

DÉMYSTIFICATIONS LES DARKNETS



CSIRT
BOURGOGNE-FRANCHE-COMTÉ

RÉGION
BOURGOGNE
FRANCHE
COMTÉ

Soutenu
par



**RÉPUBLIQUE
FRANÇAISE**
*Liberté
Égalité
Fraternité*



QUI SOMMES-NOUS?



Un CSIRT en BFC

- 🕒 **Le CSIRT-BFC est le centre régional de coordination des différents acteurs et des moyens en cas de cyberattaque**
- 🕒 **Il va organiser la réponse à l'incident**
- 🕒 **Il a également des rôles d'alerte, de sensibilisation et d'animation de la filière**
- 🕒 **Il a été créé via une convention tripartite : ANSSI, Région et ARNia**

Cyber-résilience : un écosystème structuré

Un écosystème national à 3 niveaux

Cybermalveillance.gouv.fr

Tout le monde

Plateforme Web

CSIRT-BFC

Etablissement public,
PME, ETI, association

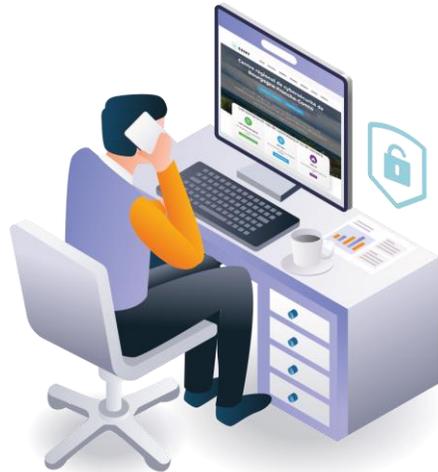
Plateforme
téléphonique

CERT-FR

Région, département,
métropole, OIV, OSE

Plateforme
téléphonique

Centre régional de cybersécurité CSIRT BOURGOGNE-FRANCHE-COMTÉ



**Vous êtes victime
d'une cyberattaque ?**

Collectivités, organismes
publics, PME, ETI et
associations nationales
à ancrage régional
de Bourgogne-Franche-Comté.

0970 609 909
(appel non surtaxé)

Consultez notre site
www.csirt-bfc.fr

Le CSIRT-BFC assiste les victimes de cyberattaques en coordonnant les acteurs et les moyens : vers des **prestataires** pour la remédiation, vers les **forces de l'ordre** (Gendarmerie, Police) pour le dépôt de plainte, vers la **CNIL** en cas de violation de données à caractère personnel et l'**ANSSI** pour le suivi de l'incidentologie. Le CSIRT-BFC **alerte et sensibilise aux bonnes pratiques** en matière de cybersécurité.

Une mission
de service
public
créée par

RÉGION
BOURGOGNE
FRANCHE
COMTÉ

Soutenu
par

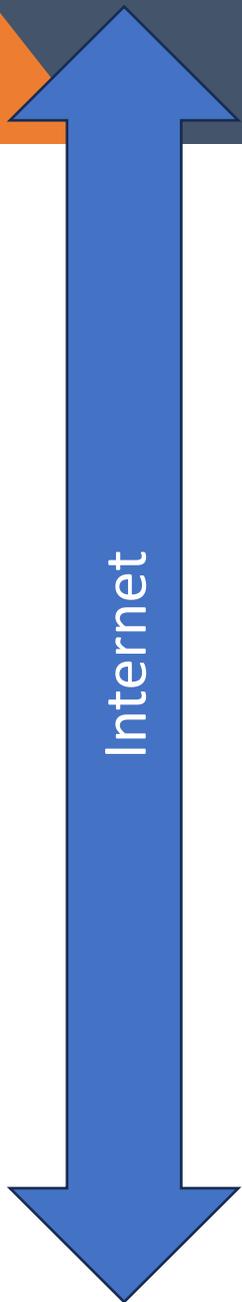
RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité



DÉMYSTIFICATIONS DARKNETS

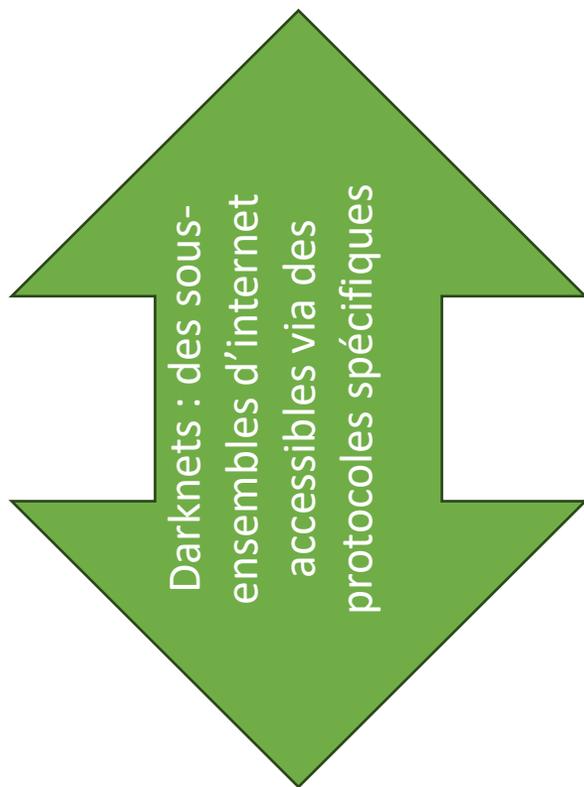
LES





Web (dit de surface), ce qui est référencé par un moteur de recherche car librement accessible.
Exemple : csirt-bfc.fr, elysee.fr etc...

Deep Web (web profond), ce qui n'est accessible par un moteur de recherche mais accessible via une authentification, par exemple.
Exemple : compte bancaire, espace client etc...

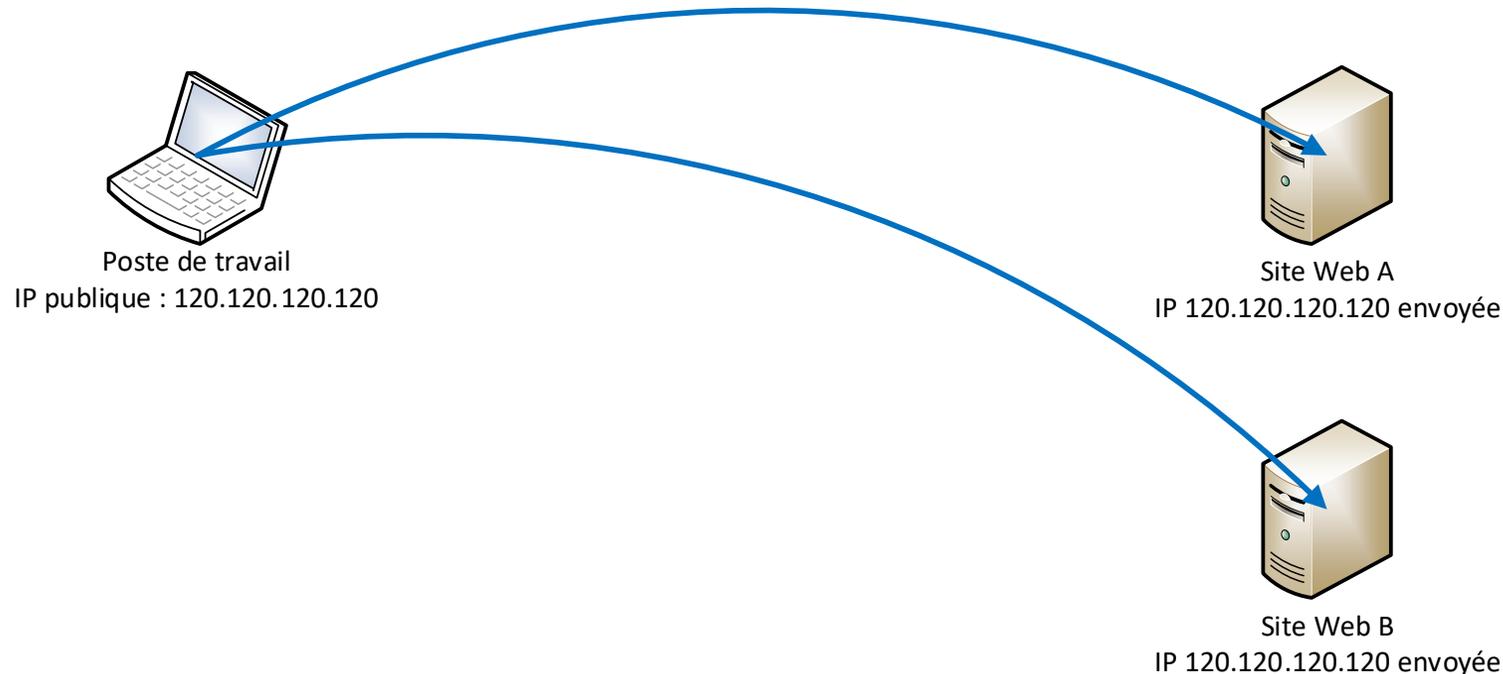


Deep web (web caché), ce qui est accessible avec un navigateur mais dans un darknet

Démystifions les darknets

🕒 **Principe 1 : comme dans la vie réelle où une maison dispose d'une adresse postale, sur le réseau internet, tout équipement est accessible par une adresse réseau, dit adresse IP (ex : 127.0.0.1).**

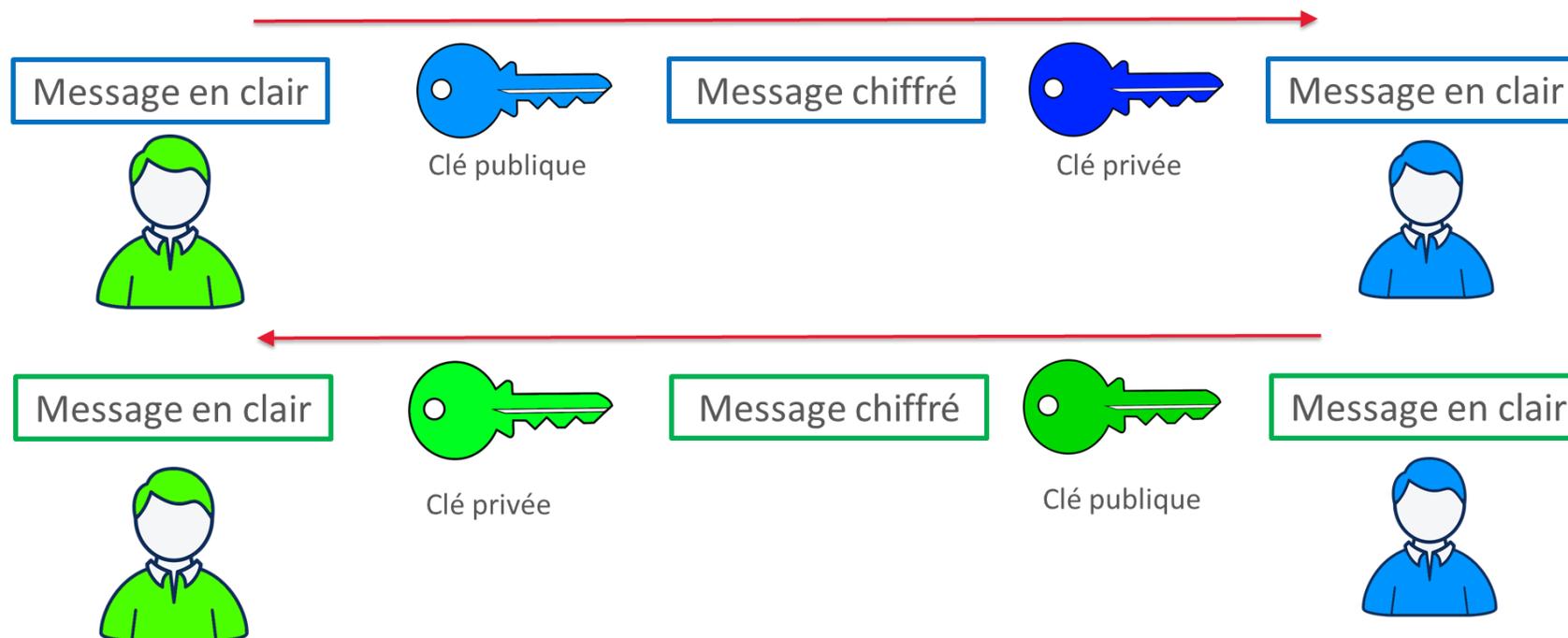
🕒 **Cette adresse est communiquée au site auquel vous accédez**



Démystifions les darknets

🕒 Principe 2 : il est possible d'utiliser un jeu de clés publique/privée pour chiffrer des données.

🕒 La clé publique sert à chiffrer les données que seule la clé privée associée peut déchiffrer



Démystifions les darknets

☺ Il existe de nombreux darknets dont la principale caractéristique est que l'ensemble des échanges est chiffré par défaut :

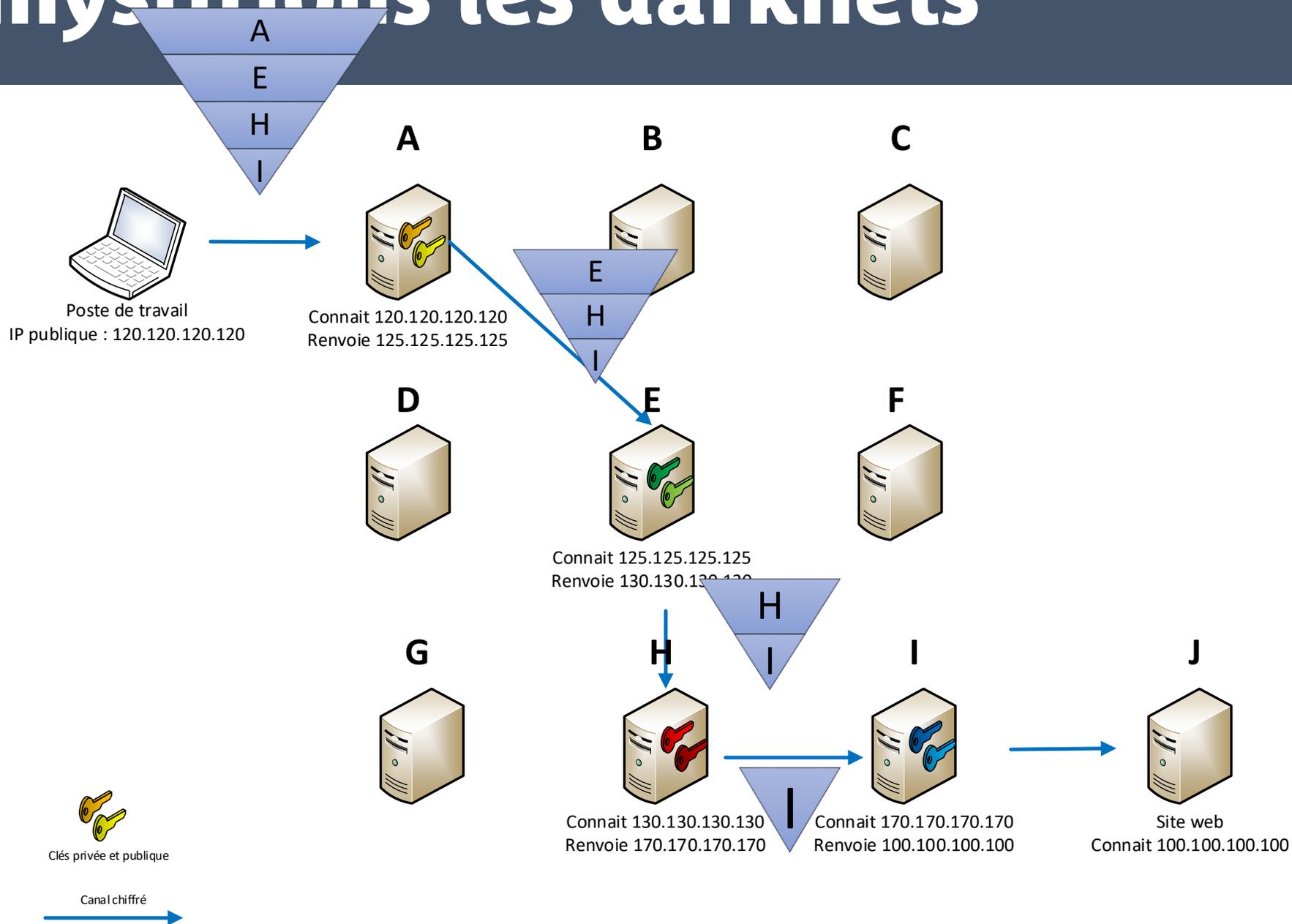
- Dans les darknets, ce n'est pas votre IP qui est proposée mais une autre, celle d'un des nœuds du réseau.
- Afin de renforcer la difficulté à remonter à la source, les flux réseaux passent par plusieurs serveurs et sont chiffrés.

☺ Le réseau le plus connu est TOR (ou réseau en oignon)

- Chaque serveur du réseau Tor dispose d'une clé privée et d'une clé publique. Chaque clé publique est copiée sur tous les serveurs du réseau. Une clé publique permet de chiffrer un message.

☺ Chaque serveur du réseau Tor a la liste de tous les autres serveurs formant le réseau.

Démystifions les darknets



Démystifions les darknets

🕒 Exemple

- Quand le poste de travail souhaite aller sur le serveur J, il établit un chemin aléatoire entre tous les serveurs du réseau Tor.
- Une fois la liste des serveurs établie, il utilise la clé publique dernier serveur (I) pour chiffrer les données. Le résultat est lui-même chiffré par la clé publique l'avant dernier serveur (H) et ainsi de suite jusqu'au serveur A. Chaque chiffrement peut être vu comme une couche, comme une couche d'un oignon, d'où le nom du réseau.
- Le cryptogramme peut ainsi transiter, il va vers le serveur A où il sera déchiffré avec sa clé privée, ce sera la première couche de l'oignon à être supprimée et ainsi de suite.

🕒 Environ **10000** serveurs dans le réseau Tor -
<https://www.dan.me.uk/tornodes>

Démystifions les darknets

🕒 Se connecter au réseau Tor:

- Utiliser un VPN afin de masquer son IP à l'entrée du réseau Tor
- Utiliser le navigateur Tor Browser

🕒 On est connecté au réseau Tor. L'accès à des services du réseau se fait avec des adresses suffixées en .onion

- Ex : lockbitapt2yfbt7lchxejug47kmqvqqxvvpqkmevv4l3azl3gy6pyd.onion

🕒 La navigation se fait comme sur le web classique, en cliquant sur des liens.

🕒 La difficulté est de trouver les sites qui ne sont pas référencés dans les moteurs de recherche classiques

Démystifions les darknets

 **Démonstration**

Démystifions les darknets

Dark Web Hackers

[Products](#) [Register](#) [Login](#)

Welcome to the Dark Web Hackers

Have you tried to buy hacking services on the dark web before? Not happy with the results? Only empty promises but no one getting the job done?

Then you should try Vladimir and George, the dark webs most trusted hackers for getting things done.

Unlike others, our prices are not the cheapest, but if we can't do a job, you will get a full refund!

Vladimir



Hello, my name is Vladimir.
I am the technical expert at dark web hackers.

My expertise is programming, running exploits, setting up DDOS attacks and i like the challenge of doing things where most others give up.
I can "recover" passwords of most social networks easily, remote control smartphones, and most other things that are useful because i spent years to find methods that really work.

Here you can find a list of my services, if it is not listed, then minimum price will be \$600 and we will discuss the final price once you gave me all information and i accept the job.

Product	Price	Quantity
Remote control the phone of someone else, most new models supported	700 USD = 0.01662 ₿	<input type="text" value="1"/> X Buy now
Facebook and Twitter account hacking	500 USD = 0.01187 ₿	<input type="text" value="1"/> X Buy now
Other social network account hacks, for example reddit or instagram	450 USD = 0.01068 ₿	<input type="text" value="1"/> X Buy now
Full package deal, getting access to personal or company devices and accounts and searching for the data you need.	1800 USD = 0.04274 ₿	<input type="text" value="1"/> X Buy now

Démystifions les darknets

\$ 100000

Bowden Barlow Law PA

0 7 9 50
DAYS HOURS MINUTES SECONDS

Bowden Barlow Law PA is a company that operates in the Legal Services industry. It employs 6-10 people and has \$1M-\$5M of revenue. The main office of the company is located at 3845 5th Ave N, Saint Petersburg, Florida, 33713, United States

🕒 2023-12-05 03:00:28

1842 👁

PUBLISHED

Chetu

Chetu is an American software development company providing industry—specific software solutions for businesses around the world. The main office is located at 1500 Concord Ter Ste 100, Sunrise, Florida, 33323, United States

Démystifions les darknets

tradewindscorp- insbrok.com 11D 01h 07m 05s Being the Malaysian's leading independent insurance broker and employee benefits consultant, Tradewinds International Insurance Updated: 12 Dec, 2023, 08:04 UTC 873	petrotec.com.qa 11D 01h 09m 56s Petrotec is one of the largest providers of Engineered products and services to the energy industry in Qatar, specializing in key diverse energy-related disciplines of Updated: 12 Dec, 2023, 08:04 UTC 948	kitahirosima.jp 8D 23h 01m 56s 30gb Updated: 13 Dec, 2023, 15:24 UTC 1068	hi- schoolpharmacy.com PUBLISHED Part 2. Hi School Pharmacy has a history founded in the tradition of the classic corner drug store. The original store was opened by Dick Yetman in the early Updated: 11 Dec, 2023, 23:35 UTC 1034
greenbriersportingclub. 6D 04h 38m 23s \$ 99999 The Greenbrier Sporting Club is a private, equity club organized for the purpose of offering memberships to those that own real estate at The Greenbrier. Location Updated: 11 Dec, 2023, 23:28 UTC 984	phillipsglobal.us 1D 04h 19m 15s \$ 49000 It's in our DNA to keep our customers up and running – regardless of their industry segment. Having repaired equipment for many of the world's Updated: 12 Dec, 2023, 17:23 UTC 971	solveindustrial.com PUBLISHED https://mega.nz/folder/8691wJ7Q#pV_QkPAvcRYmGX4myqJ1a/ Updated: 11 Dec, 2023, 22:14 UTC 969	r-ab.de 00h 28m 37s Rieser Aufzugbau GmbH is a company that operates in the Health, Wellness and Fitness industry. It employs 51-100 people and has \$10M-\$25M of revenue. Updated: 11 Dec, 2023, 19:55 UTC 1065
ipp-sa.com 00h 11m 35s IPP S.A. has been producing	citizenswv.com PUBLISHED Part 1. Once again we see how greedy a	zailaboratory.com 17D 14h 23m 57s Our in-house discovery team focuses on	pronatindustries.com 413D 17h 14m 17s PRONAT Industries was hacked. All the

Démystifions les darknets

Deadline: 10 Dec, 2023 17:18:35 UTC



sabre.co.uk

Our company history

Sabre Insurance is one of the most successful insurers in the UK, providing brokers and customers with excellent customer service.

We sell car insurance primarily through brokers but also directly to the public through the Insure 2 Drive, Drive Smart and Go Girl brands, and in 2021 began underwriting motorbike insurance.

Sabre Insurance Company Limited is authorised and regulated by the Financial Conduct Authority and Prudential Regulation Authority. (FRN 202795)

Registered offices are at Sabre House, 150 South Street, Dorking, Surrey RH4 2YY and the Company registration number is 2387080. VAT registration number is 793 7283 81.

UPLOADED: 20 NOV, 2023 21:35 UTC

UPDATED: 10 DEC, 2023 19:01 UTC

EXTEND TIMER FOR 24 HOURS

\$ 10000

DESTROY ALL INFORMATION

\$ 900000

DOWNLOAD DATA AT ANY MOMENT

\$ 900000

1-4 of 6

The screenshot displays a darknet marketplace interface with several product listings. The first listing is for 'Sabre Insurance Group plc (SABRE) (SABRE)', showing a price of \$10,000. The second listing is for 'BDO', priced at \$900,000. The third listing is for 'Firemark', also priced at \$900,000. The fourth listing is for 'RENEWAL INVITATION', priced at \$900,000. Each listing includes a thumbnail image and a brief description of the item.

Démystifions les darknets



LEAKED DATA

- TWITTER
- CONTACT US
- AFFILIATE RULES

- > HOW TO BUY BITCOIN >
- > PRESS ABOUT US >
- > MIRRORS >

**FILES
ARE
PUBLISHED**

Deadline: 25 Nov, 2023 18:07:13 UTC

[no photo]

martinique.no

Martinique is different. Secluded from the light trail around Vågen, this environmental space is located on Nytorget with its distinctive atmosphere. The place is a melting pot of people across professions, age, environment and interests. Here, restless students can find peace

Démystifions les darknets

[Login](#)[Register](#)[Products](#)

Tom and Jerry Store

We have been active during the Agora, Evolution, Silkroad 3 era, then continued through Alphabay and Nucleus, and even the late Dream Market and also Wallstreet, with the same successful concept: High quality drugs combined with an extremely discreet and fast shipping.

Extremely stealth shipping from the netherlands!

High Quality Cocaine [90%]



We offer High Quality Cocaine 90%+ with FREE SHIPPING !
All orders that come in before 14:00 Dutch local time are shipped the very same day !
Shipping internationally!

Product	Price	Quantity
2g High Quality Cocaine	90 EUR = 0.00234 ₿	1 X Buy now
5g High Quality Cocaine	200 EUR = 0.00520 ₿	1 X Buy now
10g High Quality Cocaine	350 EUR = 0.00910 ₿	1 X Buy now

Démystifions les darknets

Amazon Gift Cards



You Only Pay 25% of the Card Value



HOME

GIFT CARDS

HOW TO BUY

ESCROW SERVICE

FAQ

REVIEWS

CONTACT

Amazon Gift Cards - France

Buy a Amazon Gift Card for only 25% of the value.

You can choose between six different amount:
\$100, \$200, \$400, \$600, \$800, \$1000

Amazon France \$100



Use this Gift Card to make purchase on [Amazon France Marketplace](#).

Amazon France \$200



Use this Gift Card to make purchase on [Amazon France Marketplace](#).

Amazon France \$400



Use this Gift Card to make purchase on [Amazon France Marketplace](#).

Démystifions les darknets

UK Guns and Ammo Store

Products Info Login Registration

Guns



Only 3 x P99 and 2 x Glock 19 left, we will get new stock of similar weapons once those are sold.

Product	Price	Quantity
Glock 19 - 9mm - new and unused	500 GBP = 0.01480 B	<input type="text" value="1"/> X Buy now
Walther P99 - 9mm - new and unused	650 GBP = 0.01924 B	<input type="text" value="1"/> X Buy now

Démystifions les darknets

captaingoat@airmail.cc'. A RSS feed icon is also visible."/>

Home Titles Publishers Years Creators Tags Scanners Recent Random Links

Search

Comic Book Library

Total Comics: 3348 Library Updated: 2023/08/05 E-mail: captaingoat@airmail.cc

Démystifions les darknets

Onion Identity Services

[Products](#)[Info](#)[Login](#)[Registration](#)

Order Process:

After buying an ID or passport send us a message with your age and gender so we can find a matching dataset, alternatively you can provide a dataset (name, age, gender, size etc). We will also need a biometric photo in high quality and signature scanned, we will give more instructions after your purchase.

Passports



Product	Price	Quantity
Lithuanian Passport	1350 EUR = 0.03508 B	<input type="text" value="1"/> X Buy now
Netherlands Passport	1500 EUR = 0.03898 B	<input type="text" value="1"/> X Buy now

Merci et contactez-nous !



Pôle Cyber : cyber@arnia-bfc.fr
(PGP : 0x169AB32B)

Sébastien Morey – smorey@arnia-bfc.fr
(PGP : 0xDFB60F1A)

CENTRE RÉGIONAL DE CYBERSÉCURITÉ

BOURGOGNE-FRANCHE-COMTÉ



CSIRT



0970 609 909

(appel non surtaxé)

www.csirt-bfc.fr



DAILYMOTION

