

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 Europol's IOCTA² and the National Risk Assessment for the Netherlands³.
- 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](https://dark.fail), a site which is used to check whether dark web domains are online, proposed the Onion Mirror Guidelines (OMG) in 2019⁴.

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

[illegible]

pgp.txt

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA512

http://w6a47tienfk6vycx.onion/
http://rxrxuvb6jufh3emqi7tf4hxff2ka6ajfgbgqh5lztgx4mkcldnk6q7ad.onion/
http://srrc4q4pia3nqx34wjczerdgqjmlbftetgzl57rdbbh6cygcmrpaayoyd.onion/
-----BEGIN PGP SIGNATURE-----

iQEzBAEBcGAdFiEEaDt5FCneiixE0M6VJJ3yXl3sjwFAl8ahO4ACgkQVJJ3yXl3sjwBEQf+JnwoprCpu5jnSv4H4EjEHYNdcBd1LV8D+M5VDj1dx5xNucSeXj7uIKCnfnZmZozMRvt+G1lFuaz5UVMfPLS9X008gFszy+zuq1Ik9z5UmKhgEs7rrkWnnqjvIIBUPwZVb8QWRaYyAkF9Ni4WnEVNLI1sHXAW7Qe8Exb6MMW852pCuRUPzncdh4zFf7J0+vfGXcWfMGL6iF0ZlflYAdXZv09LX/nfcvaVN3wzxF+pZWB5bC3gfPHLYoanFENlqs6g3PTW2l/D1V2tcpTWMQ0g2WobL+ft/wAUwKEITbOQpXCgfpE5rVTQZ2mhhR3Ufrk4BUzbZiGHa8u2ZE7AKkaQ==

=lr0j

-----END PGP SIGNATURE-----

mirrors.txt

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

```
I am the admin of Abyss 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:

```
00000000000000000000009fffd9446949c24103acd0e2af860f249fffad8118ba1
```

-----BEGIN PGP SIGNATURE-----

iQIZBAEBCAAdFiEEU4Tv/fB8sz8twTE6HJKFvQrtoWoFamAsV68ACgkQHJKFvQrt
oWri5hAAmJaYA9qdzq0zQHY+5RviUJohbH71hAUAm7TId10nOrbZF+le9ixIOkxm
GjNDBNuA1e3woCLJ8cm0q9E4CksxNAJfJWjZXBliUGqjyJDPzq7bHxaf7+PVn14J
V4YHNySrGUvMiYeET05cEL/WNh75k33Y6bsBR01HL00YPDBDgkdI+ZIDNKTv6uSE
toxBbTS+mDVFCnTSKU6trq+bwW1uU5mH4ncqVtF/Rv9YoQU3fsD//IYjvUsDHc5u
8irf0IYFCCeMJHi+rJNzLZJHyCCxpq5focMfyZ/IWPZbsPX1PLwUATuD1NthH38G
aJuWt8p0UuYUmJcnU6UzmaczFGGrS+vIEbi+BUw0EvuceqUDb+rYZankZON5t9P6
Axi01zAdqYG3fHUvlyws9dDtunFlcKrSRljEy5bz0uTqLgUv1zibPzujGC8x9fd5
V7VjrfdWU58TkCPIkmd8DgkbUxGSCwnt6po7dIW0UGD4UV1/1jwDc+hqvJJvJEBc
AXMrvFfDG/Uxaj4VhcZ8fIOxWG0mbKHSDfMEYcbCSQ0Z0iPNL2fN6ccFicG0+Rmn
y1aAJ/01268oBh3TGFPoCm6VdkXDIw9pubzGUNvzr9fsHYGk/8S1K/Sx/zk5qDvh
wvXfCubifqMoy8d3IkMkZm0bHfTseGZW0s29FzMyhbVUs9g7gfU=
=iDvd

-----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	Cleartnet 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 ↕
<u>/mirrors.txt</u> 📄	No title found	200	Cached Page Source HTTP Header	50	Welsh
<u>/canary.txt</u> 📄	No title found	200	Cached Page Source HTTP Header	49	English
<u>/.htaccess</u> 📄	No title found	200	Cached Page Source HTTP Header	48	English
<u>/robots.txt</u> 📄	No title found	200	Cached Page Source HTTP Header	49	Breton
<u>/login/</u> 📄	Quest - Sign In		Cached Page Source HTTP Header	10	English
<u>/pgp.txt</u> 📄	No title found	200	Cached Page Source HTTP Header	49	Welsh

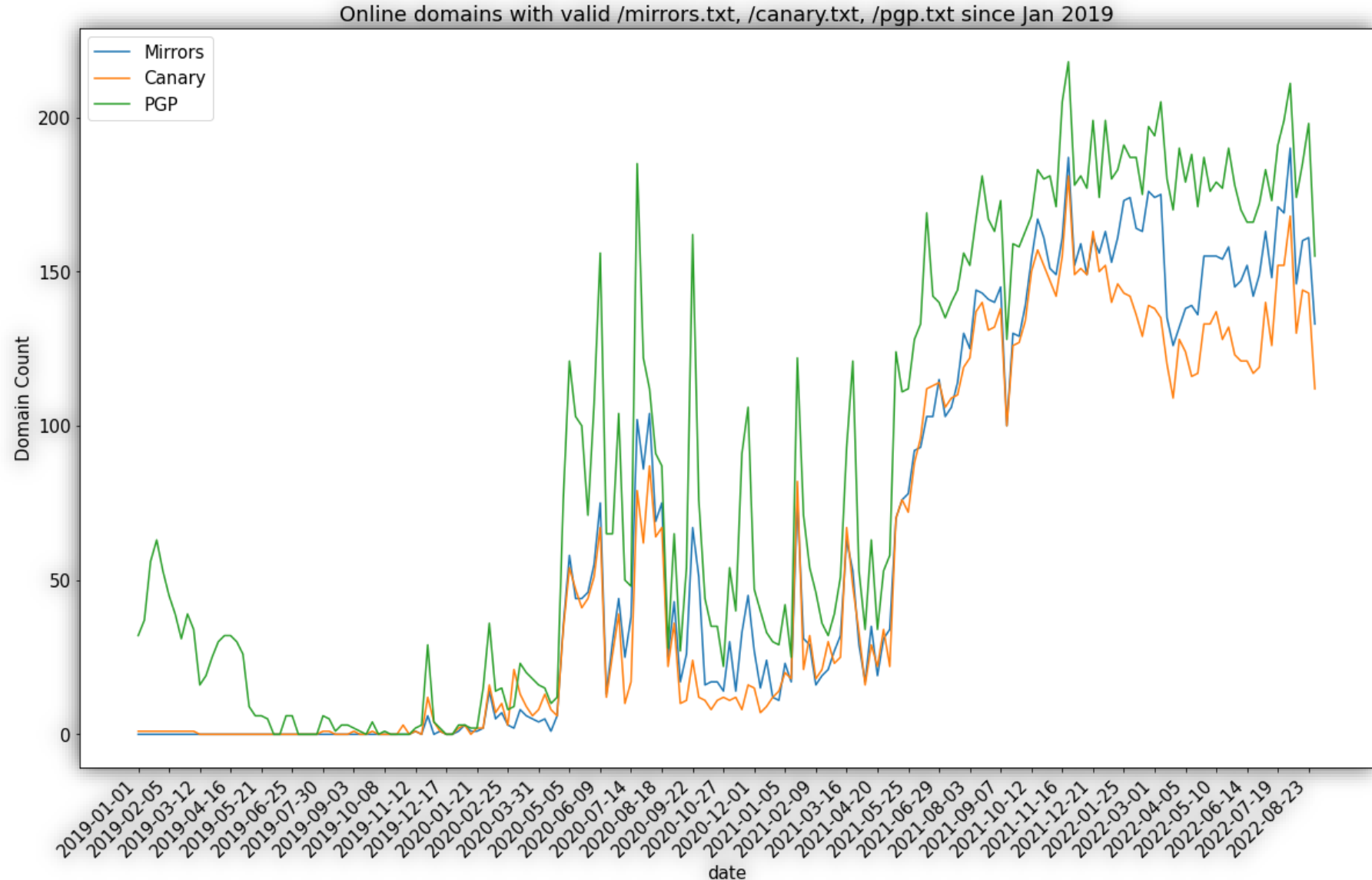
OMG files discover in domain: <http://questxwvkwvsw2qgeeljz4fbv6cq2kbmapo7tw5heu4nng2ufgykapid.onion>

Adoption of OMG

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

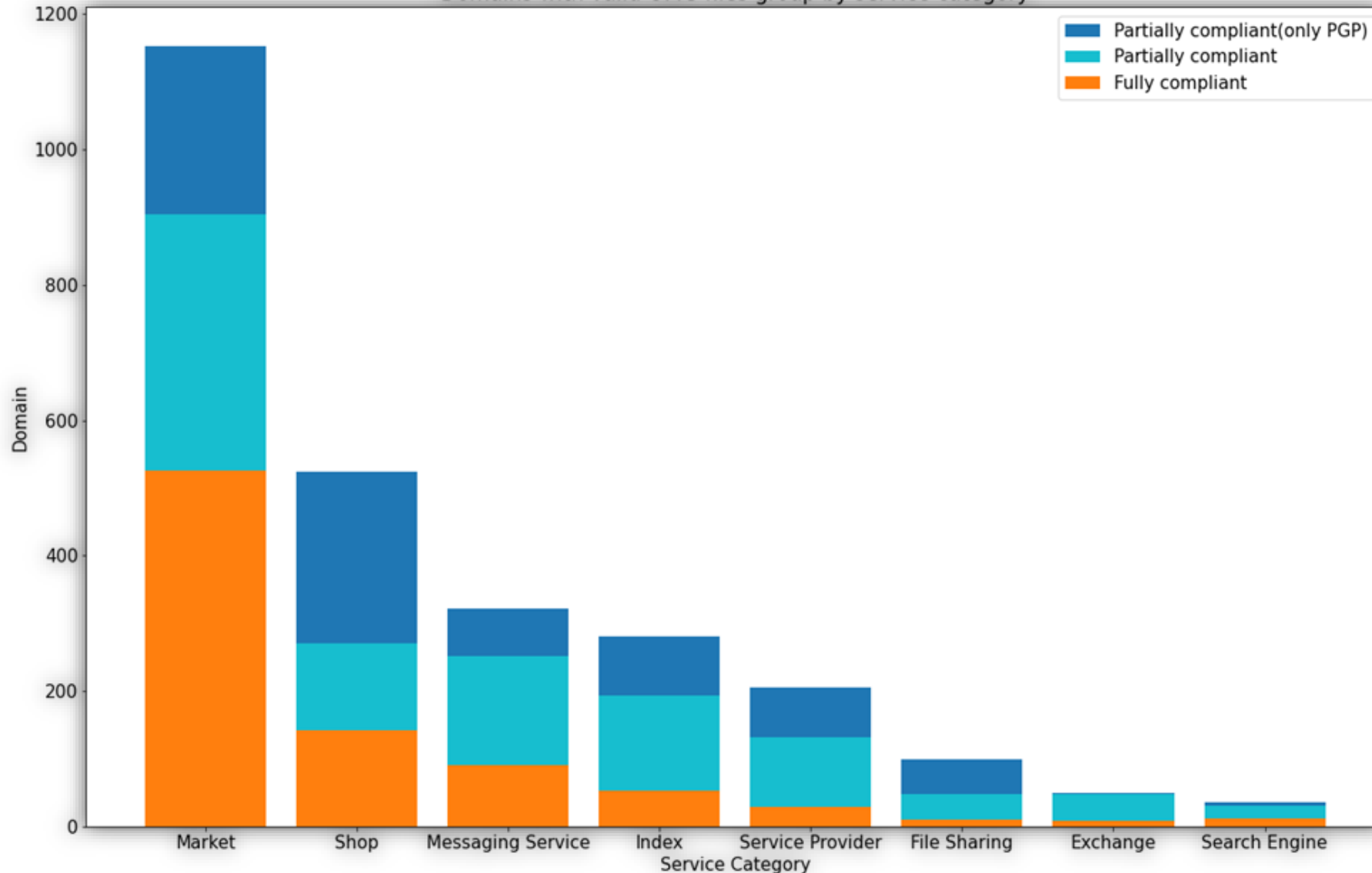
The manifestations of OMG files is mapped to week level.

Interpolation methodology is explained in [Annex II](#).



Service category distribution

Domains with valid OMG files group by service category



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

questxwkwsw2qgeeljz4fbv6cq2kmapo7tw5heu4nng2ufgykapid.onion/signin

est. 2021

QUEST

Market

Important! Always double check our onions on DarkDotNet so you don't get phished. **See our verified onions**

FO
CO

Login Page



Want to reset your password?
[Reset password now](#)

[Not registered yet?](#)

Never disclose any login or registration information to third parties, keep your account safe.

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.

```
questxwkvsw2qgeeljz4fbv6cq2kbmapo7tw5heu4nng2ufgykapid.onio

Quest Market PGP Key:

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

mQINBGFW9UEBEADQDeRL8HFtTK7cgLEcSLaLYWk58CnnXi8GIUzK9B65o9hB4EQS
K1zHPUWbCcZuIYOMgcyQZcde4uAPw17zJj51qDqo5Irsdco4bM/iJKRTYk8aQy1
vKNU4Hj3eXUQEO4MxODL/xvP7I1DDJasWj8GPFvBmLGteTLaHG+66t9PbJ/Ebwz
j1agH0wIavIZCPK9Pbc4rT7LAARKZGM5U1B1i3I22Pa8dHQXZlnnxv4j6ruYGMBr
r01xUQFgkprkFvN18HqW1x3QFFedew1AW+6p6ghmM0ZVM1S8FebLWFrEgg7aUL
mTyB6xvxPkX41t3FVUYbarN5lrz/TL1mLn6ht1kuBwkvntc/ITEHN/AdJY5u6I1xk
ZDG/Rds4DAtojokk8wOh2hndAU7G63X6+H0Ljo5Z2agHw+KB7prSRyVXoWkyQXJ
K7Sg8G9GLt8fSSANQt1ja2ZhJSRjm6zqs06fgKdaXrKpSVNSkwB62HKTCT73pAT
Or149Sf7uzG77MRXdntZFRxVgxZVZ2ZbNpuPOzWzA/n9BF/6+L2OXCNpd10ghxXD
0Jw21VFIJZUWV1PGfYFmpRplnr0D6pdc6GzzU3pA4MBUtqUG8Bc1atb2jmThVHGw
5HFEJ6v9SWLH+I+24r1WeGoan1Kj/87RCMTOhLx+iWwELUjWxR1CaMKn9wARAQAB
tCFRdWVzdCBNYXJzZXQgPHF1I2XNOQGihcmtdlC5kcmVnbT6JAK4EEwEKADgWIR9
71pHryGP+IubuzQaAagYJK0dPAUCYVb1QJIBAwULCQgHAgYVCgkICWIEFIDAQIe
AQIXgAARCRAAaAgYJK0dPAKLEACbHvgOnLwyu0CtXyILK/9Atm8OUMIiB6Hs1gKq
rgqYf4rq1HEJGN6r1lSXCXCOJswsCjTNO4eDykFvRElKdDvZW11ASWnMY+N50xXq
Jc3MeoBm+J2IX96xW949h3SuyntW9gPjZEVGk3q3gPnNxbIXCtDrnLbXjA8/eu97
Enp/0uAHKb39vzY11sb201c2PBjgPaY4YgK7wZfBsDgUxIOk6+UOXKaj1Z22F
71Qj3pJ1pTl1t3R8K5Sa18ZW9Xp/5NLVcnvdG2hwejjAuyE3yVTha13oJ26MzJvOT
I3QdxSzcHXTzpBR/hEInlm1lqdg7bU2mRQ73wygqfBnc38e26/Hh/a3F43brxlsg
JPFrW2NYUkp84pVcQwuJ3GUU6bR4EwKAOwJzW8sWdjL1V1tCg3FZ22WdzB1UBYCx
0m69rYN8LhKhO8qvgz+pNV9AD13iH0aFojTCeWw/qo3l1kSHKjPzhCsOM4TPTCQ1L
bW21fKkp133J5158c26xcWNC1qYKQ1Dp/0v847KEjSKm0B2bzyCKcdZKVqQRt04w
Bu03AmKGezjB/76H++JpjiYy2++L+Br152qm1Uot2ZMvV2YEDvQFbmOL4YKfQMC
+T2WM/nWXj3cibcRovCzrmCtpUTqhTQLkZOJIKgK3tScDBCPiAkEsQx2UGpdL4Yf
QAocobcCDQRhVvVBARAA4EAENBhTdkjqAgD7+u3Ld11hNmQrH61dW91y/ompAR3b
n2qJ3p1pHvq8P6Qw/zsF4q3uCU95DYq/4/PS/Czu/12acBggQ03gXeNnBoAuL7C/p
XOMvya0DrZ3E4SsQOnFwd43Zdc+my/3KvjcFH0T1rC7Z/79LarYuCUHXA7czQazx
umoyPzFdcHBU1F4XhVOBRphrr1AhWwrmOkX0x/76Q0NtAOLRMci+rFUTf64mU9
Ve++Ygx11sihRiGyYFA7XAKJEJZ489o5zcc/oWUAeo7LQLg8qPo5SYR3Y4tf9vuJa
c6GQH1PBF7UNvPmENk8S/IN+Kj52Z1BCewTt6vL2xU1atV7xunoJ229et8IzoQum
1bvw1zStc08BEOLQSN5kJjwCxo1RfEMwZfJb3+DUIEAarh4OI8kKXtAcR0U8vkv3+Xx
JwcuCGmvp1e1r921cggORo2Pa62yt6X5DRvV+0t8Aa24mU8Zho8OdR60jJ6Q7u
qPfQBHBk0TS548WInEWKLm814ZEm0t2c6fgXMaFjM/C4ARhYmVhFYA5/CTR96p0
SaImXk7E62J1pMzwBmkXhYLEYVWVGfGGLyk+fmI4RbANOoaFxi9pQX9e9ihdIJ
HKFXGUEwA1Ck3Pk3wR1S2rEG7bm9WpR5K1ZhdZ2UUA7A4BJFRFPUKT61H6M0A
EQEAAYkCNgQYAQoAIBYhBH3s1kdHIY/7W5u51BoBoZgkrR08BQJhVvVBABsMAAOJ
EBBoZgkrR08108QAjUgUwWxXatfFVA8C1LrjuK2+0ZKTIVtUiAZnZH0i1/RK587
yrvP+ciIFuwBQfO7fGt1+Mwweu02Ik+te1aB/O1Sh3dgd9u0UHgfXAS21KU9458j
J8kiGM1hH/59ePUSydxSP+bnK2Ljt0O028W0zhedKYDx6Q66R2zkrBff8a8wsg/J
5cTK/871rnAhEWtXQ4SfgUFO/eQKzfKawR7uh8Gpw6+2/xCVhvnHf4SRarQVVS1r
hxpupmfh2Pb7beCnd6grLaKiGZxwuhS5x3/36H/EQ61Gj2Piu6a3c+e80unH7X9r
jJKNANxiWzCMN1K0C2Ew3wc+p6bITiWhVdhUMMocmr5b2NeMGZjJQNCGCiP1cSG9U
xTgEDeF/02kmzXuwCZGm8kd6Bih61Nns5e7sy311zHkKBWnQJqS5B7uV14cUyxX
fPY4FiicKRnm+8w0j22ANAAhChpNrh4V5UIVAZ2Wb44cPguUkGj4akF5n6S6CZLa
Qb/4AIretd7EchKB+zHxDudWqGtWU2P14g9wS3dLQq2BVL/rwsgpmXOWEgJ0k9g
XFh8u1fC2Z2D/4nQjKzTD2P6L/C9wXLVOWZS9RciM6VsaYcP8B1DsUq96IyQa/3
pj8ohGLc/7yxvVGM/SGKGSyM7ZYfEb8cGgiN1znMUWxtz1WT8vbBo84fRJI2
=r/EX
-----END PGP PUBLIC KEY BLOCK-----
```

```
questxwkvsw2qgeeljz4fbv6cq2kbmapo7tw5heu4nng2ufgykapid.onion/mirrors.txt

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

questxwkvsw2qgeeljz4fbv6cq2kbmapo7tw5heu4nng2ufgykapid.onion
questx50lhiv35lrydy5glk6x64zcxlrepqqic7jlzi3uqyurqtltfad.onion
questx4pxdwytksnodzsraxwajkseonfbu2lc74pnmy74tok3lnuhmad.onion
questxpskfwwxcjlrroiyye4y6m2ce4tcuu6r7wd5zt3wychgszuj2qd.onion
questx7deerotyvnnoejn7omvxs26m6nvxsxeb642dqs2zxw5peqc6qd.onion
questxi4tp34jbd7vowuk6njqc7bi6xlqqziwz7rbwtj4ckj23j4jmqd.onion
questxrbeu2f26msqobh35xfsyc5pfvesdfngwdc3q2x2zhntbjt6aqd.onion
questxnywufqzbzfn2h2hezifkty3feipybjb73e77r3abq2bvvy4ikqd.onion
questx24eprwsvoilphdrdpihcfssza5aeje3x4mlifugc2zclx2zmid.onion
questxkqz7yhkdvw7e4k6i4t7vo6i22ccvtuyf7b5zyobau4faqbxad.onion

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEfeyKR0chj/tbm7mUGGhmcStHTwFamFa2yQACGkQGgGhmCSt
HTylgw//XM4YYMexZywlkNlmaX5oYmx96FLJoDLk262+jTSsULZZfGU7sgkOKRtn
f/LE/Pzql4ghPv4Rr1x98NdlDyb2WQ26ghxH8YCIAPj7F8em/lMmnwnCJeNIIf
fmwH+lyMOPLyn1rlRWXW6hSzz0cVxOx06JlbgDV4WdFmK+R6nfOrKrps0mQIHLGq
vnAEab4NCf06P32GHfNygXLCvXXmEzD/k4sQZ6ZN6HNO4x179YcPSZPxYfa7DLM
1PB1y1J/bi3x9Aki87Z2eSpF/+f5xvkBtxZsfBmpbAj9Hqbps3u32TSYDDdyugEU
1Dzy+oumQFX7zIciwNRdjKdUxSzaq77uBgO560+qBtxNNkaWmesCQ0jebNELjGE
5nNVcbnojj85Y3AWaVMS5ScFUMVqFa6YribwDexmBqlv1EkIN0h1MwXnrhQDLEBx
zar4X1LudAo+ndCJVOTPxuotw96G2/u27vBeBXXK406iDm5+GXUq3rF4YEiEOCXb
+d/PnlzdZ9992D1xsaNPwi/sVZMf2WpLMYA7gMg+pE3nQwdh0SpNdbOfQfUSJdVR
r1OYvZlzo+FW6s1+EaCVi6SxpQwVdqpCnVawX2iP5x1gB74bjb+yUx6pIjfaVz
Fbh6Uz+Q0e7p808ThXwhuWmftqSLHYXFKxurl5OnuerX9fk/ZfQ=
=EEO
-----END PGP SIGNATURE-----
```

Mirrors.txt

```
questxwkvsw2qgeeljz4fbv6cq2kbmapo7tw5heu4nng2ufgykapid.onion/canary.txt

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

Canary update May 1 2022.
All Quest servers are stable uncompromised and in control of Quest staff.
The latest bitcoin hash is:
00000000000000000019a4980c40123e49b8a6314f26d66ea6e2d748dbea9df
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEwYrlgd4+0aYqvVs9k08dWJ5QJIFAmJu0sQACGkQ9k08dWJ5
QJQKSHQ/+Ky7JFD0BzHBry5hxsJcSuQLFCaxTo1h1NptypKiRDFEZAfHqvsalqWJC
B+vwZLR2jW2cK7wMPVoI6Nmn4rFzEOseUK63DtQZDPgHzinw4b9xpmUDJEwUUNL7
8vLOESvh3nVufXpVn4pN25cZHCznLiVg4t4cKaK8/xDnQGeCVCynIwXrKwto3jy
NRdR6YAJo4kMTbVVgnBUWEy49SSm0aGolw7/P/bDiHnTODwgI+zQBzfHvMDS1pL
g2jytFJlqpLa8i308NwXSPGBJ/Wiylme7E501xGGxmsKdz+VpxVXwQ+zLftfn0Bu
eSe4xh4ues4m9NaW/hk3ETcRDyVDleuFfLO/h6IGPupcpnzCd6wnIiRMHjp8CeJE
tAabCkI8ztEJ4OqFbrtE3ear6UTkJLSehmLAtBdidboQKDdhFITVvyv20kNXsOI
KGxraOwQ6Hbh80vZoeJvgFmiNGouNNQ/w3uCNpJTQgRe/PrYg71zf1B0cRPYYx
pEhpSn9vNdOYC41Ib3zKTJUPh81lZGwO9aZjJnhD6DvIY7QB1uo9/OfhVfV+10wm
Kb6Zs36cRCR5LJCJY7ztKNLts+sIijKVKjholBBsBfviAl1Lw7RiMhL61ORvtlyEF
Bl2CB1p1m6pNNPxfJqp7hACufUJkIIfOjAiZy9k0aHnwpFK84Aw=
=+lYp
-----END PGP SIGNATURE-----
```

Canary.txt

est. 2021

QUEST

Market

Important! Always double check our onions on DarkDotNet so you don't get phished. **See our verified onions**

Quest Market Onions

Open one of these Quest onions in your Tor Browser:

- questxwkwsw2qgeeljz4fbv6cq2kmapo7tw5heu4nng2ufgykapid.onion
- questx5olhiv35lrydy5glk6x64zcxlrepgqic7jlzi3uqyurqtltfad.onion
- questx4pxdwytknsodzsrxawjkseonfbu2lc74pnmy74tok3lnuhmad.onion
- questx4pxdwytknsodzsrxawjkseonfbu2lc74pnmy74tok3lnuhmad.onion
- questxpskfwwxcjlroi qye4y6m2ce4tcuu6r7wd5zt3wychqszykj2qd.onion
- questx7deerotyvnnoejn7omvxs26m6nvxsxeb642dqs2zxw5peqc6qd.onion
- questxi4tp34jbd7vowuk6njqc7bi6xlqqziwz7rwbjtj4ckj23j4jmqd.onion
- questxrbeu2f2m6sqobh35xfsy5pfvesdfngwdc3q2x2zhntbjt6aqd.onion
- questxnwyufqbzfn2h2hezifkty3feipybj73e77r3abq2bvy4ikqd.onion
- questx24eprwsvoilphdrdpihcfsxza5aeje3x4mlifugc2zclx2zmid.onion
- questxkqz7yhkdvwe7e4k6i4t7vo6i22ccvtuyf7b5zyobau4faqbxad.onion

Public PGP Key

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

mQINBGFw9UEBEADQDeRL8HFtTK7cgLEcSLaLYwk58CnnXi8GIUzKB965o9hB4EQS

→ questxwkwsw2qgeeljz4fbv6cq2kmapo7tw5heu4nng2ufgykapid.onion/mirrors.txt

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

questxwkwsw2qgeeljz4fbv6cq2kmapo7tw5heu4nng2ufgykapid.onion
questx5olhiv35lrydy5glk6x64zcxlrepgqic7jlzi3uqyurqtltfad.onion
questx4pxdwytknsodzsrxawjkseonfbu2lc74pnmy74tok3lnuhmad.onion
questxpskfwwxcjlroi qye4y6m2ce4tcuu6r7wd5zt3wychqszykj2qd.onion
questx7deerotyvnnoejn7omvxs26m6nvxsxeb642dqs2zxw5peqc6qd.onion
questxi4tp34jbd7vowuk6njqc7bi6xlqqziwz7rwbjtj4ckj23j4jmqd.onion
questxrbeu2f2m6sqobh35xfsy5pfvesdfngwdc3q2x2zhntbjt6aqd.onion
questxnwyufqbzfn2h2hezifkty3feipybj73e77r3abq2bvy4ikqd.onion
questx24eprwsvoilphdrdpihcfsxza5aeje3x4mlifugc2zclx2zmid.onion
questxkqz7yhkdvwe7e4k6i4t7vo6i22ccvtuyf7b5zyobau4faqbxad.onion
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEfeyKR0chj/tbm7mUGGghmCStHTwFAMFa2yQACgkQGgGhmCSt
HTylgw//XM4YYMexZywlkNlmaX5oYmx96FLjoDLk262+jTSsULZzfgU7sgkOKRtn
f/LE/Pzql4gHpv4Rr1x98Nd1Dyb2WQZ6ghxHS8YCIAjPj7F8em/lMmnwnCJeNIIf
fmwH+lyM0PLYnlr1RWXW6hSzz0cVxOx06JlbqDV4WdFmK+R6nfOrKrps0mQIHLGq
vnAEab4NCf06P932GHfNygXLCvXXmEzD/k4sQZ6ZN6HNO4x179YCPsZPxYfa7DLM
lPB1y1J/bi3x9Aki87Z2eSpF/+f5xvkBtxZsfBmpbAj9Hqbps3u32TSYYDdyugEU
1Dzy+oumQFX7zIciwMJRdjKdUxSzaq77uBgO560+qBtxNNkaWmesCQOjebNELjGE
5nNVcbnoj785Y3AWaVMS5sCfUMVqFa6YribwDexmBqlv1EkIN0h1MwXnrhQD1EBx
zar4X1LudAo+ndCJVOTPxuotw96G2/u27vBeBXXK406iDm5+GXUq3rF4YEiEOCXb
+D/Pnlzdz9992D1xsaNPWi/sVZMf2Wp1MYA7gMg+pE3nQwdh0SpNdbOfQFUSJdVR
r10YvZ1zOR+FV6sI+EeCVi6SxPQwVdqPCnVAwx2iP5x1gB74jbJo+yUx6pIJfaVz
Fbh6Uz+Q0e7p808ThXwhuWmftqS1HYXFKxurlSOnueRX9fk/ZfQ=
=+EEO
-----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

ASAP

Search for listings

LoginRegister

Menu

PGP

Mirrors

Introduction

FAQ

Rules

DNSTATS.NET DAKR FAIL PHISHING ALERT!

Categories

Stimulants 8666

RCs 98

Cannabis & hashish 14680

Drug paraphernalia 49

Steroids 992

Barbiturates 4

Fraud 5142

Lab Chemicals 18

Weight loss 68

Ecstasy 3819

Drug Precursors 7

Prescription 1668

Tobacco 7

Opioids 2290

Counterfeits 172

Dissociatives 2406

Digital goods 6773

Benzos 1631

Psychedelics 4338

Links

ASAP Primary Link

Dark.fail

Dread Sub

Home

Featured listings



Requires FE

25x LSD

Vendor: frenchdealer (115)

Category: LSD

Price: 171.15 USD

Ships from: France

Ships to: European Union

Positive 0 Negative 0



White Trufflez - Exotic (\$180/OZ - \$2875/LB)

Vendor: prettypacks (1641)

Category: Buds & flowers

Amount: Ounce (OZ) - 180.90 USD

Ships from: United States

Ships to: United States

Positive 22 Negative 0



NEEDLE KETAMINE 91% | UK | Europe | United States ...

Vendor: cokingupbritain (1)

Category: Ketamine

Price: 32.20 USD

Ships from: United Kingdom

Ships to: Worldwide

Positive 0 Negative 0



Requires FE

MDMA 84% Champagne PURE | USA 2 USA

Vendor: xxMarlborOxx (2298)

Category: MDMA

Amount: 1g - 35.20 USD

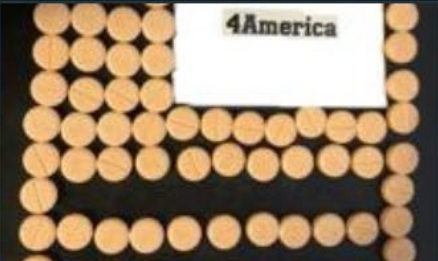
Ships from: United States

Ships to: United States

Positive 0 Negative 0







4America



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

<https://dark.fail/asap>

Is ASAP Market online on Tor?

Yes.

Check your URL! Make sure you are on our official domain, don't get phished. There is always a dot between dark and fail. No com, no live, the TLD is .fail.

All online links

Prove you are not a bot to [view all links](#).

ASAP Market's Top Onion Links

<http://asap2u4pvpplnkz17ecle45wajojnftja45wvov13jrvhangeyq67ziid.onion>

<http://asap4u7rq4tyakf5gdahmj2c77blwc4noxnsppp5lzlhk7x34x2e22yd.onion> - Last Online: Fri Sep 30 04:44:33 2022 UTC

<http://asap4u2ihunfdsumm66pmado3mt3lemdiu3fbx5b7wj5hb3xpgmwkqd.onion> - Last Online: Fri Sep 30 09:34:30 2022 UTC

asap4uqsmdujt6ehoktmxogday X +

asap4uqsmdujt6ehoktmxogdaypfmucznnerdggfg6ol5vzrtwod6oid.onion/mirrors.txt

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

http://asap2u4pvpplnkz17ecle45wajojnftja45wvov13jrvhangeyq67ziid.onion/
http://asap4u2ihunfdsumm66pmado3mt3lemdiu3fbx5b7wj5hb3xpgmwkqd.onion/
http://asap4u7rq4tyakf5gdahmj2c77blwc4noxnsppp5lzlhk7x34x2e22yd.onion/
-----BEGIN PGP SIGNATURE-----

iQIzBAEgAdFiEEFyH4Dj1Jsz57T1V4MIquH46ztPwFAMIs+s0ACgkQMIquH46z
tPzr77//Ku7RCfuJ6709KoUzLoZQa2vyouuIzeYiFEsGYV7mRoS32zTN1008+WS4
38ZIM/x0LianQp/mS4nYUvKXtqMx/6NP5E3lg/01bqtZ4P0AkQRnXnKRvwZk6OX
SzC1YL2pEVob+1IjkdNv+Q0JWou2DLMG1dhmpiCCfihduuc41v1q91YIU1wMXUH
ZAjwRR31tx35+6Zr6vq4k0bTsL3HI9C5kcBiDG+8NiQQrDmKSmD4P9iJJ4d/Jwge
9WsfGJmHqe4dpQ83RYBibg02aJYYildXxU9DQ3yMHYHGeChaGLE5giyWN1qZRio
BOKY3m7ab1BNAoqERakox4KXYVEsm46eCcg00itvUOGjRpdeI6hP/BuFs4Q1Ika
edVTpjEUCiM/Ej3Ay1tylWoRRnxMW4csNmt2OTvdMYphLCPxGCnAW/vpYhX542fu
GtTGFwYl3g+44//HebRf1H7mucMghdp7+e6CymZiLFD0/KkFxf+elxZJ3a+XbYc
fVlsCOoJ2Lw/gY/mK6TGtKTr8vUxH4s9dHET4JOWxdpgrJtcJ29yw1bYNaG3Qec
1vQNDtHwEsmZtPt6ZGGtaRREUPfMmFMvwX80m0ts5k0AvzR816jDVTbWtaCU1VS1
wp380Wa7wx5DeL+XOmypt6H6qcN5EFEMTJOIoqyUw55CdZ22710=
=3bey
-----END PGP SIGNATURE-----
```

3. The .onion adress does not match any of the addesses 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.

Darknet Domain

Title	Home - ASAP Market
Domain	http://asap4uqsmdujt6ehoktmxogdaypfmucznnerdggfg6ol5vzrtwod6oid.onion  
Tags	Market (16,294) ASAP Market (1,508) Drugs / Narcotics (13,042) English (511,649)
Discovered	20 Jan 2022, 06:22 UTC
Last Seen Online	29 Sep 2022, 17:31 UTC
Last Checked	29 Sep 2022, 17:31 UTC

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

Case 3: TOR market

Hash: SHA512

```
Bitcoin block number: 754859  
block hash: 0000000000000000066cbc50347de6520f2268e35a28b3718fc20bed7344c3
```

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

1. The canary.txt is implemented

→ rrlm2f22lpqgfhyydqxxzv6snwo5qvc2krjt2q557l7z4te7fsvhbid.onion/mirror.txt

404 route not found

→ rrlm2f22lpqgfhyydqxxzv6snwo5qvc2krjt2q557l7z4te7fsvhbid.onion **pgp.txt**

404 route not found



Login	Register	Help
-------	----------	------

Product sample selection



TescoExpress approved, tried and tested!

Product details

0.5 g	25.00 GBP
1 g	45.00 GBP
1.7 g	80.00 GBP
3.5 g	130.00 GBP
7 g	210.00 GBP
14 g	400.00 GBP
28 g	750.00 GBP
56 g	1,400.00 GBP



Product de

Product details

0.5 g	40.00 GBP
1 g	75.00 GBP
3.5 g	180.00 GBP
7 g	360.00 GBP
14 g	730.00 GBP
28 g	1,350.00 GBP
56 g	2,600.00 GBP
112 g	5,000.00 GBP



0.5 g	32.00 GBP
1 g	57.00 GBP
2 g	112.00 GBP

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 it 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

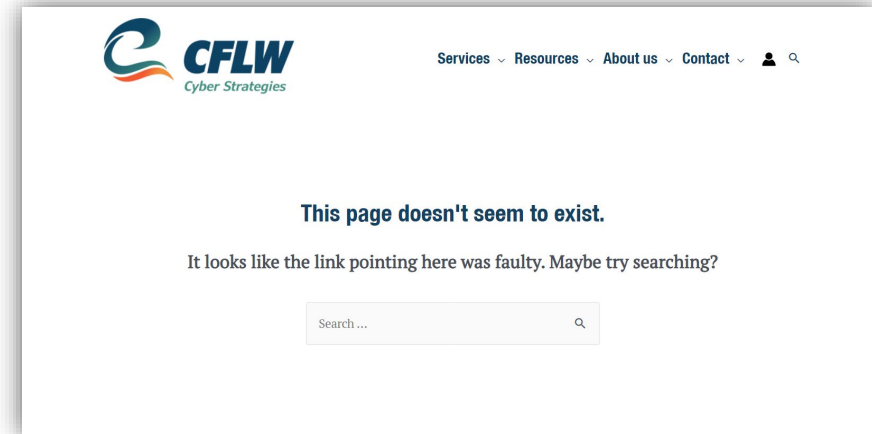


DARK WEB MONITOR
Strategic Insights, Operational Perspectives

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.

