DÉMYSTIFIONS 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

CSIRT
BOURGOGNE-FRANCHE-COMTÉ

Cyber-résilience : un écosystème structuré

Un écosystème national à 3 niveaux

Cybermalveillance.gouv.fr	CSIRT-BFC	CERT-FR
Tout le monde	Etablissement public, PME, ETI, association	Région, département, métropole, OIV, OSE
Plateforme Web	Plateforme téléphonique	Plateforme téléphonique

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

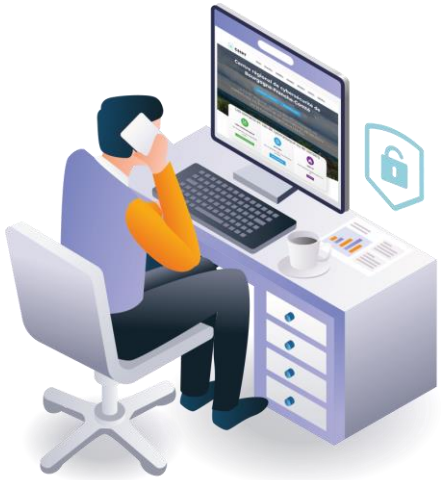
CSIRT
BOURGOGNE-FRANCHE-COMTÉ

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

CSIRT
BOURGOGNE-FRANCHE-COMTÉ

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 assise 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

FRANCE RELANCE

CSIRT BOURGOGNE-FRANCHE-COMTÉ

DÉMYSTIFIONS LES DARKNETS

Internet

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…

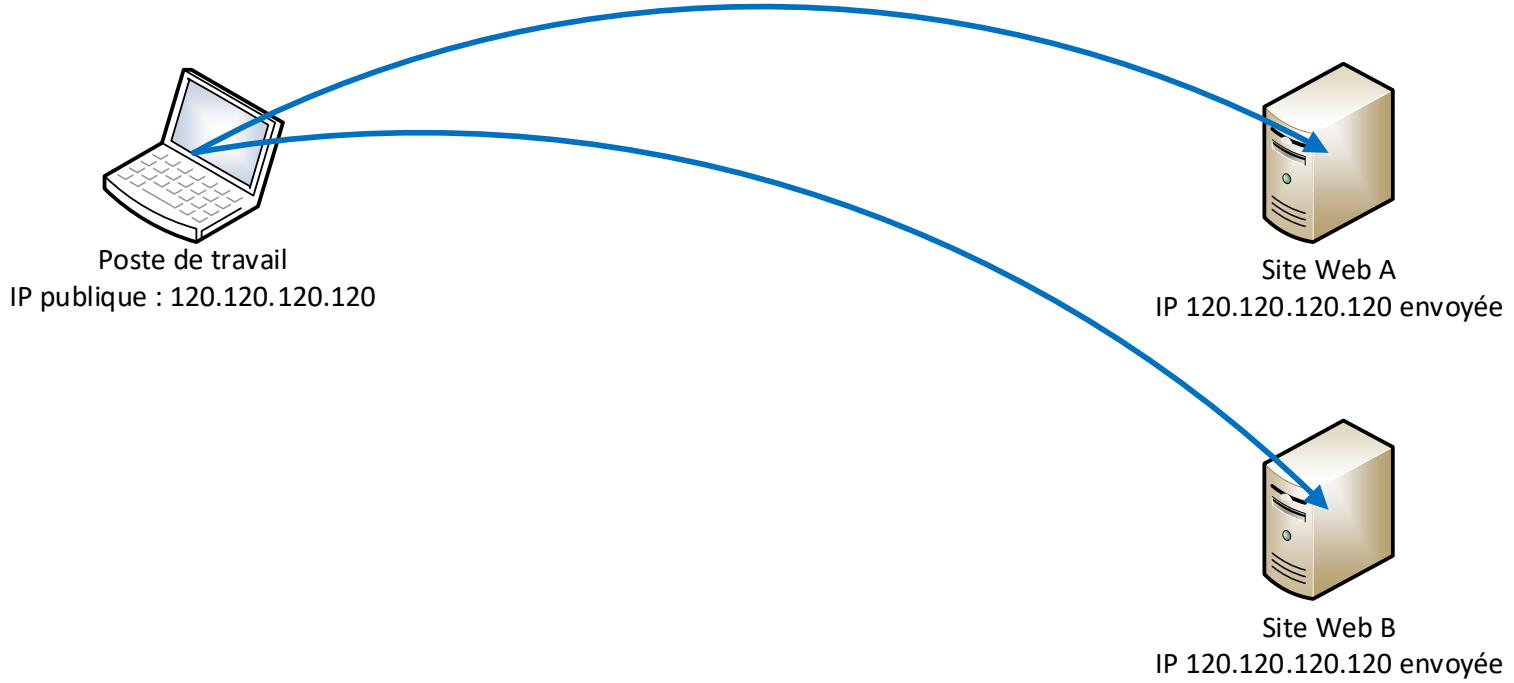
Darknets : des sous-ensembles d'internet accessibles via des protocoles spécifiques

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

CSIRT
BOURGOGNE-FRANCHE-COMTÉ

Démystifions les darknets

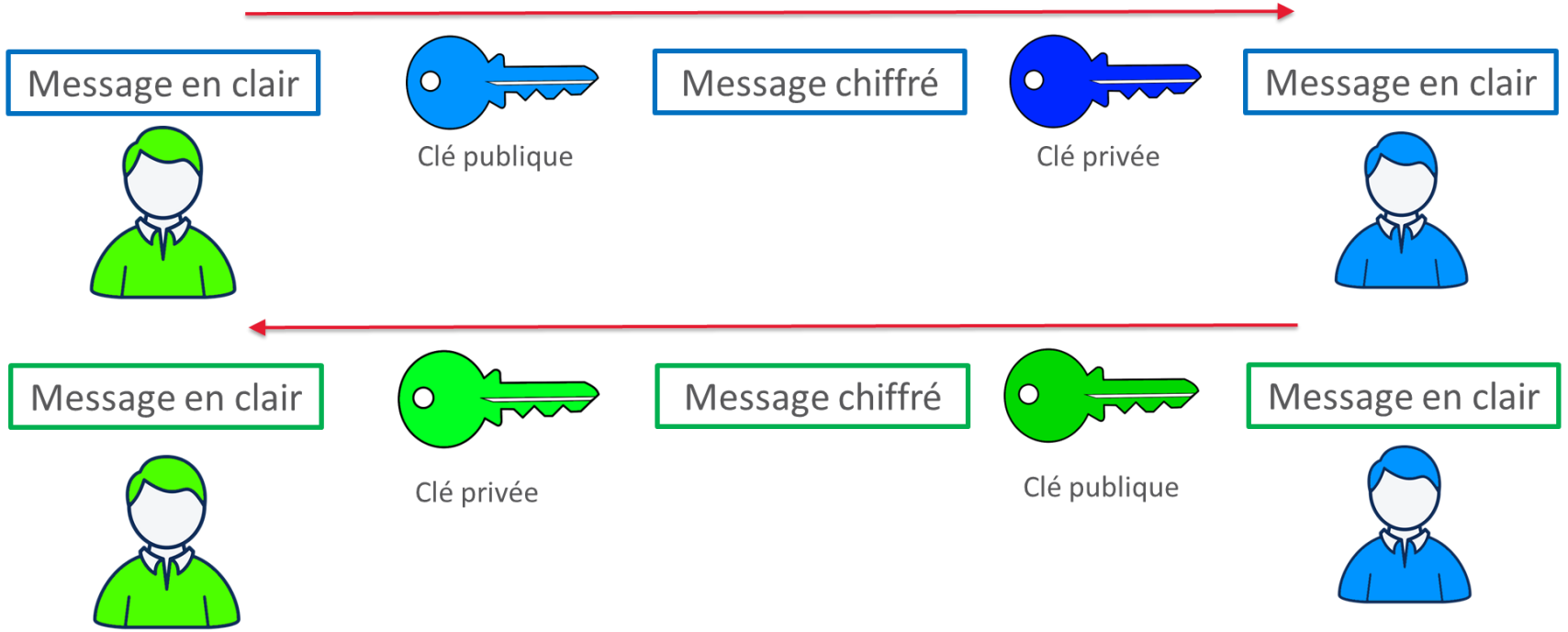
- **Principe 1 : comme dans la vie réelle où une maison dispose d'une adresse postale, sur le réseau internet, tout équipement est accessible par une adresse réseau, dit adresse IP (ex : 127.0.0.1).**
- **Cette adresse est communiquée au site auquel vous accédez**



CSIRT
BOURGOGNE-FRANCHE-COMTÉ

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 :

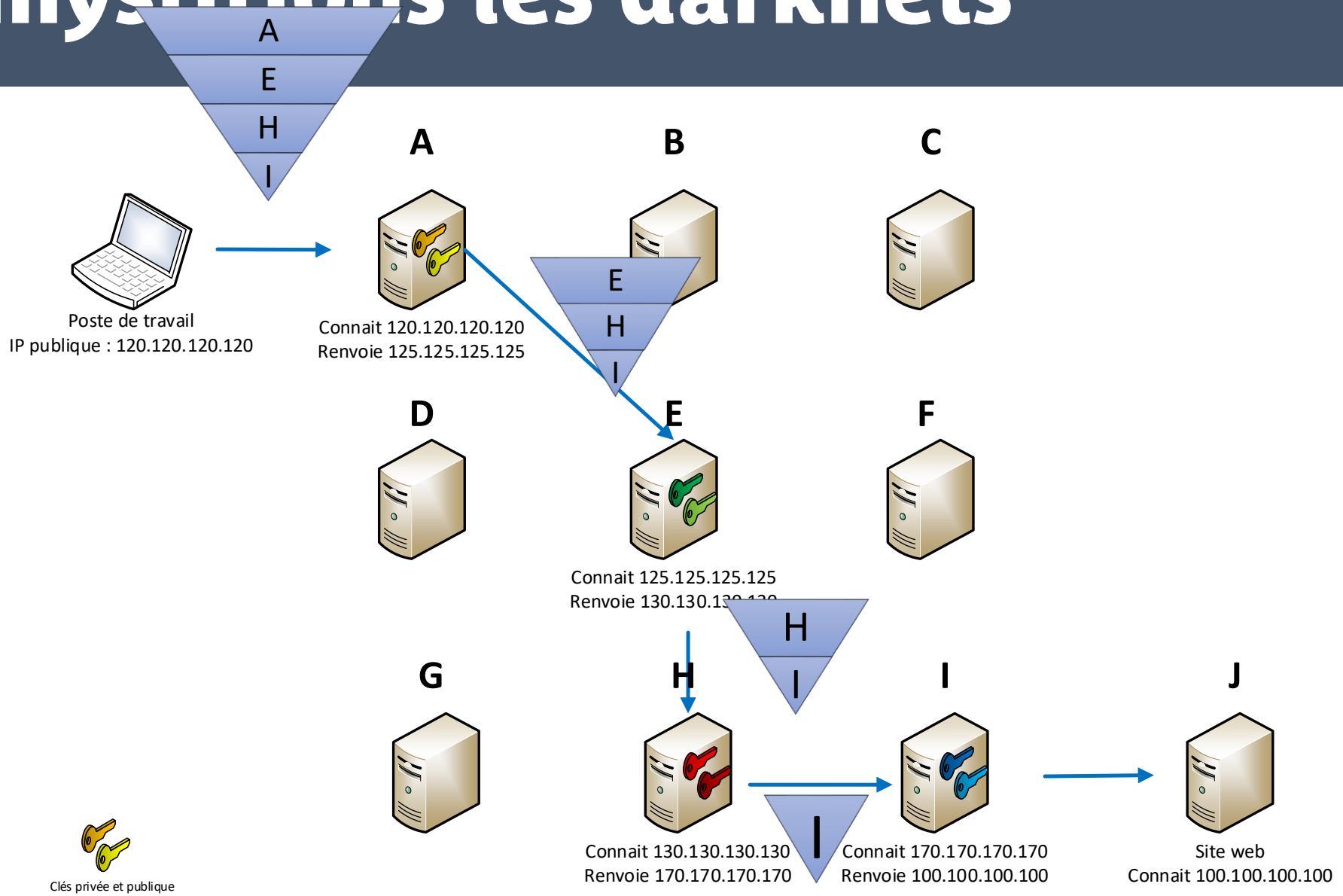
- Dans les darknets, ce n'est pas votre IP qui est proposée mais une autre, celle d'un des nœuds du réseau.
- Afin de renforcer la difficulté à remonter à la source, les flux réseaux passent par plusieurs serveurs et sont chiffrés.

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



CSIRT
BOURGOGNE-FRANCHE-COMTÉ

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 : lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.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

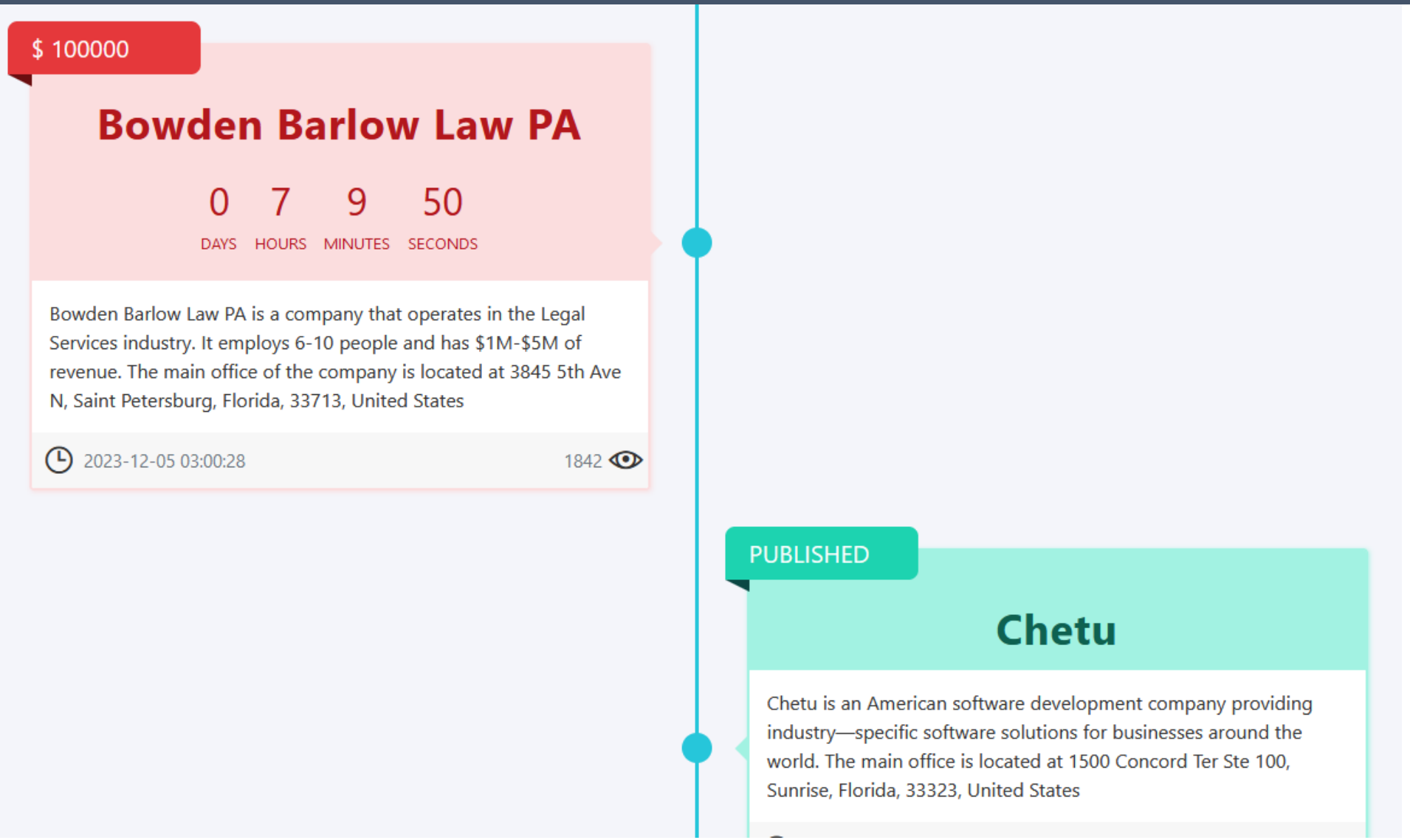
Hello, my name is Vladimir.
I am the technical expert at dark web hackers.

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 ฿	1 X Buy now
Facebook and Twitter account hacking	500 USD = 0.01187 ฿	1 X Buy now
Other social network account hacks, for example reddit or instagram	450 USD = 0.01068 ฿	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 ฿	1 X Buy now

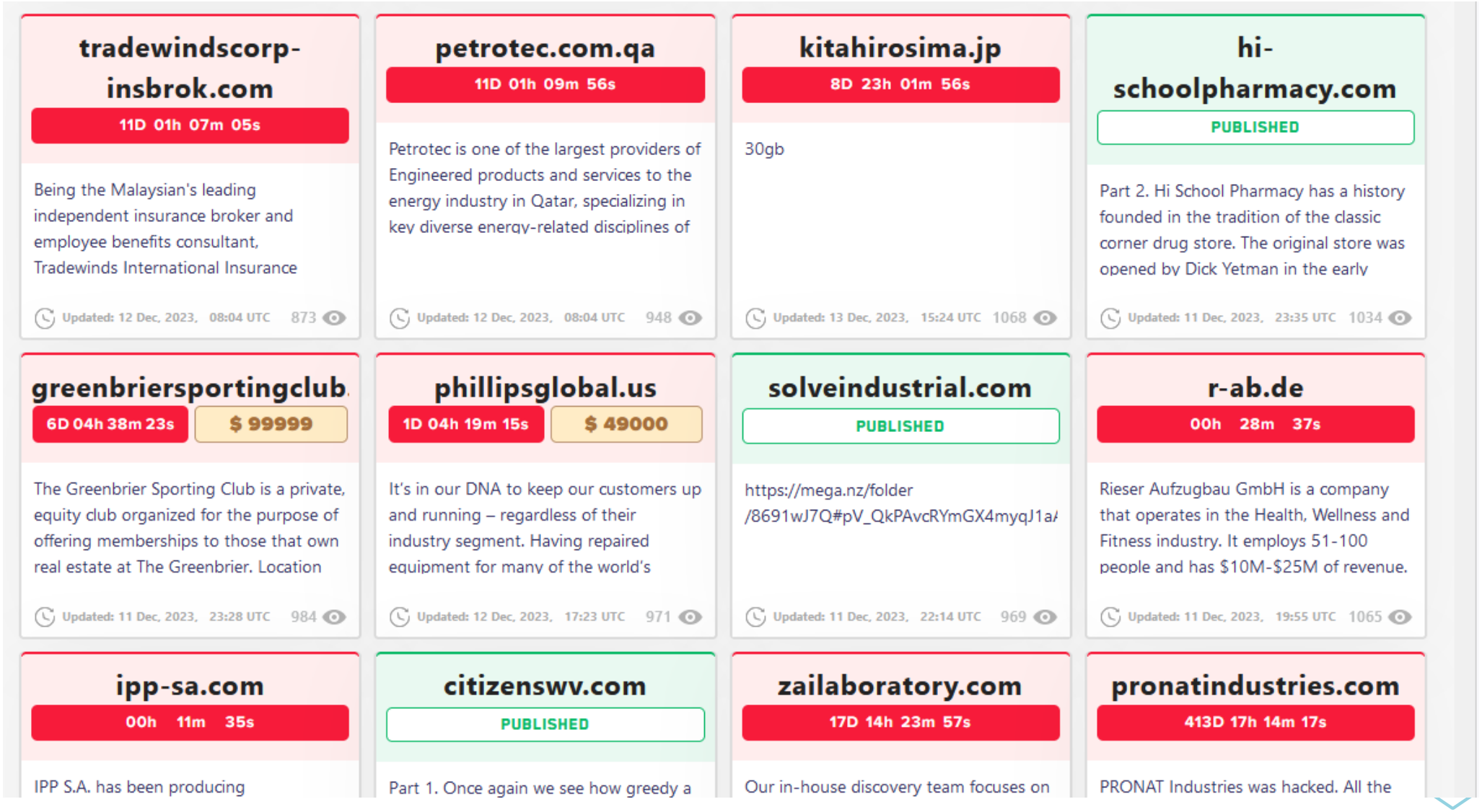
CSIRT BOURGOGNE-FRANCHE-COMTÉ

Démystifions les darknets



CSIRT
BOURGOGNE-FRANCHE-COMTÉ

Démystifions les darknets



CSIRT BOURGOGNE-FRANCHE-COMTÉ

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.

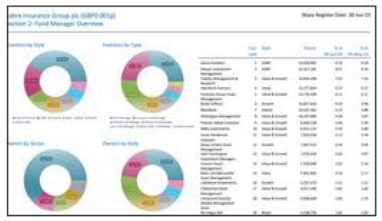
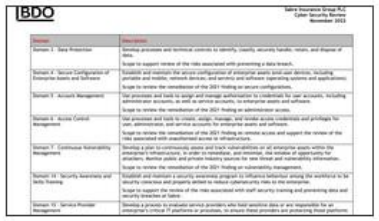
Sabre Insurance Company Limited is authorised and regulated by the Financial Conduct Authority and Prudential Regulation Authority. (FRN 202795)

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	DESTROY ALL INFORMATION	DOWNLOAD DATA AT ANY MOMENT
$ 10000	$ 900000	$ 900000

1-4 of 6

CSIRT BOURGOGNE-FRANCHE-COMTÉ

Démystifions les darknets

CSIRT BOURGOGNE-FRANCHE-COMTÉ

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

CSIRT BOURGOGNE-FRANCHE-COMTÉ

Démystifions les darknets

CSIRT
BOURGOGNE-FRANCHE-COMTÉ

Démystifions les darknets

UK Guns and Ammo Store

Products | Info | Login | Registration

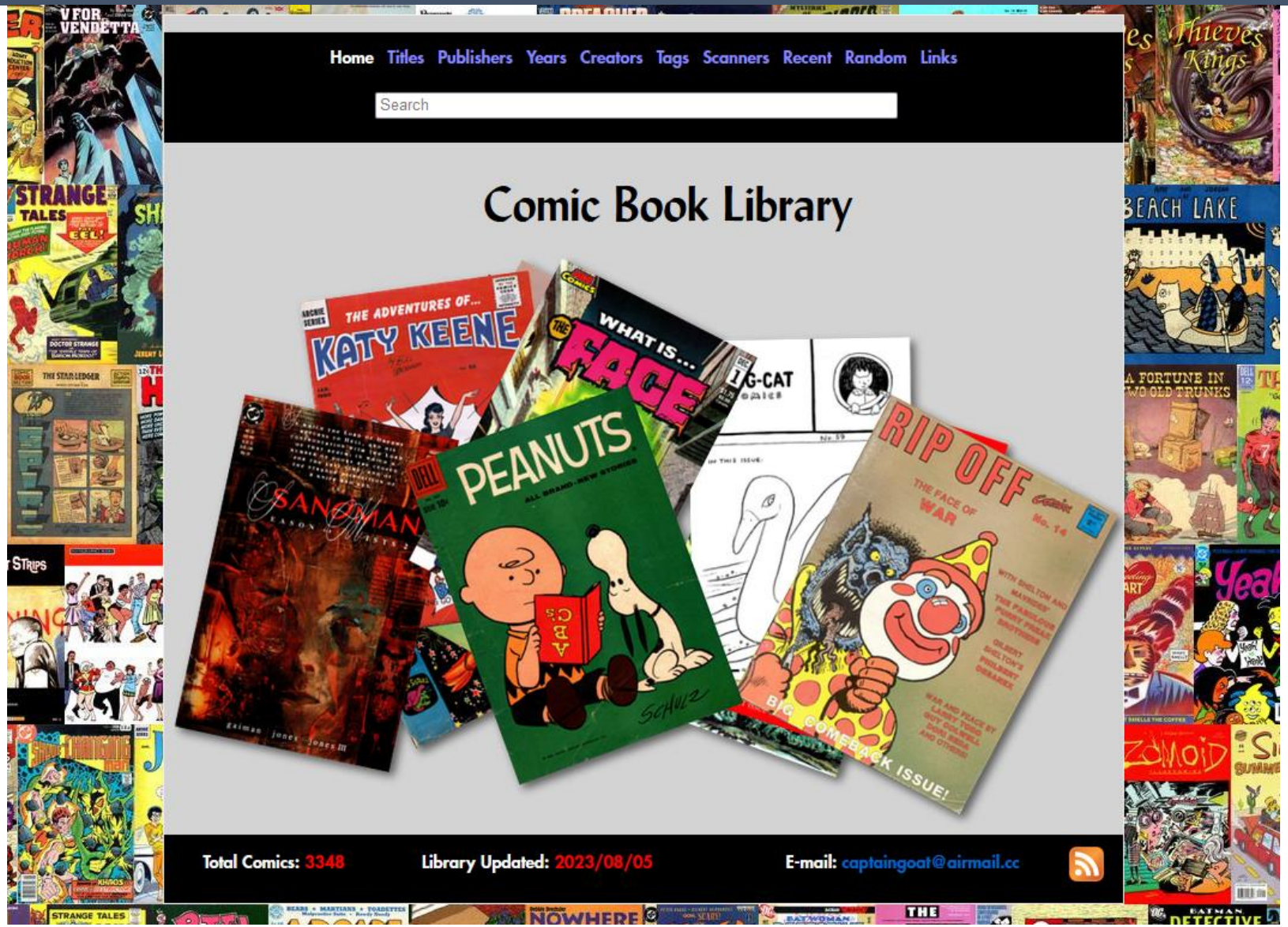
Guns

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 Ƀ	1 X Buy now
Walther P99 - 9mm - new and unused	650 GBP = 0.01924 Ƀ	1 X Buy now

CSIRT BOURGOGNE-FRANCHE-COMTÉ

Démystifions les darknets



CSIRT
BOURGOGNE-FRANCHE-COMTÉ

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 ฿	1 X Buy now
Netherlands Passport	1500 EUR = 0.03898 ฿	1 X Buy now

CSIRT BOURGOGNE-FRANCHE-COMTÉ

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

CSIRT BOURGOGNE-FRANCHE-COMTÉ