# Unhiding the Dark Web at scale

Patrice Auffret

patrice.auffret@onyphe.io



#### **ONYPHE** search engine

- ONYPHE « Your Internet SIEM »
- Internet connected devices indexation and more
  - clear Web, deep net, Dark Web
  - threat feeds
  - passive DNS
  - Certificate Transparancy Logs
  - pastebin
  - Internet background noise
- Made accessible via a Web search engine and an API
  - dedicated to open-source intelligence and threat data
  - correlation between all those sources of information



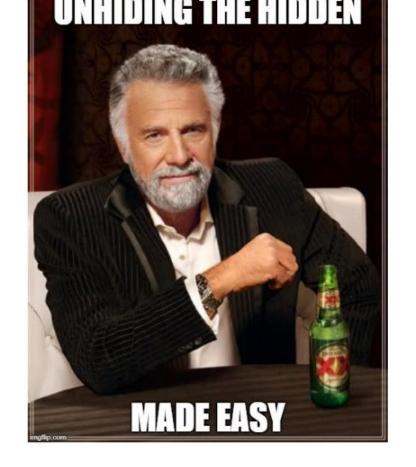
#### Scanning the Dark Web

- The Dark Web is small
  - compared to the clear Web
- Tor hidden services
  - 45 000 .onion identified
  - 9 100 answering to requests

onion v2 armdzvcnd63t3k2i.onion
onion v3 armdzvcnd63t3k2i.onion
onion v3 armdzvcnd63t3k2i.onion



- Short answer : yes
  - longer
    - to some extent
    - based on a configuration error
- Web server exposed
  - on the Dark Web
  - and on the Internet
- Correlation made possible
  - between the Dark Web
  - and clear Web scanning





- For some hidden services
  - it is by design
  - most cases





- For a few of them, it is an issue
  - example with a Carding Web site

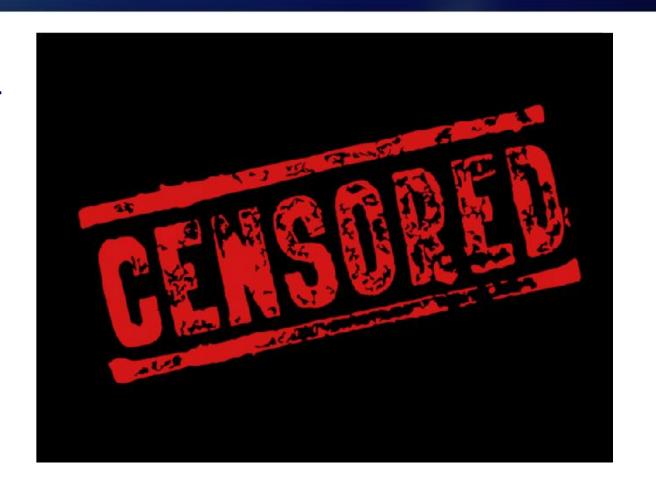








- Connection from a Web browser
  - on found IP address
- It really looks like the same site
  - even though links are broken





#### OPL: Onyphe Processing Language

category:onionscan url:/ -since:7d -exists:app.http.bodymd5 !tag:default

merge category:datascan app.http.bodymd5:\$app.http.bodymd5 -exists:app.http.bodymd5

category:onionscan url:/!tag:default

```
| dedup onion
| whitelist exclude.csv
| merge category:datascan app.http.bodymd5:$app.http.bodymd5
```

onyphe -autoscroll 1 -fields app.http.bodymd5,onion,classification,ip,city,country,organization -search



whitelist exclude.csv

-verbose U > onion-ip.txt

dedup onion

#### At scale?

- Unhiding at scale
  - query all data from Dark Web scanning
- On 9 100 hidden services
  - 300 are also exposed on the clear Web
- Unhiding possible
  - 3,3% of all .onion
  - number increases over time



### Samples of unhidden services

app.http.bodymd5|city|classification|country|ip|onion|organization

e27d648a0bb771f2e85e6fe091016e2e
72509cac305b0f7b9b246269b59c3d72
d2d7d1f5ec88fc150f15f06efde6b00c
7f381b22592260563f16c80e0a0dc487
bcc58401ae806080d5459dd2d144b8df
4963d5b17b2177c9ecd7d9eb902915ee
08b551648b7bad73e0393ed40a959708
4ed8a839e0e056f461d5d45e7849fdd0
1b8b6d095cbb225d1645fe3286386703
ebece2ce5a9a8a58678ae8e7820b3521





#### Tool available on Github

- Tool available on *Github* 
  - https://github.com/onyphe
- A Splunk-like language to use the ONYPHE API
  - OPL: Onyphe Processing Language

```
onyphe -autoscroll 1 -fields ip,domain,organization,country,fingerprint.md5 -search '
    category:datascan organization:"Cloudflare, Inc." -exists:fingerprint.md5
    | dedup fingerprint.md5
    | merge category:datascan fingerprint.md5:$fingerprint.md5 !organization:"Cloudflare, Inc."
-maxpage 10
```



### Thank you.

Twitter: @onyphe, @PatriceAuffret

Github: <a href="https://github.com/onyphe">https://github.com/onyphe</a>

Register: <a href="https://www.onyphe.io/login/#register">https://www.onyphe.io/login/#register</a>

Pricing: <a href="https://www.onyphe.io/pricing">https://www.onyphe.io/pricing</a>

