Together for a safer cyber space

OPSEC Measures by Dark Web Markets and Service Providers

OMG, cybercriminals have their security guidelines too!

November 2022

Case study conducted by

TNO innovation for life

CFLW Cyber Strategies

DARK WEB MONITOR
Strategic Insights, Operational Perspectives

Outline

- Introduction operations security (OPSEC) on the Dark Web
- How does the Onion Mirror Guidelines (OMG) work?
- Trends in OMG adoption with Dark Web Monitor
- Review of the OMG use in practice
- Law enforcement implications
- Future research and development recommendations

OPSEC on the Dark Web

- An increase in the value of traded commodities or trading platforms itself results in an increased urgency to implement OPSEC measures.
- Due to successful law enforcement operations on one hand and threats from cyber criminals on the other hand, security measures are important to protect the assets of the Dark Web service providers and end users. This is no different from the open internet!
- Operations Security (OPSEC) becomes increasingly important on the Dark Web. This study provide insights into the following question:

Research Question

How have the Onion Mirror Guidelines (OMG) as an OPSEC measure been developed and implemented since its launch in 2019?

OPSEC Background

- OPSEC is the systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities.
- The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.[1]
- OPSEC measures are relevant for several dark web actors like financial service providers, market owners, single-vendor shop owners, end users or clients and the relation between these entities.
- The relevance of OPSEC measures taken by cybercriminals is addressed in various studies, such as Europols IOCTA[2] and the National Risk Assessment for the Netherlands[3].
- The Onion Mirror Guidelines standard is a measure which can be implemented to increase OPSEC on the dark web. It is rather simple to implement and we have access to data to analyse its adoption.

1. https://csrc.nist.gov/glossary/term/operations_security
2. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf
3. https://www.nctv.nl/documenten/publicaties/2022/09/26/themarapportages-cyberdreigingen-2022

OMG Introduction

Dark.fail , a site which is used to check whether dark web domains are online, proposed the Onion Mirror Guidelines (OMG) in 2019[4].

The objectives:

1. Reduce the impact of phishing;
2. Ease automatic PGP verification of mirrors.


```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Admins,

To reduce the impact of phishing and to ease automatic PGP verification
of mirrors, dark.fail is now defining the Onion Mirror Guidelines. (“OMG”)

Admins that implement this standard show a commitment to user safety
by proving ownership of all URLs associated with their site, and by
committing to regularly prove control of their PGP key.

Sites which do not implement these guidelines by Dec 1, 2019 will be
marked as "unverified" on dark.fail and listed below all other sites.

DarkDotFail
```

dark.fail: Is a .onion site online?

Updated Fri, 30 Sep 2022 07:38:16 UTC
Mastodon | Twitter

You are on the clearnet. It is not recommended to view our site here. Domain names are not as secure as Tor hidden services. Install Tor Browser and visit us at our .onion instead:

4. https://dark.fail/spec/omg.txt

How does the OMG standard work?

By implementing the OMG standard, site admins show that they are in control of their domains. The following three text files must be hosted on all of the admins' onion services to fully implement the standard:[4]

- **/pgp.txt** → A list of all PGP Public keys allowed to announce the official mirrors. It may contain multiple PGP keys. All keys must be ASCII armored.

- **/mirrors.txt** → A PGP signed list of all official mirrors of the site. Mirrors must be signed by a PGP key that is mentioned in the **pgp.txt** hosted at all of the URLs.

- **/canary.txt** → a PGP signed message that must be updated every 14 days. The message must contain the latest Bitcoin block hash and the current date in YYYY-MM-DD format, with the string 'I am in control of my PGP key'. It must also include the string 'I will update this canary within 14 days'.

4. https://dark.fail/spec/omg.txt

Example per .txt file

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: OpenPGP v2.0.8

xsFNBF8GsEsBEADEkogYTlRt369av51BuJCSVYGovm3w7SYXdNLlGotnkJjSaq3R
2aiYF9z5f3Ptin9ySpvLhc1JolQl6UwjZvHZNYgudz/4uOyyhbqoQYCucBC0Uou0
k3KY2bnzbuWrZl8tgUpO9Sm1+VKa5pWRoyMr9cNQhHz8vAlKRwM6LTg5yxO1JHFY
hiZu2gRGtshTSnVZdbQ5wfRpGD6hvr5k3Pi/ulakGjQfJsYhqXTrEN8VrRxipE1v
ZtYR6zUmjy1iSAtuGPnUOtFSEi1oCqnN+V8OGpYX5kJGBCLEZyf3WEkSo5nLj4T1
Pec2QhVrhqdDOmV8CL2bZLb/jqf69QHMHgg32AZJsRMtiS7Kg2FvK+kdSKVa1S8Q
siZU8XYWQ3Bukq/C/vWD7sYp51TvXYoaqub4CnNPoqtflsw1ZE8Rg4XBO9MUb25G
NtmrLRCZ4YR5OAXyE3f9uqUBG0A+UEYOOZeHrQy1KecvNvGe0IFSxgaYbue4Z2OS
MocGGwobrntTcqXMVFBVTDmgLLE9YNfBPWhF+L3H9empsF/R4uDsupklKhTTKzUV
9V+XACBSpotZJDAf7bHXkypvNkdPSFLHAWt1nojMZ3WHMIaM9VG8z3SfjiXAE5g1
udEXvlzqXC/1Ci5yii13seb7yuCjbxiP3xMQ/sKXH5vsQmgWdznlEdxNzQARAQAB
zQ1kZWVwc2VhbWFya2V0wsFwBBMBCgAaBQJfBrBLAhsvAwsJBwMVCggCHgECF4AC
GQEACgkQFZUUY+d8tDiClg//eadjObyujNueFG98NH/qxejL71aDNEMOwHiTOuiy
UdtQOBEI2mVin6uCOCFd4IPT1Rgma+TUdDRJPtV4OAlRlbJaC06EZNdVVQNm/rb5
UaG6JRLDMQC8V2y3NEw7HFR8/vOwJGsn04d/OKdBAAd32Y88wfOTMkogjx4vbod7
vxgNEgPzagjeR5efIpM4ttvimtLAtJzzwN3M+LUfvtgkyN5Ew/lLFeYG5tLoEjjB
h1G8mTNVvhl2weH4GAFd8cMz3l/e565TDu3lp21x1WEnFxvEa6NhVKzK5puyvZKT
YT/IEbZGxwNRD12/Cb8usMX+XTamxgbbR5ozsKsSikdywgUnahrXngKDSOqq/aO3
MXK6h8AjWKsUZ+sl161YZDnPNgZAyvBeG5Eil/GBv/x7VRwFA2IcPVqD/ueOgAFs
2YryfKJdhcqsopZ3dAt9mo5HyDErXfBv4dKWtsB6T95o7lBHa1T85z8I6J7wEtcp
ds7+lbuG4hg3zqbSmgPBcPex+xLEGEXg2ZAnjLWBQ5dvXPyFTKbE2SEi5+yiF94O
LE1fALoLAepCKctA7DuGnSILG4OIswaKOTlE3gzqftvmpug+CsSsaGpZoCAe+wPI
rcVlcmtu6Ju/XJsnDRSQcnMropRVtb/aWW7g10LlhUE/RHDDe6mM2cy6yrXhJ5z4
oLLOwE0EXwawSwEIAN2JrSENLdfwmq0WviOsYJSUcJBIFq2qp30W9Ev+/PqTFLBk
xHc3p46LGAl55d852Fu9e/H9vhoI2dPXNdGG8cGpvAOOZd2wT8rzsLgrYESLxDWh
BNmGqNxr+YLX9OhYjGqpFVJsHwkEGlzb/7Uyjzo2UYSuQigaF4TjYGaJOu4qjDPR
/Pgjs7InpQVZSbxURupd8GFRRru70xCSSBoEZny2HyVF0aK/I3I0IvPqev8EbZb4
KxpjBpsyZlFzFKU+xw9M9A5DwFkUGyRA1Epaqe70IodHt943yFcfeapWwVYt+SfZ
0irP3lQlg+mEqD1dBLc7e4LekXaC0vOjHGf/AA0AEQEAAcLChAQYAQoADwUCXwaw
SwUJDwmcAAIbLgEpCRAVlRRj53y0OMBdIAQZAQoABgUCXwawSwAKCRBUknfJeXey
```

pgp.txt

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

http://w6a47tienfk6vycx.onion/
http://rxxruvb6jufh3emqi7tf4hxff2ka6ajgfbgqh5lztgx4mkcldnk6q7ad.onion/
http://srrc4q4pia3nqx34wjczerdgqjmlbftetgzl57rdbh6cygcmrpaayoyd.onion/
-----BEGIN PGP SIGNATURE-----

iQEzBAEBCgAdFiEEaDt5FCneiiuxE0M6VJJ3yXl3sjwFAl8ahO4ACgkQVJJ3yXl3
sjwBEQf+JnwoprCpu5jnSv4H4EjEHYNdcBdlLV8D+M5VDj1dx5xNucSeXj7uIKCn
nfZmZozMRvT+G1lFuazz5UVMfPLS9X0O8gFszy+zuqlIk9z5UmKhgEs7rrkWnnqj
vIiBUPwZVb8QWRaYyAkf9Ni4WnEVNL1I1sHXAW7Qe8Exbx6MW852pCuRUPzncdh4
zFf7J0+vfGXcWFmGL6iF0ZlfLyAdXZv09LX/nfcvaVN3wzxF+pZWB5bC3gfpHLYo
anFENlqs6g3PTW2l/D1V2tcpTWMQ0g2WobL+Ft/wAUwKEITbOQpXCgfpE5rVTQ2Z
mhhR3Ufrk4BUzbZiGHa8u2ZE7AKkaQ==
=lr0j
-----END PGP SIGNATURE-----
```

mirrors.txt

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

I am the admin of Abysse Market.
I am in control of my PGP key.
I will update this canary within 14 days.
Today is 2021-03-02

Latest bitcoin block hash:
0000000000000000009fffd9446949c24103acd0e2af860f249fffad8118ba1
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEEu4Tv/fB8sz8twTE6HJKFvQrtoWoFAmAsV68ACgkQHJKFvQrt
oWri5hAAmJaYA9qdzq0zQHY+5RviUJohbH71hAUAm7TId10nOrbZF+le9ixIOkxm
GjNDBNuAle3woCLJ8cm0q9E4CksxNAJfJWjZXBLiUGqjyJDPzq7bHxaf7+PVnl4J
V4YHNySrGUvMiYeET05cEL/WNh75k33Y6bsBRO1HLo0YPDBDgkdI+ZIDNKTV6uSE
toxBbTS+mDVFCnTsKU6trq+bwW1uU5mH4ncqVtF/Rv9YoQU3fsD//IYjvUsDHc5u
8irf0IYFCCeMJHi/rJNzLZJHyCCxpq5focMfyZ/IWPZbsPX1PLwUATuDlNthH38G
aJuWt8p0UuYUmJcnU6UzmaczFGgRs+vIEbi+BUw0EvuceqUdB+rYZankZON5t9P6
Axi01zAdqYG3fHUvlyws9dDTunFlcKrSRljEy5bzOuTqLgUvlzibPzujGC8x9fd5
V7VjrfdWU58TkCPIkmd8DgkbUxGSCwnt6po7dIW0UGD4UV1/1jwDc+hqvJJvJEBc
AXMrvFfDG/Uxaj4VHcZ8fIOxWG0mbKHSdFmEYcbCSQ0ZOiPNL2fN6ccFicG0+Rmn
y1aAJ/0l268oBh3TGFPoCm6VdkXDIw9pubzGUNvzr9fsHYGk/8SlK/Sx/zk5qDvh
wvXfCubifqMoy8d3IkMkZm0bHfTseGZWOs29FzMyhbVUs9g7gfU=
=jDvd
-----END PGP SIGNATURE-----
```

canary.txt

Who has to use it?

- Admins of onion services have to implement these guidelines to show a commitment to user safety by proving ownership of all URL's associated with their site and by committing to regularly prove control of their PGP key.
- Admins that do not implement this guideline will be marked as "unverified" on dark.fail and listed below all other sites.

- In practice, several implementations have been observed:
  - Compliant domains that share all three files correctly
  - Partially compliant domains that share one or two of the envisioned files, for example by only uploading pgp.txt

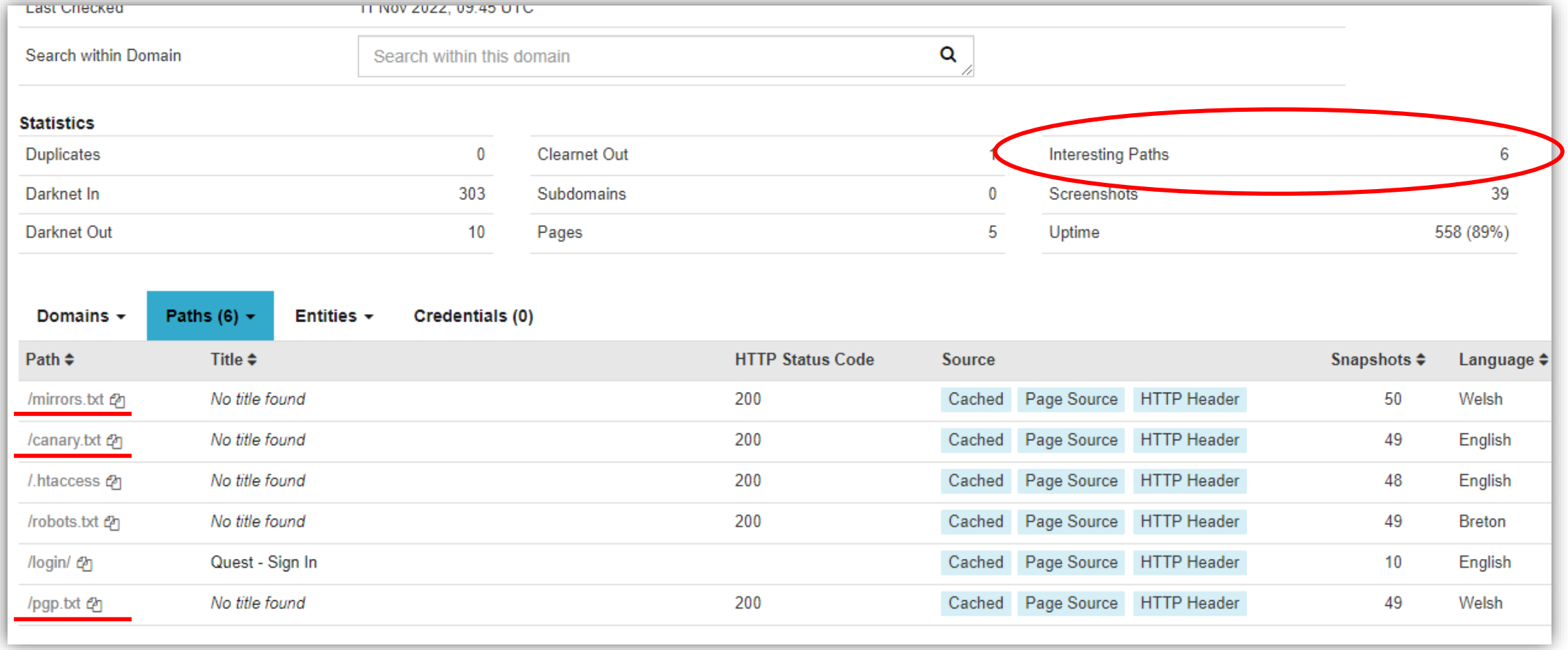
Trend of OMG adoption

DARK WEB MONITOR
Strategic Insights, Operational Perspectives

- Dataset used from Dark Web Monitor (DWM): https://cflw.com/dwm
- DWM is an Open-Source Intelligence (OSINT) repository that provides insights into criminal and fraudulent activities facilitated by dark web and virtual assets.
- DWM aims to monitor all active onion services in the Tor Network. ~100k active domains were included in the monitor when this study was conducted.

- For each dark web domain, the monitor checks whether the OMG files are uploaded. See the next slide for how those files can be found in the DWM.
- For each file is checked whether it is a valid format, see Annex I for details about the issue with invalid formats.
- On 4 October 2022, a total number of 1946 domains with valid OMG files have been identified.
- For an active domain, DWM downloads the OMG files at least every 6 six weeks.

The function ‘interesting paths’ show OMG files in DWM



Last Checked 11 Nov 2022, 09:45 UTC

Search within Domain — Search within this domain

Statistics

Duplicates	0	Clearnet Out	1	Interesting Paths	6
Darknet In	303	Subdomains	0	Screenshots	39
Darknet Out	10	Pages	5	Uptime	558 (89%)

Domains ▾ | Paths (6) ▾ | Entities ▾ | Credentials (0)

Path	Title	HTTP Status Code	Source	Snapshots	Language
/mirrors.txt	*No title found*	200	Cached Page Source HTTP Header	50	Welsh
/canary.txt	*No title found*	200	Cached Page Source HTTP Header	49	English
/.htaccess	*No title found*	200	Cached Page Source HTTP Header	48	English
/robots.txt	*No title found*	200	Cached Page Source HTTP Header	49	Breton
/login/	Quest - Sign In		Cached Page Source HTTP Header	10	English
/pgp.txt	*No title found*	200	Cached Page Source HTTP Header	49	Welsh

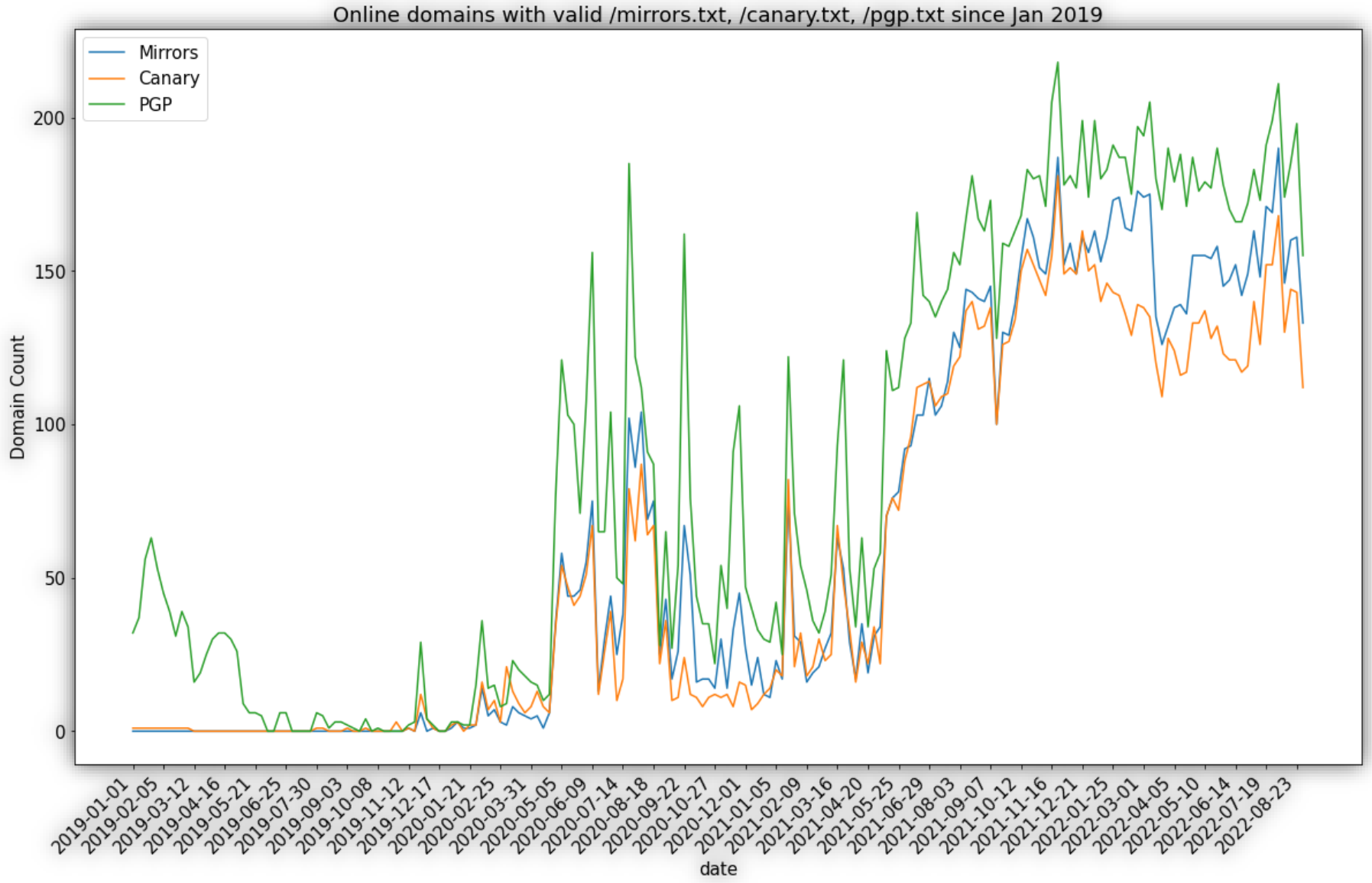
OMG files discover in domain: http://questxwvkwvsw2qgeeljz4fbv6cq2kbmapo7tw5heu4nng2ufgykapid.onion

Adoption of OMG

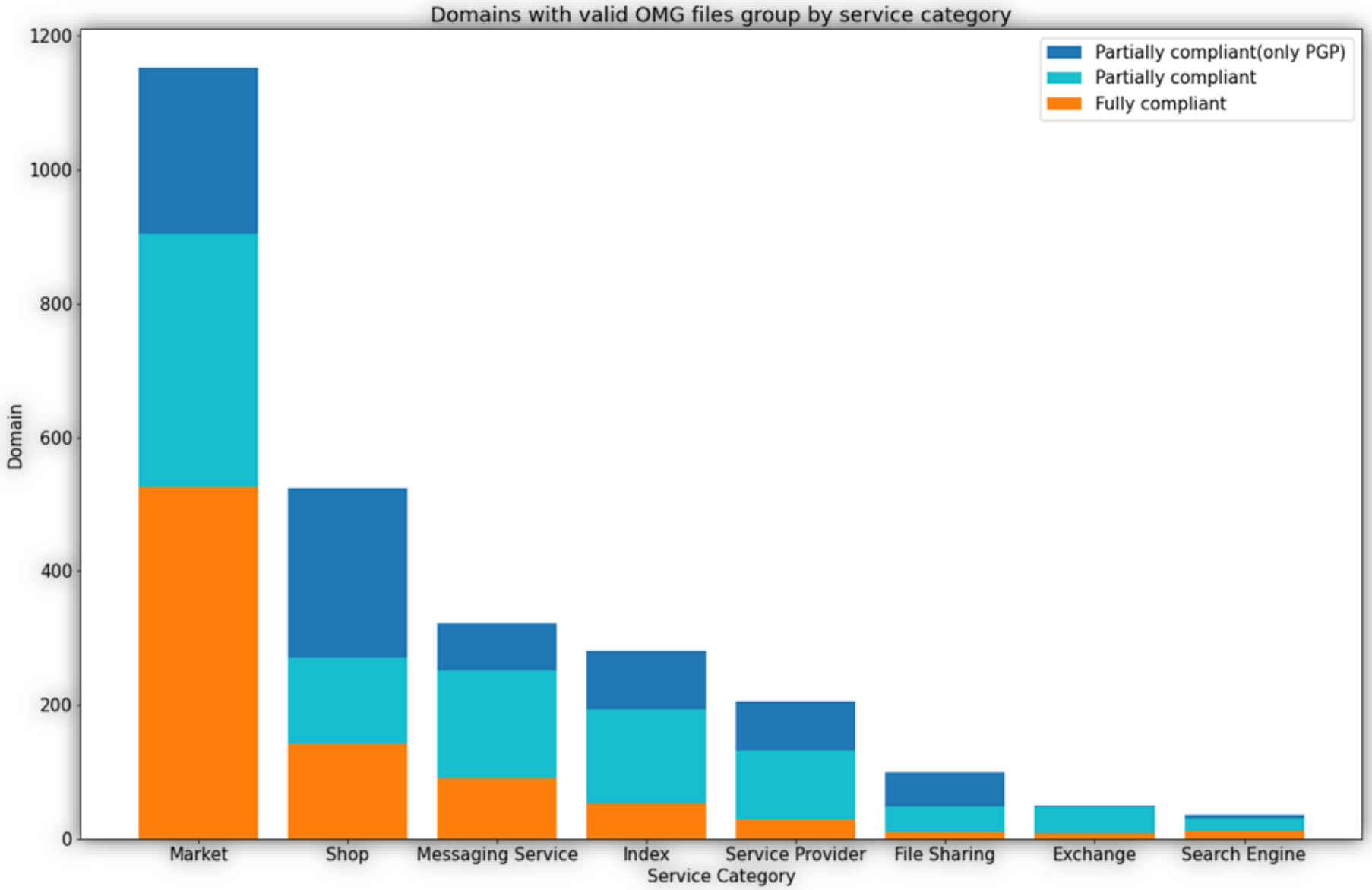
The OMG adoption within the 1946 domains developed as follows since Jan 2019.

The manifestations of OMG files is mapped to week level.

Interpolation methodology is explained in Annex II.



Service category distribution



Market – 43.22%
Shop – 19.64%
Others – 37.14%

Total domains adopted OMG
= 1946 domains

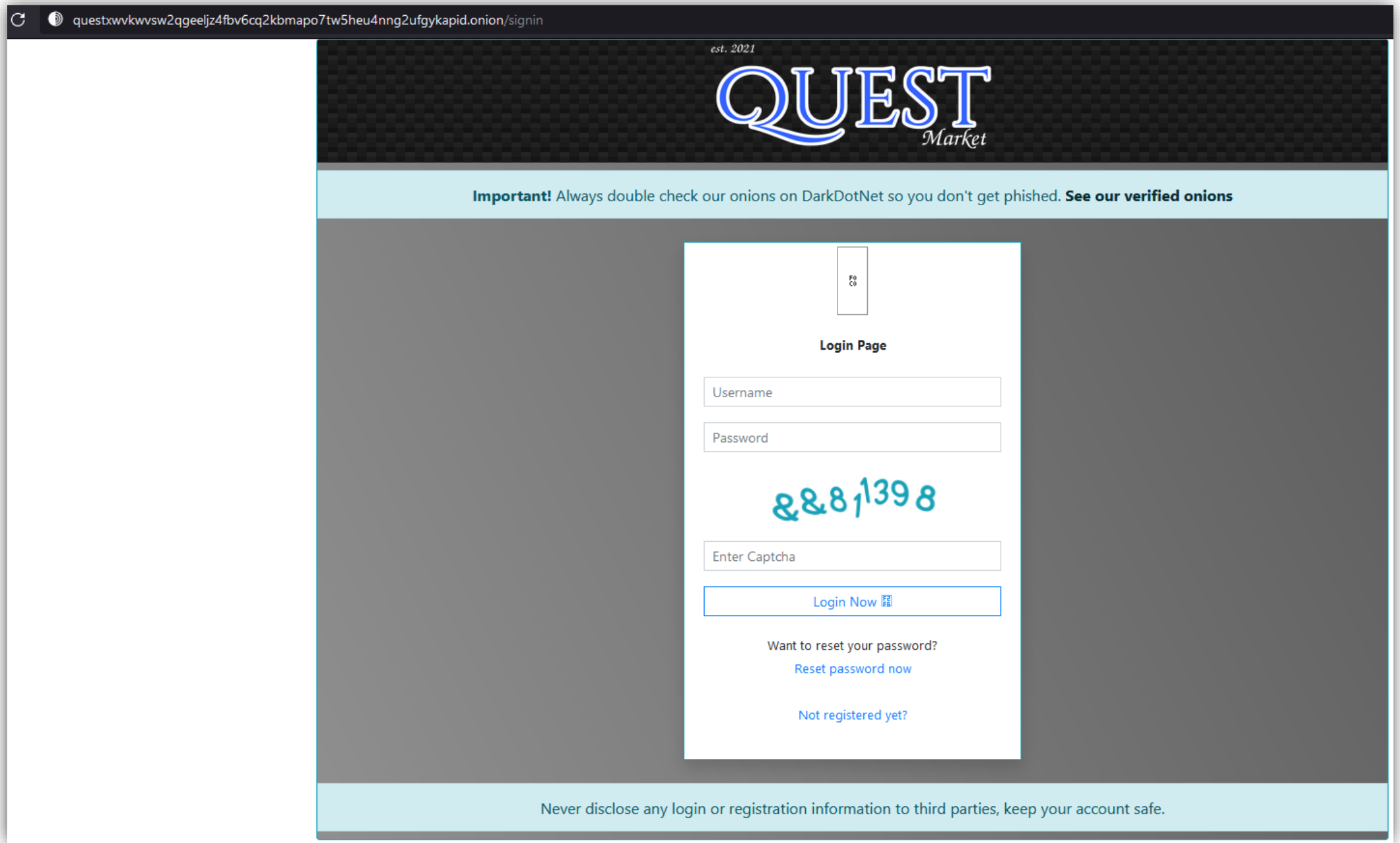
Fully compliant : Have all three OMG files
= 724 domains

Partially compliant: Have one or two OMG files
= 1222 domains

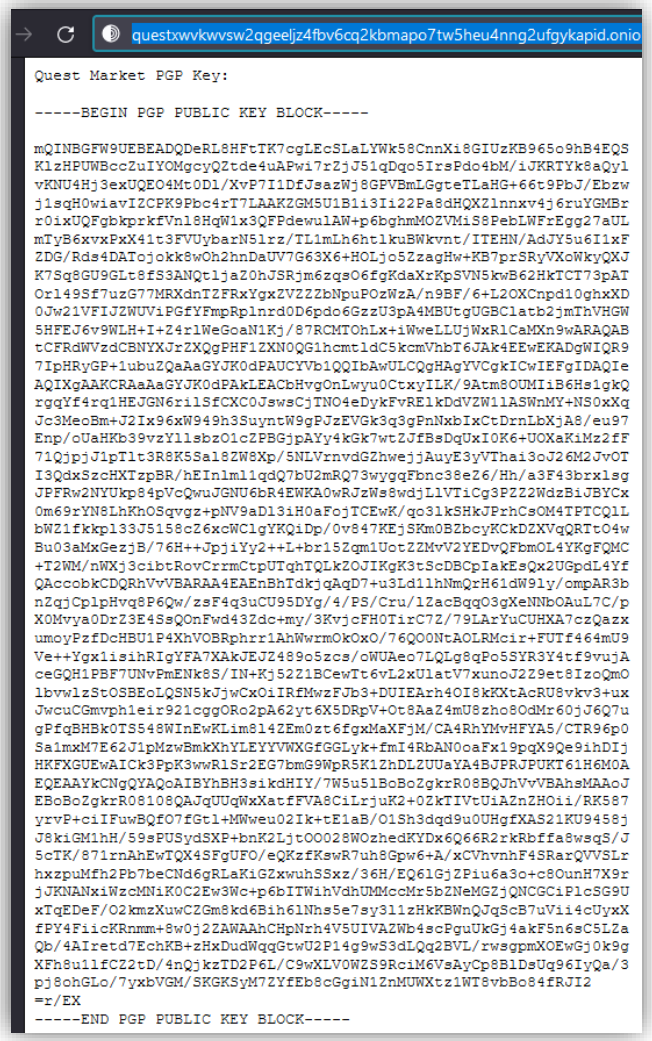
Analysis of the OMG standard use in practice

- Apart from the general statistics, it is relevant to check whether marketplaces and other service providers have (correctly) implemented the standard.
- Have well known marketplaces implemented OMG correctly?

Case 1: Quest Market



Examining Quest Market shows that they have fully implemented the standard. Quest also refers to DarkDotNet.com on their landing page for a list of their verified onions. This list corresponds with the mirrors.txt file (see next slide for the comparison). However, the canary.txt has not been updated since May 2022.



Pgp.txt

Mirrors.txt

Canary.txt

Quest Market Onions

Open one of these Quest onions in your Tor Browser:

- questxwvkwvsw2qgeeljz4fbv6cq2kbmapo7tw5heu4nng2ufgykapid.onion
- questx5olhiv35lrydy5glk6x64zcxlrepgqic7jlzi3uqyurqtltfad.onion
- questx4pxdwytknsodzsraxwajkseonfbu2lc74pnmy74tok3lnuhmad.onion
- questx4pxdwytknsodzsraxwajkseonfbu2lc74pnmy74tok3lnuhmad.onion
- questxpskfwwxcjlroiqye4y6m2ce4tcuu6r7wd5zt3wychqszukj2qd.onion
- questx7deerotyvnoejn7omvsx26m6nvxsxeb642dqps2zxw5peqc6qd.onion
- questxi4tp34jbd7vowuk6njqc7bi6xlqqziwz7rwbtj4ckj23j4jmqd.onion
- questxrbeu2f2m6sqobh35xfsyc5pfvesdfngwdc3q2x2zhntbjt6aqd.onion
- questxnwyufqbzufn2h2hezifkty3feipyjbj73e77r3abq2bvy4ikqd.onion
- questx24eprwsvoilphdrdpihcfsxza5aeje3x4mlifugc2zclx2zmid.onion
- questxkqz7yhkdvwe7e4k6i4t7vo6i22ccvtuyf7b5zyobau4faqbxad.onion

Public PGP Key

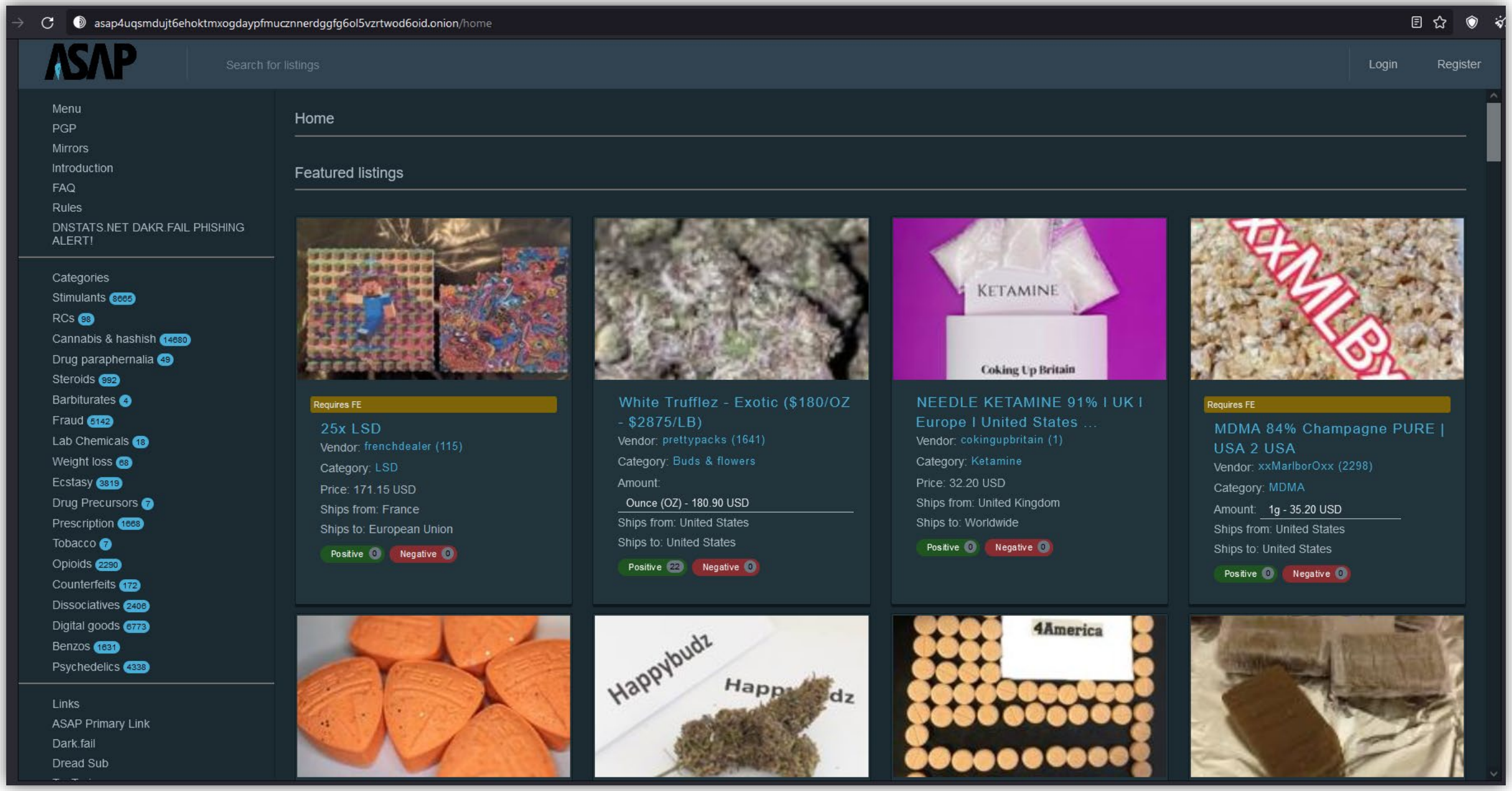
```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGFW9UEBEADQDeRL8HFtTK7cgLEcSLaLYWk58CnnXi8GIUzKB965o9hB4EQS
```

questxwvkwvsw2qgeeljz4fbv6cq2kbmapo7tw5heu4nng2ufgykapid.onion/mirrors.txt

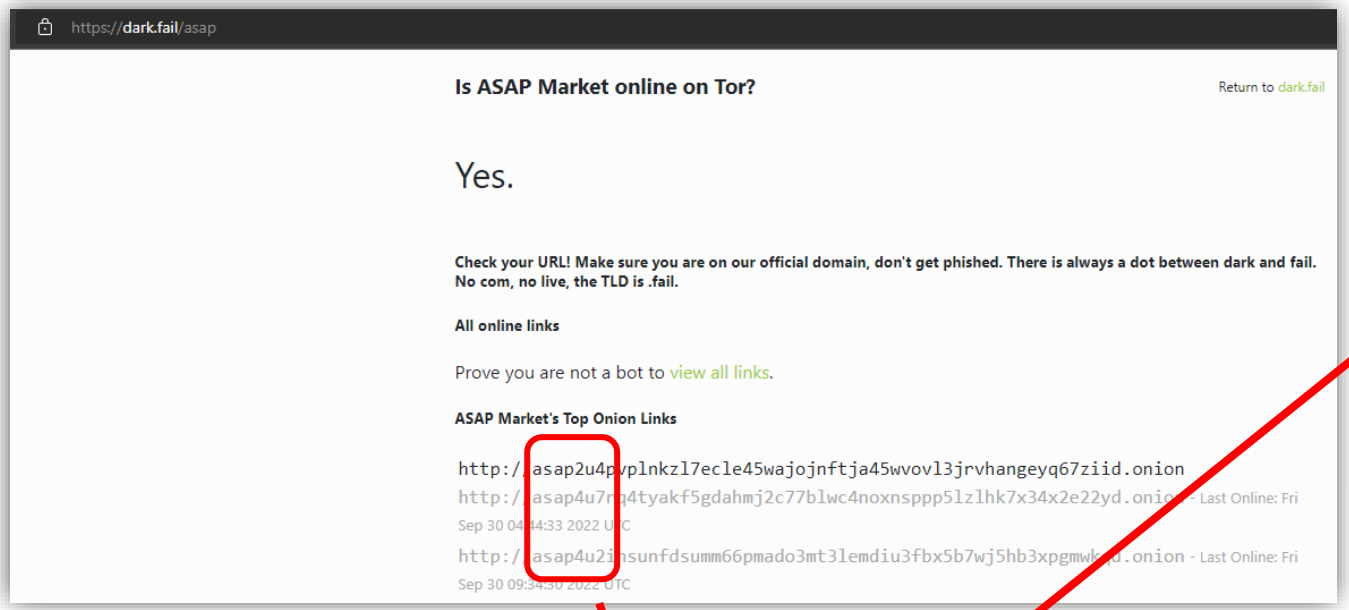
```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

questxwvkwvsw2qgeeljz4fbv6cq2kbmapo7tw5heu4nng2ufgykapid.onion
questx5olhiv35lrydy5glk6x64zcxlrepgqic7jlzi3uqyurqtltfad.onion
questx4pxdwytknsodzsraxwajkseonfbu2lc74pnmy74tok3lnuhmad.onion
questxpskfwwxcjlroiqye4y6m2ce4tcuu6r7wd5zt3wychqszukj2qd.onion
questx7deerotyvnoejn7omvsx26m6nvxsxeb642dqps2zxw5peqc6qd.onion
questxi4tp34jbd7vowuk6njqc7bi6xlqqziwz7rwbtj4ckj23j4jmqd.onion
questxrbeu2f2m6sqobh35xfsyc5pfvesdfngwdc3q2x2zhntbjt6aqd.onion
questxnwyufqbzufn2h2hezifkty3feipyjbj73e77r3abq2bvy4ikqd.onion
questx24eprwsvoilphdrdpihcfsxza5aeje3x4mlifugc2zclx2zmid.onion
questxkqz7yhkdvwe7e4k6i4t7vo6i22ccvtuyf7b5zyobau4faqbxad.onion
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEfeyKR0chj/tbm7mUGgGhmCStHTwFAmFa2yQACgkQGgGhmCSt
HTylgw//XM4YYMexZyw1kNlmaX5oYmx96FLjoDLk262+jTSsULZZfGU7sgkOKRtn
f/LE/Pzql4gHpv4Rr1x98NdlDyb2WQZ6ghxHS8YCIAjPj7F8em/lMmnwnCJeNIIf
fmwH+lyM0PLYn1r1RWXW6hSzz0cVxOxO6JlbqDV4WdFmK+R6nfOrKrps0mQIHLGq
vnAEab4NCf06P932GHfNygXLCvXXmEzD/k4sQZ6ZN6HNO4xl79YCpSZPxYfa7DLM
lPB1y1J/bi3x9Aki87Z2eSpF/+f5xvkBtxZsfBmpbAj9Hqbps3u32TSYYDdyugEU
1Dzy+oumQFX7zIciwMJRdjKdUxSZaq77uBgO56O+qBtxNNkaWmesCQOjebNELjGE
5nNVcbnojj85Y3AWaVMS5sCfUMVqFa6YribwDexmBq1vlEkIN0h1MwXnrhQDlEBx
zar4X1LudAo+ndCJVOTPxuotw96G2/u27vBeBXKK406iDm5+GXUq3rF4YEiEOCXb
+D/Pnlzdz9992D1xsaNPWi/sVZMf2WplMYA7gMg+pE3nQwdh0SpNdbOfQfUSJdVR
rlOYvZlzOR+FV6sI+EeCVi6SxPQwVdqPCnVAwx2iP5x1gB74jbJo+yUx6pIJfaVz
Fbh6Uz+Q0e7p8O8ThXwhuWmftqSlHYXFKxurlsOnueRX9fk/ZfQ=
=+EOO
-----END PGP SIGNATURE-----
```

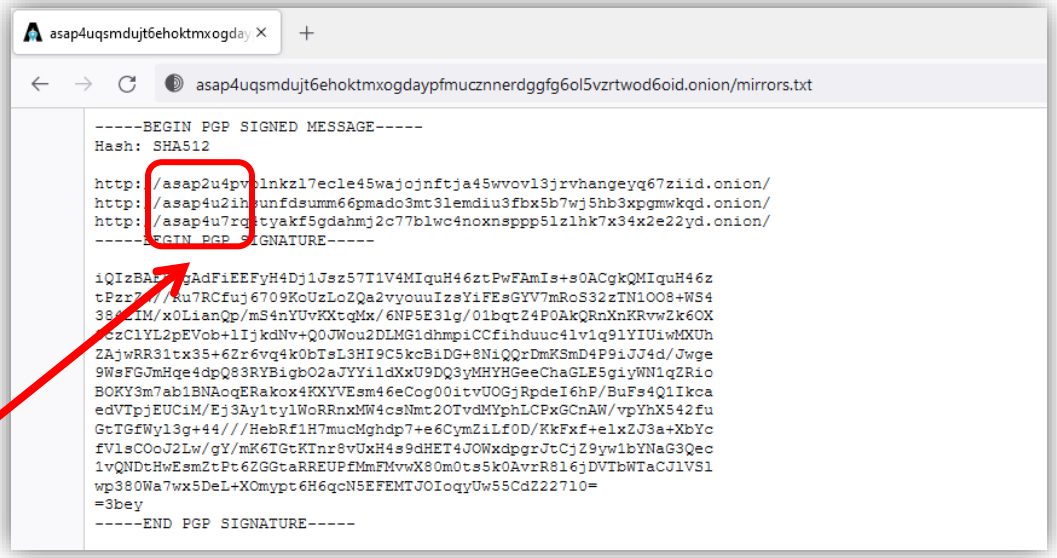
Quest market refers to DarkDotNet.com for a list of their verified .onions, along with their PGP key, to ensure users they can safely use the site. This is an extra trust measure in addition to the implementation of the OMG standard. Perhaps it is also a more directly visible one, since it is shown on their landing page.

Case 2: ASAP market

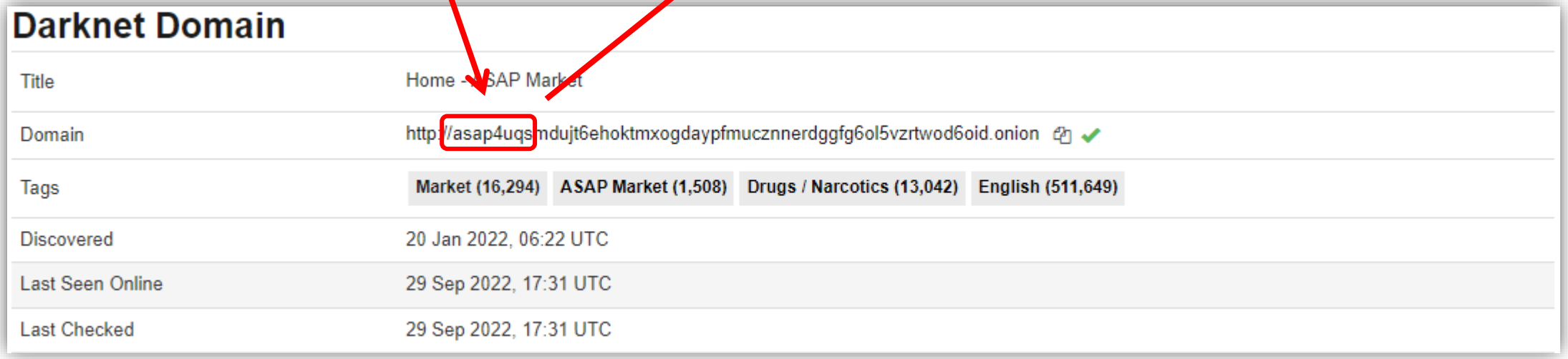


1. Dark.fail shows the .onions for ASAP market





3. The .onion adress does not match any of the adresses in the mirror.txt file. Conclusion: according to the standard, this may be a phishing website! The other possibility is that the market admins did not update their mirror.txt file.

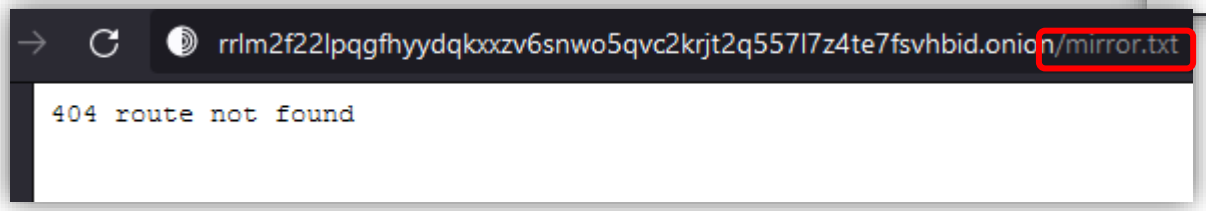


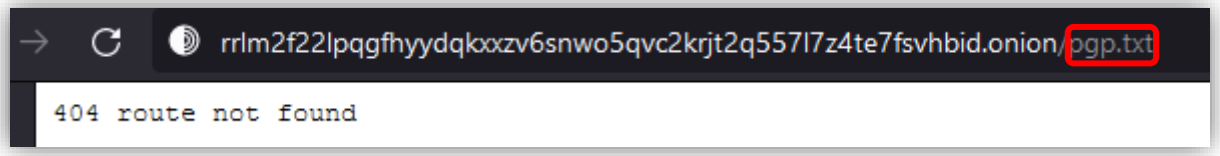
2. However: a different .onion is found in the Dark Web Monitor, this one is not listed on Dark.fail.

Case 3: TOR market

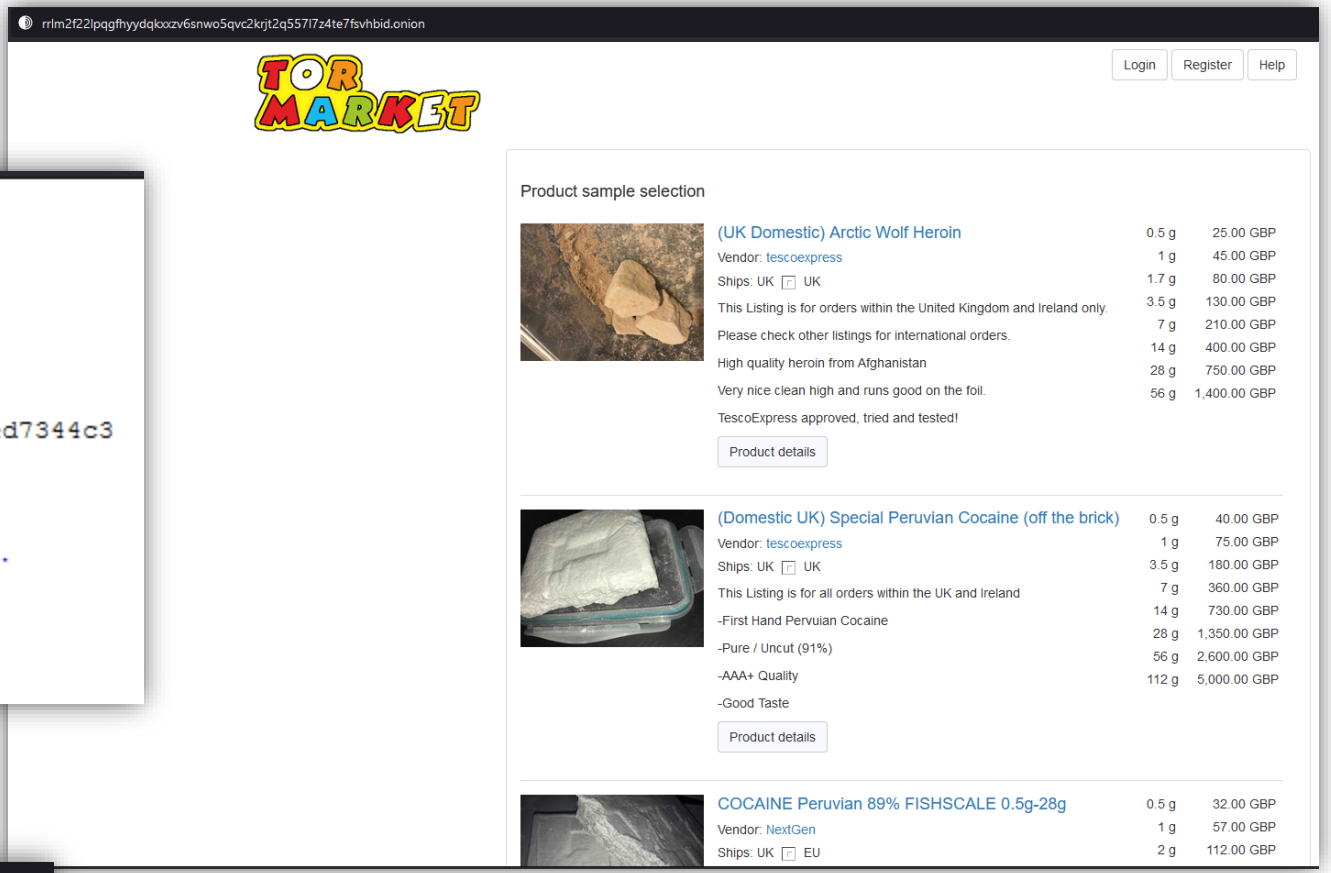
```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

This is the Tormarket canary message generated 2022-09-20 00:00 UTC.
It will be replaced every two weeks.

Bitcoin block number: 754859
block hash: 00000000000000000066cbc50347de6520f2268e35a28b3718fc20bed7344c3

If this file remains unchanged after 2022-10-05 00:00 UTC then
those in control of the infrastructure may be incapacitated
and/or the public systems may have been taken over / seized.

The key used to sign this message is kept isolated from the
public market systems so even if they are compromized, the
key will not be accessible.
```

1. The canary.txt is implemented





2. However, there are no mirror.txt or pgp.txt file. Conclusion: the implementation of the standard is incomplete on this market



Implications for Law Enforcement

- OPSEC measures are important to monitor, because markets and service providers have a lot to lose and therefore have an interest in properly implementing OPSEC measures.
- In addition to security, this guideline demonstrates to end-users the intention to be a reliable and trustworthy market or service provider.
- We argue that the level of OPSEC indicates how significant the market or service provider is on the Dark Web, as these domains have more exposure and assets to protect.
- Adoption of OMG has grown significantly since January 2019 but has not (yet) been fully adopted and implemented. At least it shows that many markets and service providers are experimenting and finding better ways to secure their assets.
- It is not only market places that adopt OMG, more than 50% of domains who implemented the standard are not market places.
- The exploration of OMG practices shows that many complications are being discovered and that it is either not easy to correctly implement the standard correctly and keep it up-to-date, or that is does not have the highest priority for site admins.

Future Research and Development

- Get a better understanding of the full landscape of OPSEC measures used in the Dark Web.
- Develop technologies to automatically identify implemented OPSEC measures, this could be used as an indicator for determining the significance of a market or service provider.
- Develop Dark Web typologies which can be used as input for proper impact and risk assessment of specific dark web activities, for example to quantify the difference between a major marketplace and a “Hello world” domain that was just launched.
- Conduct size and nature analysis on the full Dark Web space using these technologies and typologies. This provides law enforcement with data-driven guidance to select the most impactful interventions.

Colophon

For any question about this Case Study

OPSEC Measures by Dark Web Markets and Service Providers – OMG, cybercriminals have their security guidelines too!

For example, on how we retrieved the data, or how we obtained the analytical insights from Dark Web Monitor.

Feel free to contact

support@cflw.com

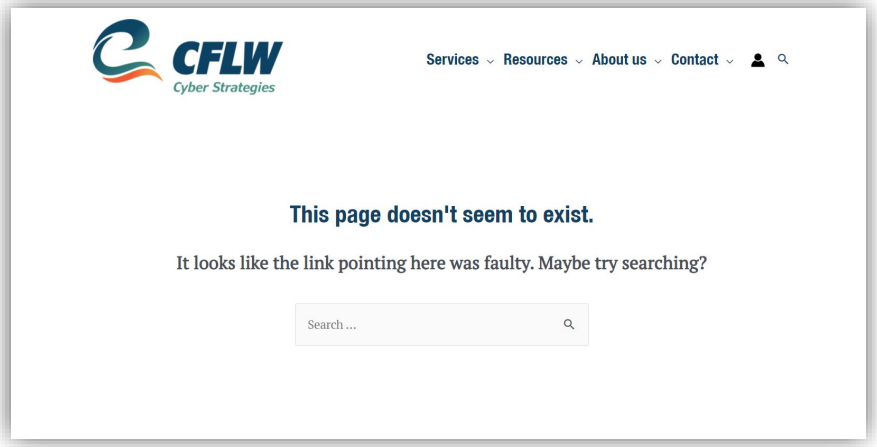
DARK WEB MONITOR

Strategic Insights, Operational Perspectives

Annexes

Annex I. Cause invalid OMG formats

- Dark Web Monitor checks whether the OMG files are uploaded.
- Many servers are configured to give a default response (404) including an HTML page if a request is made to a file that does not exist.
- Those default responses cause OMG files with invalid format.
- The invalid formats are obtained comparable to making a request to the none existing page /abc: https://cflw.com/abc



Default response by CFLW.com on none existent page

Annex II. Interpolation of OMG file manifestations

Interpolation technique was required since Dark Web Monitor crawls a Dark Web domain at least every 6 weeks.

In the case a domain is online in a particular week and it was also found online within 6 weeks later, it is assumed that it was online in the weeks in between. By interpolation, it gives a more accurate result for the adoption overview.