	
32	2021-01-09 16:22:51	yjvt6hhwvaf44bgzpqbg4rrluas6u375mgkmf3maa6tyjf	N/A	503	2019-04-23 00:49:07	
33	2021-01-09 21:45:29	asfjasifadisisfoasfcps.onion	N/A	503	Never	
34	2021-01-09 09:54:56	vy4ch3gie3sr6526t3u2ptbj5hw7ynklrfndfm6oq43ar37	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	4nst65mv6z3abojfjr5wtit66ylxyrrrtsquziuberhzoxwkr	N/A	503	2019-06-04 10:35:12	
37	2021-01-09 16:01:07	qxabu76bzgu5fd6jw7mx56lwmk5znxnzt5e4v2bfylwu	N/A	503	2019-04-22 20:29:29	
38	2021-01-09 22:07:08	zphbuaiglb5bbhy4bpk56bgbxzyhabr6iobvcxjircxy4tvt	N/A	503	Never	

Onion Link Scan Tools

- OnionScan
- Onioff
- Onion-nmap



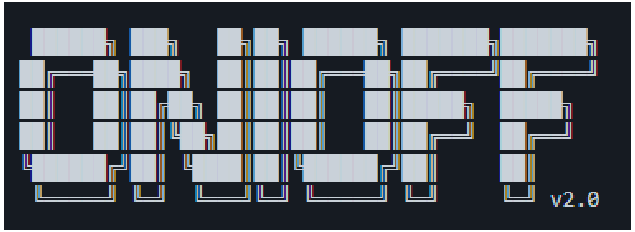
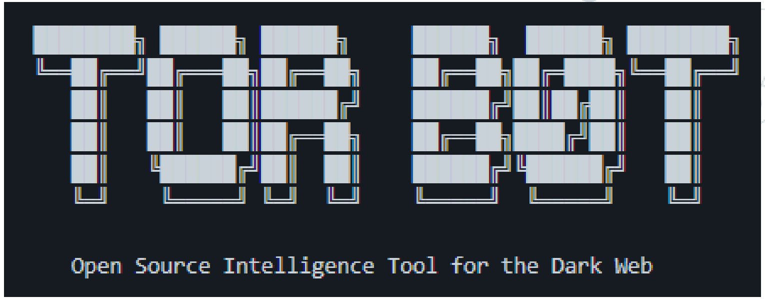


Image Sources: OnionScan, Onioff

OnionScan

Onion Link Scraping Tools

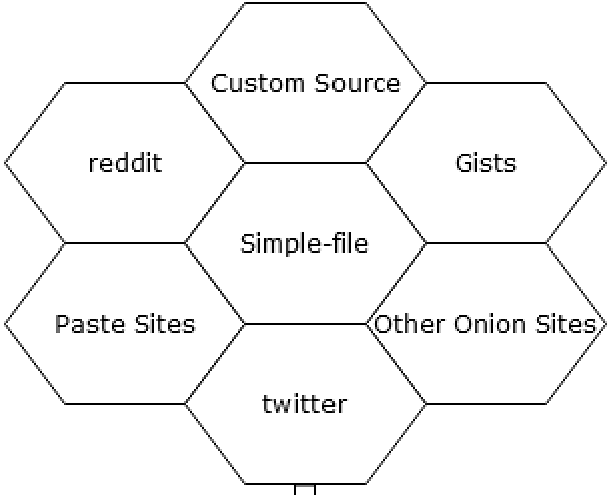
- TorBot
- TorCrawl
- OnionIngestor

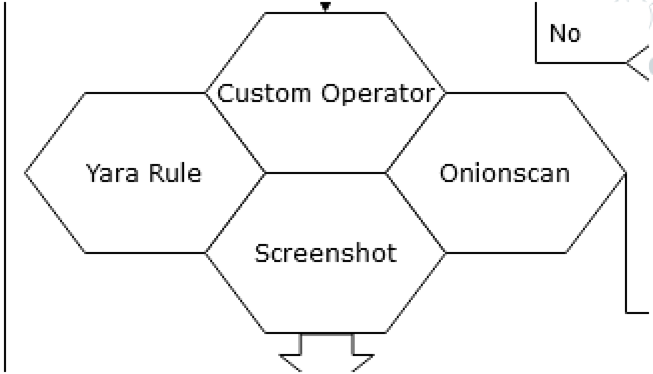


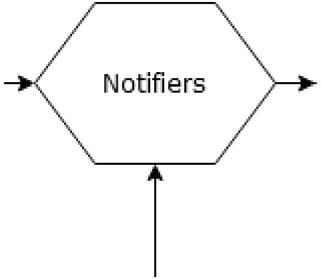
Open Source Intelligence Tool for the Dark Web

Image Sources: TorBot, OnionIngestor

OnionIngestor



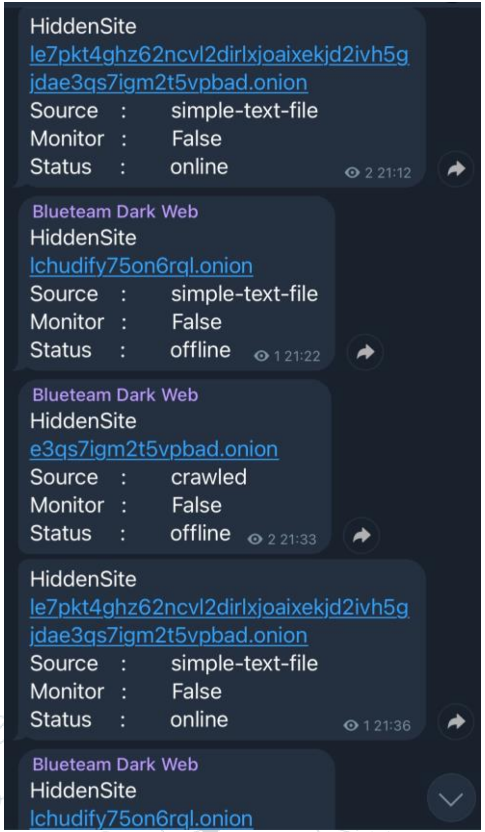




Daily Report

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

OnionIngestor (Contd.)



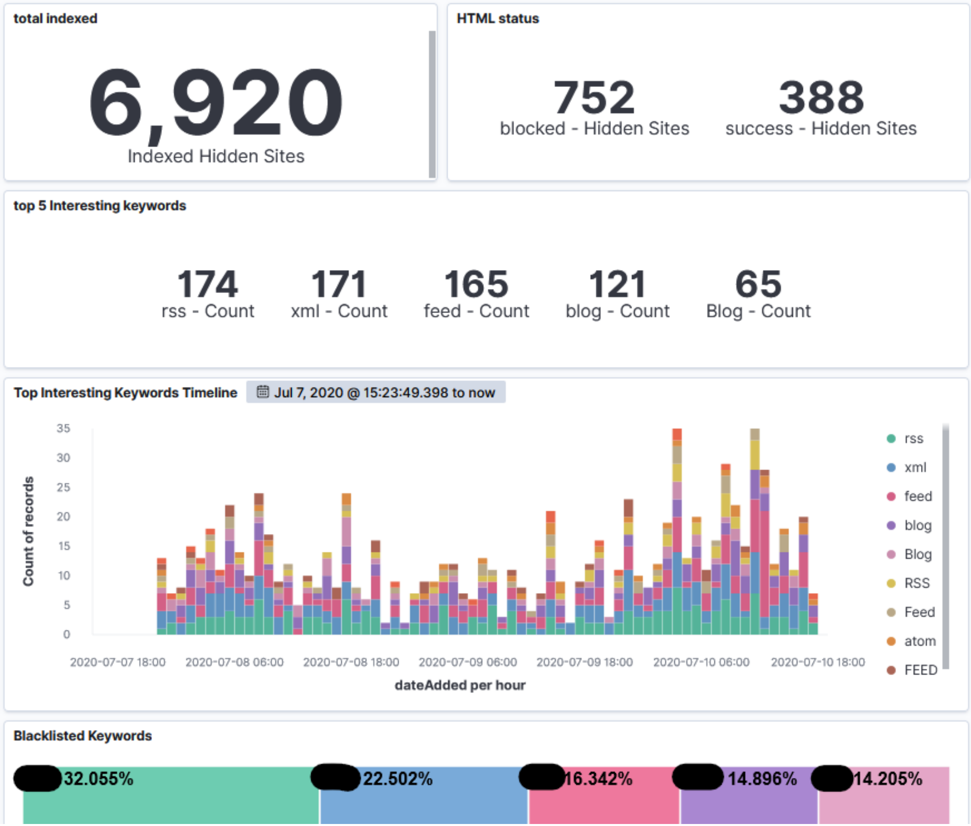
HiddenSite
le7pkt4ghz62ncvl2dirlxjoaixekjd2ivh5gjdae3qs7igm2t5vpbad.onion
Source : simple-text-file
Monitor : False
Status : online
2 21:12

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

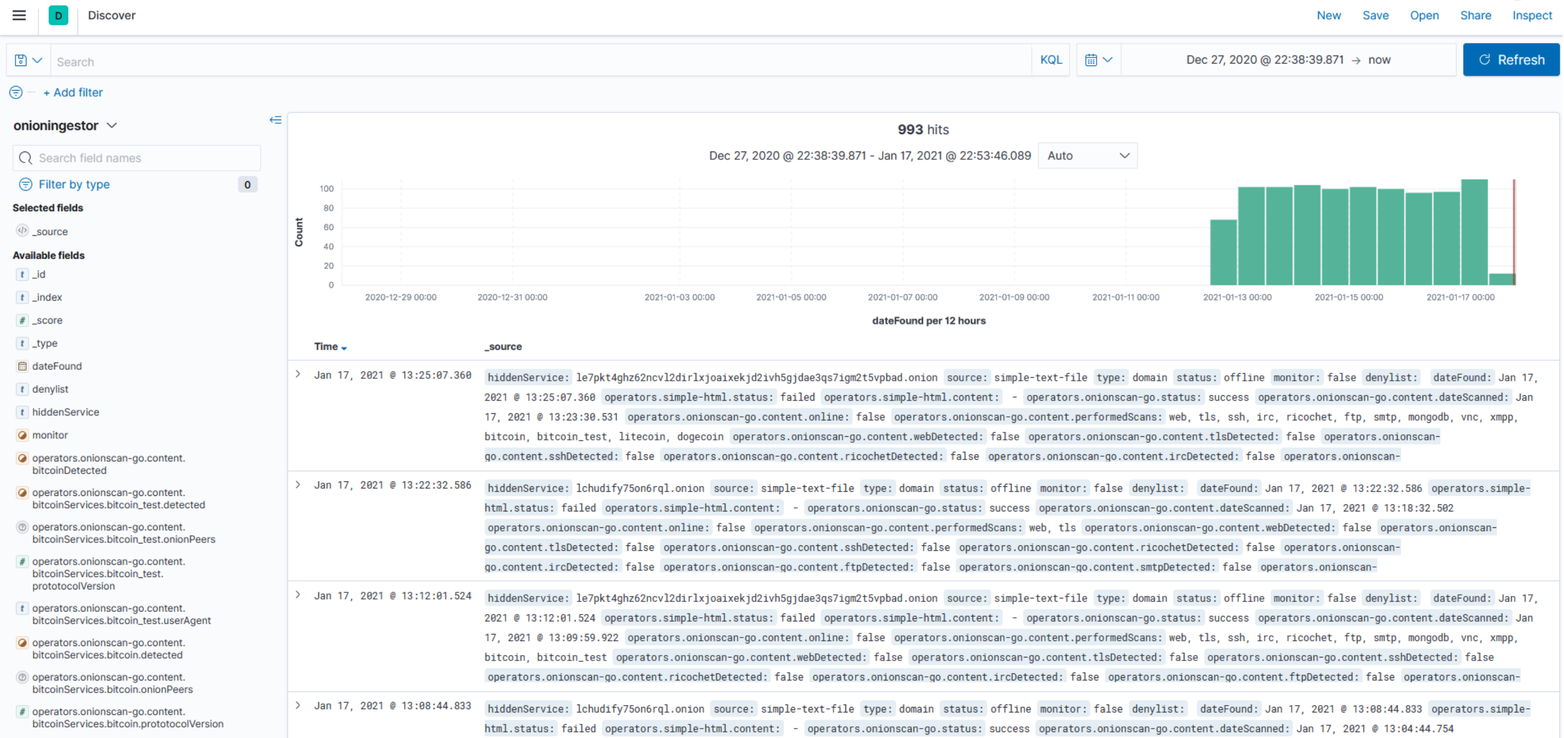
174	171	165	121	65
rss - Count	xml - Count	feed - Count	blog - Count	Blog - Count

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.)


D
Discover
New
Save
Open
Share
Inspect
Search
KQL
Dec 27, 2020 @ 22:38:39.871 → now
Refresh
+ Add filter
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.prototocolVersion
993 hits
Dec 27, 2020 @ 22:38:39.871 - Jan 17, 2021 @ 22:53:46.089
Auto
Count
100
80
60
40
20
0
2020-12-29 00:00
2020-12-31 00:00
2021-01-03 00:00
2021-01-05 00:00
2021-01-07 00:00
2021-01-09 00:00
2021-01-11 00:00
2021-01-13 00:00
2021-01-15 00:00
2021-01-17 00:00
dateFound per 12 hours
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
```

Create your own tools

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

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

6.

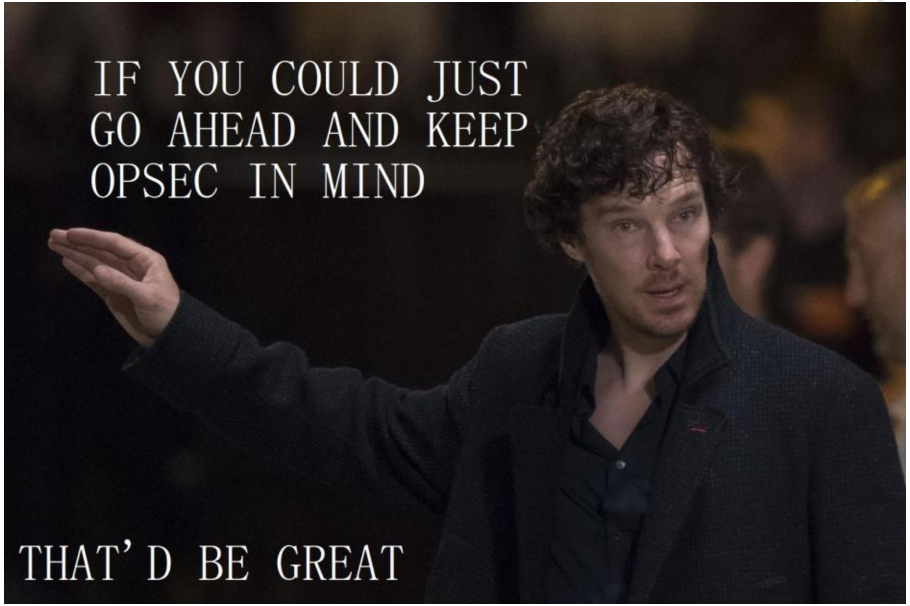
OpSec? What’s that?

What is OpSec?

- Actions taken to ensure that information leakage doesn't compromise you or your operations
- Derived from US military – Operational Security
- PII – Personally Identifiable Information
- Not just a process – a mindset
- OpSec is Hard

Maintaining OpSec in your lifestyle

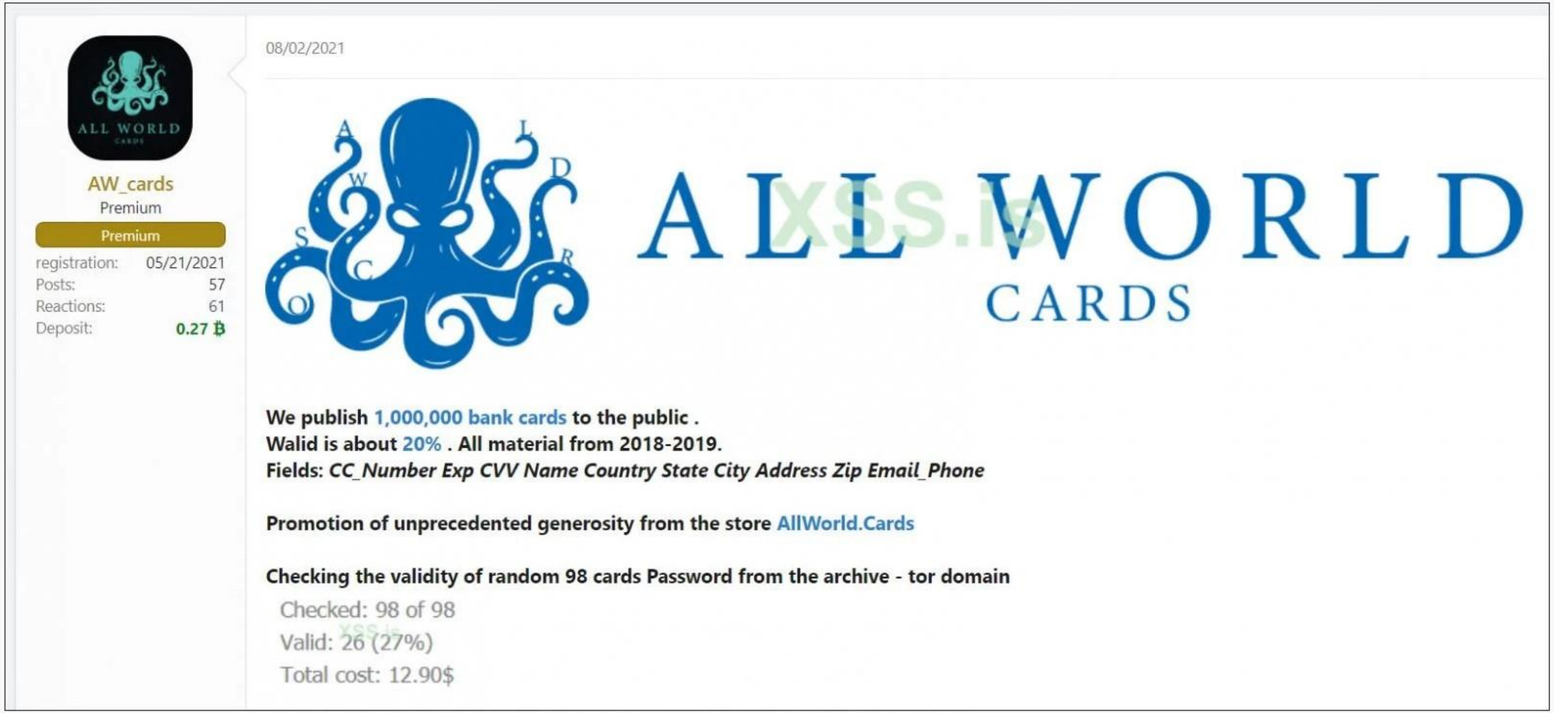
- Use VM/Lab or an isolated system
- Use Tor over SOCKS or VPN
- Change Time zones
- Never talk about your work
- Maintain different persona
- Take extensive notes
- Use password manager



7.

Case Study

All World Cards 1M Credit Cards



AW_cards
Premium
Premium
registration: 05/21/2021
Posts: 57
Reactions: 61
Deposit: 0.27 ₿

08/02/2021

We publish 1,000,000 bank cards to the public .
Walid is about 20% . All material from 2018-2019.
Fields: *CC_Number Exp CVV Name Country State City Address Zip Email_Phone*

Promotion of unprecedented generosity from the store AllWorld.Cards

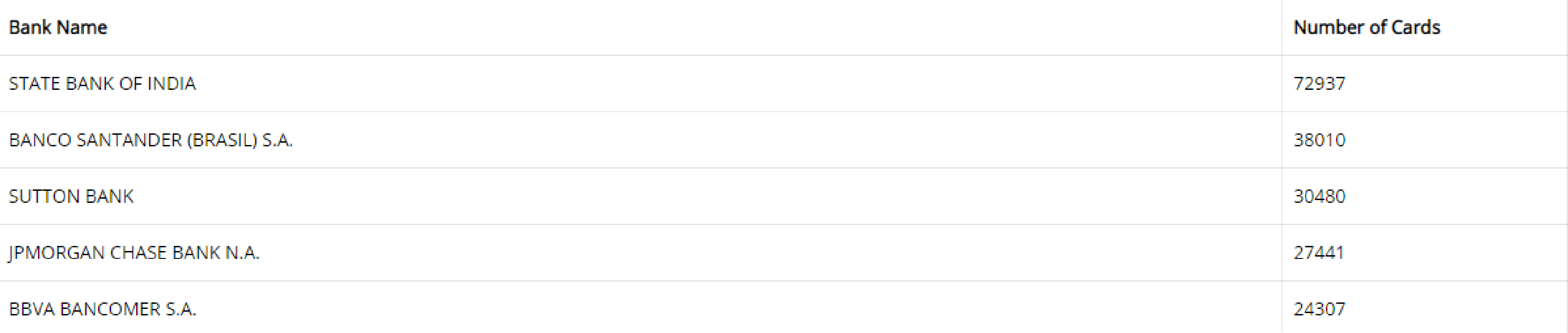
Checking the validity of random 98 cards Password from the archive - tor domain

Checked: 98 of 98
Valid: 26 (27%)
Total cost: 12.90$

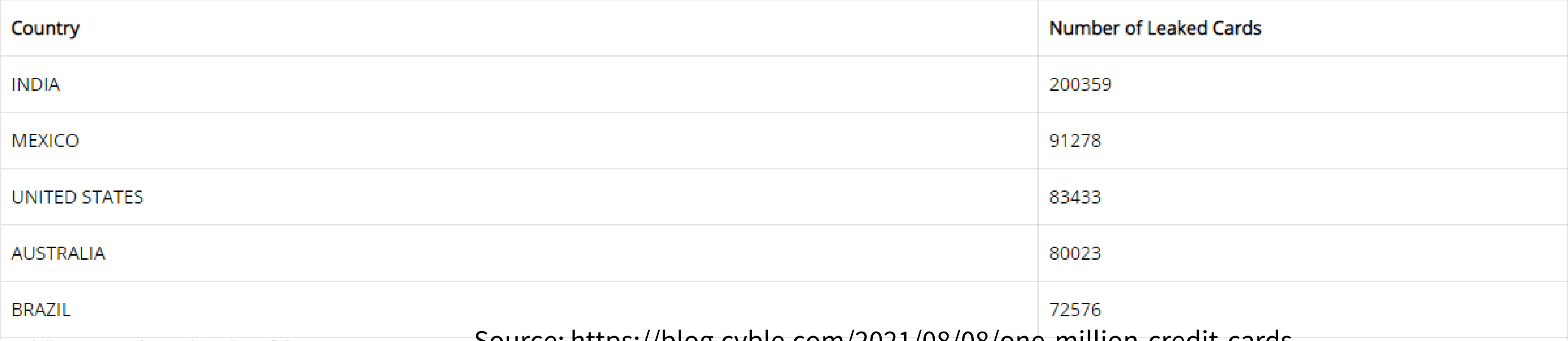
Type of Data Leaked

- CC number
- CVV
- Name
- Country
- Address
- Email/Phone

Affected Banks/Countries



Bank Name	Number of Cards
STATE BANK OF INDIA	72937
BANCO SANTANDER (BRASIL) S.A.	38010
SUTTON BANK	30480
JPMORGAN CHASE BANK N.A.	27441
BBVA BANCOMER S.A.	24307



Country	Number of Leaked Cards
INDIA	200359
MEXICO	91278
UNITED STATES	83433
AUSTRALIA	80023
BRAZIL	72576

Source: https://blog.cyble.com/2021/08/08/one-million-credit-cards-leaked-in-a-cybercrime-forum-for-free/

8.

Conclusion

What we discussed so far?

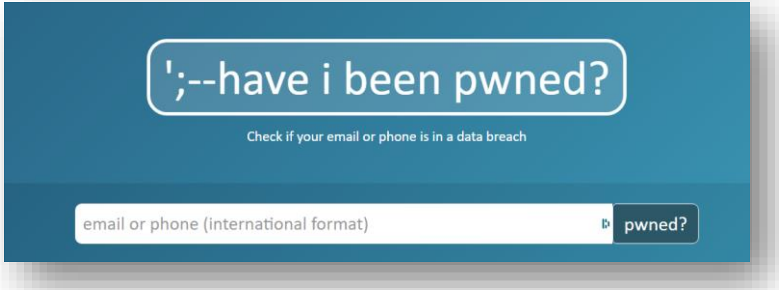
- Types of web
- Misconceptions of Dark web
- Why Dark web is important to monitor
- Skills needed to perform Dark Web monitoring
- OSINT, HUMINT
- OSINT tools
- Methods to create your own scripts

I don’t know how to conclude but..

- Dark Web monitoring is hard but worth the effort
- Keep OpSec in mind
- Look at more than one resource
- Takes a lot of resources and team effort
- It can be fun if you enjoy research and investigations

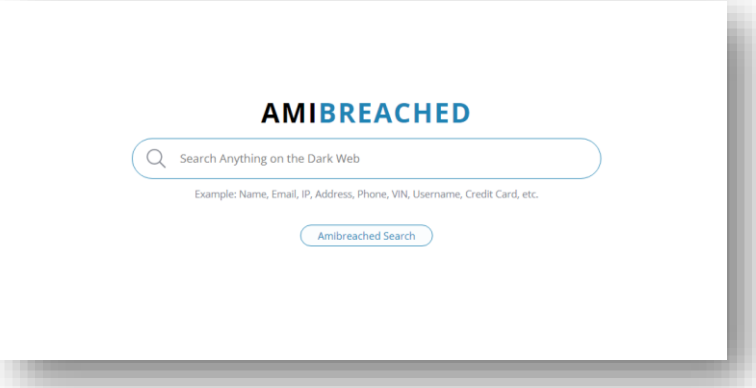
How to protect yourself

- Search on surface web to identify the information available
- Utilize services like AmIBreached or HaveIBeenPwned to see how much data is exposed



';--have i been pwned?

Check if your email or phone is in a data breach



AMIBREACHED

Example: Name, Email, IP, Address, Phone, VIN, Username, Credit Card, etc.

Source: https://haveibeenpwned.com/, https://www.amibreached.com/

Resources

- Read White papers & blogs from different security organizations
- Follow people on LinkedIn and Twitter
- Follow hashtags - #darkweb, #threatintelligence
- Search Terms – darkweb, tor, deepweb, cybercrime forums
- OSINT Framework - https://osintframework.com/
- OSINT Combine Dark Web Searching - https://www.osintcombine.com/post/dark-web-searching

Resources (Contd.)

- Jake Creps Blog - https://jakecreps.com/2019/05/16/osint-tools-for-the-dark-web/
- SANS Cyber Defense Forum - Automating Threat Hunting on the Dark Web and other nitty-gritty things talk by Apurv Singh Gautam
- DEFCON Recon Village - Ambly the Smart Darknet Spider talk by Cytisus Eurydice (@levitannin)

Thanks!

Any questions?

You can contact me at:

Twitter: @ASG_Sc0rpi0n

LinkedIn: /in/apurvsinghgautam