Case Study

Latest Covid-19 Developments in Dark Web

December 2021

DARK WEB SOLUTIONS

Strategic Insights, Operational Perspectives

CFLW

Cyber Strategies

Covid-19 in the Dark Web

- Covid-19 remains a global concern given another wave of infections, and second the new concerns resulted from the recent spread of the Covid-19 Omicron variant.
- Discussions regarding the new variants and their transmissibility and severity, the efficacy of existing vaccines, and border restrictions are ongoing all over the world.
- This case study answers questions on the role played by the Dark Web in frustrating efforts to contain Covid-19 and exacerbating the impact of the virus.

Case Study Questions

- What use cases are supported by the Dark Web?
- How do these use cases affect different countries?
- What other observations are noteworthy?

Domain provides overview of corona passes per country:
http://dzsjmkkbakqgel54h65o72dfxrnsghbly3rm77xeixpe3m4r7fkyelad.onion

Revendeur Véritable Pass Sanitaire :
(Tout ces sites ce font copier, faite attention à l'adresse)
(Tout les sites avec des liens commançant par "covid" sont des scams/arnaques)

Collectif Médical :
http://uayitjsfxr2lswmr5bdmahm6xpquc5velokem3xf6tbdtksg3vepynqd.onion/

Fuck The Covid :
http://ebpymvvxy7vgklfdxzp6r2kdqe2gekc3vvu23zx7tnl5xpoarjnfjnqd.onion/

Intermediaire Sanitaire :
http://oy4zbz62xqxrnad3sbpxcx5c2vwffygr3uxyk6yie75ihlliwfrkazyd.onion/

COVID certificate SUISSE :
http://7jvorw5otnqr3tw6uh6okertjzweuiqxsjkujy6nw36fi5piu26gegyd.onion/

Green PASS (Italie):
http://yeb7ya4aspvwgfhgk5hx7q7rkoah5qdvafi3akogi5eiiygao54ifwid.onion/

Corona Check (Pays-Bas) :
http://6vv7zw4w6rr4oxqyecgeyllgbswor4wuztkibbuhhf2lwrgvvsgsswqd.onion/

Corona Pass Danemark :
http://ebc3luxbk5b4k5iazwj3adocbqnbgplz2htaxi5tpi7ua6sxhaqpzoqd.onion/

USA Certificate :
http://7pwcvofvrarfy2vj4dtdxivcqfl6vubs3a3suh7o2v54g4vawd7tteqd.onion/

En bonus le meilleur market FR - Coq Market :

http://axispkba2ewgxrnxzhwvdktbx7ugkkn5vrudu7xxbcjgvto66pjtbhad.onion/

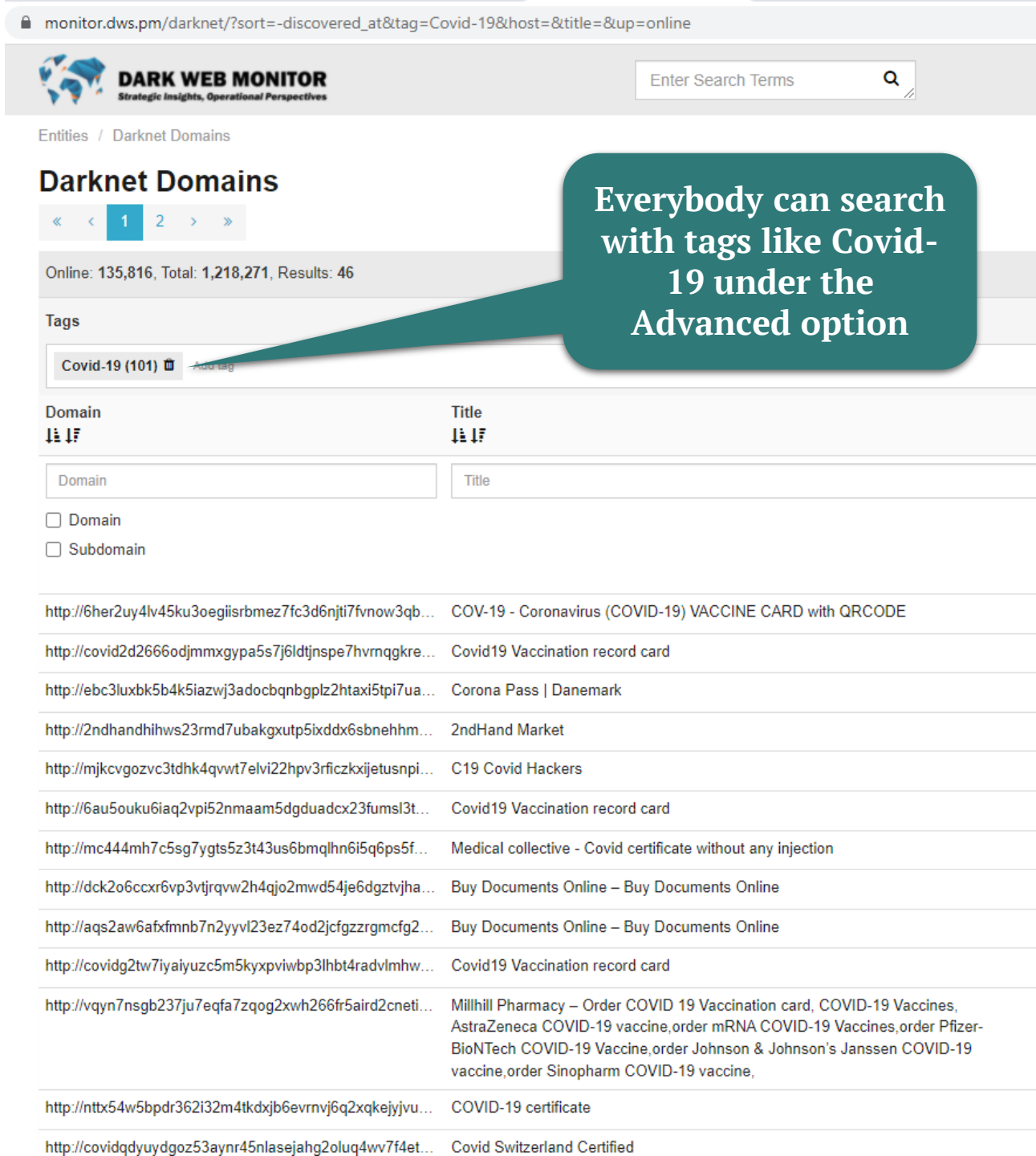
Profitez bien !

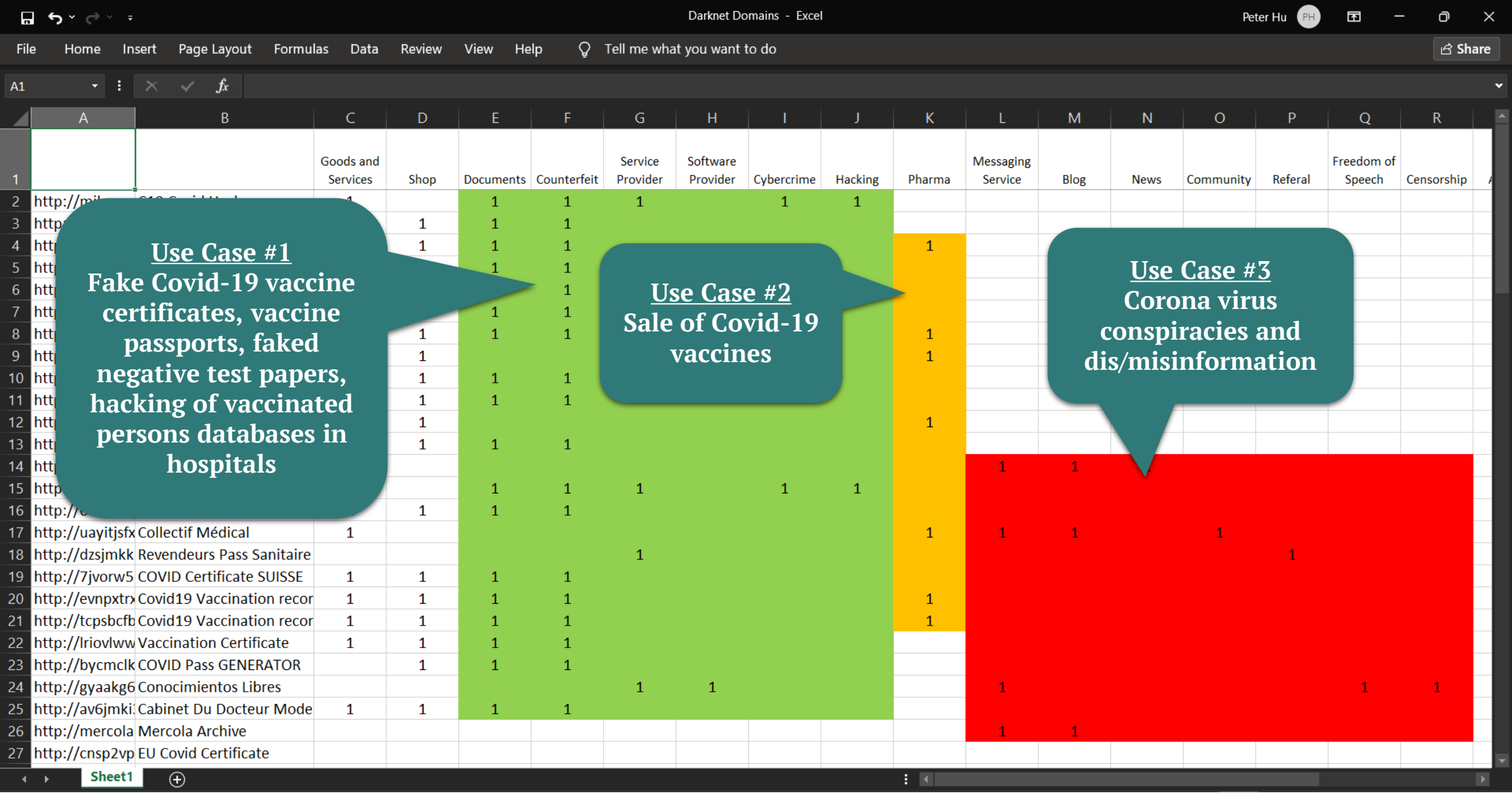
Use Cases in Dark Domains tagged Covid-19

Top 3 Use Cases

1. Fake Covid-19 documents:
   - Vaccine certificates
   - Vaccine passports
   - Faked negative test papers
   - Hacking of vaccinated persons databases in hospitals
2. Sale of Covid-19 vaccines
3. Coronavirus conspiracies and dis/misinformation

https://monitor.dws.pm/darknet/?sort=-discovered_at&tag=Covid-19&host=&title=&up=online



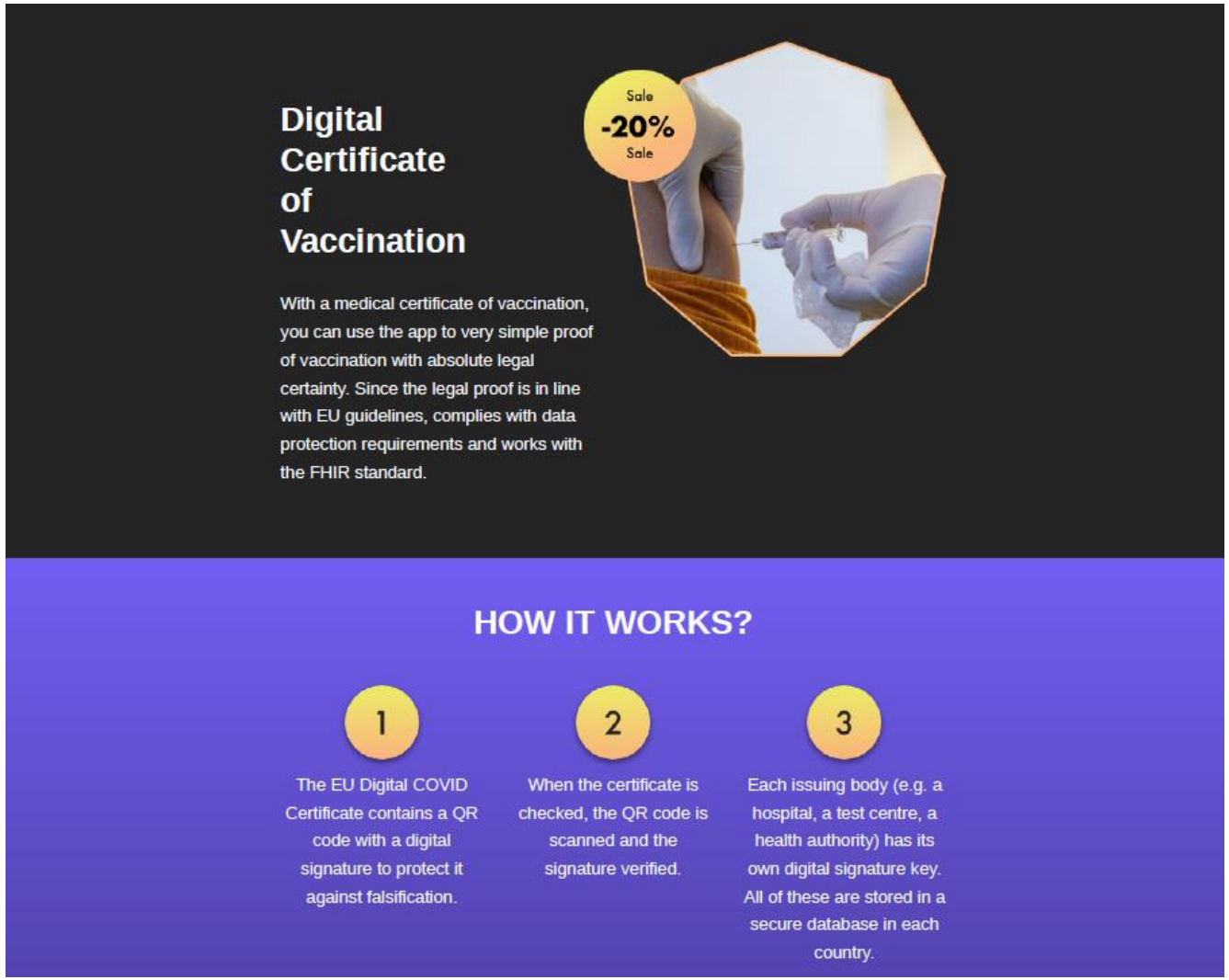


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1			Goods and Services	Shop	Documents	Counterfeit	Service Provider	Software Provider	Cybercrime	Hacking	Pharma	Messaging Service	Blog	News	Community	Referal	Freedom of Speech	Censorship
2	http://mi		1		1	1	1		1	1								
3	http			1	1	1												
4	htt			1	1	1					1							
5	htt				1	1												
6	htt					1												
7	htt				1	1												
8	htt			1	1	1					1							
9	htt			1							1							
10	htt			1	1	1												
11	htt			1	1	1												
12	htt			1							1							
13	htt			1	1	1												
14	htt											1	1					
15	http				1	1	1		1	1								
16	http://c			1	1	1												
17	http://uayitjsfx	Collectif Médical	1								1	1	1		1			
18	http://dzsjmkk	Revendeurs Pass Sanitaire					1									1		
19	http://7jvorw5	COVID Certificate SUISSE	1	1	1	1												
20	http://evnpxtrx	Covid19 Vaccination recor	1	1	1	1					1							
21	http://tcpsbcfb	Covid19 Vaccination recor	1	1	1	1					1							
22	http://lriovlww	Vaccination Certificate	1	1	1	1												
23	http://bycmclk	COVID Pass GENERATOR		1	1	1												
24	http://gyaakg6	Conocimientos Libres					1	1				1					1	1
25	http://av6jmki	Cabinet Du Docteur Mode	1	1	1	1												
26	http://mercola	Mercola Archive										1	1					
27	http://cnsp2vp	EU Covid Certificate																

Fake Covid-19 vaccination certificates

Use Case #1

- “Work has asked that I get vaccinated, but for various reasons I don’t want to.”
- Most vaccine certificates bought on cybercriminal platforms are likely intended to circumvent travel restrictions.
- Sale of Covid-19 “vaccine passport” to buyers who “want to travel freely without being jabbed.” Cost starts from as low as $25.

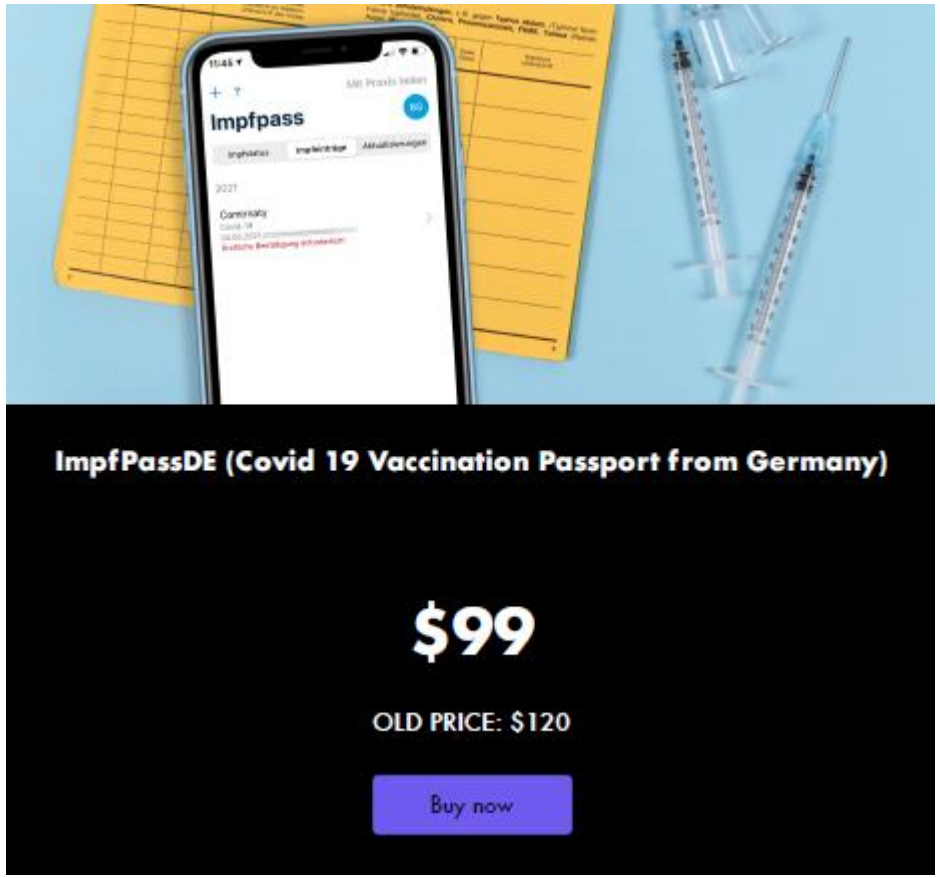


https://www.bbc.com/news/technology-56489574

Fake Covid-19 vaccination certificates

Use Case #1

- Some domains charge a standard rate for Covid Certificates for various countries. For example, the domain in screenshot charges a standard rate of $99 for Covid Certificates for France, Germany, USA, Romania, Czech Republic, UK, Ukraine, Fiji, New Zealand, Austria, Switzerland, Greece, Belgium, Spain, Netherlands, Finland, Ireland, Canada, Australia, Italy, Portugal, Latvia, Estonia, Slovenia, Russia, Morocco, Brazil, and even “Other Country”.
- Each Covid Certificate is customized to the healthcare system of each country (example on the right).
- The prices are dynamic. For example, the price from this domain was $75 on 4 Nov 2021. On 1 Dec 2021, it had since increased to $99.

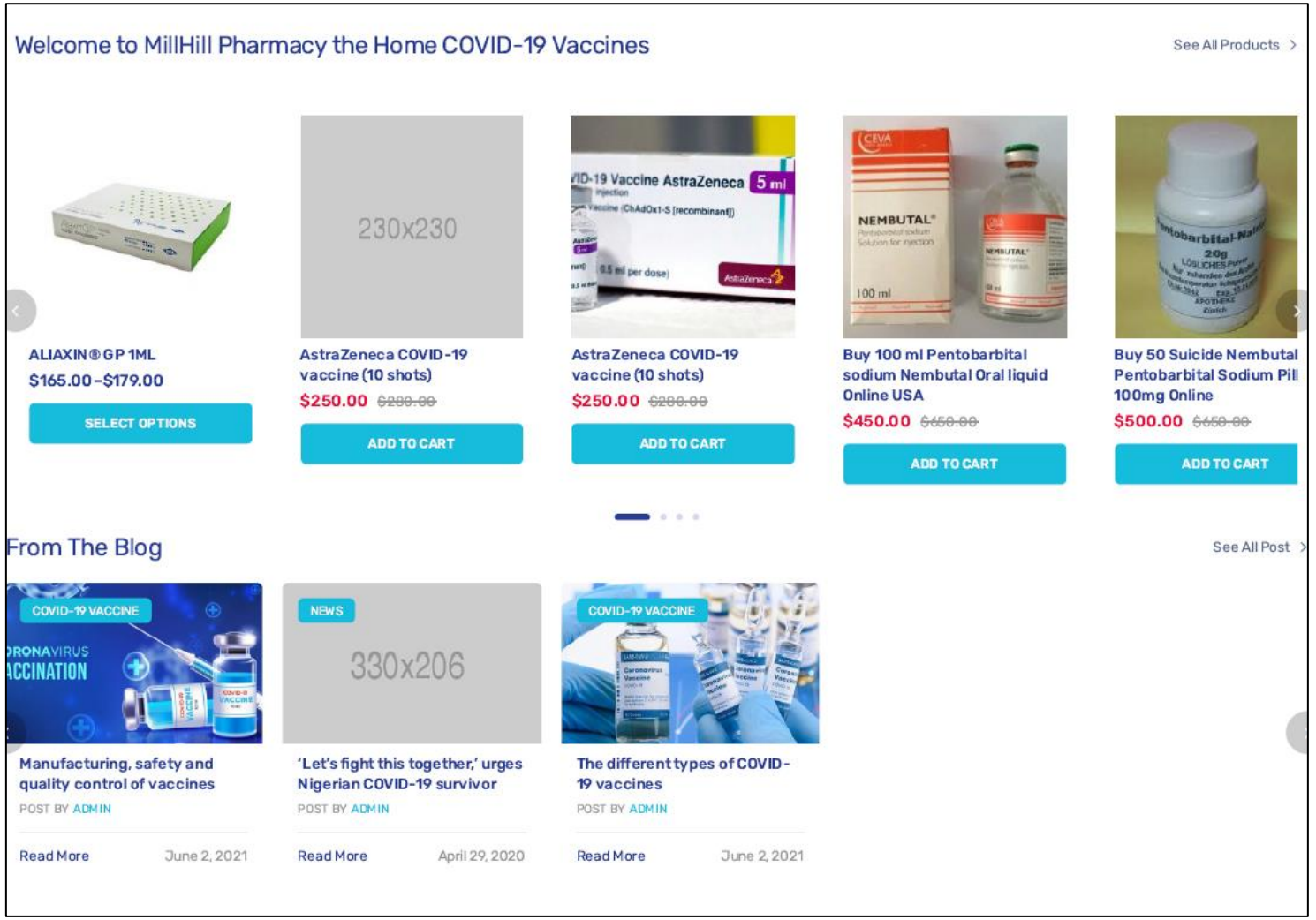


Discovered and online between 4 Nov and 1 Dec 2021:
http://covidg2tw7iyaiyuzc5m5kyxpviwbp3lhbt4radvlmhwwfceb7j7uyid.onion

Covid-19 vaccines offered

Use Case #2

- Covid-19 vaccines are being sold on the darknet. Prices range between $150 – $500 for doses of AstraZeneca, Sputnik, Sinopharm, or Johnson & Johnson jabs.
- Vendors are cashing in on people desperate to leapfrog the line.



https://www.wired.com/story/dark-web-teeming-with-vaccine-listings/

Covid-19 vaccines

Use Case #2

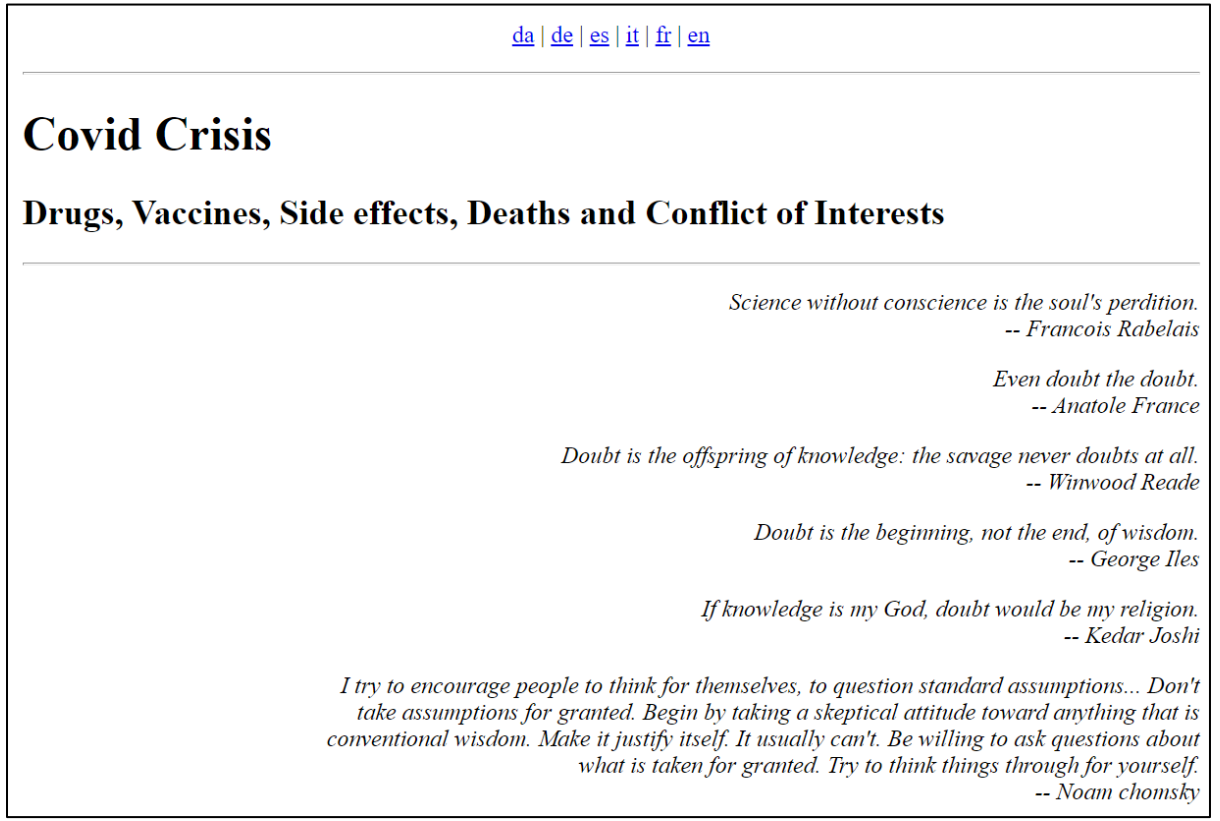
- As early as April 2020, we found the first online advertisements for Covid-19 vaccines, which were obviously scams.
- Nowadays, it is much more difficult to ascertain the authenticity of vaccines sold.
- The fact that transportation of vaccines requires them to be stored at temperatures between -50 to -80 degrees Celsius, makes such sales highly suspicious in general.

Discovered and online between 26 April and 2 May 2020, currently offline: http://zhhmcrde4eibgnepxmo4qr4okw6cmfesxa64el2lo6unc5tdvalicsid.onion

Conspiracies & dis/misinformation

Use Case #3

- Conspiracy theorists are “exploiting the fear, uncertainty and doubt people are experiencing during the pandemic, and using the anxiety and desperation to get people to buy things or click on things they wouldn't have otherwise,” and as a result these items are not cheap.
- These forums often act as a gateway to marketplaces, for people to plug their products or services to a targeted audience.
- Hackers are more interested in your money, information, and identity for exploitation.



da | de | es | it | fr | en

Covid Crisis

Drugs, Vaccines, Side effects, Deaths and Conflict of Interests

Science without conscience is the soul's perdition.
-- Francois Rabelais

Even doubt the doubt.
-- Anatole France

Doubt is the offspring of knowledge: the savage never doubts at all.
-- Winwood Reade

Doubt is the beginning, not the end, of wisdom.
-- George Iles

If knowledge is my God, doubt would be my religion.
-- Kedar Joshi

I try to encourage people to think for themselves, to question standard assumptions... Don't take assumptions for granted. Begin by taking a skeptical attitude toward anything that is conventional wisdom. Make it justify itself. It usually can't. Be willing to ask questions about what is taken for granted. Try to think things through for yourself.
-- Noam chomsky

Domain was discovered and active between: 14 July 2021 and 13 October 2021
http://pcr6k5krxwcvmessygjmfsbxgnyju6ipq5236ki55n2i5u4uylpq.b32.i2p

Note this domain was not hosted within the Tor network but in I2P

Exit Scam
Observation #1

A small shop had opened to sell International Vaccination passports in Germany.

COVID-19 Impfnachweis ausgestellt in Bayern

Add To Cart

EUR 70.00

Es handelt sich um originale Impfnachweise mit original Impf-Vignetten (Chargen-Aufkleber nebst passendem Datum der Verimpfung), Stempel und Unterschrift des Arztes. Es wird nur Impfstoff von BioNTech/ Pfizer bestätigt mit min. 3 Wochen Abstand zwischen den Impfungen.

Dieser Nachweis ist offiziell zugelassen und wurde dafuer gemacht, in **IHREN ORIGINALEN** Impfausweis eingeheftet zu werden, wo es normalerweise noch keine Seite fuer COVID-19-Impfungen gibt.

Ausstellungsort ist ein Impfzentrum in Bayern

Lieferzeit: ca. 2-3 Werktage

COVID-19 Impfnachweis ausgestellt von einem Hausarzt ohne Ortsangabe

Add To Cart

EUR 80.00

Es handelt sich um originale Impfnachweise mit original Impf-Vignetten (Chargen-Aufkleber nebst passendem Datum der Verimpfung), Stempel und Unterschrift des Arztes. Es wird nur Impfstoff von BioNTech/ Pfizer bestätigt mit min. 3 Wochen Abstand zwischen den Impfungen.

Dieser Nachweis ist offiziell zugelassen und wurde dafuer gemacht, in **IHREN ORIGINALEN** Impfausweis eingeheftet zu werden, wo es normalerweise noch keine Seite fuer COVID-19-Impfungen gibt.

Generalstaatsanwaltschaft Bamberg
Zentralstelle Cybercrime Bayern

Diese Plattform und der kriminelle Inhalt wurden beschlagnahmt
durch das Landeskriminalamt Sachsen im Auftrag der Generalstaatsanwaltschaft Bamberg - Zentralstelle Cybercrime Bayern.

The platform and the criminal content have been seized
by the State Office of Criminal Investigation Saxony (LKA) on behalf of Attorney General's Office Bamberg.

After two weeks, the shop closed and displayed this Law Enforcement Notice.

However, this notice was NOT gazetted by Law Enforcement authorities and appears to be fake (likely an exit scam).

Cyber Scams?
Observation #2

Same cryptocurrency address / wallet used to sell the Covid pass had also been used to sell Child Sexual Abuse archives.

This address has transacted 176 times on the Bitcoin blockchain. It has received a total of 0.06495977 BTC ($3,153.97) and has sent a total of 0.06495977 BTC ($3,153.97). The current value of this address is 0.00000000 BTC ($0.00).

Address	1AgdFs8LPtEhN8b4W7GVepp2Db6Uo8CcgE
Format	BASE58 (P2PKH)
Transactions	176
Total Received	$3,153.97
Total Sent	$3,153.97
Final Balance	$0.00

Last transaction on 18 Oct 2021

monitor.dws.pm/crypto/5735265

DARK WEB MONITOR
Strategic Insights, Operational Perspectives

Enter Search Terms

Entities / Cryptocurrencies / 1AgdFs8LPtEhN8b4W7GVepp2Db6Uo8CcgE

Cryptocurrency Address

Cryptocurrency	Bitcoin [BTC]
Address	1AgdFs8LPtEhN8b4W7GVepp2Db6Uo8CcgE [redacted]
Discovered	05 Jul 2021, 02:59 UTC
Last Discovered	20 Aug 2021, 16:20 UTC
Domains	9
Appearances	11

Domains (9) Pages (11)

Domain	Title	Online	Tags
http://xxxxz3zxd3vegsqk.onion	CP - FTP	✔	7
http://xonixyvdf64r7pfc7756etrpgtwkdwarhtkleu6pge7wuu...	Porn Videos - XONIONS - THE BEST ONION PORN SITE - Onion link Porn	✔	4
http://zyse6s5slvpmhin7vgzgo7j3uezymefijtonevz4wwmb...	CP - FTP	✔	7
http://ygxa4cxjguefmgdne5ri2h26est7bv225gifefexx2ep4...	!!!HARD PORN!!!	✔	5
http://maenvnmyvct7za6kme4e4ksugzzddjkvvnfi6edgaojy...	My daughters Marzia and Enza	✔	7
http://nwdiker3rzrsg62bgkjmya6nzhtlpvqwjok2os6msrr26...	Little Love	✔	7
http://hackttfkc5lu4id7ajcf7qkeozoyjdn5wxds4ftzbjnu4fcg...	Porn Site Hacker	✔	4
http://macpkf6afkyoyot3fd5ofdbwl6asu26mbr5marlb7ueq...	Pedo lola	✔	7

CovidpassGENERATOR

Generate to covid pass to free EU

After payment, the covid pass will be generated in both paper and digital versions.

0.0015 BTC

Deposit to this wallet BTC:

1AgdFs8LPtEhN8b4W7GVepp2Db6Uo

Status: Waiting for the payment...

CANCEL THE PAY

Concluding Remarks

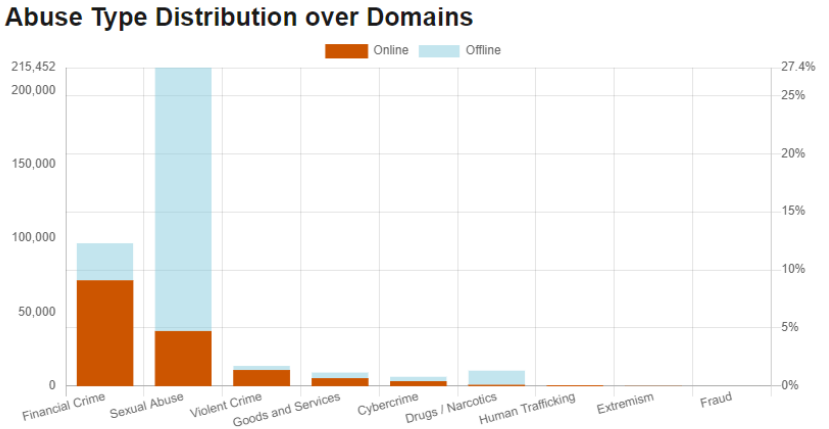
- Dark Web is used to frustrate Covid-19 measures with use cases
    1. Counterfeit documents, certificates and proofs,
    2. Fake or stolen vaccines and
    3. Spread of dis/misinformation.
- Illicit purchasing of vaccination proofs is a worrying trend, especially given they are offered for a large range of countries
- Covid-19 scams abound and are correlated to other crimes and scams. These initiatives have attracted a significant number of transactions, and should not be taken lightly.

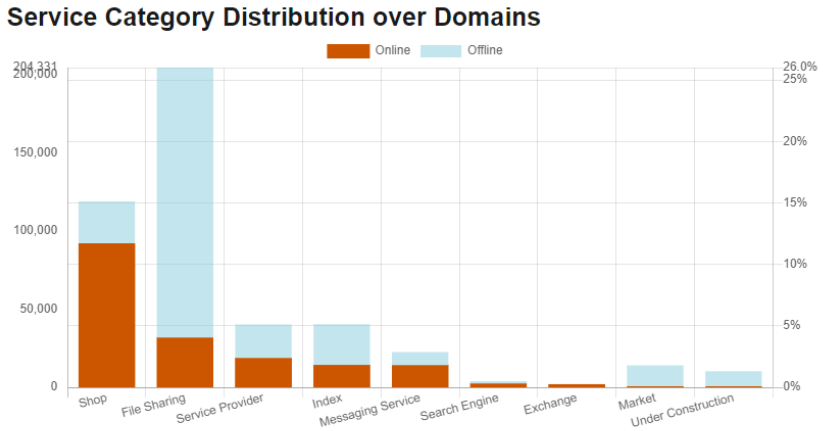
Dark Web Monitor

- DWM is an Open Source Intelligence (OSINT) repository that provides insights into criminal and fraudulent activities facilitated by the Dark Web and Virtual Assets.

- Active monitoring (Dated December 2021)
  - > 1.2 million Dark Web domains
  - > 130,000 active Dark Web domains
  - > 7.5 million Cryptocurrency addresses discovered in Dark Web

- Targeted monitoring of online illegal activities: https://cflw.com/dwm





Colophon

For any questions on this case study how we retrieved the data, or how we obtained the analytical insights from Dark Web Monitor?

Latest Covid-19 developments in Dark Web

Feel free to contact the

CFLW Intelligence team

info@cflw.com

Intelligence Services

Strategic Insights, Operational Perspectives


CFLW
Cyber Strategies