



Darknet: visite guidée de la partie sombre du Web



Francois Paget
Intel Security – McAfee Labs



Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur.

Darknet: visite guidée de la partie sombre du Web

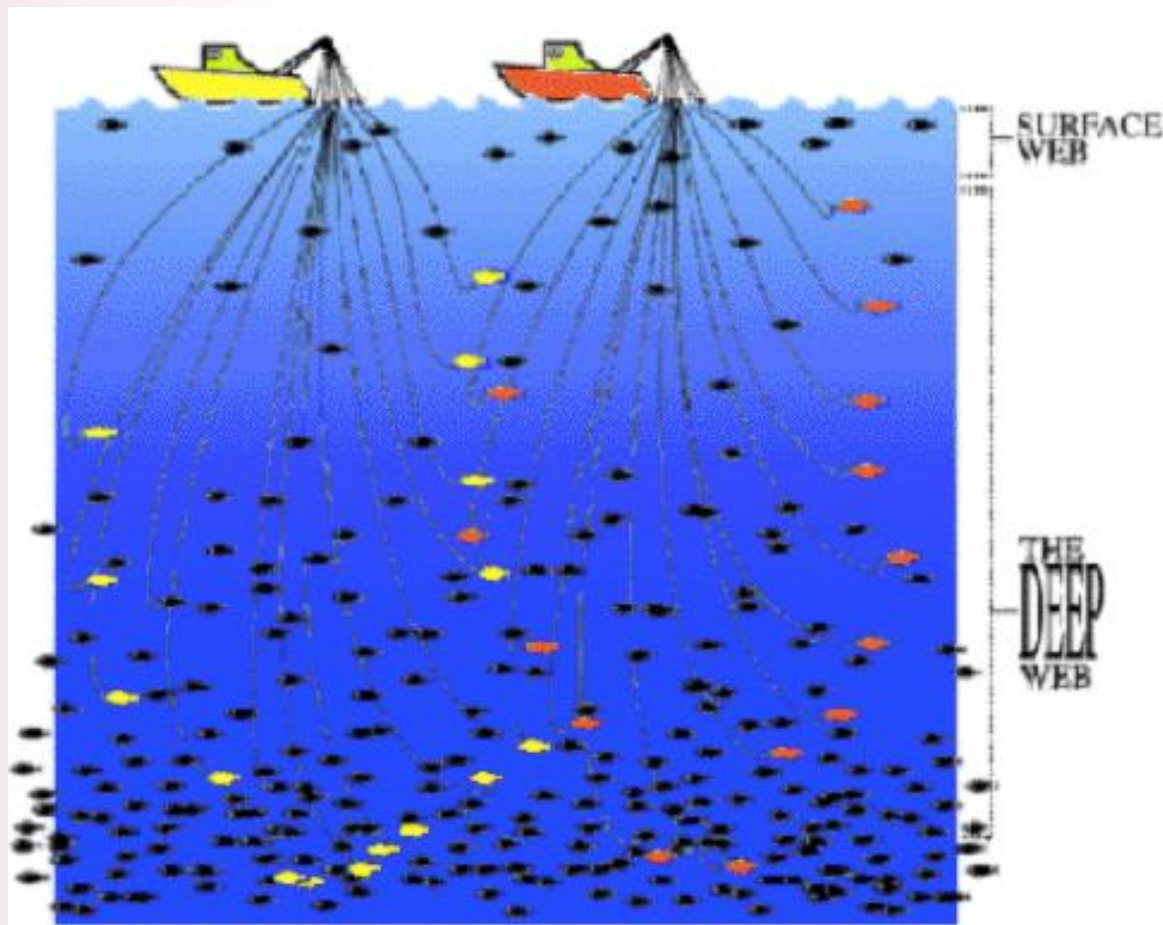
Sommaire

- Brève introduction,
- Suivez le guide (*pourboire en Bitcoin SVP*)

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Départ pour le web invisible

Définitions – « Deep Web » & « Dark Web »



Source: <http://davidenewmedia.wordpress.com/workingterms/deep-web/>

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Le *web invisible* (*deep web*) désigne la partie du web non indexée par les moteurs de recherche classiques. Le web invisible contient des sites légitimes (bases et banques de données, bibliothèques en ligne gratuites ou payantes, etc..) ainsi que des sites douteux et criminels. Certaines parties du web invisible ne sont accessibles qu'au travers d'outils spécifiques tels que Tor, Freenet ou I2P qui offrent, de surcroit, l'anonymat aux visiteurs.

Départ pour le web invisible

Définitions – « Deep Web » & « Dark Web »



Source: <http://davidenewmedia.wordpress.com/workingterms/darkweb/>

Le *web sombre* (*dark web*) désigne la partie du web constituée de sites douteux, malsains et criminels. Le web sombre est, en partie, contenu dans le web invisible tout comme il est en partie anonymement accessible via les outils spécifiques précédemment cités (Tor, Freenet ou I2P). Il ne contient que des sites douteux, malsains et criminels.

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Départ pour le web invisible & anonyme

Préalable: avoir une station anonymisée



+



+



The screenshot shows the Tor Browser interface. The title bar reads 'Navigateur Tor'. The address bar contains 'about:tor'. The main content area features a green onion icon and the text: 'Félicitations ! Ce navigateur est configuré pour utiliser Tor. Vous pouvez maintenant naviguer sur Internet de manière anonyme. [Tester les paramètres du réseau Tor](#)'. Below this is a search bar with the text 'Rechercher en toute sécurité avec Startpage.' and a magnifying glass icon. Two boxes provide further instructions: 'Que faire ensuite ?' and 'Vous pouvez aider !'. The 'Que faire ensuite ?' box contains the text: 'Tor n'est PAS tout ce dont vous avez besoin pour assurer votre anonymat ! Vous devrez peut-être changer certaines de vos habitudes de navigation pour garder votre identité en sécurité. [Conseils pour rester anonyme](#)'. The 'Vous pouvez aider !' box contains the text: 'Vous pouvez aider à rendre le réseau Tor plus rapide et plus puissant de plusieurs manières :' followed by a list: '• Faire fonctionner un relai Tor', '• Devenir bénévole', and '• Faire un don'. At the bottom, a paragraph states: 'Le projet Tor est une organisation à but non lucratif (US 501(c)(3)) dédiée à la recherche, le développement et l'éducation sur l'anonymat et la vie privée en ligne. [En savoir plus sur le projet Tor](#)'.

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Départ pour le web invisible & anonyme

Préalable: avoir une station anonymisée



+



+



CONSOLE DU ROUTEUR I2P

I2P Success On 31C3

The I2P team has visited the 31C3 event in Hamburg, Germany at the last days of 2014. Like the year before we gathered a table in the noisysquare area beside EFF and in front of the escalators. This brought us lots of attention and hours of talk and discussion on each of the 4 days. A lot of stickers and sweets were distributed upon the visitors. Also a I2P team dinner was organized and lots of topics about I2P development and future were talked about. See you all on 32C3!

0.9.17 Released

0.9.17 is primarily a bugfix release, but it also continues our migration to stronger cryptographic signatures. We have moved the news feed system used for the news on your console and the latest router version indication to a signed format using RSA 4096-bit keys for enhanced security. New eepsites and servers will be ECDSA-signed by default, if ECDSA is available. There is now a warning in the console sidebar if ECDSA is not available. For RedHat users, we have reports of successful installs of the BouncyCastle Provider (bcprov) jar to add ECDSA support. See [this wiki page](#) for details. We've fixed several serious bugs, including an SSU packet corruption problem, and a SAM bug affecting i2p-messenger and other SAM applications. There are several fixes for the preliminary ECDSA router signatures added in the last release but not yet enabled. Many of us will be attending 31C3 in Hamburg in December. Stop by our table and say hi! As usual, we recommend that you update to this release. The best way to maintain security and help the network is to run the latest release.

Actualités mises à jour il y a 2 heures Cacher les actualités

Bienvenue sur I2P !

Eepsites d'intérêt

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Silk Road a ses jumeaux...

La face visible de l'iceberg ne doit pas cacher sa face cachée

Silk Road
anonymous marketplace

Welcome: messages(0) | orders(0) | account(B0) | settings | log out

Shop by category:
Drugs(881)
Cannabis(232)
Ecstasy(69)
Dissociatives(18)
Psychedelics(145)
Opioids(70)
Stimulants(94)
Other(112)
Benzos(73)
Lab Supplies(12)
Digital goods(97)
Services(83)
Money(66)
Weaponry(14)
Home & Garden(6)
Food(1)
Electronics(6)
Books(69)
Drug paraphernalia (28)
XXX(44)
Medical(3)
Com... (6)
Appa... (1)
Ticke...
Forg...
Frev...

MDMA crystals (5 gramm) **B51.71**

Bitcoin exchange to paypal 50c **B18.19**

12,000 Term Paper Mega Archive **B0.70**

REICH **B5.56**

Coca Berries x 10 E novogranatense... **B11.87**

Dexedrine 10mg Instant Release... **B49.53**

News:

- Escrow hedging update
- New feature to help protect sellers
- Seller ranking and feedback overhaul
- Change your Mt. Gox password

BlackMarket Reloaded

Deposit Address: 1FDG...
 Account Balance: 0.00000 BTC
 Pending: 0.00000 BTC

Categories:
 Drugs (2863)
 Services (1202)
 Data (371)
 Weapons (223)
 Collectables (21)
 Metals/Stones (20)
 Other (347)
 Software (160)
 Movies (23)
 Tobacco (166)
 Counterfeits (237)
 Alcohol (13)
 eBooks (2237)
 Weight Loss (19)

Exchange

1.45299 BTC

0.17336 BTC

0.06838 BTC

1.73359 BTC

UTOPIA
A MARKET WITH THE DISCREETNESS OF THE SUBJECT

Drugs (904)
 Services (31)
 Data (99)
 Weapons (3)
 Weight loss (4)
 Collectables (2)
 Jewelry (11)
 Metals, Stones (4)
 Others (13)
 Tobacco (3)
 Counterfeits (10)
 Alcohol (3)
 eBooks (141)
 Sport supplements (9)

14 g / 1/2 oz - Dense and Delicious Nugs
 Seller: [waffle shark\(100\)](#)
 Ship from: Canada
 Ship to: Worldwide except USA.
 186.08 USD

Ultimate Guide to Using Tor privately and anonymously
 Seller: [BlackHerd\(100\)](#)
 Digital Item
 7.50 USD

FREE SHIPPING 1oz 28g AAA+ Medical Grade 1oz or 28 grams
 Seller: [chillone4\(100\)](#)
 Ship from: United States of America
 Ship to: United States of America
 300.00 USD

25 x XTC Bentley Pills (110mg MDMA)
 Seller: [Luffner\(100\)](#)
 Ship from: Germany
 Ship to: Worldwide
 140.36 USD

Sheep

Account Orders Messages Gallery Forum Help Logout

Welcome plasticplate Account: 0.00000000 Orders: 0 Messages: 0

14 g / 1/2 oz - Dense and Delicious Nugs
 Seller: [waffle shark\(100\)](#)
 Ship from: Canada
 Ship to: Worldwide except USA.
 186.08 USD

Ultimate Guide to Using Tor privately and anonymously
 Seller: [BlackHerd\(100\)](#)
 Digital Item
 7.50 USD

FREE SHIPPING 1oz 28g AAA+ Medical Grade 1oz or 28 grams
 Seller: [chillone4\(100\)](#)
 Ship from: United States of America
 Ship to: United States of America
 300.00 USD

25 x XTC Bentley Pills (110mg MDMA)
 Seller: [Luffner\(100\)](#)
 Ship from: Germany
 Ship to: Worldwide
 140.36 USD

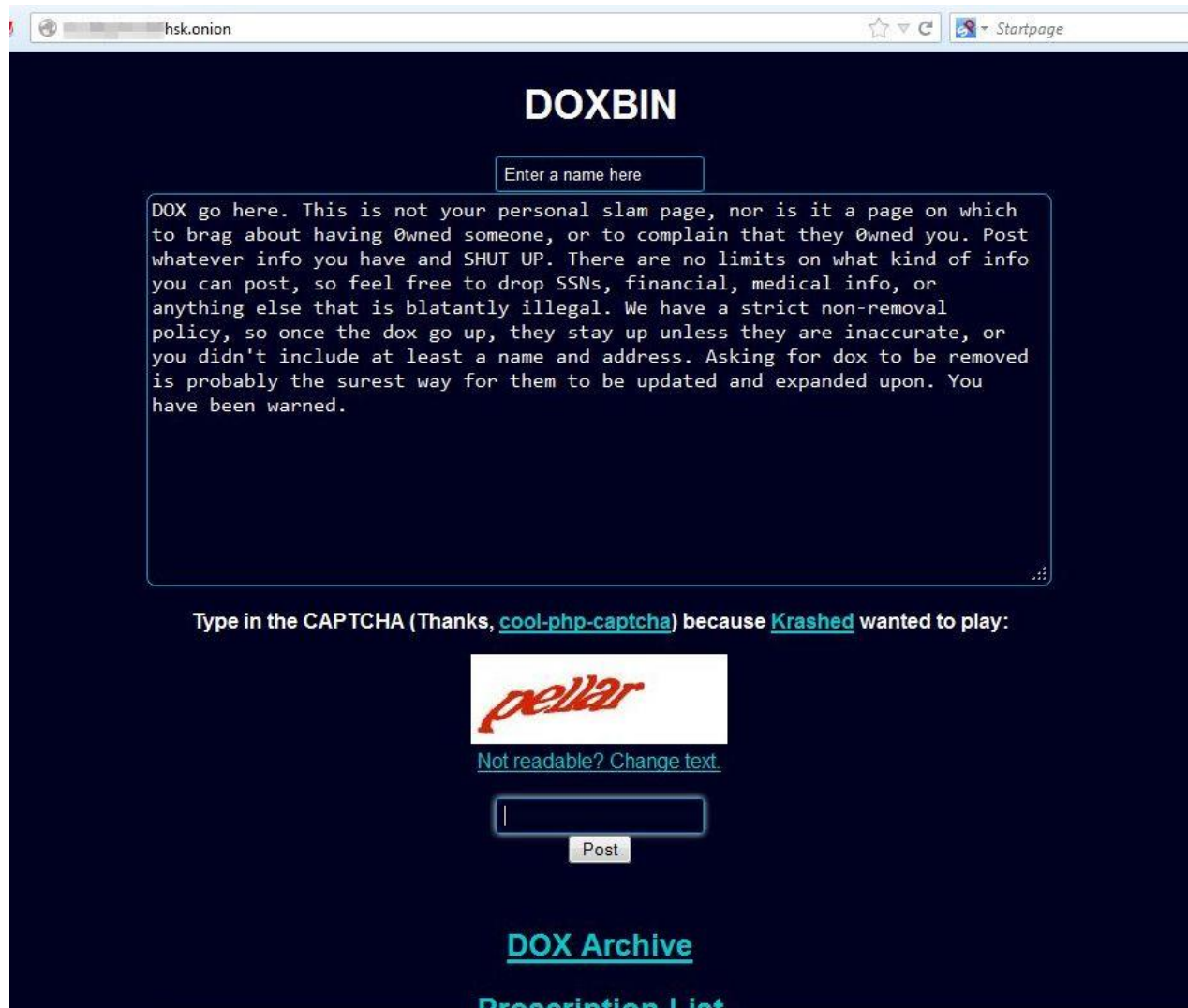
2.5 CLEAN COC

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Les trouvailles du Web sombre

Doxing

Le doxing consiste en la publication de photos, de coordonnées et de données personnelles et familiales en représailles à une action menée par l'individu qui en est la victime.



Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Les boutiques du Web sombre

Cigarettes

The screenshot shows the homepage of 'CigarettesStore'. At the top, there is a navigation bar with 'ALL PRODUCTS', 'F.A.Q.', 'FEEDBACKS', and 'CONTACT US'. A shopping cart icon indicates '0 items' for '\$ 0.000'. The main content area features a 'FEATURED' section with a list of cigarette types: Menthol, Full Flavor, Lights, and Ultra Lights. Below this is a 'BESTSELLERS' section listing Camel, Marlboro, Parliament, and Winston. A large product display for 'Marlboro Gold' is prominent, showing a pack of cigarettes and a 'more info' button. A security notice states that orders are processed and shipped from outside the USA to ensure data security. At the bottom, there are sections for 'Bestselling Cigarettes' with details for Marlboro Gold (0.5 mg Nicotine, 6 mg Tar) and Winston Classic (0.8 mg Nicotine, 10 mg Tar). Security logos for McAfee and Bitcoin are also visible.

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Les boutiques du Web sombre

Carding

CC.Planet.union

bitcoin ACCEPTED HERE

DISCOVER MasterCard VISA

Home Buy cards Account Add Funds Create a ticket Back

Hi [redacted]
Your Balance [redacted]
Your BTC Address: [redacted]

Add funds
Logout

W3C CSS
MTGOX

Cards

Search

Just search our DB using country and type. You can also check for specific Bins.
(Bin search disabled)

Bins: [input]
Type: Any Country: US +DOB +Email

Search

Number	Type	N	Y	City	Phone	Mail	DOB	Price	Select
456103XXXXXX	VISA	IT	FR	83600 FR7JUS	Y	N	Y	40\$	[checkbox]
456103XXXXXX	VISA	BEL	FR	83600 FR7JUS	Y	N	Y	40\$	[checkbox]
513697XXXXXX	MasterCard	GER	FR	56000 VANNES	Y	N	Y	40\$	[checkbox]
536588XXXXXX	MasterCard	FIN	FR	64600 ANGLET	Y	N	Y	40\$	[checkbox]
513381XXXXXX	MasterCard	DK	FR	92000 NANTERRE	Y	N	Y	40\$	[checkbox]
513612XXXXXX	MasterCard	SWE	FR	37200 TOURS	Y	N	Y	40\$	[checkbox]
513697XXXXXX	MasterCard	JPN	FR	34300	Y	N	Y	40\$	[checkbox]
536588XXXXXX	MasterCard	AUS	FR	69300	Y	N	Y	40\$	[checkbox]
513658XXXXXX	MasterCard	Any	FR	69001 LYON	Y	N	Y	40\$	[checkbox]
456136XXXXXX	VISA	BEL	FR	33500	Y	Y	Y	40\$	[checkbox]

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Les boutiques du Web sombre

Carding

CHIPPED CARDS

• (1) One Card	• \$145 USD
• (3) Three Cards	• \$380 USD
• (5) Five Cards	• \$575 USD
• (10) Ten Cards	• \$1040 USD
• (20) Twenty Cards	• \$1870 USD

MAGNETIC CARDS

• (1) One Card	• \$110 USD
• (3) Three Cards	• \$290 USD
• (5) Five Cards	• \$440 USD
• (10) Ten Cards	• \$790 USD
• (20) Twenty Cards	• \$1390 USD



Contact: financialhack@safe-mail.net

Financial_Hack Group

Pre-Paid Products

- Home
- About
- Contact
- FAQ
- Feedback

Pre-Paid Debit Cards

Cards that we've loaded with funds from various accounts. Once the funds are loaded onto the prepaid cards, they are secure and only you will have access to them, making them risk free.

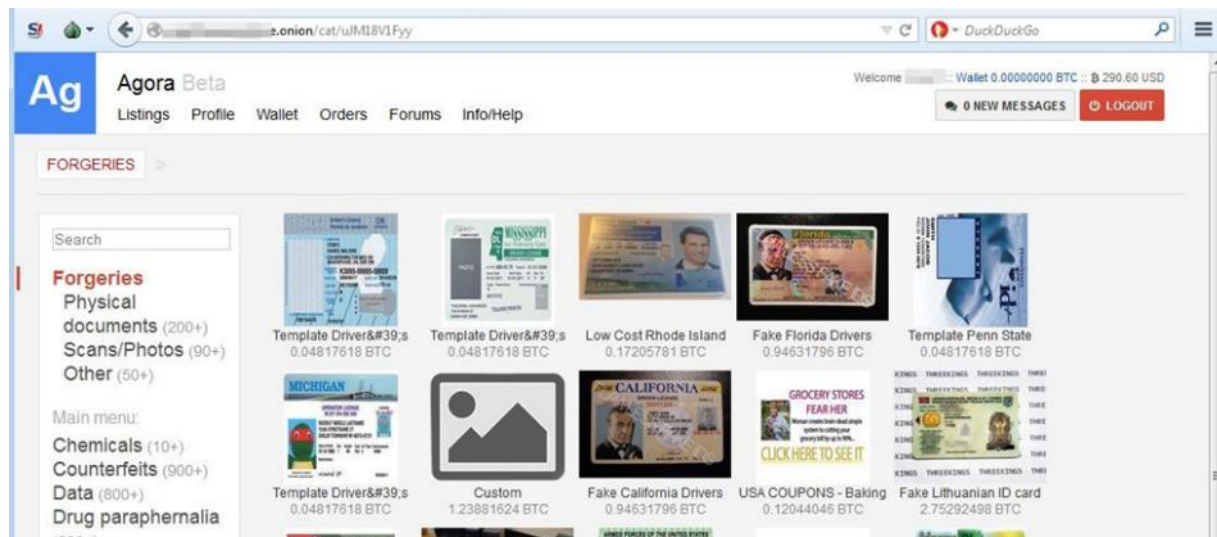
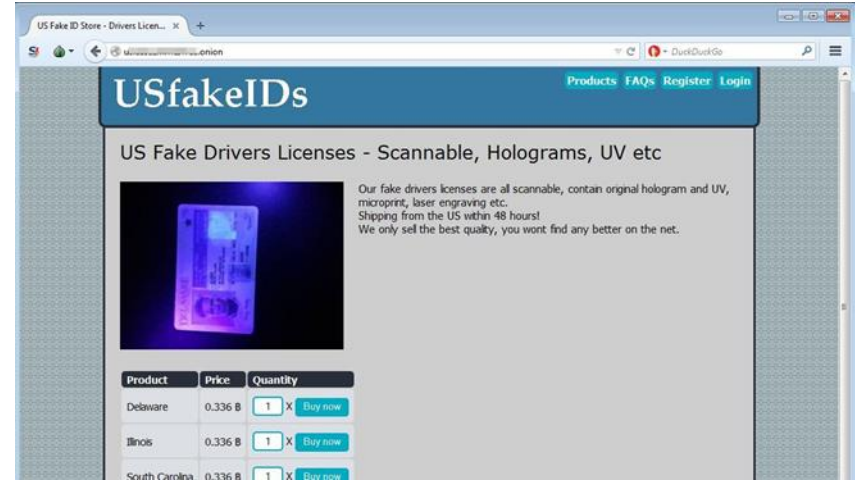
We are only accepting bitcoin for payment. No other type of payment is accepted due to obvious security

We have both plain magnetic stripe cards and chipped cards. Our chipped card balances come in euros and cost

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Les boutiques du Web sombre

Faux papiers



Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Les boutiques du Web sombre

Fausse monnaie

The screenshot shows a web browser window with three product listings for counterfeit banknotes. Each listing includes an image of the banknote, a title, a description, specifications, and a price in Bitcoin (BTC).

Product	Price (BTC)
50 EUR Counterfeit	3.036
20 USD Counterfeit	2.2
50 GBP Counterfeit	3.63

50 EUR Counterfeit
Euro Banknotes perfectly manufactured. All customers that have use them say that is really easy in everyday use in europe. Taxi, restaurant, bar or to buy clothes.
Very good quality, micro-print, provided with watermarks, security thread, pass pen test, etc. These are made with exactly the same techniques the ECB uses to make genuine currency.
Specifications:
Producer: EU Printer
Quantity: 200 x 50eur
Quality: 99%
- UVI incorporated with magnetic ink
- Security strip
- Watermarked
- Unique serials
- Pen tested
Value on market 10000€
Price on market 3300€
our price **3.036 BTC**

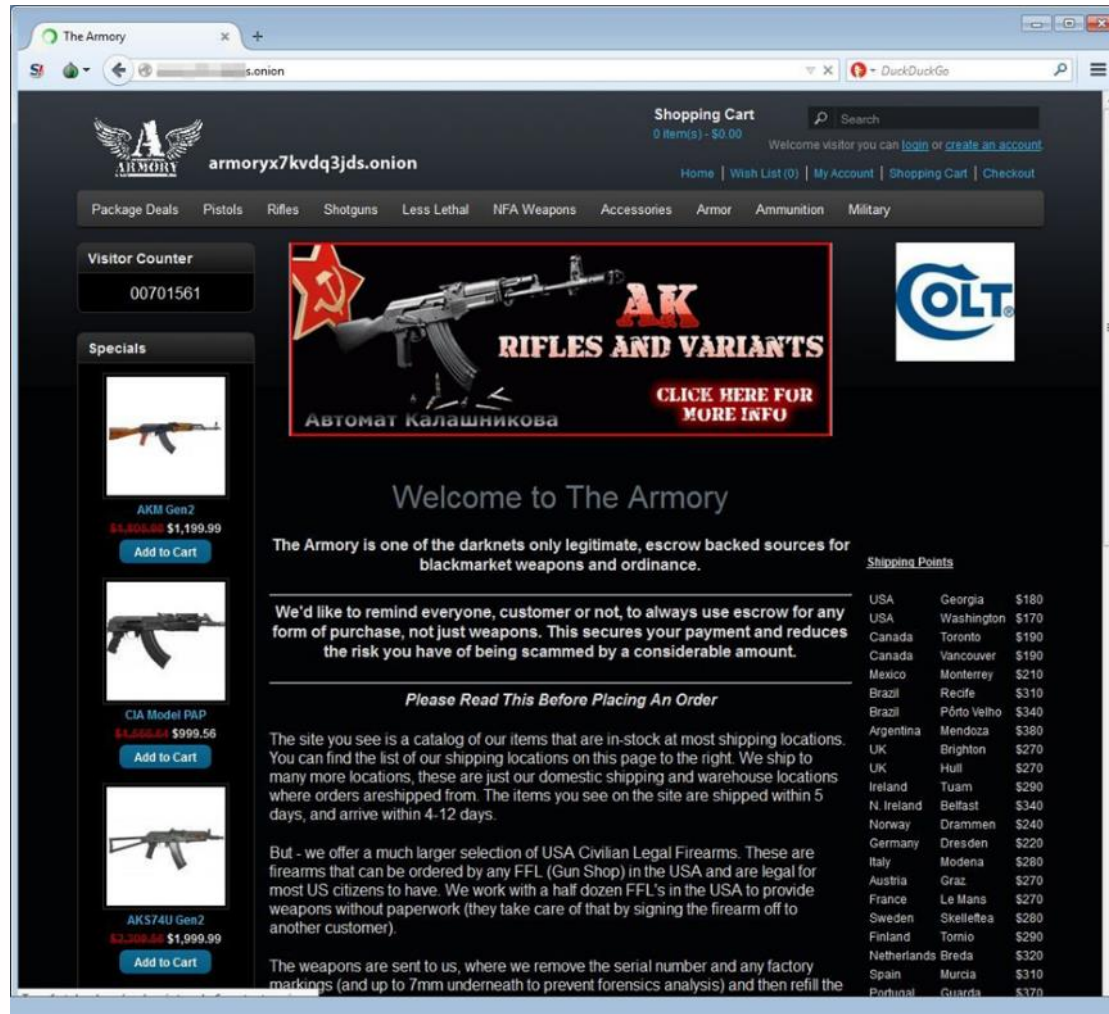
20 USD Counterfeit
USD Banknotes perfectly manufactured. All customers that have use them say that is really easy in everyday use in United States. Taxi, restaurant, bar or to buy clothes.
Very good quality, micro-print, provided with watermarks, security thread, pass pen test, etc. These are made with exactly the same techniques the Fed uses to make genuine currency.
Specifications:
Producer: US Printer
Quantity: 500 x 20usd
Quality: 99%
- UVI incorporated with magnetic ink
- Security strip
- Watermarked
- Unique serials
- Pen tested
Value on market 10000\$
Price on market 3300\$
our price **2.2 BTC**

50 GBP Counterfeit
GBP Banknotes perfectly manufactured. Seems real, already passed them in a lot of places in London. Pretty easy.
Very good quality, micro-print, provided with watermarks, security thread, pass pen test, etc. These are made with exactly the same techniques the BoE uses to make genuine currency.
Specifications:
Producer: EU Printer
Quantity: 200 x 50€
Quality: 99%
- UVI incorporated with magnetic ink
- Security strip
- Watermarked
- Unique serials
- Pen tested
Value on market 10000€
Price on market 3300€
our price **3.63 BTC**

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Les boutiques du Web sombre

Gun Shop



Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Les hébergements du Web sombre

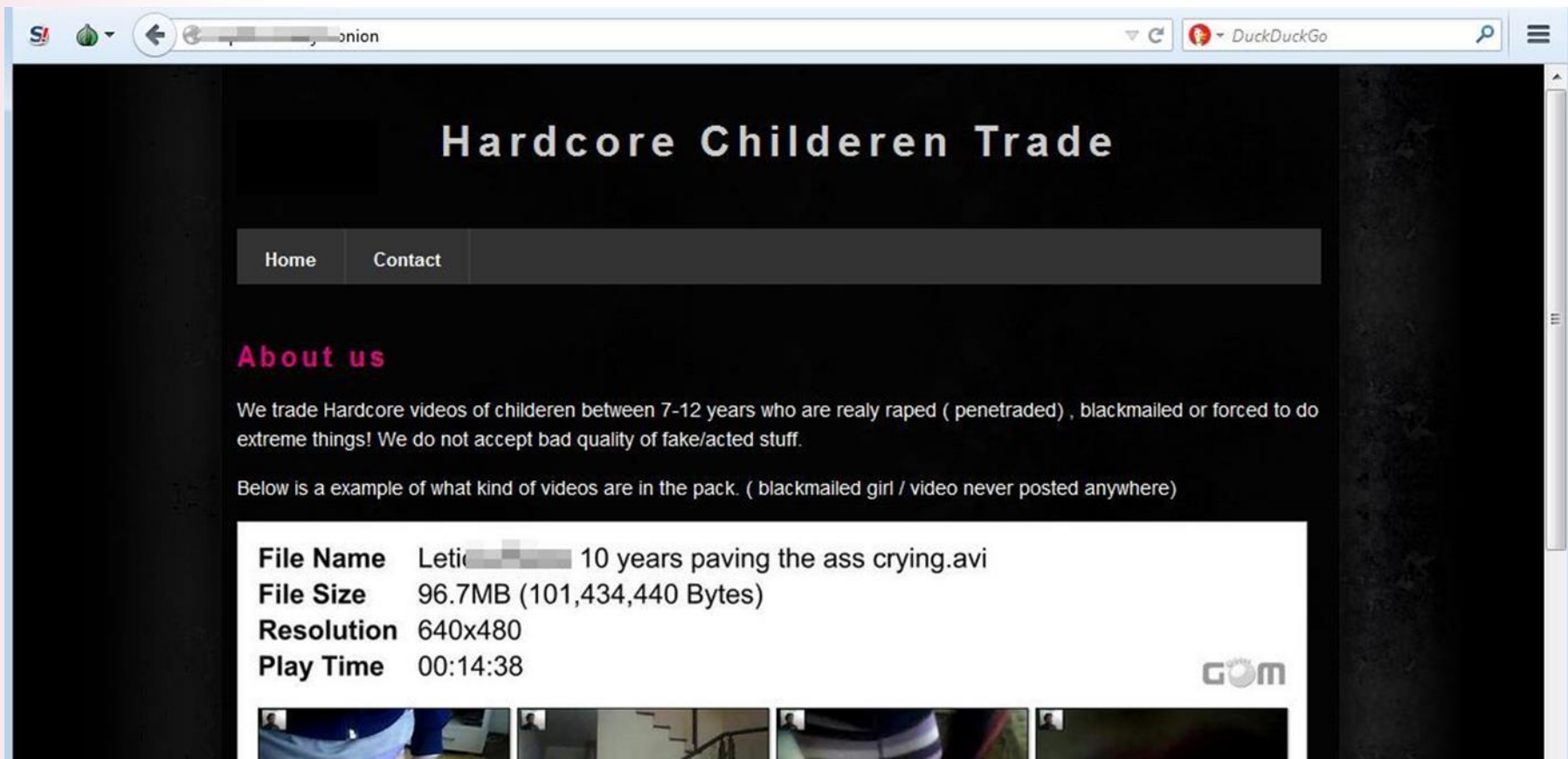
Don à des organisations terroristes



Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Les hébergements du Web sombre

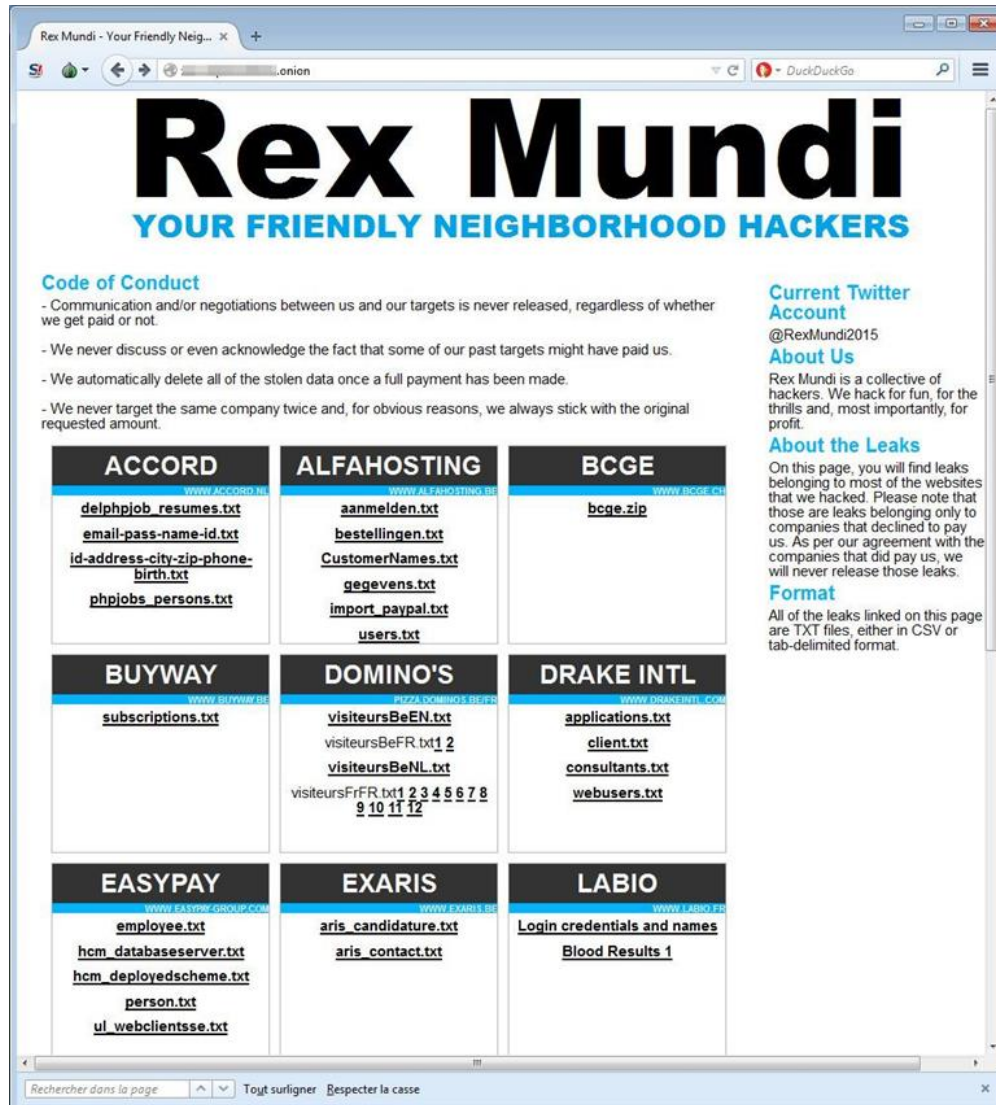
Pornographie enfantine



Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Les hébergements du Web sombre

Données dérobées



Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Les hébergements du Web sombre

Données dérobées

1.pdf
zc.onion/labio/1.pdf
Page: 3 sur 16
Zoom automatique

labio
Laboratoire de Biologie Médicale
Agrément B-55012R

Laboratoire
5 Rue des
Tel: 04 42 Fax: 04 42
Email: @labio.fr
Direction: Dr Philippe

Monsieur

Examen
De: Mon
Né(e) le
Prélevé le
Enregistré
Edité le
Prescrit par

HEMATOLOGIE
Valeurs de référence Antécédents

Résultats et dosages réalisés le 25.07.2013, validés le 26.07.2013
(Abbott Ruby - Cytométrie de flux) (JA)

Leucocytes	12,90	10 ⁹ /l	4 à 10		
Hématies	6,06	10 ¹² /l	4,0 à 5,8		
Hémoglobine	16,8	g/dl	13,0 à 17,7		
Hématocrite	50,9	%	40 à 54		
T.C.M.H	27,8	pg	27 à 31		
C.C.M.H	33,1	%	32 à 36		
V.G.M.	84	µ3	80 à 100		

FORMULE LEUCOCYTAIRE

Poly. neutrophiles	58,0	%	7,48	10 ⁹ /l	2 à 7,5
Poly. éosinophiles	0,8	%	0,10	10 ⁹ /l	< 0,5
Poly. basophiles	0,6	%	0,08	10 ⁹ /l	< 0,2
Lymphocytes	33,5	%	4,32	10 ⁹ /l	1 à 4
Monocytes	7,2	%	0,93	10 ⁹ /l	0,3 à 1

NUMERATION PLAQUETTAIRE

Plaquettes	272	10 ⁹ /l	150 à 400		
------------	-----	--------------------	-----------	--	--

HEMOSTASE

Rechercher dans la page Tout surligner Respecter la casse

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Y a t'il un DarkWeb Francophone

Oui !

Message de vict0r
RAPPEL :
Le FDW a été créé dans le but de fournir un **espace d'échange sans censure** en dehors des 2 seules limitations imposées par LH, ce forum est donc un espace où la liberté d'expression est très importante. **Quelles que soient vos croyances, vos croyances, votre couleur de peau, vous devriez avoir le droit de vous exprimer sans crainte de représailles.**

Message d'Hamster-guerrier
Pour tout souci que vous pourriez rencontrer sur le forum ou le DW français, vous pouvez me contacter par MP, lettres, pigeon voyageur, télépathie, signaux de fumée, peinture rupestre, texte de rap, tweet, missive administrative, signaux maritimes, packets RTP (SSRC:0A5h), morse, miaulement et sécrétions phéromonales.
ps : A tout les membres de FMP réfugiés ici, je me permet de vous rappeler une chose très justement dis par un de nos membres

Centralisation de liens utiles :

1. Règlement du forum
2. Rangs des utilisateurs
3. Bien sécuriser Tor Browser.
4. Installation de Bitcoin-Wallet
5. Comment utiliser PGP (messages cryptés)
6. le vocabulaire du French Deep Web
7. Combien peuvent vous coûter vos activités sur le FDW ?
8. La bienséance sur le FDW (ou comment ne pas se faire supprimer son compte)

Appel aux dons:
- Ce forum est hébergé à titre gratuit par Liberty's Hackers. Vous pouvez contribuer au maintien de ce service ainsi qu'au développement d'un market libre lié à FDW en faisant un don à cette adresse btc : 1492VyoSBu763tLowFqRn2bo34pGd5xkA

Message d'Hachi
LES ANNONCES DE VENTES SAUVAGES NE SONT PAS TOLÉRÉES. Les contrevenants seront BANNIS sans avertissement.
RAPPEL : L'assistanat est honni sur le FDW. N'espérez pas la moindre pitié de ma part en MP. Si vous venez pleurnicher en MP, vous allez vous prendre une deuxième charge.

Liens français du Deep Web :

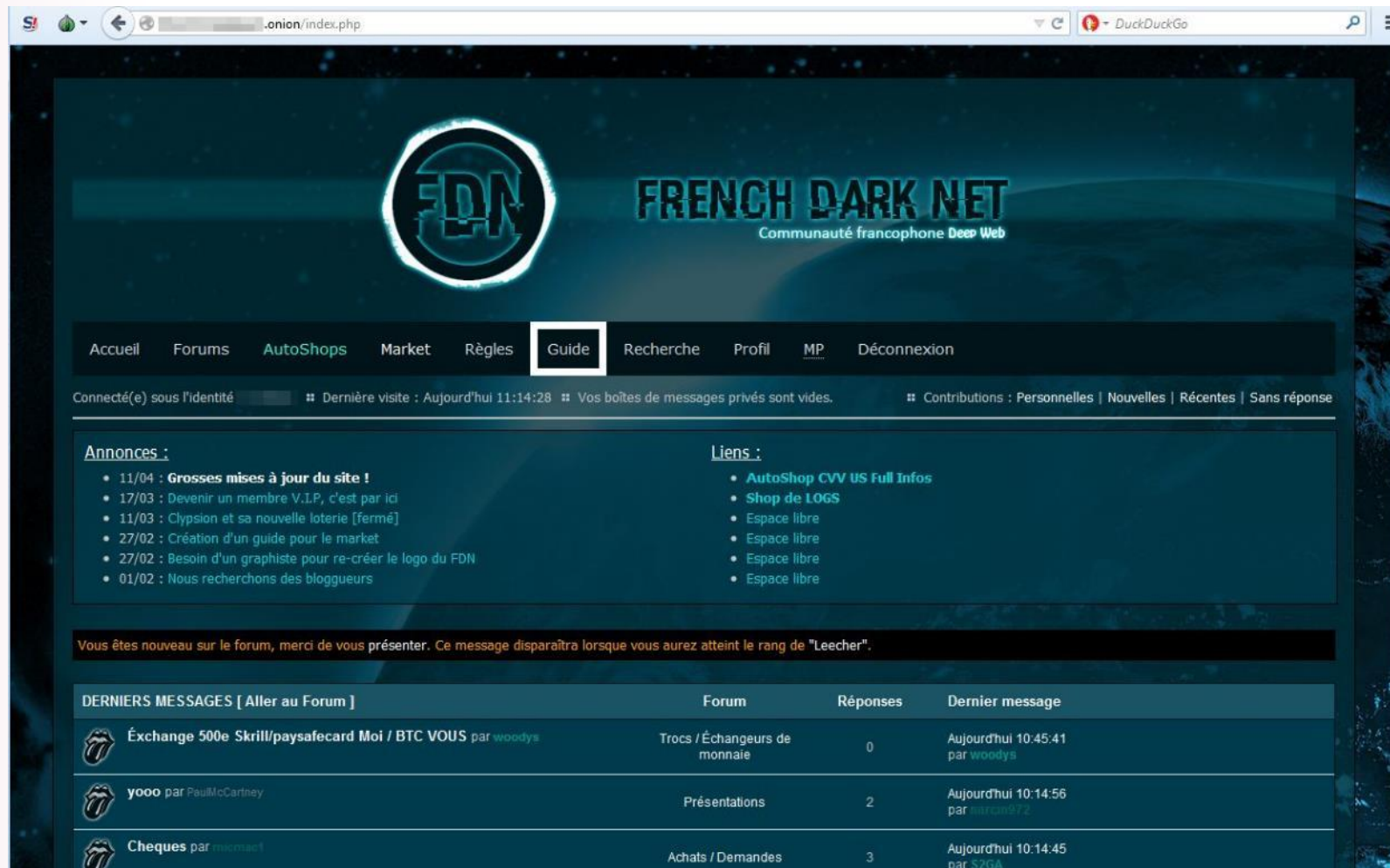
- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

Forum	Discussions	Messages	Dernier message
Actualités [Nouveaux messages] Discussions axées sur les actualités. (Modéré par 000 , Baron S , Boson de Higgs , H.Ivinshtreum , Noctua , Zanadar)	955	17 650	Aujourd'hui 16:54:34 par Niveks
Annuaire [Nouveaux messages] Discussions axées sur le partage de sites hébergés sur le réseau Tor. (Modéré par 000 , Baron S , Boson de Higgs , H.Ivinshtreum , Noctua , Zanadar)	336	5 574	Aujourd'hui 16:37:36 par Zanadar
Présentations [Nouveaux messages] Discussions axées sur la présentation des nouveaux membres. (Modéré par 000 , Baron S , Boson de Higgs , H.Ivinshtreum , Noctua , Zanadar)	3 998	23 110	Aujourd'hui 16:52:22 par Niveks

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Y a t'il un DarkWeb Francophone

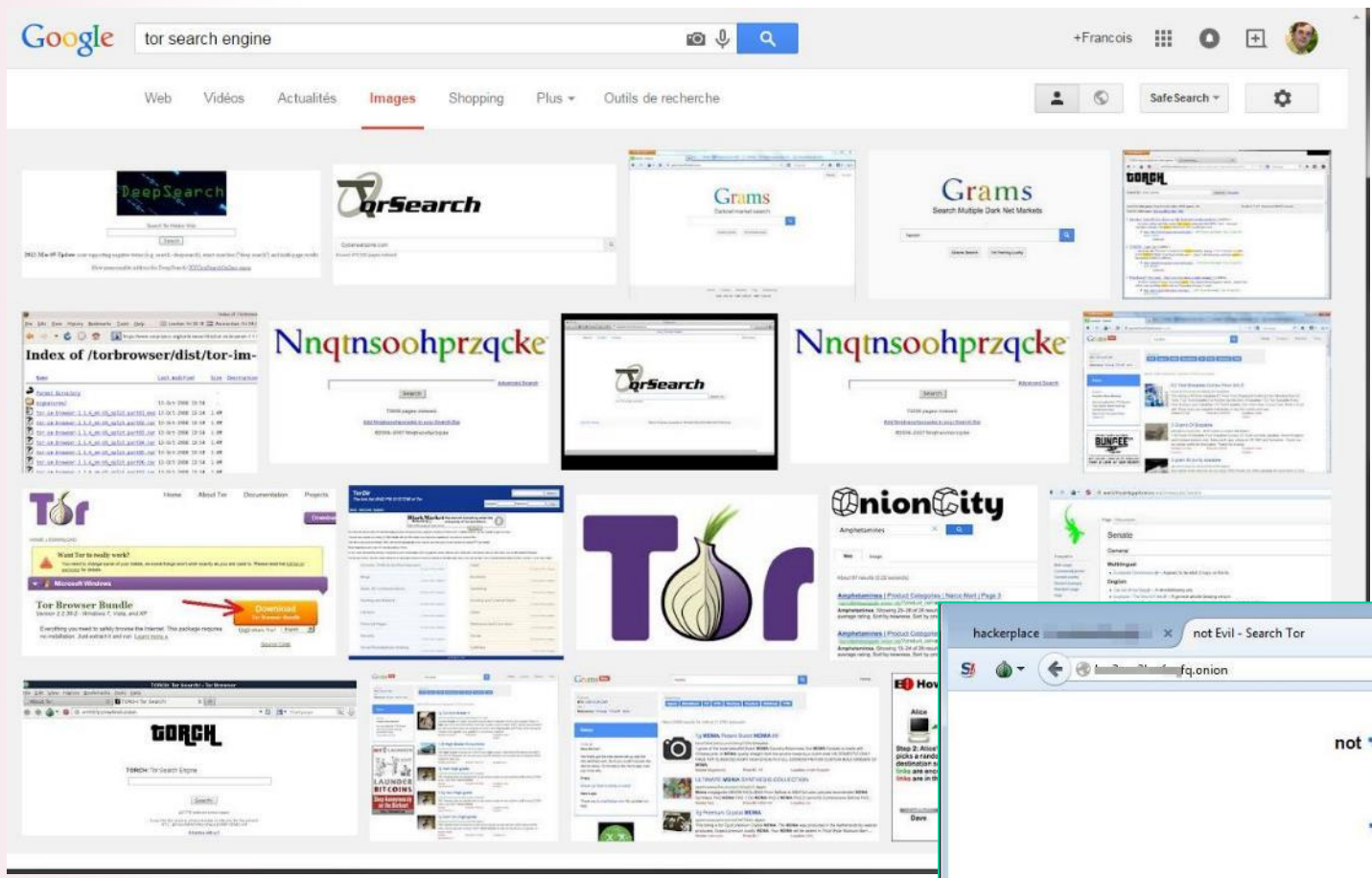
Oui !



Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Pour ne pas s'y perdre...

Des moteurs de recherche de très faible qualité



Un seul semble « un peu » plus performant!



Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Pour ne pas s'y perdre...

... rien ne vaut le flair et Pastebin ou ses équivalents...

The screenshot shows a Pastebin page with the following content:

- Header: PASTEBIN | #1 paste tool since 2002. Includes navigation links like 'create new paste', 'tools', 'api', 'archive', 'faq', and 'search...'. Social media links for 'Follow @pastebin' and 'Like 198k' are also present.
- Metadata: 'Untitled', 'BY: A GUEST ON JAN 8TH, 2015', 'SYNTAX: NONE', 'SIZE: 66.31 KB', 'VIEWS: 1,325', 'EXPIRES: NEVER'. Action links include 'DOWNLOAD', 'RAW', 'EMBED', 'REPORT ABUSE', and 'PRINT'.
- Advertisement: 'THE PRACTICAL STARTUP GUIDE TO ONLINE ADVERTISING' with a 'DOWNLOAD THE FREE EBOOK' button. Text: 'ADVERTISING IS HARD. WE DO IT ALL DAY. LET US TEACH YOU WHAT WE'VE LEARNED.'
- Main Content: A list of 23 numbered onion links. The first link is: '3. http://22[redacted].onion/ 深网中文第一页 - 首页'. Other links include 'W3B411 - Login', 'Hinrich Rosenbrock - Ein Schläger?', 'NL Growers - Coffee Shop grade Cannabis from the Netherlands - Weed, Hash, Marijuana, Cannabis for Bitcoins', 'Áiáøà | Óáiððáíey è Náiáíá sey ðàñðáíey?', 'Euro Guns - Number one guns dealer in onionland - Buy guns and ammo for Bitcoin.', 'IDC - Italian DarkNet Community', 'Hidden Service #6', 'KAVKAZ CENTER', 'Bitcoin Gym Fundraising', 'Manual de Segurança', and 'index Blog de darkcy una historia de misterio y mas'.
- Right Sidebar: 'Public Pastes' section with a list of recent pastes (e.g., 'Untitled 7 sec ago', 'ZLOEMU Errors Port... 9 sec ago'). Below it is an 'ebay' advertisement for 'DEFINITION MAXI, EFFORT MINI' with an image of a device.

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur

Conclusion

On trouverait tout sur le DarkNet ?

Les offres sont elles toutes réelles ?

La marchandise est elle bien là ?

Ne pas diffuser hors du CLUSIF sans l'accord express de l'auteur