AEC

DATA SECURITY

Ekosystém Darknetu

Ing. Martin Klubal

martin.klubal@aec.cz

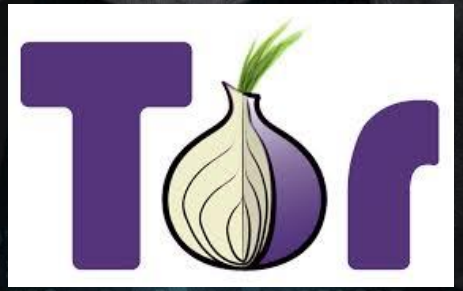
Ekosystém Darknetu - obsah

- Anonymizační sítě
- Tor
- Hidden Services
- Black Markets
- De-anonymizace v síti Tor
- Krádeže Bitcoinů
- Tor & Bitcoin aféry

AEC
DATA SECURITY

Anonymizační sítě

- Tor (The Onion Router)
- I2P (Invisible Internet Project)
- Freenet



Typy sítí z pohledy anonymity

- Clearnet (Internet)
  - http://justhack.net/
  - https://darkode.com/
- Darknet
  - Silk Road
  - Freedom Hosting
- Deepnet
  - Invite Only Boards

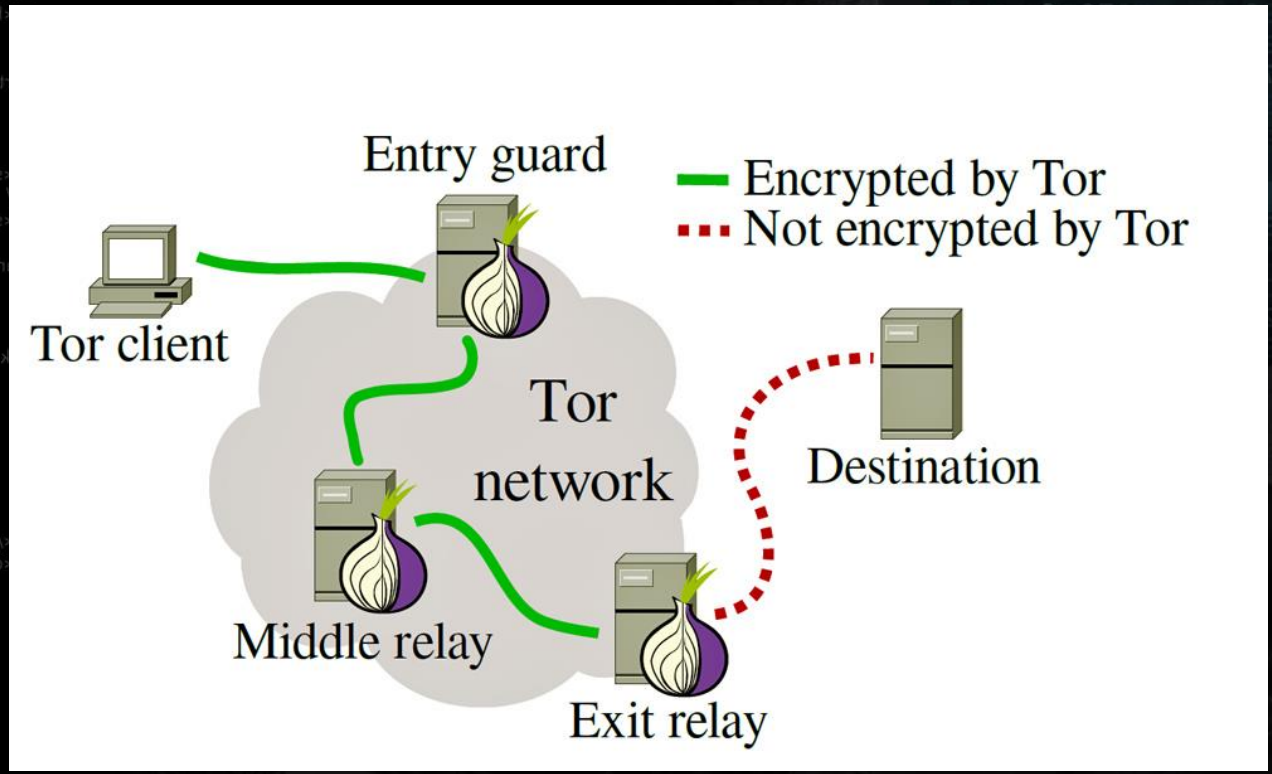
AEC
DATA SECURITY

The Onion Router

- Anonymizační šifrovaná síť
- entry/relay/exit node
- Seznam exit uzlů
  - https://check.torproject.org/cgi-bin/TorBulkExitList.py
- Tor Browser Bundle vs. Daemon
- Konzument vs. poskytovatel obsahu
  - Hidden Services

AEC
DATA SECURITY

Struktura sítě Tor



Hidden Services

- Webový server
  - LAMP
  - VPS/Raspberry Pi
- Domény
  - http://32rfckwuorlf4dlv.onion/
  - http://silkroad6ownowfk.onion/ (onioncat)

AEC
DATA SECURITY

Hidden Services - konfigurace

- /var/lib/tor/hidden_service/hostname
- /var/lib/tor/hidden_service/private_key

- /etc/tor/torrc

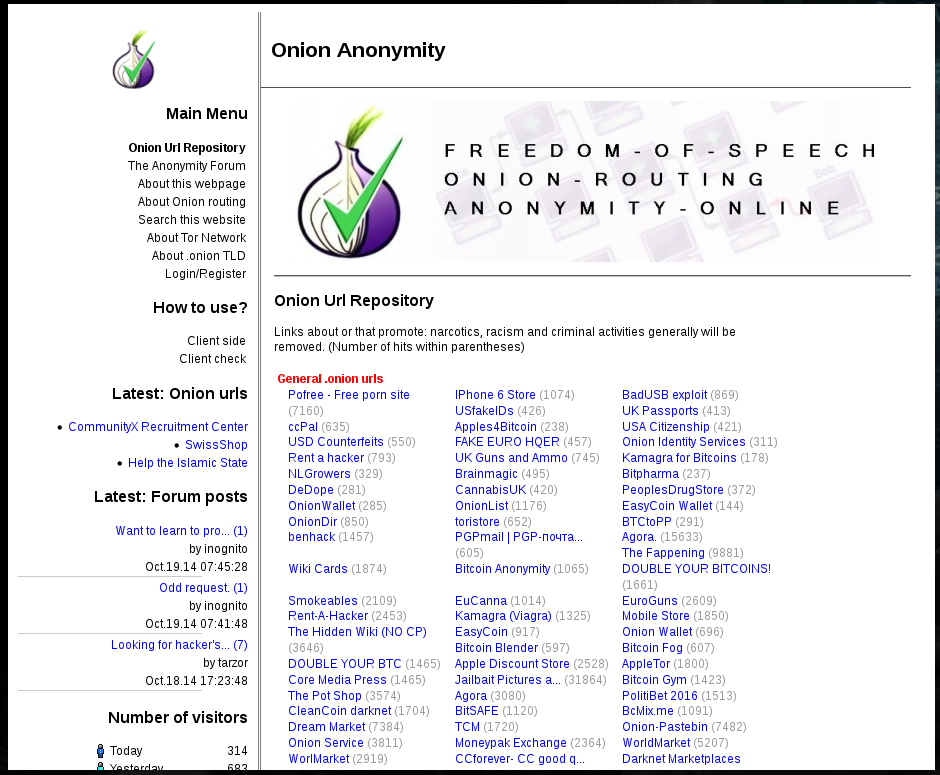
```
HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:80
```

Hidden Services - služby

- Katalogy
  - Onion Url Repository
  - http://32rfckwuorlf4dlv.onion/

AEC
DATA SECURITY

Onion Url Repository



Onion Anonymity

FREEDOM-OF-SPEECH
ONION-ROUTING
ANONYMITY-ONLINE

Main Menu

Onion Url Repository
The Anonymity Forum
About this webpage
About Onion routing
Search this website
About Tor Network
About .onion TLD
Login/Register

How to use?

Client side
Client check

Latest: Onion urls

- CommunityX Recruitment Center
- SwissShop
- Help the Islamic State

Latest: Forum posts

Want to learn to pro... (1)
by inognito
Oct.19.14 07:45:28

Odd request. (1)
by inognito
Oct.19.14 07:41:48

Looking for hacker's... (7)
by tarzor
Oct.18.14 17:23:48

Number of visitors

Today 314
Yesterday 683

Onion Url Repository

Links about or that promote: narcotics, racism and criminal activities generally will be removed. (Number of hits within parentheses)

General .onion urls

Pofree - Free porn site (7160)
ccPal (635)
USD Counterfeits (550)
Rent a hacker (793)
NLGrowers (329)
DeDope (281)
OnionWallet (285)
OnionDir (850)
benhack (1457)
Wiki Cards (1874)
Smokeables (2109)
Rent-A-Hacker (2453)
The Hidden Wiki (NO CP) (3646)
DOUBLE YOUR BTC (1465)
Core Media Press (1465)
The Pot Shop (3574)
CleanCoin darknet (1704)
Dream Market (7384)
Onion Service (3811)
WorlMarket (2919)

IPhone 6 Store (1074)
USfakeIDs (426)
Apples4Bitcoin (238)
FAKE EURO HQER (457)
UK Guns and Ammo (745)
Brainmagic (495)
CannabisUK (420)
OnionList (1176)
toristore (652)
PGPmail | PGP-почта... (605)
Bitcoin Anonymity (1065)
EuCanna (1014)
Kamagra (Viagra) (1325)
EasyCoin (917)
Bitcoin Blender (597)
Apple Discount Store (2528)
Jailbait Pictures a... (31864)
Agora (3080)
BitSAFE (1120)
TCM (1720)
Moneypak Exchange (2364)
CCforever- CC good q...

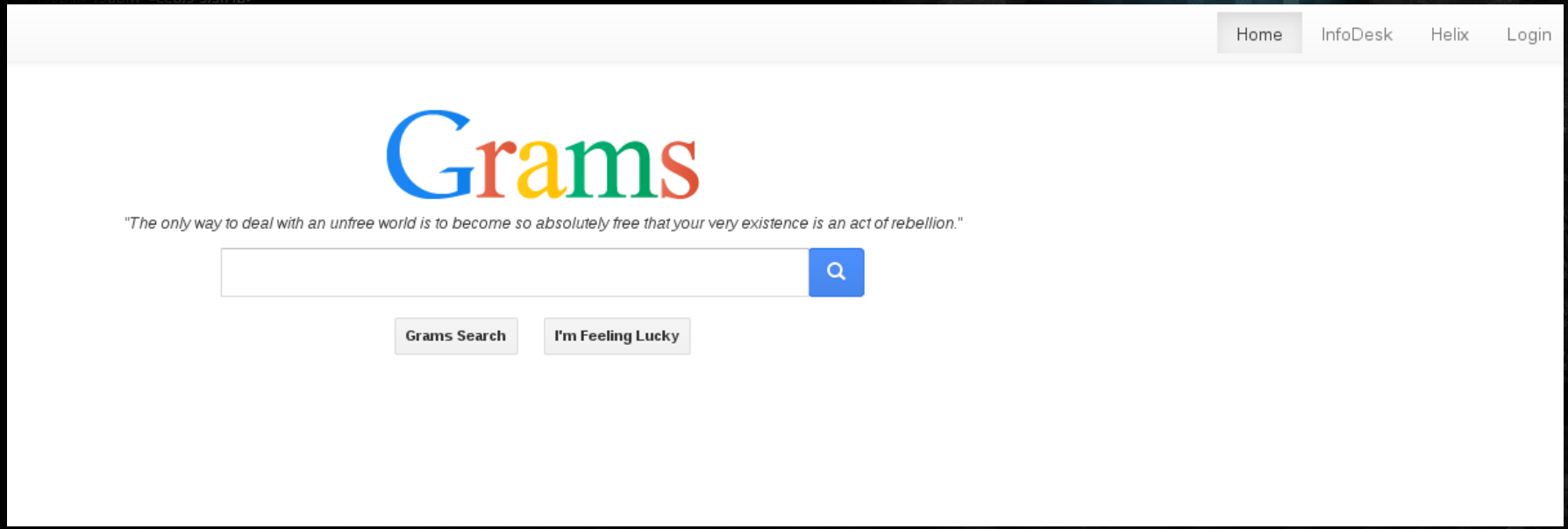
BadUSB exploit (869)
UK Passports (413)
USA Citizenship (421)
Onion Identity Services (311)
Kamagra for Bitcoins (178)
Bitpharma (237)
PeoplesDrugStore (372)
EasyCoin Wallet (144)
BTCtoPP (291)
Agora. (15633)
The Fappening (9881)
DOUBLE YOUR BITCOINS! (1661)
EuroGuns (2609)
Mobile Store (1850)
Onion Wallet (696)
Bitcoin Fog (607)
AppleTor (1800)
Bitcoin Gym (1423)
PolitiBet 2016 (1513)
BcMix.me (1091)
Onion-Pastebin (7482)
WorldMarket (5207)
Darknet Marketplaces

Hidden Services - služby

- Vyhledávače
  - Grams
  - http://grams7enufi7jmdl.onion/

AEC
DATA SECURITY

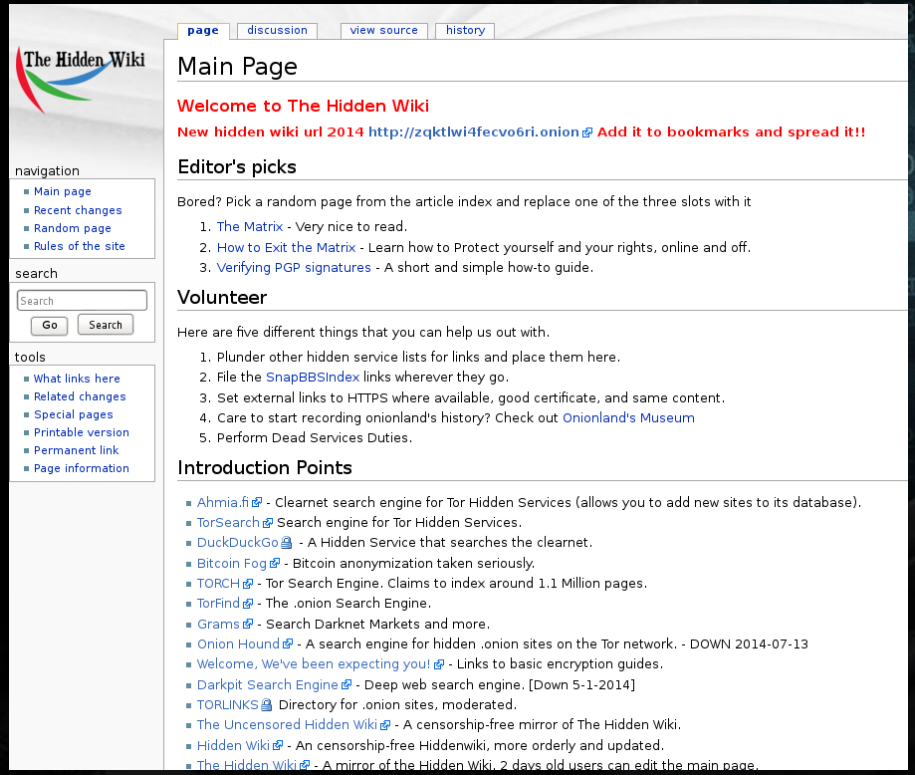
Grams


Home
InfoDesk
Helix
Login
Grams
"The only way to deal with an unfree world is to become so absolutely free that your very existence is an act of rebellion."
Grams Search
I'm Feeling Lucky

Hidden Services - služby

- Hidden Wiki
  - The Hidden Wiki
  - http://zqktlwi4fecvo6ri.onion/
  - http://kpvz7kpmcmne52qf.onion/

Hidden Wiki #1



page | discussion | view source | history

The Hidden Wiki

Main Page

Welcome to The Hidden Wiki

New hidden wiki url 2014 http://zqktlwi4fecvo6ri.onion Add it to bookmarks and spread it!!

navigation
- Main page
- Recent changes
- Random page
- Rules of the site

search
Search
Go | Search

tools
- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

Editor's picks

Bored? Pick a random page from the article index and replace one of the three slots with it

1. The Matrix - Very nice to read.
2. How to Exit the Matrix - Learn how to Protect yourself and your rights, online and off.
3. Verifying PGP signatures - A short and simple how-to guide.

Volunteer

Here are five different things that you can help us out with.

1. Plunder other hidden service lists for links and place them here.
2. File the SnapBBSIndex links wherever they go.
3. Set external links to HTTPS where available, good certificate, and same content.
4. Care to start recording onionland's history? Check out Onionland's Museum
5. Perform Dead Services Duties.

Introduction Points

- Ahmia.fi - Clearnet search engine for Tor Hidden Services (allows you to add new sites to its database).
- TorSearch Search engine for Tor Hidden Services.
- DuckDuckGo - A Hidden Service that searches the clearnet.
- Bitcoin Fog - Bitcoin anonymization taken seriously.
- TORCH - Tor Search Engine. Claims to index around 1.1 Million pages.
- TorFind - The .onion Search Engine.
- Grams - Search Darknet Markets and more.
- Onion Hound - A search engine for hidden .onion sites on the Tor network. - DOWN 2014-07-13
- Welcome, We've been expecting you! - Links to basic encryption guides.
- Darkpit Search Engine - Deep web search engine. [Down 5-1-2014]
- TORLINKS Directory for .onion sites, moderated.
- The Uncensored Hidden Wiki - A censorship-free mirror of The Hidden Wiki.
- Hidden Wiki - An censorship-free Hiddenwiki, more orderly and updated.
- The Hidden Wiki - A mirror of the Hidden Wiki. 2 days old users can edit the main page.

Hidden Wiki #2

- Welcome, We've been expecting you! - Links to basic encryption guides.
- AnonMail - Anonymous premium email service like lavabit. (Not free).
- Onion Mail - SMTP/IMAP/POP3. ***@onionmail.in address.

Financial Services

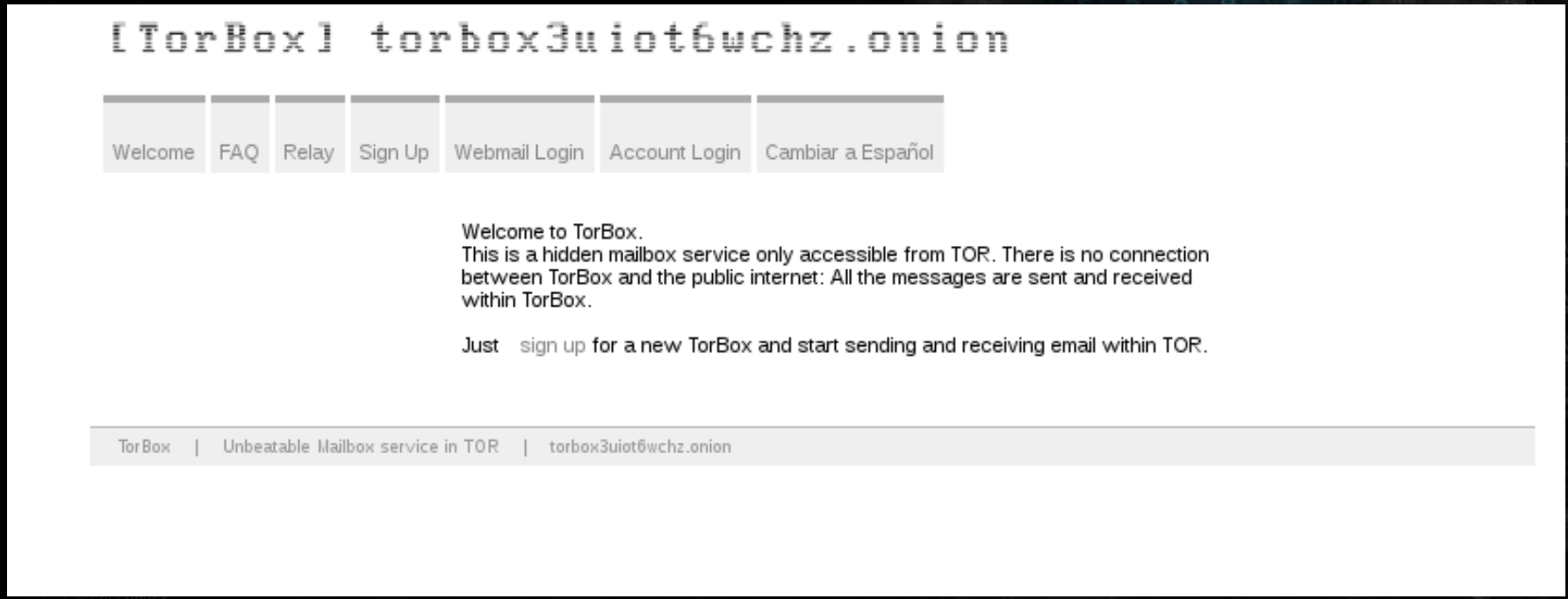
Currencies, banks, money markets, clearing houses, exchangers.

- [VERIFIED] WeBuyBitcoins - Sell your Bitcoins for Cash (USD), ACH, WU/MG, LR, PayPal and more.
- The Green Machine! Forum type marketplace with some of the oldest and most experienced vendors around. Get your paypals, CCs, etc, here!
- GreenPaper Counterfeiters Highest Quality USD and EUR Counterfeits on the market. Trusted and reputable vendor.
- [SCAM] WeBuyBitcoins - Sell your Bitcoins for Cash (USD), ACH, WU/MG, PayPal and more.
- [VERIFIED] btc-e.com - Clearnet link for buying and selling bitcoins.
- The PaypalDome Live Paypal accounts with good balances - buy some, and fix your financial situation for awhile.
- Bitiply! Multiply your Bitcoins through Bitcoin Malleability exploit!
- [VERIFIED] Tor Carders Market - Automated bitcoin marketplace of credit cards, dumps, and fullz from around the world.
- MoneyMarket! MoneyMarket has returned! VCC's, Real Credit Cards and Counterfeit money... Also portal to MoneyForum!
- [CAUTION] Fake Real Plastic - Credit Card vedor sharing my work for a reasonable price.
- [VERIFIED] Localbitcoins.com - Clearnet link for buying and selling bitcoins locally.
- Counterfeit_Currency Built to perfection currency. Euro and USD.
- [SCAM] Rachels Credit Cards - Stolen data on real cards.
- Bitcoin Smoke 0.5% fee Bitcoin Laundry Service on a dedicated server!
- YaayPal - Paypal accounts vendor. Sell for 8% of balance. Includes SOCKS5 and cashout method. Automated and livechat trades.
- Double your Bitcoins - Service that doubles your Bitcoins.
- Wall Street Tor - Paypal accounts, credit cards, we have everything!!
- [SCAM] BestPal BestPal is your Best Pal, if you need money fast. Sells stolen PP accounts.
- [SCAM] Cards and Cards CC Autoshop with up to 10% discount for bulk purchases!
- [VERIFIED] ecerv$olutions - Automated WW CC&CVV2 info selling service
- EasyCoin - Bitcoin Wallet with free Bitcoin Mixer.
- [SCAM] ecerv$olutions - Automated Paypal and CC selling store. Lowest prices!
- OnionWallet - Anonymous Bitcoin Wallet and Bitcoin Laundry.
- Clean My Coins - Clean your coins before and after every transaction with Bitcoin! 0.2% fixed fee.
- LARGE LAUNDRY - Bitcoin mixing service specializing in large amounts (>10 BTC) of Bitcoins. Uses advanced "Dynamic Mixing" process.
- [SCAM] HQER - High quality euro bills replicas / counterfeits.
- [SCAM] CC Planet - Best Autoshop for Credit Card mostly EU and US. New stocks,several sellers with automated Bitcoin system
- Stolen Paypal Accounts - Verified paypal accounts for sale.
- USD Counterfeits - High quality USD counterfeits.
- [SCAM] SOL's Euro Counterfeits - 50€ Counterfeit notes. Quality + Best Prices.

Hidden Services - služby

- Freemail
  - TorBox
  - http://torbox3uiot6wchz.onion/

TorBox

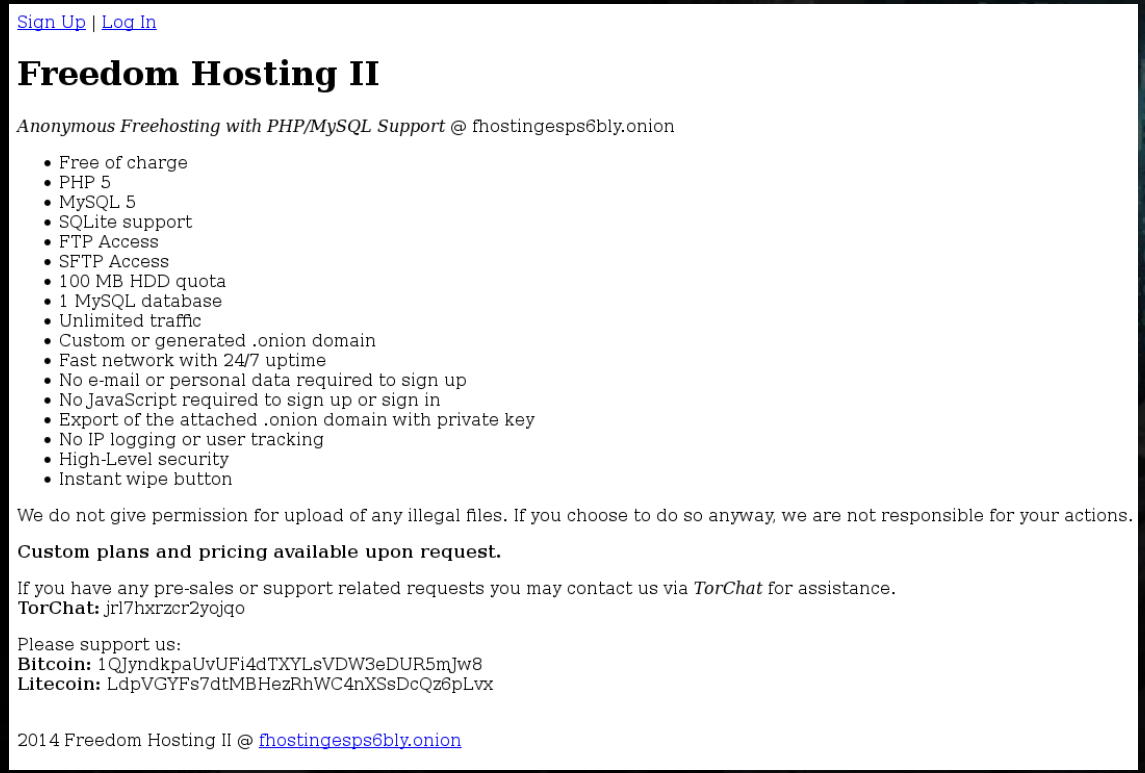

[TorBox] torbox3uiot6wchz.onion
Welcome
FAQ
Relay
Sign Up
Webmail Login
Account Login
Cambiar a Español
Welcome to TorBox.
This is a hidden mailbox service only accessible from TOR. There is no connection between TorBox and the public internet: All the messages are sent and received within TorBox.
Just sign up for a new TorBox and start sending and receiving email within TOR.
TorBox | Unbeatable Mailbox service in TOR | torbox3uiot6wchz.onion

Hidden Services - služby

- Freehosting
  - Freedom Hosting II
  - http://fhostingesps6bly.onion/

AEC
DATA SECURITY

Freedom Hosting II



Hidden Services - služby

- Webhosting
- VPS/Shells
- Image Hosting
- File Sharing
- IRC
- Dětské porno (CP)
- Black Markets
- …

AEC
DATA SECURITY

Black Markets

- Silk Road 2.0
  - http://silkroad6ownowfk.onion/
- Pandora
  - http://pandorajodqp5zrr.onion/
- Agora
  - http://agorahooawayyfoe.onion/
- Carders Market
  - http://carding2bil6j7ja.onion/

AEC
DATA SECURITY

Black Markets - zboží

- Drogy a zakázaná léčiva
- Čísla kreditních karet (cc)
- Zakázaná pyrotechnika, literatura
- Služby (hacking)
- Kradená elektronika
- Zbraně
- Falešné doklady, bankovky
- Nájemná vražda
- …

AEC
DATA SECURITY

Black Markets – systém důvěry

- Hodnocení uživatelů
- Escrow systém
- Finalize early (FE)
- Nedůvěryhodný inzerát
  - z podstaty věci (hitman)
  - Hidden Wiki „Scam“ tag
  - fotografie produktu

AEC
DATA SECURITY

Hodnocení uživatelů

MBB 6cm x 8cm 100 flat foil pouches

฿0.077639

ships from: United Kingdom
ships to: Worldwide

★★★★☆ (16)

sold by PlutoPete 93

Moisture Proof Mylar Bags (MBB) All shapes and sizes (NAME BRAND 3M)

฿0.000268

ships from: Undeclared
ships to: Undeclared

★★★★½ (13)

sold by SatoshiShop 92

MBB 8cm x 12cm 100 Flat Foil Pouches

฿0.142059

ships from: United Kingdom
ships to: Worldwide

★★★★½ (10)

sold by PlutoPete 93

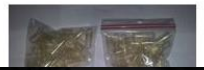
MBB 10cm x 15cm 100 Flat Foil Pouches

฿0.172532

ships from: United Kingdom
ships to: Worldwide

★★★★½ (11)

sold by PlutoPete 93



100pcs empty capsules size 00 Great to pack powdered drugs;)

฿0.015519

★★★★½ (8)

Black Markets – fotografie produktů

Black Markets - objednávka

- Produkt
- Množství
- Příplatek za Tracking number
- Sklad
- Jméno + adresa, resp. PM
- Komunikace pomocí PM (Private Message)

Black Markets - Adresa

- Anonymní P.O.Box
- Opuštěná stavba s číslem popisným
- Balík na poštu
- Internetové kavárny

AEC
DATA SECURITY

Black Markets - Platba

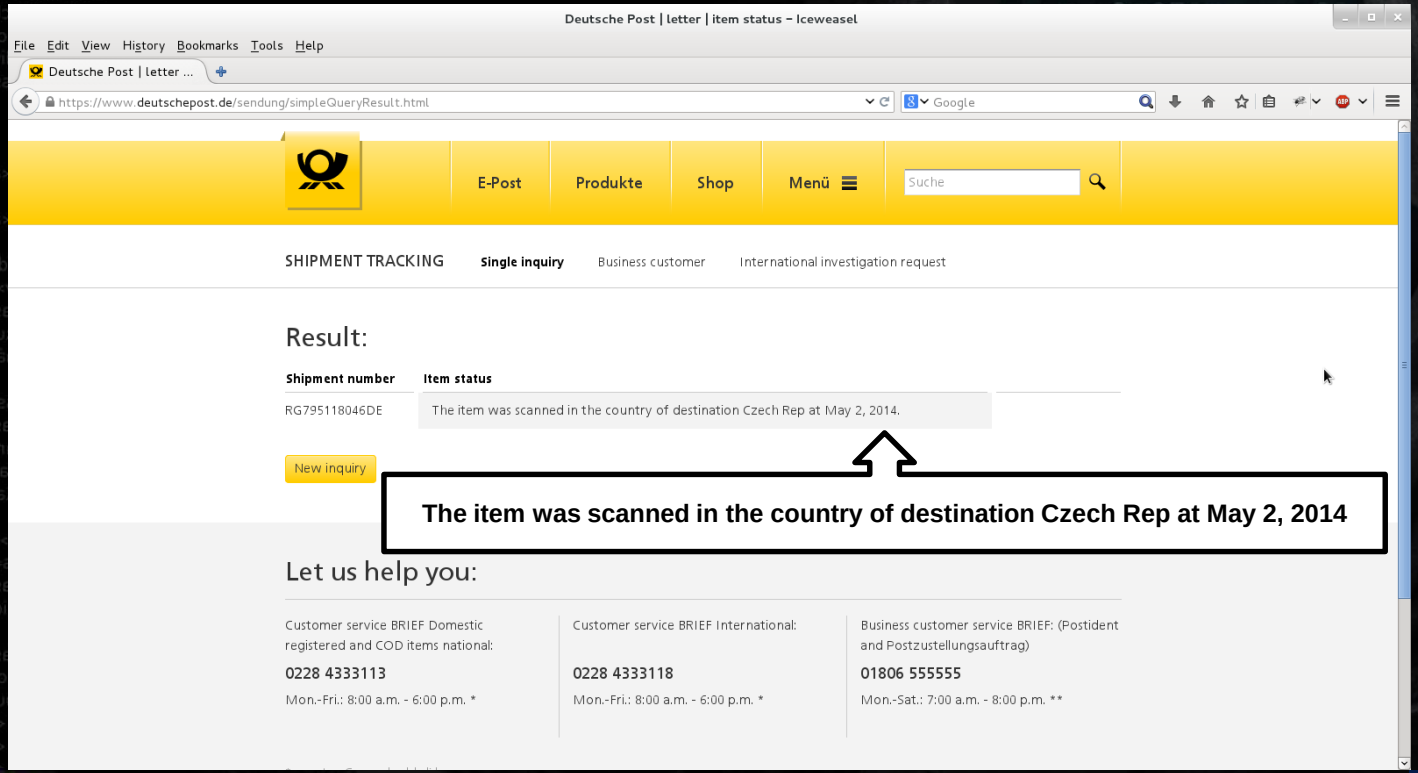
- Bitcoin
- Webmoney
- Perfectmoney
- Systémy bez Money Back Guarantee

AEC
DATA SECURITY

Black Markets - Packaging

- Obal
  - Vakuové sáčky
  - Alobal
  - Mylar fólie (MBB)
  - Knihy/časopisy
  - Systém dvojitého dna
- Balíček nedošel
  - Scam
  - Nevhodně zvolený obal – neprošel přes celnici

Zadržená zásilka



De-anonymizace v síti Tor

- De-anonymizace konzumentů služeb
- De-anonymizace provozovatelů služeb
- Hledání Deepnet služeb

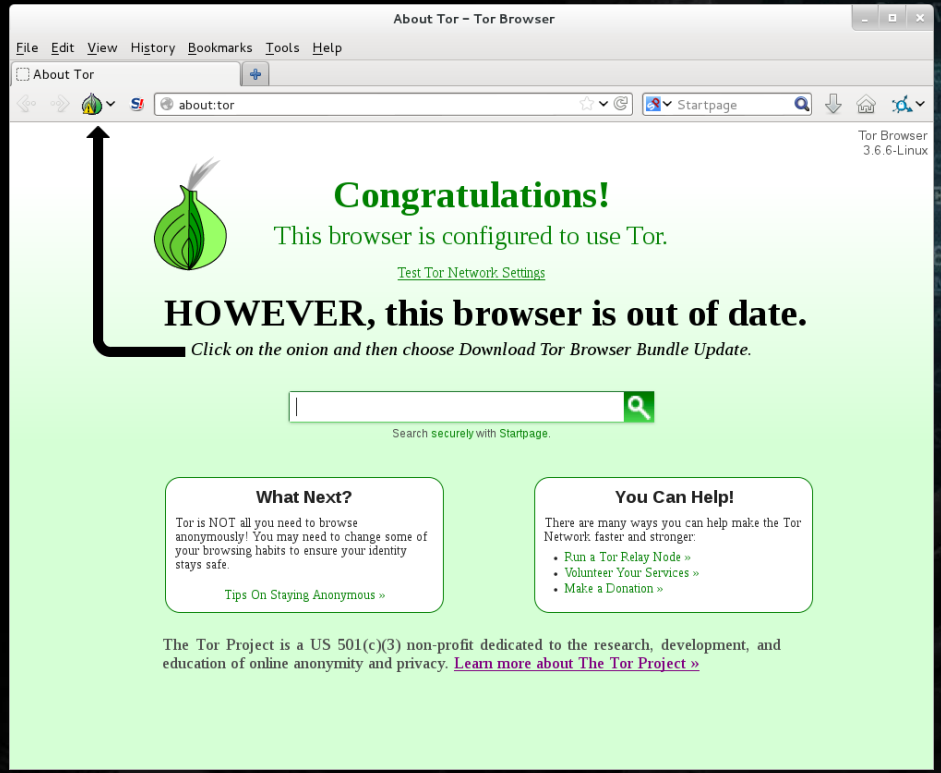
AEC
DATA SECURITY

De-anonymizace konzumentů služeb

- Zastaralý Tor Bundle Browser
  - Exploit
  - JavaScript (standardně povolen)
- Čas operačního systému návštěvníka (JS)
- Locales
  - Accept-Language: cs
- Poslat odkaz na URL v Clearnetu
- Poslat odkaz na PDF/Word dokument

AEC
DATA SECURITY

Out of Date Tor Bundle Browser



MS Word – IP Disclosure

- Vytvořit dokument se zajímavým textem
- Dokument uložit jako HTML stránku
- Vložit na konec dokumentu element s ext. Zdrojem

```
<img src="http://domain.tld/image.png">
```

- Změna přípony z .html na .doc(x)
- Funguje i v OpenOffice a LibereOffice
- MS Office 2010/2013 používá jádro IE 7

AEC
DATA SECURITY

De-anonymizace provozovatelů HS

- Poslat přes PM odkaz na URL v Clearnetu
- PDF/Word IP Disclosure
- Rogue Tor Nodes
- Hacking

AEC
DATA SECURITY

De-anonymizace - Hacking

- hostname -I
- curl ipecho.net/plain
  - iptables
- Exploit na aplikační vybavení
- Module server-status
  - date/time
  - návštěvnost
  - skrytá administrační rozhraní
  - krádeže BTC (session token v URL)

Hledání Deepnet služeb

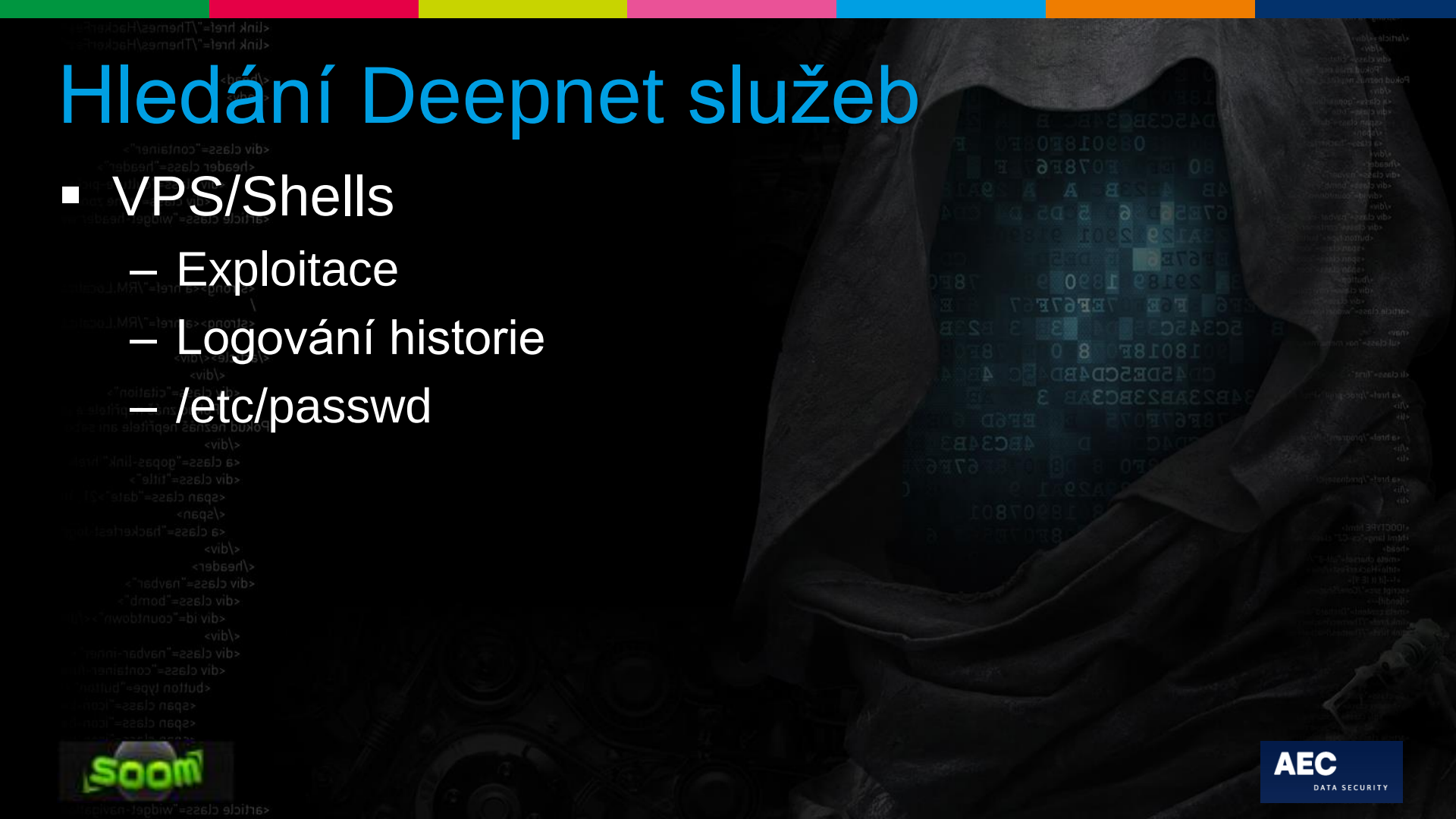
- Webhosting
  - PHP funkce *posix_getpwuid()*
  - Přístup k shellu přes PHP „exec“ funkce
  - mod_perl, mod_python
  - MySQL

```
LOAD DATA LOCAL INFILE '/etc/passwd' INTO TABLE test;
```

AEC
DATA SECURITY

Hledání Deepnet služeb

- VPS/Shells
  - Exploitace
  - Logování historie
  - /etc/passwd



Krádeže bitcoinů

- Module server-status
- wallet.dat (private/public key)
- Private Key = number
  - 256 bit unsigned integer (32 bytes)
  - 1157920892373161954235709850086879078532699846656405640394575840079131296399360 (10^{77})
- Brain Wallet
  - brainwallet.org
  - blockchain.info

Brain Wallet – bitcoind/bitcoin-cli

```
bitcoin-cli getbalance
# 0.00000000

bitcoin-cli importprivkey 5JdeQ39z8NUkNVvB37tt74Cu2WSNVj7qb9PdY651UoQnqyCm937
bitcoin-cli importprivkey 5JcHF3GtHTXHm2VVLYevaBYmp1MLEmrhQu4hL4gaPpXWxaQrJsa
bitcoin-cli importprivkey 5JXvHQfGHxUffo8BLRG1RBecRCZ2Jygtx5cNSiZoyk5Zcmhsdso
bitcoin-cli importprivkey ...

bitcoin-cli getbalance
# 0.61120000

bitcoin-cli sendtoaddress <attacker_btc_addres> <amount>
```

Praní špinavých Bitcoinů

- Všechny Bitcoinové transakce veřejné
  - https://blockchain.info/
- Mixing Service
  - https://bitmixer.io/
- Směnárny
  - BTC to USD
  - BTC to EUR

AEC
DATA SECURITY

Tor & Bitcoin aféry

- Silk Road
  - Spuštěna roku 2011
  - Vypnuta FBI roku 2013
  - Zakladatel Ross William Ulbricht aka „Dread Pirate Roberts“ (29 let, San Francisco)
  - Obviněn z praní špinavých peněz, obchodu s narkotiky, hackingu a objednání nájemných vražd
  - V roce 2013 původní admini zakládají Silk Road 2.0
  - Captcha

Tor & Bitcoin aféry

- Freedom Hosting
  - Spuštěn roku 2011
  - Vypnut FBI roku 2013
  - Zakladatel Eric Eoin Marques (28 let, Irsko)
  - Zanikla ½ všech Hidden Services v síti Tor
  - V roce 2014 spuštěn Freedom Hosting II

soom

AEC DATA SECURITY

Tor & Bitcoin aféry

- Sheep Marketplace
  - Spuštěn 2013
  - Provoz ukončen koncem téhož roku
  - Zakladatelem Čech Tomáš Jiříkovský aka Sheep
  - Odcizeno 5 400 BTC (~ 100 mil Korun)
  - Trestně stíhán
  - Webhosting snekweb.cz (Šnekweb)

Tor & Bitcoin aféry

- bitcash.cz
  - Provozovatelem Karel Minx aka Carlos
  - Fake e-mail koncem roku 2013
  - Odcizeny BTC v hodnotě 3,4 mil Kč
  - Závěr

De-anonymizační útok v Tor

- Největší dosud známý útok na anonymitu v Tor
- Od 30. ledna 2014 do 4. července 2014
- Přidáno 115 „zlých“ relay uzlů (6,4 %)
- Confirmation Attack & Sybila Attack
- Zaměřeno na de-anonymizaci Hidden Services
- Doporučen přesun HS na nové IP


?
soom
AEC
DATA SECURITY