

# Dark Web, Dark net, Deep Web : petra eo\* ?

Patrice Auffret

[patrice.auffret@onyphe.io](mailto:patrice.auffret@onyphe.io)

\* du Breton qu'est-ce que c'est ?

# Qui suis-je ?

- Expert en cybersécurité
  - depuis plus de 18 ans
- Différents rôles
  - développeur
  - auditeur et pentesteur
  - sysadmin
  - formateur
  - défenseur
- Fondateur de la société **ONYPHE**



Crédit : Michel François Salmon

# Le moteur de recherche ONYPHE

- **ONYPHE** - « Le SIEM de l'Internet »

- Collecte des données techniques

- clear Web, deep net, Dark Web
- *threat feeds*
- *passive DNS*
- *Certificate Transparency Logs*
- sites de copier/coller en ligne
- bruit de fond de l'Internet
- captures écrans

- Accessible via un moteur de recherche et une API

- dédié au renseignement d'origine source ouverte et intelligence sur la menace
- corrélation entre différentes sources d'information



# Agenda

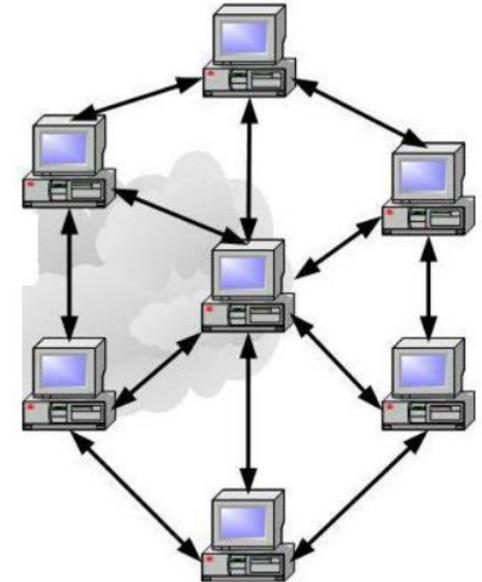
- Définitions
- Mise en perspective avec le World Wide Web (et l'Internet)
- La vision de la presse
- Que trouve-t-on vraiment dans le Dark Web ?
- Les *Hidden Services* sont-ils bien cachés ?
- Capturer le Dark Web

# Définitions

Clear Web, deep Web, deep net, Dark Web, Dark net, ...

# Commençons par définir l'Internet

- Un réseau de réseaux sur IP (v4, v6)
  - pas seulement « Web » ou « WWW »
  - d'autres protocoles existent (SSH, Telnet, FTP, HTTP, IMAP, ...)
- « Deux Internet »
  - le Web : constitué uniquement de services HTTP
  - le net : constitué de services HTTP et de tous les autres services
- L'Internet est l'ensemble des machines connectées via IP (v4 ou v6)



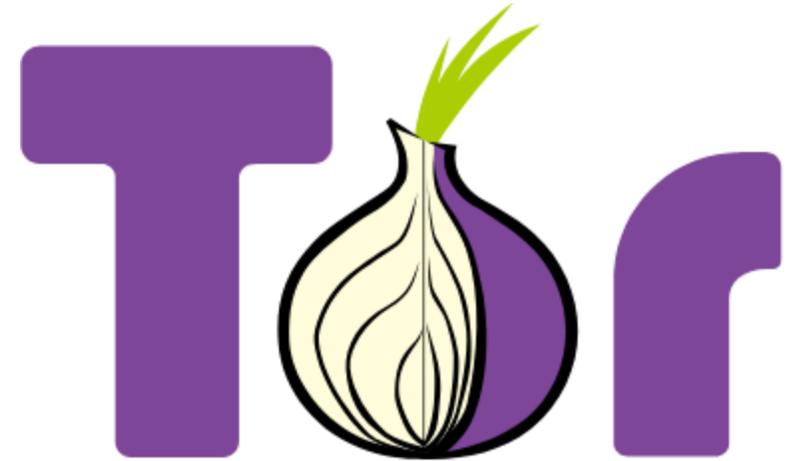
# Maintenant définissons le Dark net

- Terme détourné de son origine
  - espace IP non-attribué (RFC6018)
- Mais largement utilisé aujourd'hui pour définir le réseau Tor
  - *The Onion Routing*
  - un réseau au-dessus du réseau IP
- On peut garder la même distinction que pour l'Internet
  - le Dark Web : constitué uniquement de services HTTP
  - le Dark net : constitué de services HTTP et de tous les autres services
- Le Dark net est l'ensemble des machines connectées via Tor
  - qui constitue donc *l'onionland*



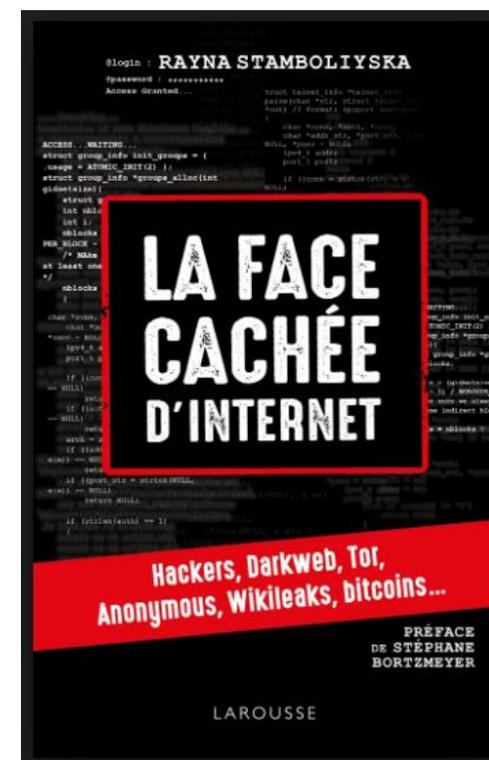
# Le réseau Tor – l'*onionland*

- Apporte l'anonymisation de l'adresse IP source
  - et le chiffrement des flux en transit
- Créé par le US NRL puis le DARPA
- Pour toutes les requêtes vers le net
  - qu'il soit clear/deep/Dark
- Naviguer dans l'*onionland* à proprement parler nécessite
  - un accès au réseau (Navigateur)
  - de connaître l'adresse d'un site Web en *.onion*
    - nommés les *Hidden Services* (services cachés)
  - mais impossible (normalement) de connaître l'adresse IP d'un *.onion*



# Les dark nets en général

- dark net avec un « d » minuscule
  - terme plus général définissant un réseau superposé (*overlay*)
  - il y a donc « des » dark nets
- Exemples
  - réseaux P2P
  - réseaux F2F
  - réseau I2P
  - Freenet
  - VoIP
- Source
  - Livre : *La face cachée d'Internet*, Rayna Stamboliyska



# Et le deep Web dans tout ça ?

- C'est la partie non-indexée du Web
  - espaces privés (protégés par mot de passe)
    - forums
    - sites bancaires
  - ou simplement des liens « inconnus »
- Le net n'est pas indexé non plus
  - on pourrait parler de deep net
- Donc, rien à voir avec les dark nets



# Pour résumer clear Web/deep Web

- Finalement, le clear Web est
  - indexé par les moteurs de recherche classiques
  - et facilement visible
- Tandis que le deep Web et le net ne sont pas
  - indexés par les moteurs de recherche classiques
  - ni immédiatement visibles
- Mais certains acteurs indexent ces réseaux
  - profils criminels, étatiques ou privés

# Enfin, qu'est-ce que le Marianas Web ?

## Le Marianas Web

- ▶ Apparemment, pour accéder au Marianas web vous avez besoin de quelque chose dont le nom est **falcighol dérivation polymère**, c'est tout simplement l'informatique quantique. Sans cela, vous ne pouvez pas accéder au Marianas web. Mais qui possèdent les connaissances nécessaires pour l'informatique quantique ? **Le gouvernement.** C'est la raison pour laquelle vous ne pouvez pas entrer dans cette partie du Web. Si jamais vous arrivez à y accéder, **soyez prudent avec ce que vous faites.**



### ■ Source

- Jean-Paul Pinte, [http://www.association-aristote.fr/lib/exe/fetch.php/pres\\_pinte.pdf](http://www.association-aristote.fr/lib/exe/fetch.php/pres_pinte.pdf)

# Mise en perspective avec le World Wide Web (et l'Internet)

Quelle taille ces réseaux font-ils ?

# Mais quelle taille ces réseaux font-ils ?

## ■ Le clear Web

- 329 millions de noms de domaine
- disons qu'ils ont tous un site Web

## ■ Bien plus en comptant en URL

- 120 milliards

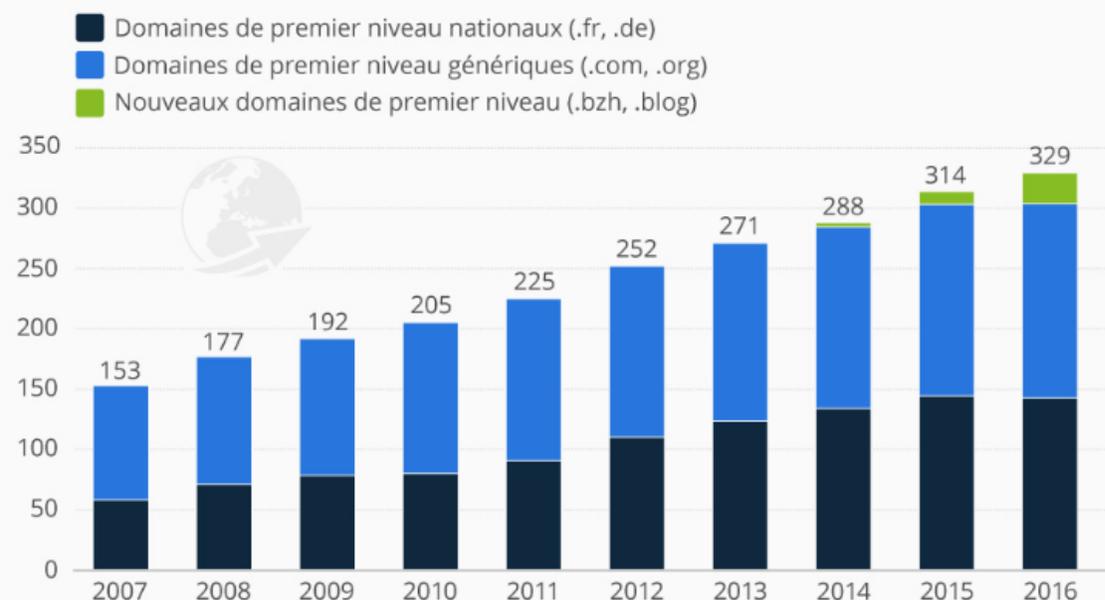
Combien de pages le moteur de recherche Google connaît-il ? Combien d'adresses URL sont présentes dans son moteur ? Selon Gary Illyes, Webmaster Trends Analyst chez Google, le moteur de recherche a connaissance de plus de 120 000 milliards d'URL. Un nombre incroyable, mais la majorité est constituée de contenu dupliqué...

Source :

<https://www.journaldunet.com/solutions/expert/62919/google-connaît-120-milliards-d-url--la-majorite-avec-du-contenu-duplique.shtml>

## Le Web tisse sa toile

Nombre de domaines de premier niveau enregistrés dans le monde (en millions)\*



\* Au quatrième trimestre de chaque année.

@Statista\_FR

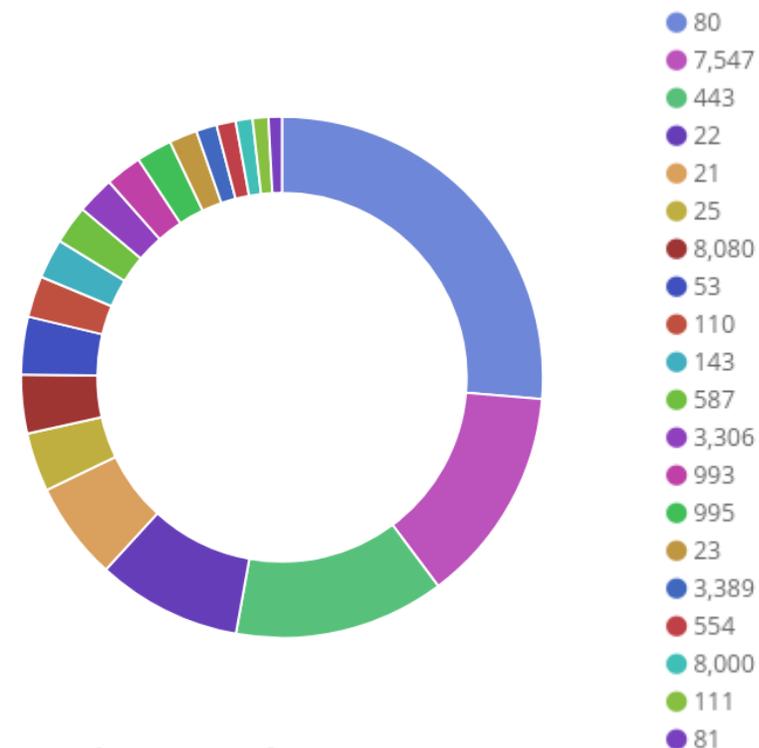
Source : Verisign

statista

Source : <https://fr.statista.com/infographie/8756/le-web-tisse-sa-toile/>

# Mais quelle taille ces réseaux font-ils ?

- Le deep net
  - 3,8 milliards d'adresses IP publiques
  - jusqu'à 65 535 services par adresse
    - uniquement pour TCP
- Estimation
  - TOP 20 ports usuels : environ 167 millions
  - ajoutons 20% pour les autres ports
  - estimation à 200 millions



Source : ONYPHE

# Mais quelle taille ces réseaux font-ils ?

- Le deep Web
  - difficile à dire



# Mais quelle taille ces réseaux font-ils ?

## ■ L'onionland

- 93 000 *.onion* identifiés
- 13 000 qui répondent

## ■ Potentiellement bien plus

- Onion v2 : Base32, 16 caractères
  - $32^{16} = 1.20892581961463 \times 10^{24}$
- Onion v3 : Base32, 56 caractères
  - $32^{56} = 1.94266889222573 \times 10^{84}$

## ■ Comparaison avec IP

- v4 : 32-bits
  - $2^{32} = 4\,294\,967\,296$
- v6 : 128-bits
  - $2^{128} = 3.40282366920938 \times 10^{38}$

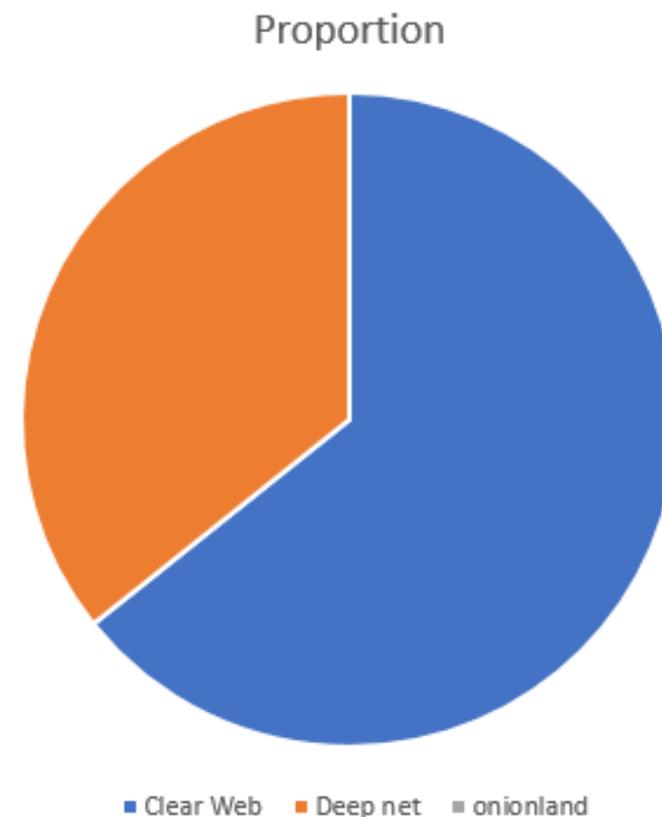
## ■ Ordonnancement par taille

- IPv4 < Onion v2 < IPv6 < Onion v3

|       |    |   |
|-------|----|---|
| onion | v2 | armdzvcnd63t3kzi.onion  |
| onion | v3 | zmt03jdlawraz2plpxdukn5namqja3dyfah345guhghqgiqlayp3ojxad.onion |

# Mais quelle taille ces réseaux font-ils ?

- Clear Web
  - 329 millions : environ 62%
- Deep net
  - 200 millions : environ 38%
- *Onionland*
  - 13 000 : environ 0,002%



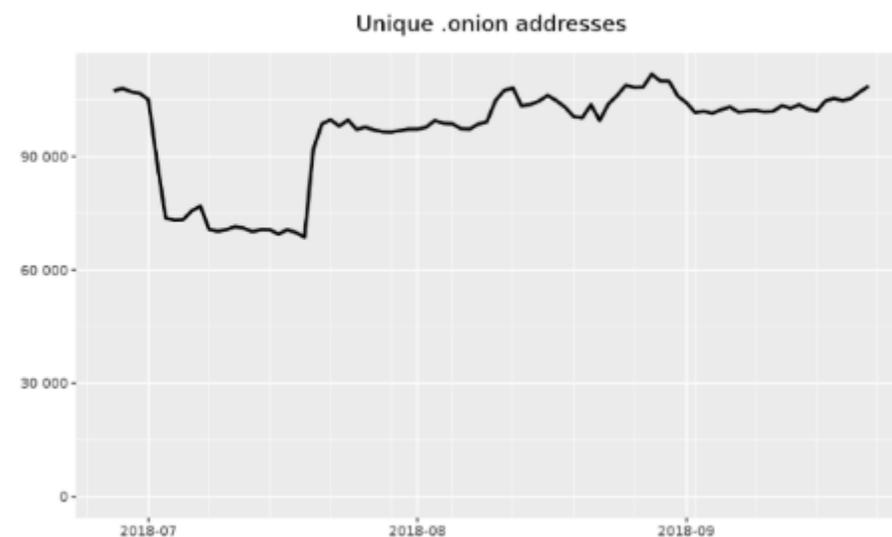
# Mais quelle taille ces réseaux font-ils ?

- 100 000 *.onion* actifs selon *The Tor Project*
  - Soit 0,02%

## THE DARK WEB IS NOT AS LARGE AS WE THOUGHT

POSTED BY: TAMER SAMEEH   OCTOBER 13, 2018   IN ARTICLES, FEATURED   2 COMMENTS

Unique .onion addresses (version 2 only)



The Tor Project - <https://metrics.torproject.org/>

Source : <https://www.deepdotweb.com/2018/10/13/the-dark-web-is-not-as-large-as-we-thought/>

# La vision de la presse

Quelques articles sélectionnés

# Déjà, c'est l'Internet illégal 😊

## Nouveau monde. Piratage de Facebook : et si le pire était à venir ?

La cyberattaque massive dont a fait l'objet le réseau social pourrait avoir des conséquences à long terme pour les victimes. L'Union européenne a ouvert une enquête.

retaper son mot de passe. En s'emparant de ces "clés", les pirates ont pu entrer dans les comptes de 50 millions d'utilisateurs sans mots de passe et ainsi récupérer toutes sortes d'informations que, normalement, les autres ne

Facebook, rien ne montre que les attaquants aient effectivement accédé à ces profils extérieurs. Cependant, en général, ce genre de données volées sont souvent revendues sur le Dark web (l'Internet illégal). Si elles tombaient entre de mauvaises mains, cela pourrait alors porter préjudice à leurs propriétaires.

Source :

[https://www.francetvinfo.fr/replay-radio/nouveau-monde/nouveau-monde-piratage-de-facebook-et-si-le-pire-etait-a-venir\\_2948059.html](https://www.francetvinfo.fr/replay-radio/nouveau-monde/nouveau-monde-piratage-de-facebook-et-si-le-pire-etait-a-venir_2948059.html)

# De quoi devenir un « grand »



## En Ukraine, le Rennais SaxX va défier l'élite mondiale des hackers !

Lui, outre son BTS, s'est formé sur le tas en passant des milliers d'heures à apprendre le code et à progresser. Aussi en utilisant le dark web où l'on trouve de multiples ressources. Rien qu'en Bretagne, les entreprises spécialisées dans ce domaine ont un mal fou à recruter. « Si j'avais un message à lancer aux jeunes femmes et aux jeunes hommes, c'est de s'y lancer. Il faut juste être motivé et inventif. »

Ouest-France

Source :

[https://quimper.maville.com/actu/actudet\\_-rennes.-en-ukraine-le-rennais-saxx-va-defier-l-elite-mondiale-des-hackers-loc-3537004\\_actu.Htm](https://quimper.maville.com/actu/actudet_-rennes.-en-ukraine-le-rennais-saxx-va-defier-l-elite-mondiale-des-hackers-loc-3537004_actu.Htm)

Des documents confidentiels ...

# French police officer caught selling **confidential police data** on the dark web

Police officer also advertised a system to track the location of buyers' gang rivals or spouses based on the telephone numbers.



By Catalin Cimpanu for Zero Day | October 3, 2018 -- 05:00 GMT (06:00 BST) | Topic: Security

Source :

<https://www.zdnet.com/article/french-police-officer-caught-selling-confidential-police-data-on-the-dark-web/>

# De la drogue ...

## French Dark-Web Drug Dealer Sentenced to 20 Years in US Prison

📅 October 10, 2018 👤 Swati Khandelwal



SPONSOR

After his arrest, US authorities found a laptop which confirmed Vallerius' login credentials for Dream Market and uncovered roughly **\$500,000 worth of bitcoins and a PGP encryption key** entitled OxyMonster, verifying his identity on the dark web marketplace.

A dark web drugs kingpin who was arrested last year when he arrived in the United States to compete in the World Beard and Mustache Championships has now been sentenced to 20 years in prison.

Source : <https://thehackernews.com/2018/10/dark-web-drugs-kingpin.html>

# Du travail ??



The screenshot shows a blog post from SpiderLabs. The header features the SpiderLabs logo and the text 'SpiderLabs® Blog'. The main title of the post is 'The Underground Job Market', which is highlighted with a red rectangular border. Below the title, the post date is 'October 18, 2018', the author is 'Posted By SpiderLabs Research', and there are 'Comments (0)'. A 'Share:' section is visible below the metadata. The main content of the post includes a quote: *"Leave your ego at the door every morning, and just do some truly great work. Few things will make you feel better than a job brilliantly done."* attributed to *Robin S. Sharma*. At the bottom, there is a paragraph of text starting with 'The last time we visited the cybercriminal underground, we introduced you to a community with its own laws and code of trust. In Part Two of the series, we take a closer look at the job market of the dark web – an investigation that sheds light on the day-to-day lives of its members and illustrates cooperation among them.'

Source : <https://www.trustwave.com/Resources/SpiderLabs-Blog/The-Underground-Job-Market/>

# Des informations de cartes bleues ...

PakCERT Threat Intelligence Report PCTI-2018-0111

## Analysis of the recent attack on Pakistani banks

By Qazi Mohammad Misbahuddin Ahmed, CISSP, CPTS, CEH, ITIL, COBIT, MBCI

[QA@PAKCERT.COM](mailto:QA@PAKCERT.COM)

4<sup>th</sup> November, 2018

### Background

During mid October, customers who subscribed to banking transaction notifications started receiving alerts of money transfer from their accounts. BankIslami noticed abnormal transactions of Rs.2.6 million on the morning of 27<sup>th</sup> October and shutdown its international payment scheme.

Subsequently several others bank issued security alerts and either completely blocked customer's debit and credit cards or blocked their online and international use. Customers were sent SMS notifications of the changes.

Source : <https://www.pakcert.org/img/PakCERT%20Threat%20Intelligence%20Report%20-%20web.pdf>

# Et même des tueurs à gage ...

## Une femme a été arrêtée pour avoir embauché un tueur à gage sur le Darknet



Tina Jones, une infirmière de 31 ans de l'Illinois aux Etats-Unis a été arrêtée pour une tentative d'embauche **d'un tueur à gages sur le Darknet**. Elle a été jugée mercredi 12 avril 2018 sur le territoire américain. Tina Jones est accusée du crime de sollicitation de meurtre par embauche et le juge a fixé sa caution à 250 000 \$.

L'enquête sur Tina Jones a commencé après que la police de Woodridge ait reçu un appel sur leur ligne de destinée à recevoir les délations, affirmant qu'une femme de la région avait été la cible d'un complot d'assassinat. Selon le bureau du procureur du comté de DuPage, le tuyau provient d'une émission de télévision couvrant les tueurs à gages du marché noir en ligne (le Darknet) sur les « 48 heures » de CBS.

Source : <https://cc-segalacarmausin.fr/femme-a-ete-arretee-embauche-tueur-a-gage-darknet/>

# Que trouve-t-on vraiment dans le Dark Web ?

N'y trouve-t-on que des choses pas nettes ?

# Que trouve-t-on vraiment dans le Dark Web ?

- Crawling du Dark Web
  - Depuis juin 2018
  - 93 000 *onion* identifiés
  - 13 000 actifs
- Captures écrans
  - Depuis mars 2019
- Techniques de « *démasquage* »
  - Trouver l'adresse IP d'hébergement
- Moteur de recherche (et API)



# Que trouve-t-on vraiment dans le Dark Web ?

- Et si on classifiait automatiquement les sites du Dark Web ?
  - identification d'un certain nombre de catégories
  - utilisation d'un algorithme (aucun détail ici)
  - actuellement, seuls 10% des *.onion* sont classés
- Au final, environ 60 catégories liées
  - à la criminalité (cyber, ou non-cyber)
  - à la pornographie
  - au libre-software
  - aux cryptomonnaies
  - aux paris sportifs
- Et bien d'autres choses encore

# Que trouve-t-on vraiment dans le Dark Web ?

|                   |              |
|-------------------|--------------|
| Child pornography | 715 (21.58%) |
| Carding           | 485 (14.64%) |
| Cryptocurrency    | 279 (8.42%)  |
| Search engine     | 210 (6.34%)  |
| Drug              | 147 (4.44%)  |
| Tor               | 143 (4.32%)  |
| Pornography       | 135 (4.07%)  |
| Hardware          | 130 (3.92%)  |
| Anonymity         | 126 (3.80%)  |
| Laundering        | 114 (3.44%)  |
| Other             | 829 (25.02%) |

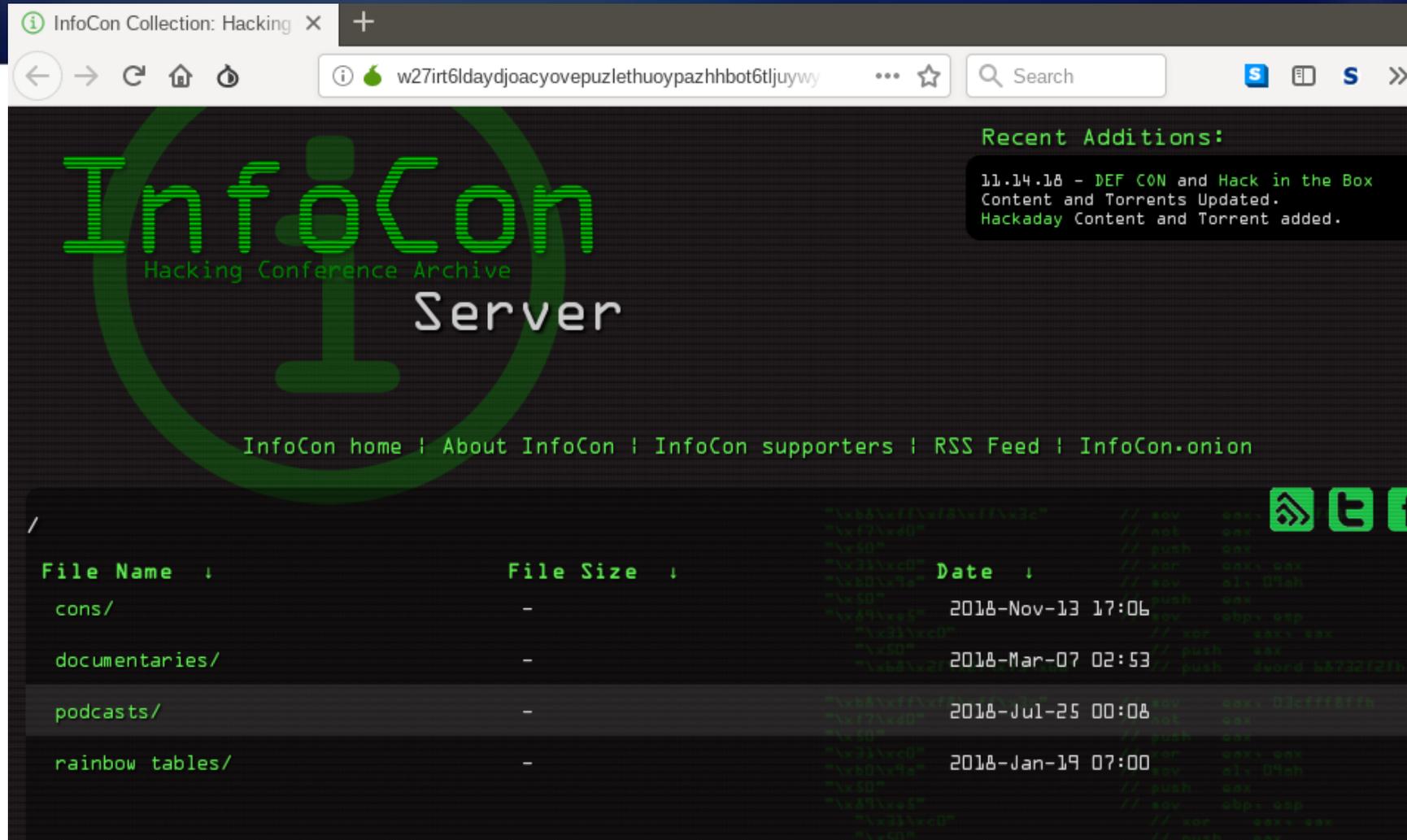
## ■ TOP 5 catégories

- Pornographie infantile
- Informations bancaires
- Cryptomonnaies
- Moteurs de recherches
- Drogue

# Que trouve-t-on vraiment dans le Dark Web ?



# De quoi apprendre le « hacking » ?

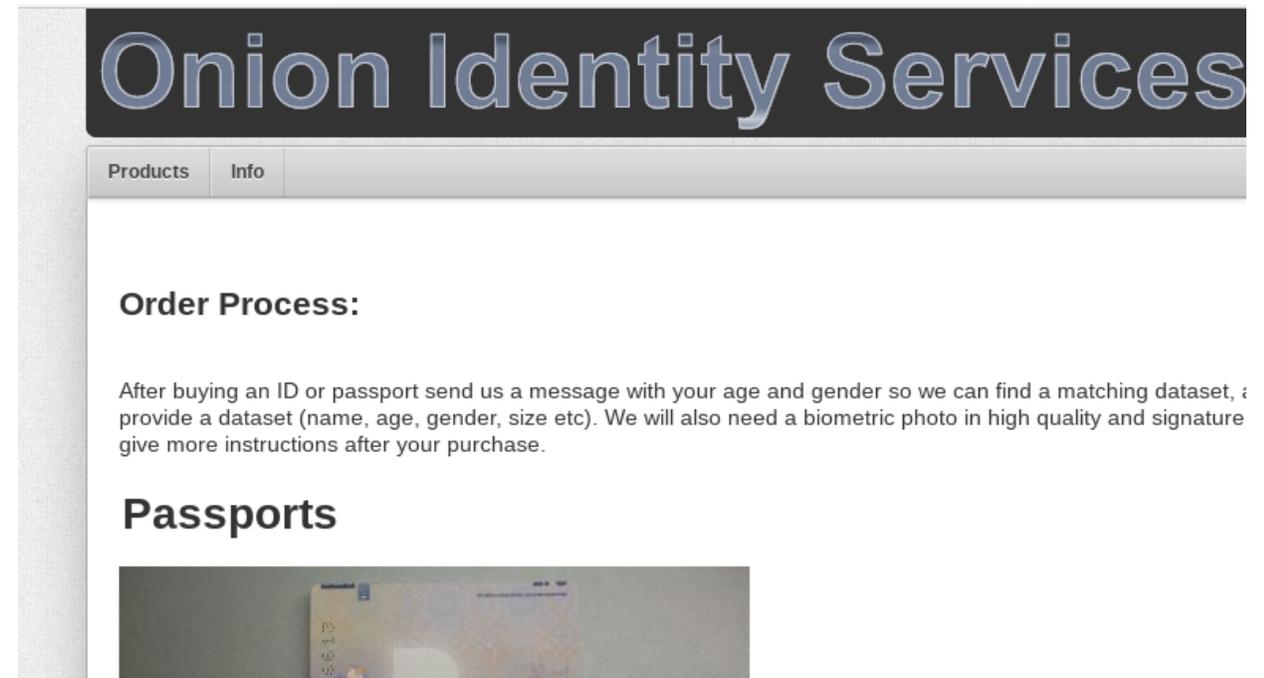


The screenshot shows a web browser displaying the InfoCon Server website. The page features a large green logo for 'InfoCon Hacking Conference Archive Server'. Below the logo, there are navigation links: 'InfoCon home | About InfoCon | InfoCon supporters | RSS Feed | InfoCon-onion'. A 'Recent Additions:' section lists updates from 11.14.18. At the bottom, a file directory listing is visible with columns for File Name, File Size, and Date.

| File Name ↓     | File Size ↓ | Date ↓            |
|-----------------|-------------|-------------------|
| cons/           | -           | 2018-Nov-13 17:06 |
| documentaries/  | -           | 2018-Mar-07 02:53 |
| podcasts/       | -           | 2018-Jul-25 00:08 |
| rainbow tables/ | -           | 2018-Jan-19 07:00 |

# Des documents confidentiels ?

- Nous n'en avons pas trouvé
  - mais cela ne veut pas dire qu'il n'y en a pas
- Par contre, de quoi commander de faux papiers

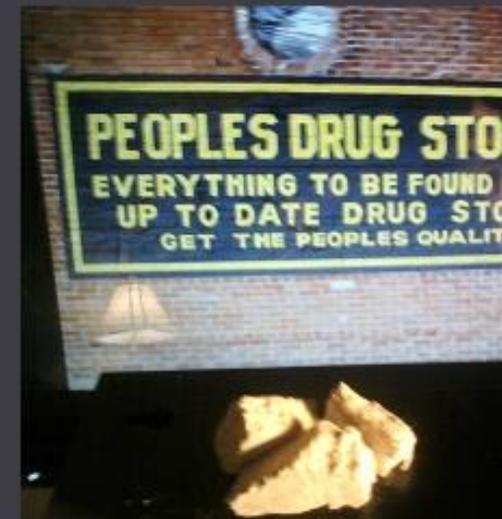


# De la drogue

## WANNA MAKE SOME FREE BTC??

Tell others about this shop, and earn 3% from every purchase they will make. Simply give them the <http://www.drugszun7tvsgsaa.onion/?ref=YOURUSERNAME>. Replace YOURUSERNAME with your own name. The money goes directly to your wallet.

### SW Asian #4 Heroin



# Du travail

- Pas exactement
  - enfin, ça dépend de quel côté de la barrière vous êtes ...

## Rent-A-Hacker

### Rent-A-Hacker

Experienced hacker offering his services!

(Illegal) Hacking and social engineering is my bussiness since i was 16 years old, hacking and i made a good amount of money last +-20 years.

I have worked for other people before, now im also offering my services for everyo

#### Prices:

Im not doing this to make a few bucks here and there, im not from some crappy e

Im a professional computer expert who could earn 50-100 euro an hour with a lega

So stop reading if you dont have a serious problem worth spending some cash at.

Prices depend alot on the problem you want me to solve, but minimum amount for

You can pay me anonymously using Bitcoin.

# Des informations bancaires



## Stolen PayPal Account

Buy cheap stolen/hacked verified Pay

Currently Available:

US - \$250-\$350 - Verified - 0.011 BTC

An advertisement for 'Clone Card Crew' with a dark, patterned background. The text is white and yellow. It includes a welcome message, a description of the service, and shipping information. An inset image shows a desk with a computer, keyboard, and stacks of credit cards.

**CLONE CARD CREW**  
Attack of the Clone

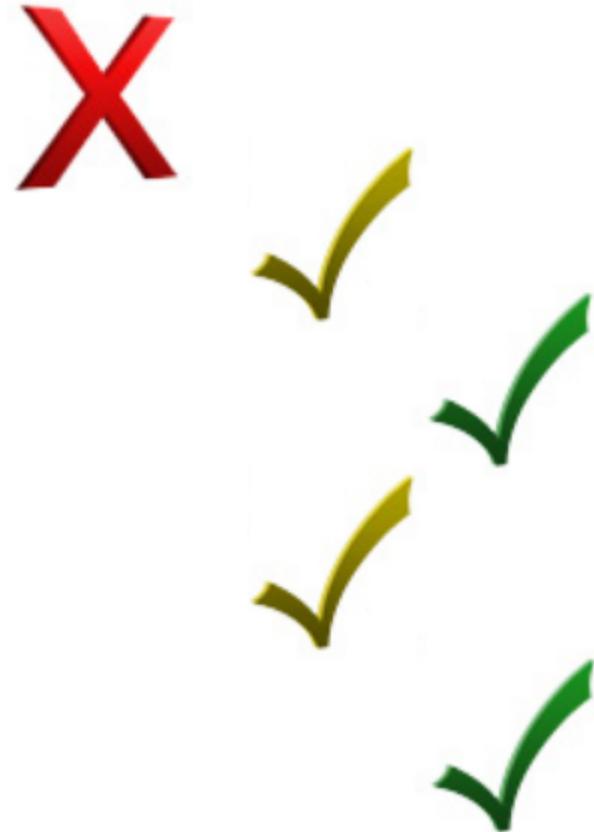
Welcome back! Thank you for giving us another chance to provide  
Here you'll find cloned credit cards at discounted price and promise

All cards are skimmed and cloned. Every card is written by high qua  
working PIN. We have a large database of credit card - ranging from  
verified for funds and validity before shipment. They work worldwide

We ship all of our cards 100% discrete via FedEx Standard Over  
International Priority for countries outside of USA. Shipping cost

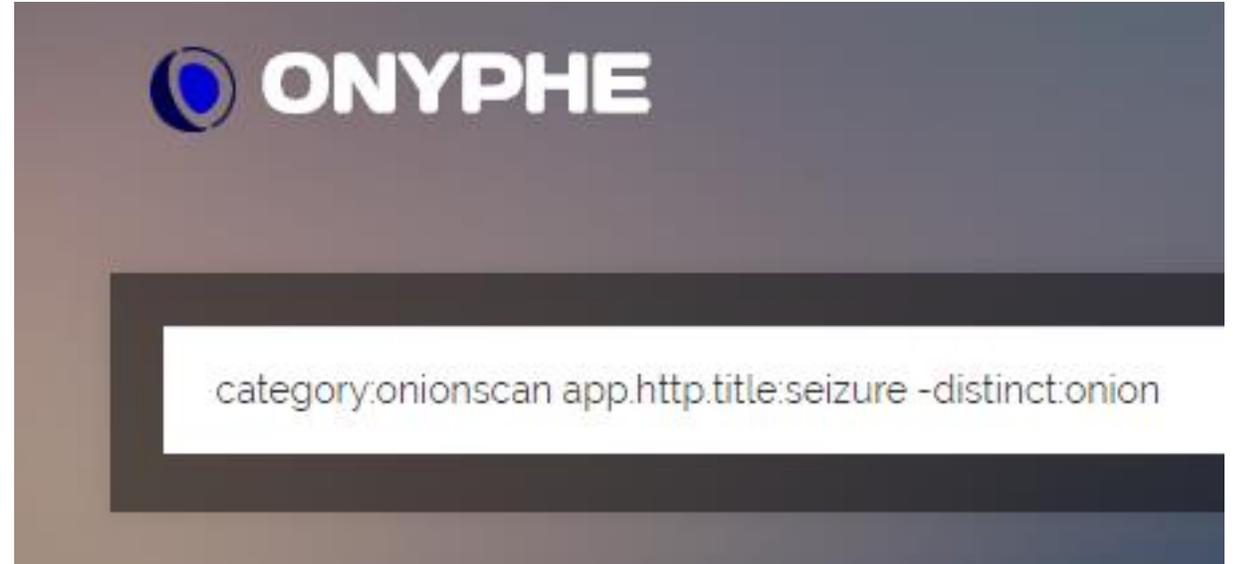
# Que trouve-t-on vraiment dans le Dark Web ?

- *Fact checking* articles de presse
  - de quoi apprendre le « hacking » ?
  - des documents confidentiels ?
  - de la drogue
  - du travail
  - des informations bancaires



# Mais que fait la police ?

- Elle travaille
  - partout dans le monde
- Elle collabore
  - à l'international
- Recherches sur *seized* ou *seizure*
  - 40 sites uniques



# Mais que fait la police ?



**Die Plattform und der kriminelle Inhalt wurden beschlagnahmt**

durch das Bundeskriminalamt  
im Auftrag der Generalstaatsanwaltschaft Frankfurt am Main

The platform and the criminal content have been seized by the  
Federal Criminal Police Office (BKA)  
on behalf of Attorney General's Office in Frankfurt am Main

- <https://www.onyphe.io/search/?query=category%3Aonionscan+app.http.title%3A%22BKA+-+Seizure+Banner%22+since%3A7M+-distinct%3Aonion>

- 30 sites uniques
  - Depuis mai 2019

# Mais que fait la police ?

Tämä piilopalvelu on suljettu viranomaisten toimesta.  
Denna dold tjänst har stängts av myndigheterna.  
This hidden service has been closed by the authorities.



- <https://www.onyphe.io/search/?query=category%3Aonionscan+app.http.title%3A%22Sipulikanava+on+suljettu%22+-since%3A7M+-distinct%3Aonion>

- 10 sites uniques
  - Depuis mai 2019

# Mais que fait la police ?



- <https://www.onyphe.io/search/?query=category%3Aonionscan+app.http.title%3A%22THIS+HIDDEN+SITE+HAS+BEEN+SEIZED%22+-since%3A7M+-distinct%3Aonion>

- 28 sites uniques
  - Depuis mai 2019

# Mais que fait la police ?



U.S. Immigration and  
Customs Enforcement



## THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by  
the Federal Bureau of Investigation, ICE Homeland Security Investigations,  
and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states  
and a protective order obtained by the United States Attorney's Office for the Southern District of New York  
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section  
issued pursuant to 18 U.S.C. § 983(j) by the  
United States District Court for the Southern District of New York



# Mais que fait la police ?



U.S. Immigration and  
Customs Enforcement



## **Your IP Address has been logged!**

as part of a joint law enforcement operation by  
the Federal Bureau of Investigation, ICE Homeland Security Investigations,  
and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states  
and a protective order obtained by the United States Attorney's Office for the Southern District of New York  
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section  
issued pursuant to 18 U.S.C. § 983(j) by the  
United States District Court for the Southern District of New York



Mais que f

Notice

# THIS HIDDEN SITE HAS BEEN SEIZED

*and controlled since June 20*

by the Dutch National Police in conjunction with the Bundeskriminalamt, Lietuvos Policija, Federal Bureau of Investigation and Europol, under the authority of the Dutch National Prosecutor's Office and the Attorney General's office of the Federal State of Hestia (Germany).



The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source code, which allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help law enforcement agencies worldwide to identify users of this marketplace. For more information about this operation, please consult our hidden service at [politiepvh42eav.onion](http://politiepvh42eav.onion).

This seizure was part of **Operation Bayonet**, which includes the takeover of Hansa Market by the National Police of the Netherlands and the takedown of AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.

 HANSA  AlphaBay Market

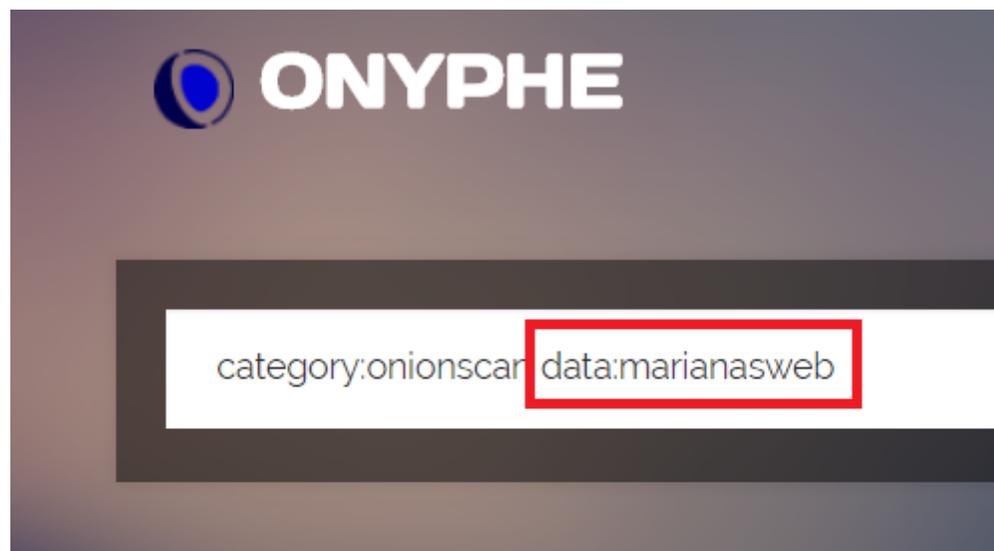
OPENBAAR MINISTERIE  POLITIE  EUROPOL

 HESSEN  Bundeskriminalamt  LIETUVOS POLICIA   U.S. Department of Justice

# Il y a aussi des justiciers



# Et le Marianas Web ? Il est classé ?



Returning **2** result(s) out of 2 in 0.035 second(s)

Le voilà ...



**ACCESS THE SHADOW WEB**

shadowznwuiugi7w.onion

# 1 - Shadow Web is a myth or true

**ANSWER: IT IS TRUE**

# Mais il y a vraiment des tueurs à gage ?

A screenshot of a web browser displaying a website for a private military company. The browser's address bar shows a redacted domain name followed by ".onion". The website features a background image of a black cobra snake on a dark, textured surface. The text on the page includes a redacted name, the phrase "Private military company", and a description: "is a independent Private Military Company formed by ex military corps and ex special forces. We operate worldwide." Below this, it states: "We offer these services with total maximum-privacy. Prices varies case by case. You must ask." A red-bordered box highlights a list of services:

- Killing people**
- Kill common people
- Kill important people (without bodyguards)
- Kill very important people (with bodyguards)
- Kill a big boss (with many bodyguards)
- Kidnapping**
- Kidnapping common people
- Kidnapping important people
- Kidnapping very important people (with bodyguards)
- Stealth Work**
- Murder that seems an accident
- Sabotage (house, car, etc.)

# Les *Hidden Services* sont-ils bien cachés ?

Ou autrement dit est-il possible de retrouver l'adresse IP d'un site .onion ?

# Est-il possible de retrouver l'IP d'un .onion ?

- Réponse courte : oui
- Plus longue
  - Dans une certaine mesure
  - Basé sur des erreurs de configuration



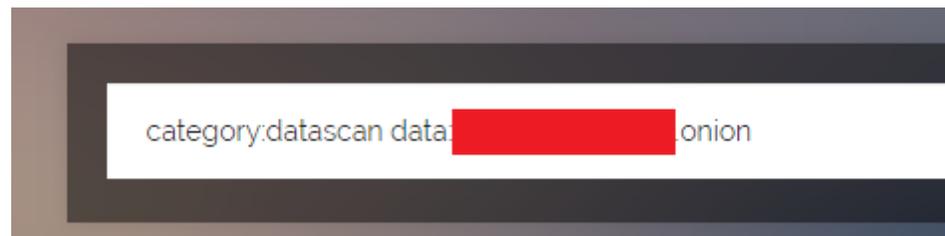
# Où comment retrouver l'IP d'un .onion

Différentes techniques

- Recherche dans les bannières clear Net
  - Site *.onion* affiché dans une bannière (SMTP, par exemple)
- Fuite d'information
  - Apache *mod\_status* - `/server-status`
  - Apache *mod\_info* - `/server-info`
- Certificats X.509
  - Sur le clear Web
  - Sur le Dark Web
- Corrélation entre scan du Dark Web et du clear Web
  - Exposition du serveur Web
    - sur *l'onionland*
    - et sur l'Internet

# Ou comment retrouver l' IP d'un .onion

Recherche dans les bannières clear Net



# Ou comment retrouver l'IP d'un .onion

Recherche dans les bannières clear Net

```
cpe cpe:/a:exim:exim:4.86
data 220 [REDACTED].onion ESMTTP Exim 4.86_2 Ubuntu Tue, 12 Mar 2019
250-[REDACTED].onion Hello <hostname> [<srcip>]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
datamd5 2efdc509c6c5e57b12834e9e6bcd14e4
device { class => "Email Server" }
domain [REDACTED].org
host [REDACTED]
hostname [REDACTED].org
ip [REDACTED].42
ipv6 false
location 52.3824.4.8995
organization WorldStream B.V.
```

# Où comment retrouver l'IP d'un .onion

Fuite d'information

- Modules Apache de supervision
  - *mod\_status* & *mod\_info*
- Exécution de requêtes GET sur tous les sites du Dark Web
  - Mais qui peut laisser passer une erreur pareil ?

| Slot    | Client                        | Protocol | VHost                       | Request  |
|---------|-------------------------------|----------|-----------------------------|--|
| 3103.65 | [REDACTED]4d:ae03:a890:286d:7 | http/1.1 | www.torproject.org:443      | GET /static/images/circle-pattern.png HTTP/1.1 |
| 3176.51 | [REDACTED]10                  | http/1.1 | 2019.www.torproject.org:443 | GET /images/tbb-bgrad.png HTTP/1.1             |
| 3271.46 | [REDACTED].165                | http/1.1 | www.torproject.org:443      |  |
| 3065.56 | [REDACTED]00::14              | http/1.1 | aus1.torproject.org:443     | GET /torbrowser/update_3/release/WINNT_x86_6   |
| 3168.76 | [REDACTED].18                 | http/1.1 | www.torproject.org:443      | GET /static/images/tb85/tb85@2x.png HTTP/1.1   |
| 3084.97 | [REDACTED]20                  | http/1.1 | www.torproject.org:443      | GET /static/images/circle-pattern.png HTTP/1.1 |
| 3119.99 | [REDACTED].163                | http/1.1 | aus1.torproject.org:443     | GET /torbrowser/update_3/release/WINNT_x86-gc  |
| 3214.90 | [REDACTED]9:160:dead:beef:ca  | http/1.1 | aus1.torproject.org:443     | GET /torbrowser/update_3/release/WINNT_x86-gc  |

# Ou comment retrouver l' IP d'un .onion

Fuite d'information



|                |       |          |
|----------------|-------|----------|
| /              | 4,860 | (91.27%) |
| /server-status | 442   | (8.30%)  |
| /server-info   | 23    | (0.43%)  |
| Other          | 0     | (0.00%)  |

# Ou comment retrouver l' IP

Certificats X.509

- Recherche de tous les *Top-Level-Domains*
  - de type *onion*
  - ayant activé SSL/TLS

```
category:datascan tls:true tld:onion -since:7M
```

Returning 10 result(s) out of 174 in 8.632 second(s)

Page > 1 2 3 4 5 6 7 8 9 10

```
@category    datascan
@timestamp   2019-03-28T09:21:05.000Z
@type        doc
```

```
{
  extract => {
    domain => [redacted]
    file => [redacted]
    hostname => ["redacted"]
    url => [
      "https://redacted",
      "http://redacted",
      "https://redacted"
    ],
  },
}
```

# Où comment retrouver l'IP d'un .onion

Corrélation entre scan du Dark Web et du clear Web

- Exposition du serveur Web
  - Sur *l'onionland*
  - Et sur l'Internet
- Une syntaxe pour interroger l'API **ONYPHE**
  - Splunk-like
  - Outil disponible sur *Github* - <https://github.com/onyphe>

```
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
```

# Demo

En vidéo, moins de risques 😊

# Où comment retrouver l'IP d'un .onion

Corrélation entre scan du Dark Web et du clear Web

- Pour certains sites de *l'onionland*
  - C'est *by-design*
  - Majorité des cas

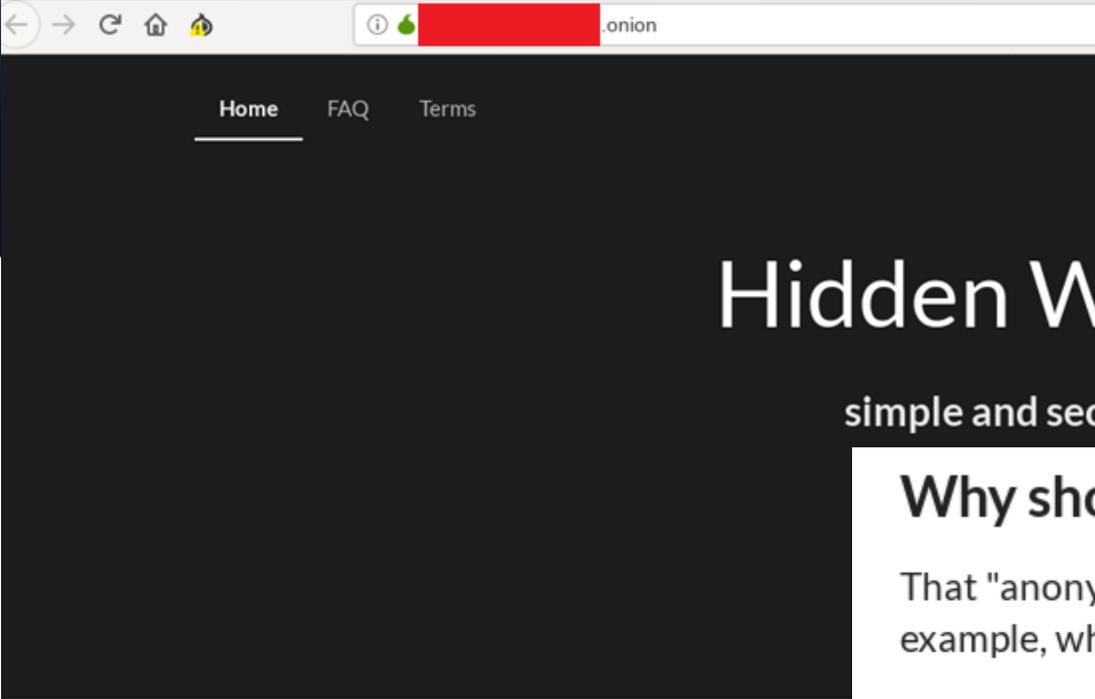


# Ou comment retrouver l'IP d'un .onion

Corrélation entre scan du Dark Web et du clear Web

- Mais pour une minorité, c'est une faille
  - exemple avec un site de *Wallet* « anonyme »





l' IP d'un .onion  
du clear Web

### Why should you choose us?

That "anonymity" is easily destroyed when you deal with Bitcoin Exchanges for example, which know your real identity.

Most of the Bitcoin Exchange services comply with AML and KYC policies so it's really hard to be anonymous to government agencies when dealing with bitcoins.

Hidden wallet is the most popular an  
to build a more open, anonymous, a

Hidden Wallet helps you break that chain since it's hosted on Tor, noone knows who you are because we don't comply to any AML or KYC policies, so we can't be forced to reveal our users informations.

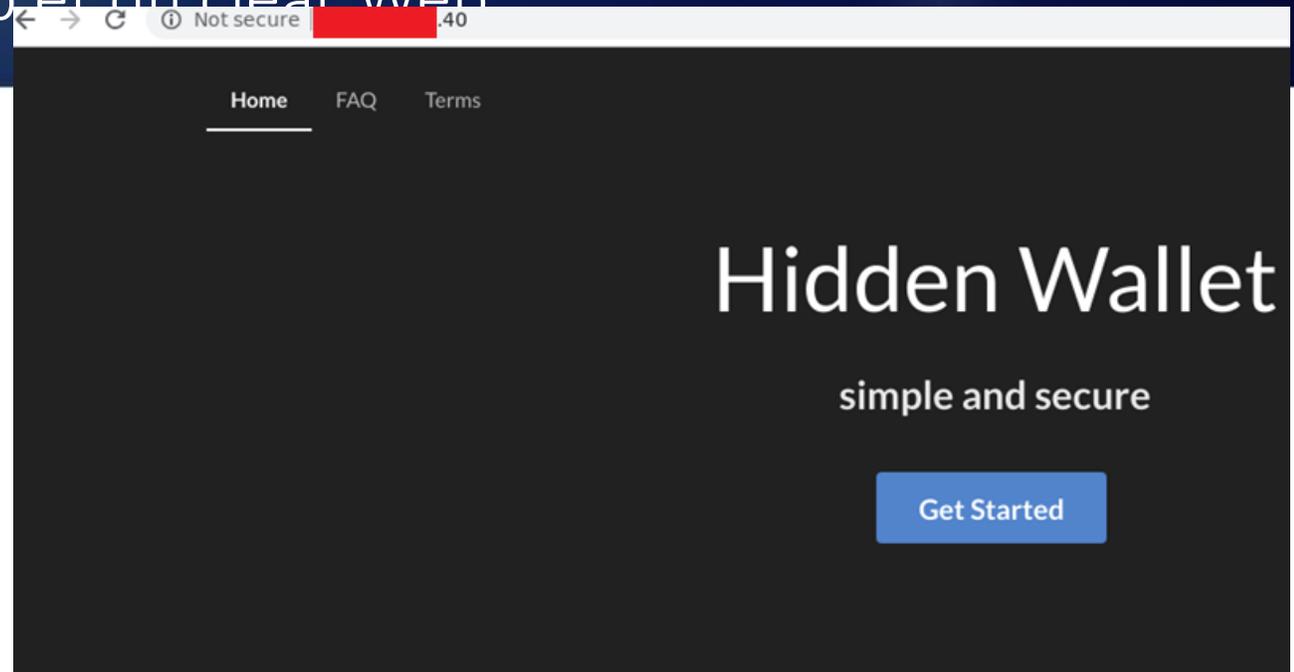
Bank-grade security for your Bitcoin.



# Ou comment retrouver l'IP d'un .onion

Corrélation entre scan du Dark Web et du clear Web

- Connexion avec un navigateur
  - sur l'adresse IP
- C'est bien le même site
- Démasquage possible
  - **5% de tous les .onion**



Hidden wallet is the most popular anonymous wallet on the de  
to build a more open, anonymous, and fair financial future int  
software.

# Ou comment retrouver l' IP d'un .onion

Corrélation entre scan du Dark Web et du clear Web

- Et si c'est une IP protégée par Cloudflare ?

```
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
```

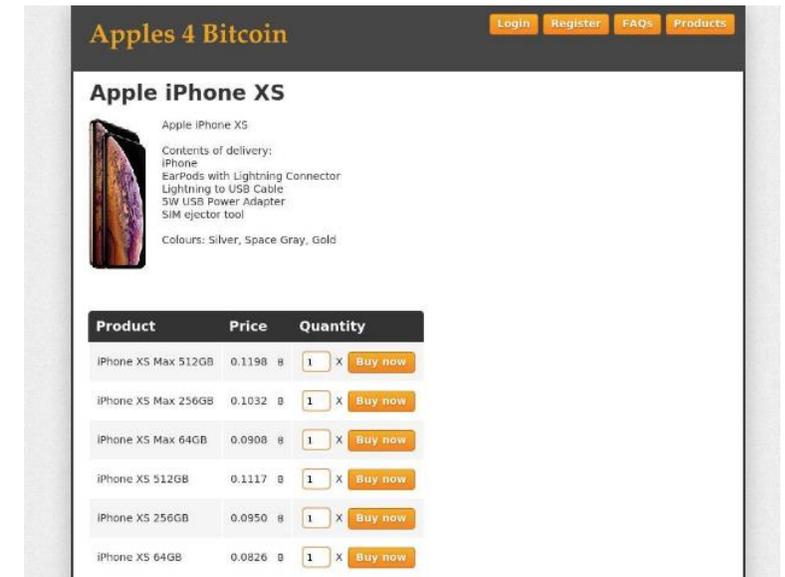
# Capter le Dark Web

Faire des captures écran de tous les sites pour garder une trace

# Capturer le Dark Web

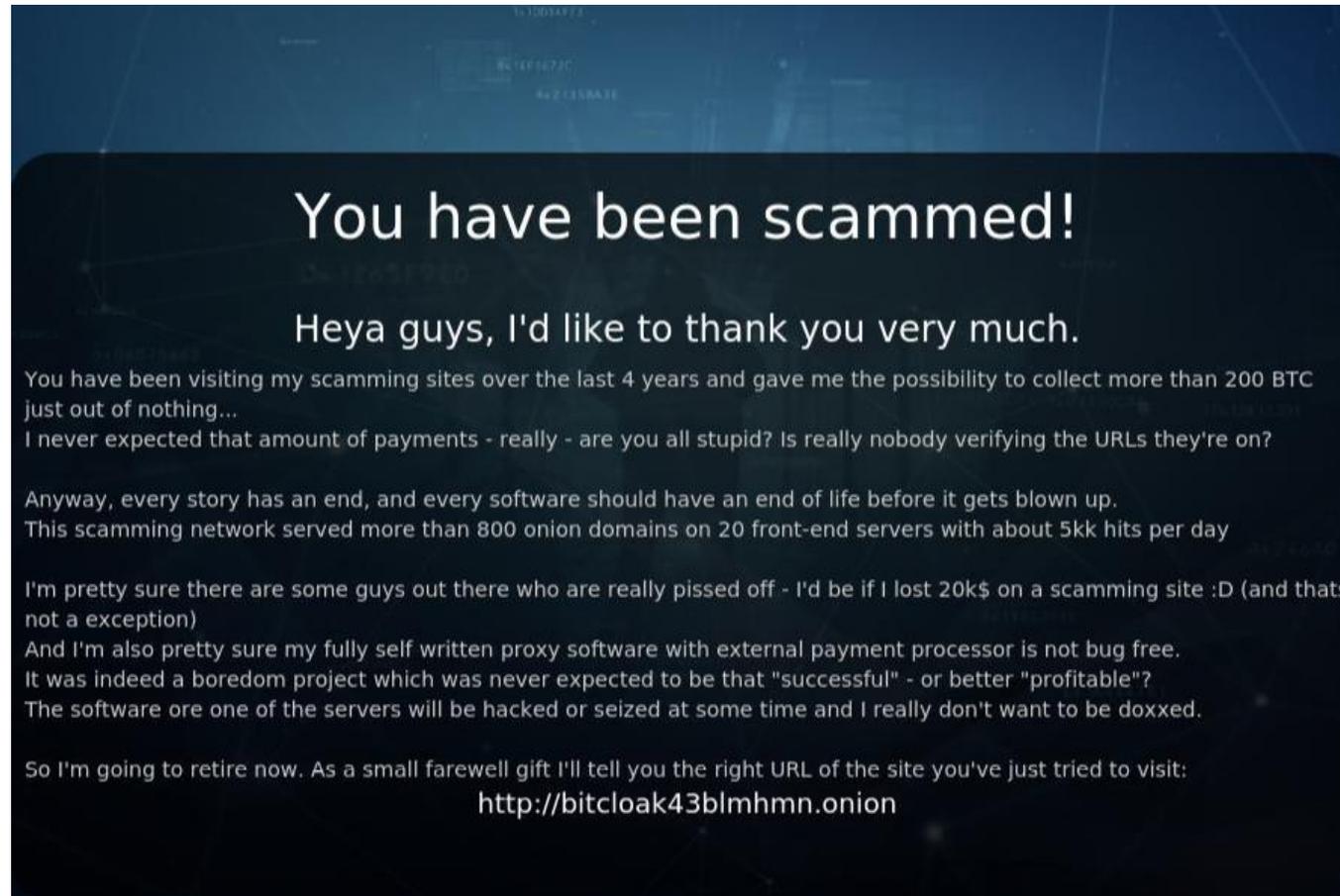
## Méthode éthique

- Faire une capture écran de chaque site .onion
  - Garder une trace visuelle
  - Accessible uniquement aux entreprises
  - 1 fois par semaine
- Protéger l'accès aux sites classés *CP*
  - Uniquement accessibles aux forces de l'ordre
  - Ne pas participer au partage d'information
- Combinaison
  - Algorithme de classification automatique
  - Validation visuelle humaine



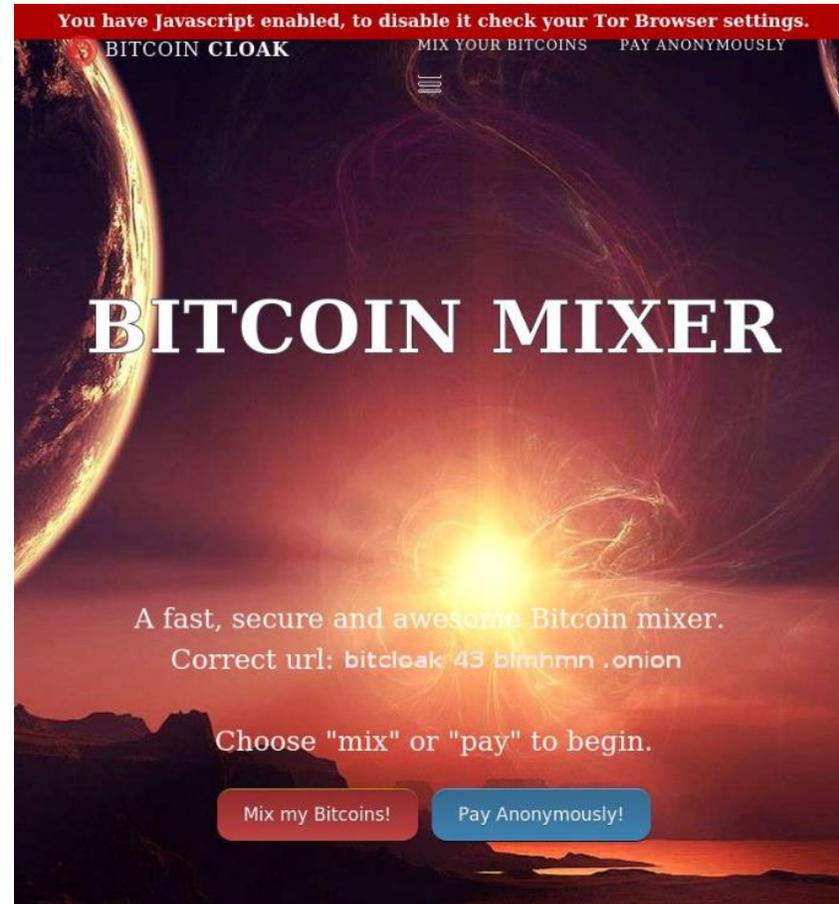
# Capturer le Dark Web

You have been scammed!



# Capturer le Dark Web

You have been scammed!



# Capturer le Dark Web

You have been scammed!

```
category:onionscan data:"you have been scammed" -since:7M -distinct:onion
```

464

# Capturer le Dark Web

Le loto



16DUQRxWUB65vcotfyVZCGAqActPtdrUvE

theonionlotto@sigaint.org

## How to play:

Send a payment of 0.002 BTC to **16DUQRxWUB65vcotfyVZCGAqActPtdrUvE** then send an email to containing the address that you made the payment with. We will match the address you provide with the address that made the payment for verification.

### ■ How are the winners selected?

One of the members of our team **has made a randomizing program** that will select one of the addresses that purchased a ticket and give them a percentage of the total spent on tickets. It will do it up to 3 times, only leaving 0.1% of the total spent on tickets.

### ■ Is it secure?

**No names or personal information are taken or released.**

### ■ How will I know if I won?

**You will receive a significant amount of BTC in your wallet, and we will send you an email with the amount won.**

### ■ Why do you do this?

We do this so we can help **stimulate the BitCoin economy** while helping our beloved friends around the world make some easy money.

# Capturer le Dark Web

Le loto ; encore

The screenshot shows a dark-themed advertisement for a lottery. At the top, the text '222Lotto' is displayed in large, 3D-style letters, with '222' in yellow and 'Lotto' in red. Below this, a yellow banner contains the text 'Participate for ONLY 0.001 BTC!!'. Underneath the banner, it says 'YOU CAN WIN +1.8072 BTC!'. A section titled 'But... How?' in red text is enclosed in a dashed border. Inside this section, it instructs to 'Send 0.001 BTC to' followed by the Bitcoin address '136i2jEoAnw8a4AMTksf7x1jZt9V1GBLkf'. Below the address is a QR code. In the top right corner of the screenshot, there is a small white box containing the text '23:5' and '1'. On the left side of the screenshot, there is a partial view of a smartphone screen with the text 'Products or coins' visible.

# Capturer le Dark Web

Services de hacking



**CISSP, CEH, GIAC, and multiple other industry certifications**



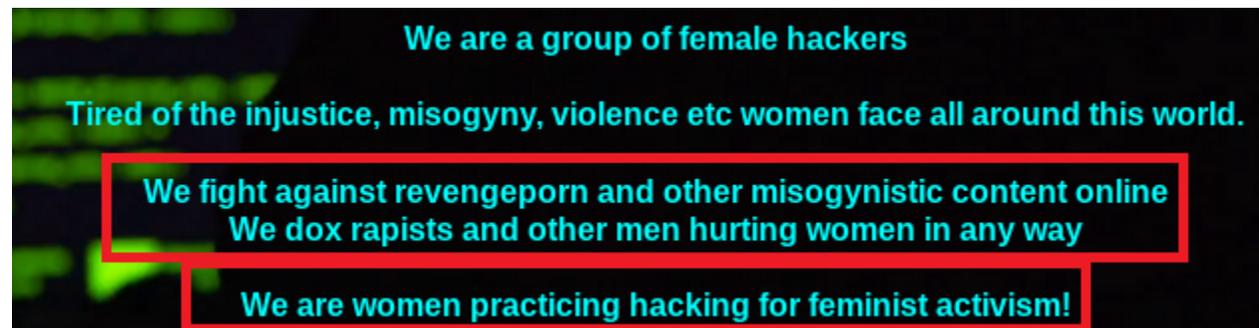
**Blackhat experience 15+ years**



**University degrees in Computer Security & Computer Science**

# Capturer le Dark Web

Les féministes justicières



# Capturer le Dark Web

NDDL ...

**WIR SIND ALLE INDYMEDIA. WIR SIND ALLE LINKSUNTEN!**  
LINKSUNTEN.INDYMEDIA.ORG

# Solidarity

*dont hate the media, become the media.*

**pour PUBLIER cliquez ici**

ACCUEIL NEWS AGENDA BRÈVES ZINES GROUPES AMI-E-S INTIMITÉ ((( ))) Rechercher

## Invitation à nous rejoindre

Mis a jour : le jeudi 14 mars 2019 à 13:20 par zad NDDL



Pour un jour ou pour toujours, sur la ZAD de Notre Dame des Landes !

Nous vous invitons dès à présent à nous rejoindre sur place entre l'Est, La Grée, le Rosier, la Wardine et Bellevue, puis particulièrement à partir du 6 avril, pour lancer des chantiers de constructions, plantations, discussions et bien plus...

| Plus →

## [Expulsions en cours ZAD] 2ème journée

Mis a jour : le mercredi 13 mars 2019 à 15:36



Pour le 2ème journée consécutive les flics sont sur la ZAD et expulsent et détruisent des lieux Hier, YoupiYoupi2, Lama Fâché et une plateforme ont ét... | Plus →

## [Nantes] Rassemblement contre les expulsions

Mis a jour : le lundi 4 mars 2019 à 23:08



Le jeudi 7 mars 2019 à 9h au TGI (19 Quai François Mitterrand) Depuis le 26 octobre 2018, le gymnase du lycée Jeanne Bernard, à Beauséjour, est réquisit... | Plus →

## Local

- [COMPTE-RENDU ACTE XIX - NANTES - Samedi 23 Mars 2019] le 23 mar 2019 à 20:52
- [nantes] rapide c.r Gilets Jaunes route de vanes - samedi 23 mars 2019 - "" contrôle abusif et arbitraire "" le 23 mar 2019 à 17:35
- 8 mars à Bordeaux le 19 mar 2019 à 11:52
- soutien aux occupantEs suites aux dernières destructions le 19 mar 2019 à 10:25
- [Repression judiciaire Nantes] Compte-rendu des comparutions immédiates du 18/02/2019 le 18 mar 2019 à 21:52
- #Nantes: INCERTAIN FUTUR (confusionnisme quand tu nous tiens...) le 16 mar 2019 à 19:12
- Caen, France : Rien n'est fini... le 16 mar 2019 à 00:49
- Problèmes techniques - zad@riseup ne répond plus le 15 mar 2019 à 02:13
- St Père en Retz: Opération greenwashing sur le Surf Park

## Agenda

- [Turin] Bloquons la ville ! le 30 mar 2019 à 08:00
- [Poitiers] Inauguration de La Grotte, local anarchiste communiste et féministe le 30 mar 2019 à 17:00
- [St Nazaire] Concerts de soutien à la maison du peuple le 30 mar 2019 à 20:00
- [Nantes] Café Medic, le troisième ! le 5 avr 2019 à 17:00
- [Nantes] Ciné-débat le 9 avr 2019 à 20:30
- [B17] Projection anticarcérale le 12 avr 2019 à 20:00
- RadicalEs de la couture à la soudure - Par et pour

Plus →

## Lieux

Nantes Rennes ZAD  
Notre-Dame-des-Landes  
Angers paris Saint-Nazaire  
Tours Bordeaux Poitiers  
Brest partout france b17 / Bure nddl la Vannes Rezé

# Capturer le Dark Web

Des news du monde

ENGLISH (英文) | 中文 | ESPAÑOL (西班牙语)

纽约时报中文网 国际纵览

The New York Times

紐約時報生活季刊  
The New York Times  
点击阅读网络版

搜索纽约时报 搜索

2019年3月25日星期一 北京时间 18:37 更新

简体 | 繁體

首页 国际 中国 商业与经济 镜头 科技 科学 健康 教育 文化 时尚 旅游 房地产 观点与评论 时报普利策获奖作品

## 黄金地段 无敌景观

GALERIE

新闻分析

### 特朗普摆脱最大阴云

#### 穆勒调查未发现“通俄”意味着什么

PETER BAKER 16:12

报告结论根除了弹劾总统的威胁，为他任期的最后22个月甚至连任竞选提供了助推。民主党将处于守势，但他们将努力迫使司法部交出完整报告和关键证据。

### 中国承诺开放经济，以期结束贸易战

KEITH BRADSHAW 13:12

中国重复了此前的承诺，如加大金融领域对外资的开放力度等。特朗普则表示，美



Dale De La Rey/Agence France-Presse — Getty Images

香港的高楼大厦。根据香港差饷物业估价署的数据，从2018年7月到12月，住宅价格降低近10%。

观点与评论 • OPINION

### 别再用可爱来“赞美”亚裔女性

R.O. KWON

为何那些进步人士不觉得在工作场合评价一个亚裔女性的外貌是一种种族歧视？如果有人跟你探讨她的工作，请不要说她可爱。



### 中国的“金钱舞曲” (漫画)

HENG

当蔡英文前往南太平洋邦交国访问，试图拉拢仅存的盟友，习近平“金钱外交”的诱惑也正在发挥作用。台湾的国际生存空间进一步缩小。



### FBI前局长：我不希望特朗普被弹劾或罢免

# Capturer le Dark Web

Lancer des alertes



The screenshot shows the Whistleblower Aid website. At the top left is the logo "WHISTLEBLOWER AID" with a stylized eye icon. At the top right is a hamburger menu icon. The main content area features a dark blue background with a central white text box containing the headline "Report Government & Corporate Lawbreaking. Without Breaking The Law." Below this, a smaller white text box states "WHISTLEBLOWERS ARE MORE IMPORTANT THAN EVER IN KEEPING OUR NATION UNIFIED UNDER THE RULE OF LAW." A prominent red button with the text "CONTACT LAWYERS FIRST" is centered below the text. At the bottom center, there is a circular orange play button icon with the text "Watch Video" underneath it.

# Capturer le Dark Web

La blockchain \o/

## Wownero Blockchain Explorer

(no cookies - no web analytics trackers - no images - open sourced)

Server time: 2019-03-25 12:05:16 | Transaction pool | Transaction pusher | Key images checker | Output keys checker  
Network difficulty: 242000000 | Hard fork: v12 | Hash rate: 806.666 kH/s | Fee per byte: 0.00000107459 | Median block size limit: 292.97 kB  
Wownero emission is 15447708.201 (9822.115 fees) as of 91707 block

### Transaction pool

(no of txs: 16, size: 49.77 kB, updated every 5 seconds)

| age<br>[h:m:s] | transaction hash  | fee/per_kB<br>[µg] | in/out/pID | tx_size<br>[kB] |
|----------------|---|--------------------|------------|-----------------|
| 00:02:29       | 039195d9a3f35e9cleab80f5743b1aa786a263b5e7bb921da1b8ac023d1f35b1  | 7815/3072          | 1/2/e      | 2.54            |
| 00:02:29       | 289c8a27d05ca3ec91149c071dae19378c2cac750952ec9063c74bf4bcaa7ed   | 7815/3072          | 1/2/e      | 2.54            |
| 00:02:30       | f93ce4eb8ed921a3341bb7dae87148639b1f48c143874a66d9259d108f248798  | 7803/3072          | 1/2/e      | 2.54            |
| 00:02:30       | 292231ffb7b4e87cbf81d4935039fe2bf79c046b57345c109d265229387bddd2  | 7824/3072          | 1/2/e      | 2.55            |
| 00:02:31       | a7222d001468974eafbb86bc28e1c07d908a2baa996dfcecf693a7109a6f58    | 12465/3072         | 2/2/e      | 4.06            |
| 00:02:31       | e5914940629f8cbad22f75070f1f9e4ea3b9c803629b80de64adbea006afc4e9  | 12480/3072         | 2/2/e      | 4.06            |
| 00:04:31       | b3d67cc16344d1c0449d266bec3e9eb1ad9a8c85b95c04be26dd7e3b6f5e304b  | 7821/3072          | 1/2/e      | 2.55            |
| 00:04:31       | f83e73b9c6a9afd296b3cf3145c1726563cf38c14abf22544ce8654dc1cb84a7  | 7809/3072          | 1/2/e      | 2.54            |
| 00:04:51       | 0a5d7be781476450fa1df67800a0201eca7d23d066c0b5e7cb79503cc26633b8  | 12462/3072         | 2/2/e      | 4.06            |
| 00:04:55       | 9b84a7834ab3235a731e18d44ecd6d6ca8b576fca3d9588d3c47fd2b3b928a8   | 7809/3072          | 1/2/e      | 2.54            |
| 00:04:58       | fae9bd665d33cd0dfd37acbabb755f27af2cf671ba03b5080863abc950f82d213 | 7812/3072          | 1/2/e      | 2.54            |
| 00:05:02       | 55aeffd9c5d96e3a0a475052adc278aac1a8529078740b23714384dad41b71fe  | 7824/3072          | 1/2/e      | 2.55            |
| 00:05:06       | 09a2789fee01103ea48f38c6595afb840a54c0d933333af1c71deaf8f8a2e930  | 7794/3072          | 1/2/e      | 2.54            |
| 00:05:09       | 24f44e9c614271413224a890538b5c29ef564f829663daaec35aab187e5fa245  | 12444/3072         | 2/2/e      | 4.05            |
| 00:05:13       | 692640dfee49052bd9f0a08b90e6b21120cdd84d23549653472ab36b7496258   | 12459/3072         | 2/2/e      | 4.06            |
| 00:05:17       | 6dc4db95ec40d2f7193056ebb2f05a4e902eb93f1c7709ec2de1f7bfb70a71e   | 12468/3072         | 2/2/e      | 4.06            |

### Transactions in the last 11 blocks

(Median size of 100 blocks: 292.97 kB)

# Capturer le Dark Web

Un dernier pour la fin

## **Attention!**

You have reached the very last of the onion servers.

We hope you have enjoyed your browsing.

Now turn off your computer and go outside and play!

# Merci.

Twitter: @onyphe, @PatriceAuffret

Github : <https://github.com/onyphe>

Register: <https://www.onyphe.io/login/#register>

Pricing: <https://www.onyphe.io/pricing>

