RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: CCT-R06

Journey into The Darknet

Greg Jones

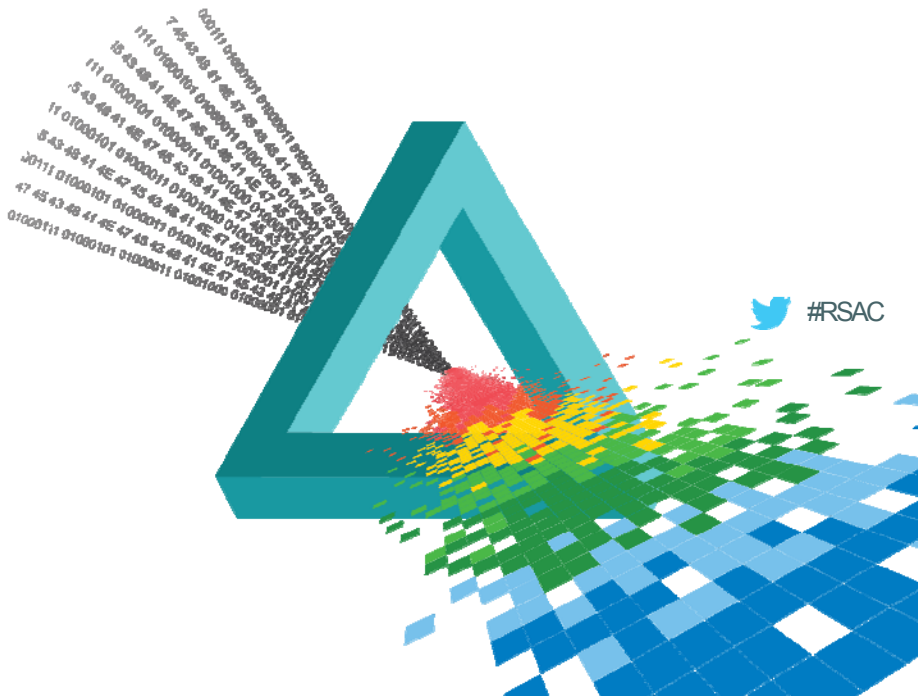
Director
Digital Assurance
@da_security

#RSAC

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Some scenarios



Darknet concept in one slide

- Consider a web-site. From the address we can derive:
  - The domain name (and associated registration details)
  - The IP address (and thus the physical location and registered owner)
- Consider a darknet hosted website. From the address we can derive nothing:
  - No physical location
  - No owner details
- **A darknet allows the hosting of content or services in a way that make it VERY HARD to identify who is running a server and where it is thus making it VERY HARD to take any lawful action against.**

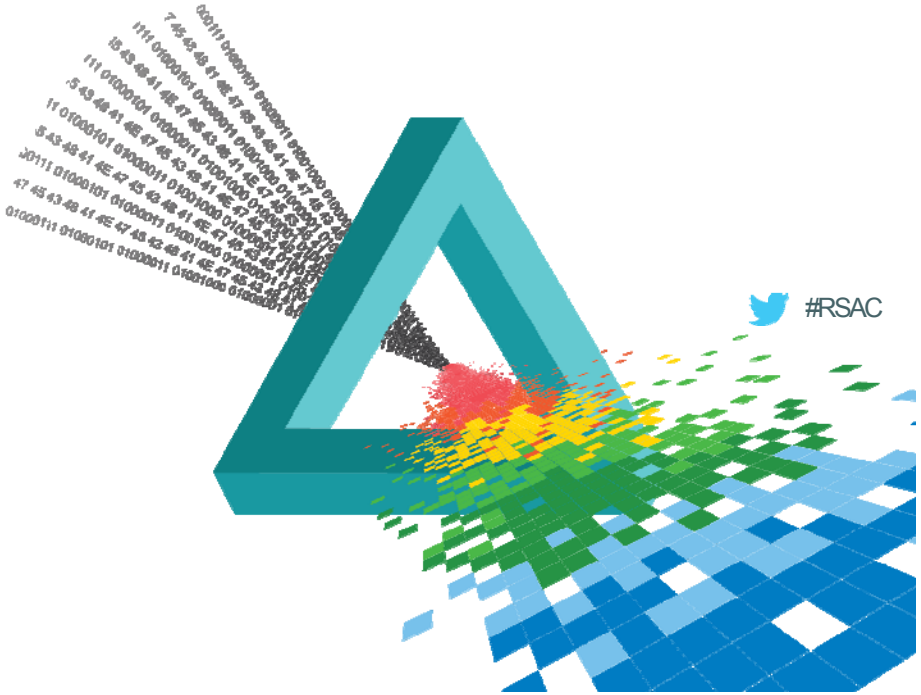
What's in a name?

- The phrase "darknet" was coined by Microsoft in or around 2002
- Their definition implied that all participants trusted each other (f-2-f)
- In general usage today, the term implies a hidden network layered on top of the Internet
- Terminology in common use includes:
  - Darknet
  - Darkweb
  - Deepweb
- You will frequently see these three names used interchangeably
- There is not a single Darknet but rather a collection of distinct darknets

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Darknet Technical Primer



Darknet characteristics

- Must have
  - Allow all client nodes to communicate with all publishing nodes
  - Ensure that the underlying IP address (if any) of a node cannot be readily determined
  - Ensure that all node to node communications are both authenticated and encrypted
  - De-centralised architecture, no “trusted” systems or people (SPoF)

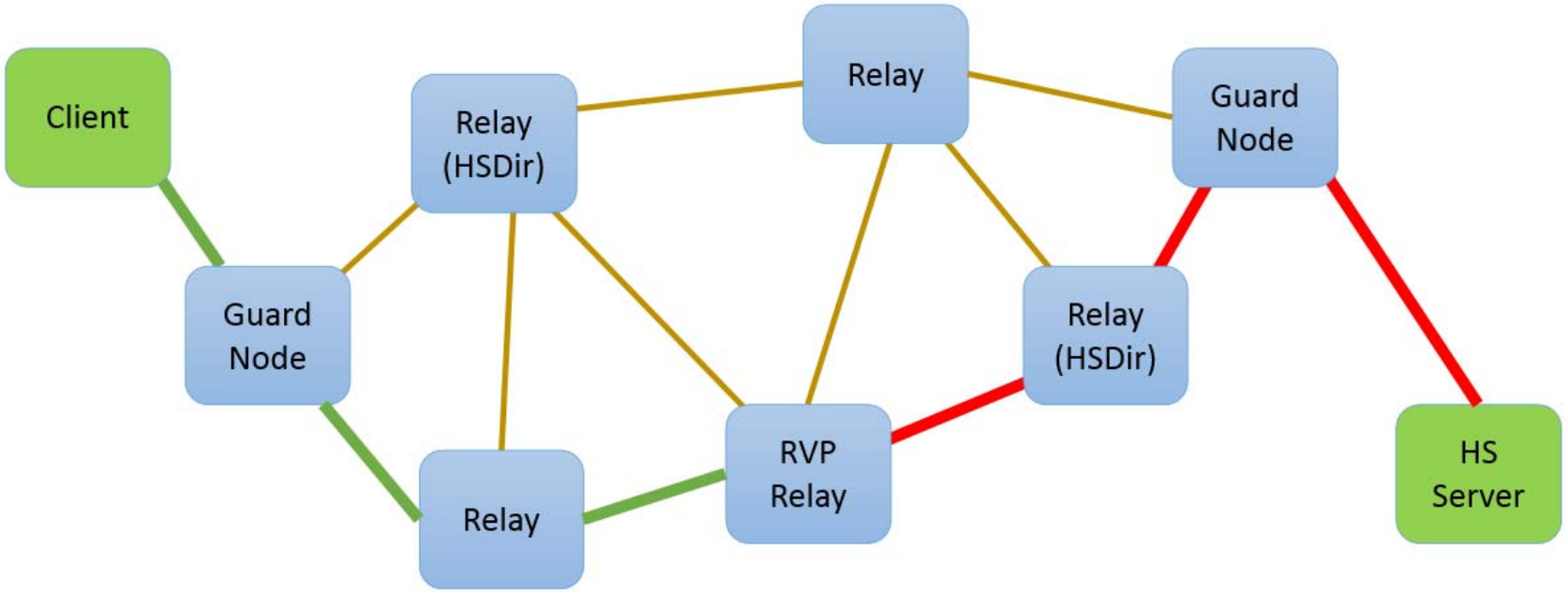
- Nice to have
  - Variable latency options
  - Asymmetric traffic paths
  - Underlying network independence
  - Portability

Current Implementations

- Currently four main darknet technologies in use:
  - Freenet (1999) – one of the first and still going strong – P2P based, focused on storing distributed content
  - GNUnet (2001) – P2P based, focus on hosting content/files although arbitrary circuits available for messaging, voice etc.
  - I2p (2003) – P2P, packet switched network that comprehensively supports darknet operation through the use of “eep sites”
  - Tor (2004) – Primarily an anonymising network but also supports darknet operation through the use of “Hidden Services” (ONION LAND)
- All four platforms have strengths and weaknesses in different areas
- Tor Hidden Services almost certainly the most popular technology for interactive applications at the moment

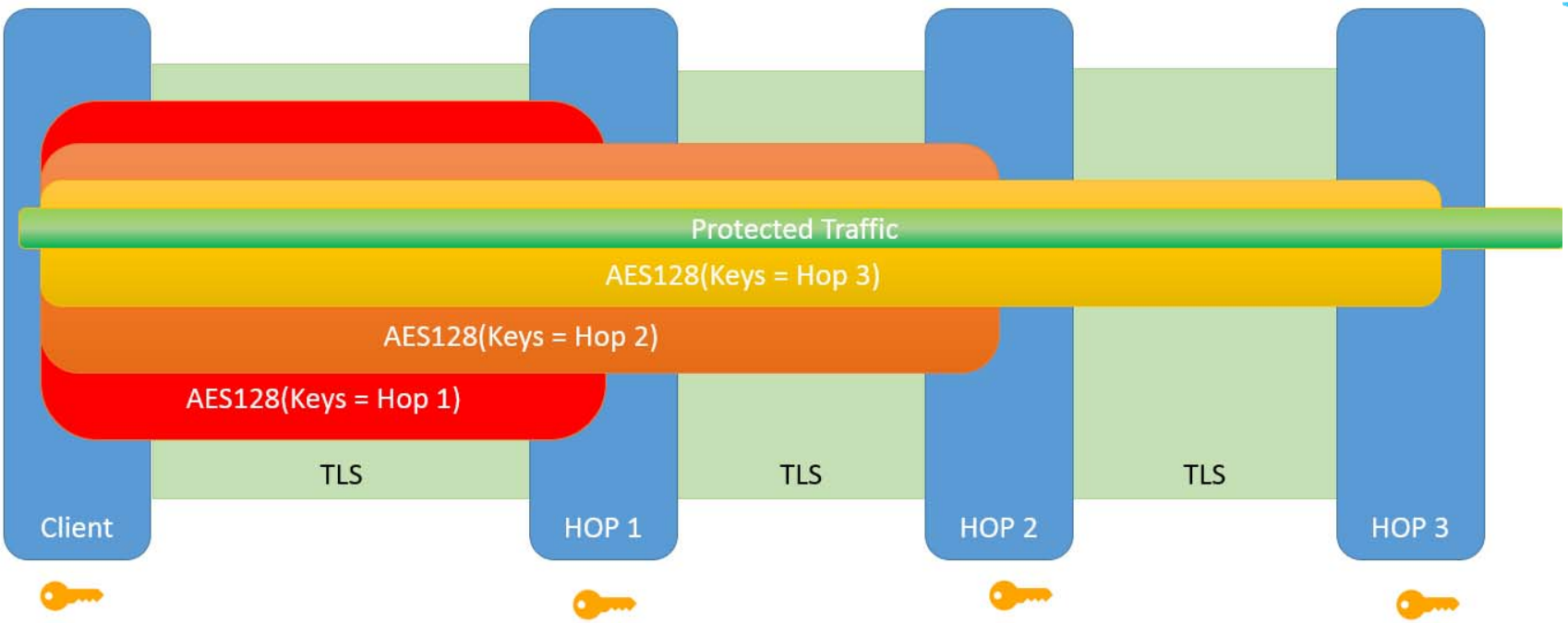
Tor Hidden Services

- Hidden Services are TCP end-points that exist inside the Tor network.
- Clients <> Hidden Service communications are usually routed through 6 hops and are end-to-end encrypted
- All Tor hidden services are accessed using a special '.onion' TLD e.g.
  - 3g2upl4pq6kufc4m.onion – Duck Duck Go search engine
  - silkroad6ownowfk.onion – Silk Road (v 2) – [Defunct as of Oct 2014]
  - facebookcorewwwi.onion – Facebook – [Launched 12 months ago]
  - digitalass6qi2nt.onion - DA
- Any Tor node including clients can publish a Hidden Service Descriptor that any other Tor node can connect to irrespective of underlying IP topology
- The main property of a hidden service is that it is non-trivial to determine where the service is hosted



Simplified Tor Hidden Service communications path

7 relays are shown for simplicity, currently there are around 6500 operational relays



Simplified view of traffic protection in Tor

Public RSA keys for node authentication and identities

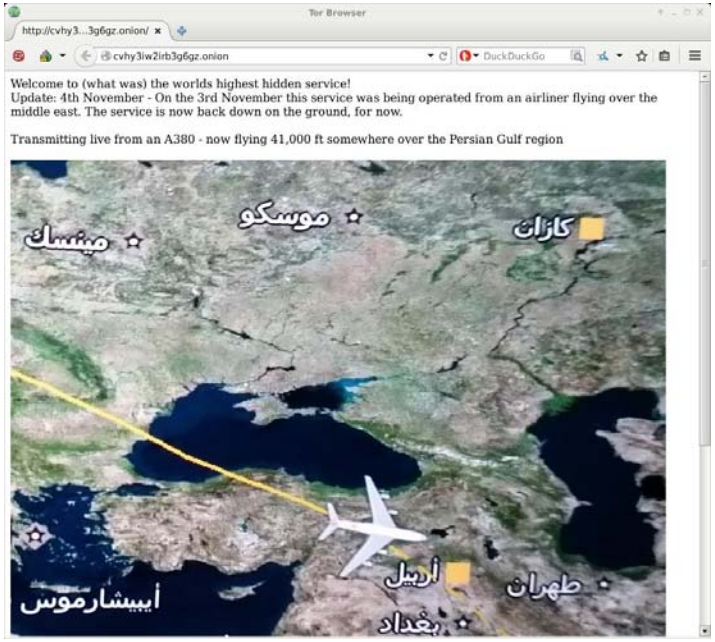
Symmetric AES keys for traffic protection

A tail of two hidden services

- http://cvhy3iw2irb3g6gz.onion
- http://pmswzoaidurnniz7.onion:8080

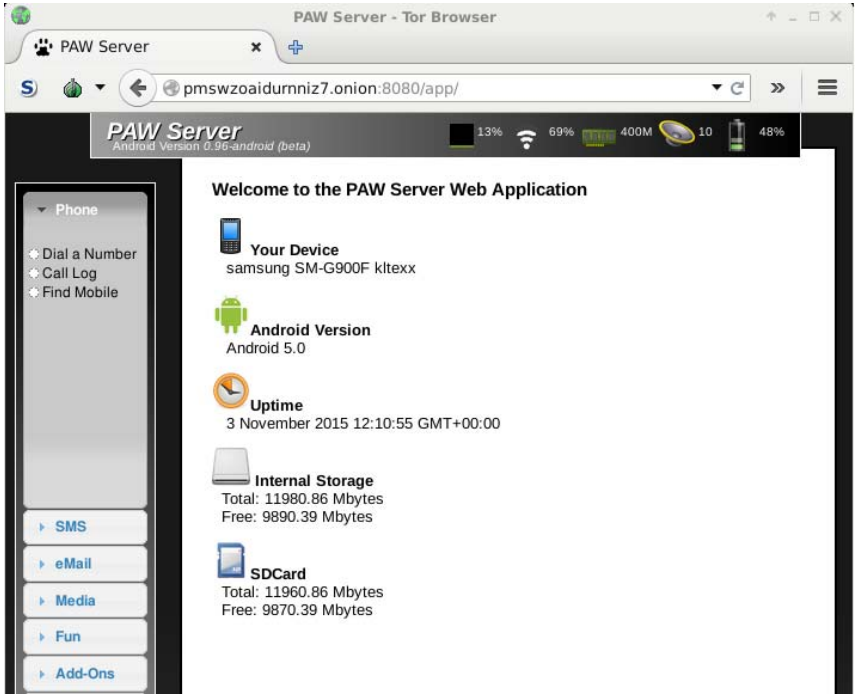
- The first address is now “down”
- The second is live and close by

- Any guesses?



HS 1: The worlds highest hidden service

Served from 41,000 ft via http://cvhy3iw2irb3g6gz.onion



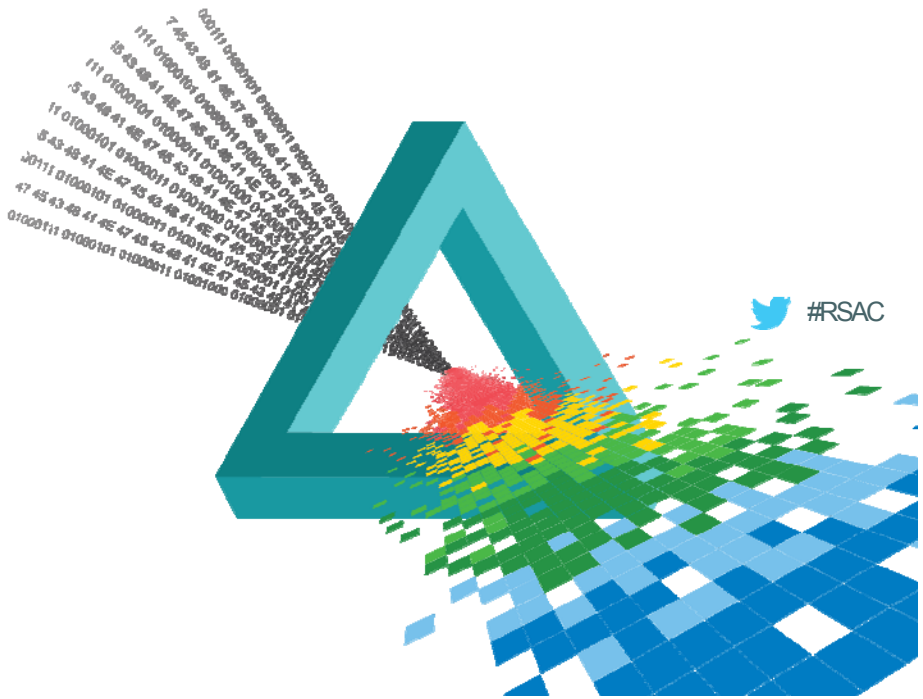
HS 2: A Darknet webserver on a smartphone

Served from my pocket via http://pmswzoaidurnniz7.onion:8080

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

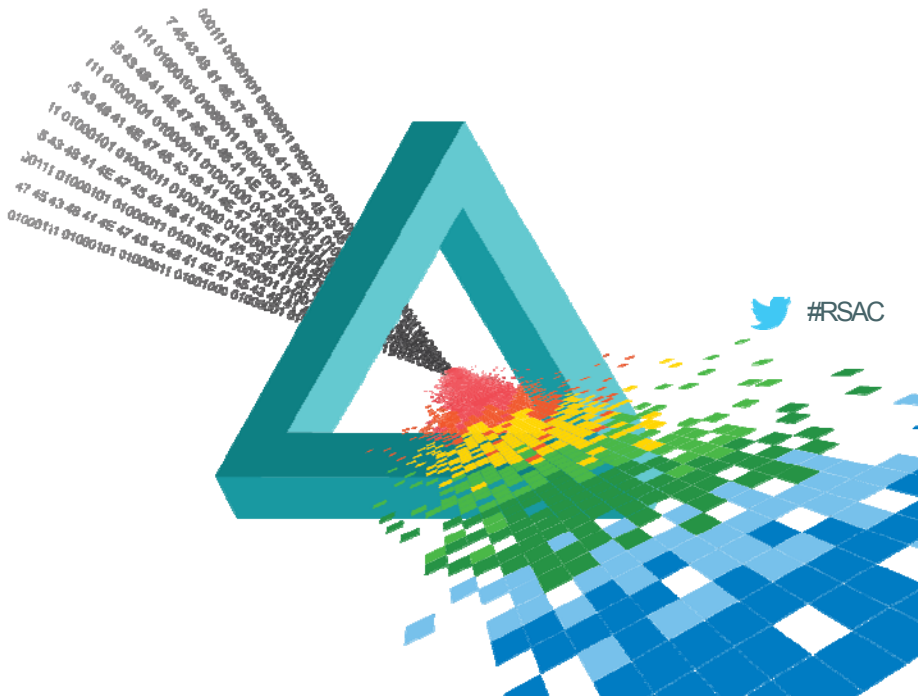
Any questions so far?



RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

The New (Dark) Economy



Crime - Traditional vs New (Dark) Economy

Traditional

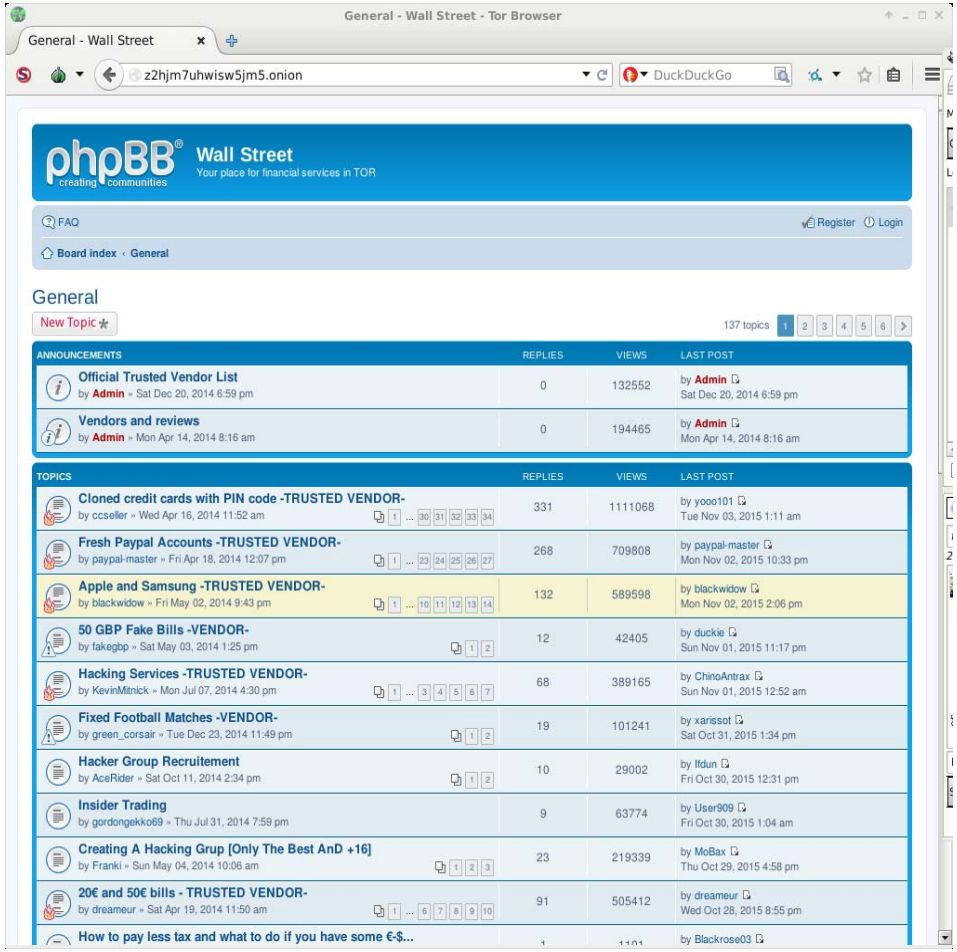
- Need to know the “right person”
- Need to meet counter-party
- Danger of physical violence
- Lack of accountability – high chance of being ripped off
- Cash = high anonymity

Dark Economy

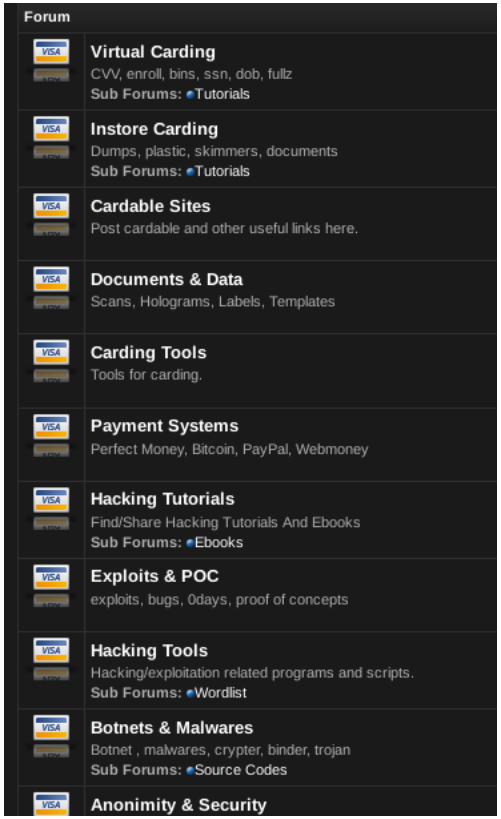
- On-line catalogues of the “right people”
- No need to leave home
- Ability to view and add to counter-party feedback and reputation
- Crypto-currency = perceived anonymity

Forums

- Forums sites are very common on the Darknet
- A large range of topics both legal and illegal are catered for
- Hacking and fraud related forums present participants with an opportunity for trading and knowledge sharing
- Some of the more public recent breaches have been discussed and in a number of instances the actual ‘dumps’ themselves are posted
- A very active hacking forum (Hell) was recently shutdown when the operator (Ping) was arrested on hacking and fraud charges

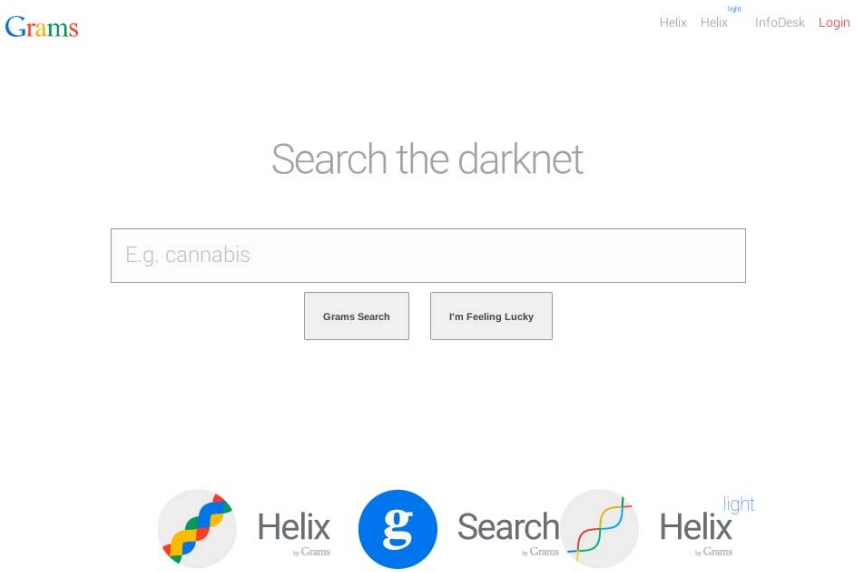

General - Wall Street - Tor Browser
General - Wall Street
z2hjm7uhwisw5jm5.onion
DuckDuckGo
phpBB creating communities
Wall Street
Your place for financial services in TOR
FAQ
Register
Login
Board index ‹ General
General
New Topic
137 topics
ANNOUNCEMENTS
REPLIES
VIEWS
LAST POST
Official Trusted Vendor List
by Admin » Sat Dec 20, 2014 6:59 pm
0
132552
by Admin
Sat Dec 20, 2014 6:59 pm
Vendors and reviews
by Admin » Mon Apr 14, 2014 8:16 am
0
194465
by Admin
Mon Apr 14, 2014 8:16 am
TOPICS
REPLIES
VIEWS
LAST POST
Cloned credit cards with PIN code -TRUSTED VENDOR-
by ccseller » Wed Apr 16, 2014 11:52 am
331
1111068
by yooo101
Tue Nov 03, 2015 1:11 am
Fresh Paypal Accounts -TRUSTED VENDOR-
by paypal-master » Fri Apr 18, 2014 12:07 pm
268
709808
by paypal-master
Mon Nov 02, 2015 10:33 pm
Apple and Samsung -TRUSTED VENDOR-
by blackwidow » Fri May 02, 2014 9:43 pm
132
589598
by blackwidow
Mon Nov 02, 2015 2:06 pm
50 GBP Fake Bills -VENDOR-
by fakegbp » Sat May 03, 2014 1:25 pm
12
42405
by duckie
Sun Nov 01, 2015 11:17 pm
Hacking Services -TRUSTED VENDOR-
by KevinMitnick » Mon Jul 07, 2014 4:30 pm
68
389165
by ChinoAntrax
Sun Nov 01, 2015 12:52 am
Fixed Football Matches -VENDOR-
by green_corsair » Tue Dec 23, 2014 11:49 pm
19
101241
by xarissot
Sat Oct 31, 2015 1:34 pm
Hacker Group Recruitement
by AceRider » Sat Oct 11, 2014 2:34 pm
10
29002
by Ifdun
Fri Oct 30, 2015 12:31 pm
Insider Trading
by gordongekko69 » Thu Jul 31, 2014 7:59 pm
9
63774
by User909
Fri Oct 30, 2015 1:04 am
Creating A Hacking Grup [Only The Best AnD +16]
by Franki » Sun May 04, 2014 10:06 am
23
219339
by MoBax
Thu Oct 29, 2015 4:58 pm
20€ and 50€ bills - TRUSTED VENDOR-
by dreameur » Sat Apr 19, 2014 11:50 am
91
505412
by dreameur
Wed Oct 28, 2015 8:55 pm
How to pay less tax and what to do if you have some €-$...
by Blackrose03

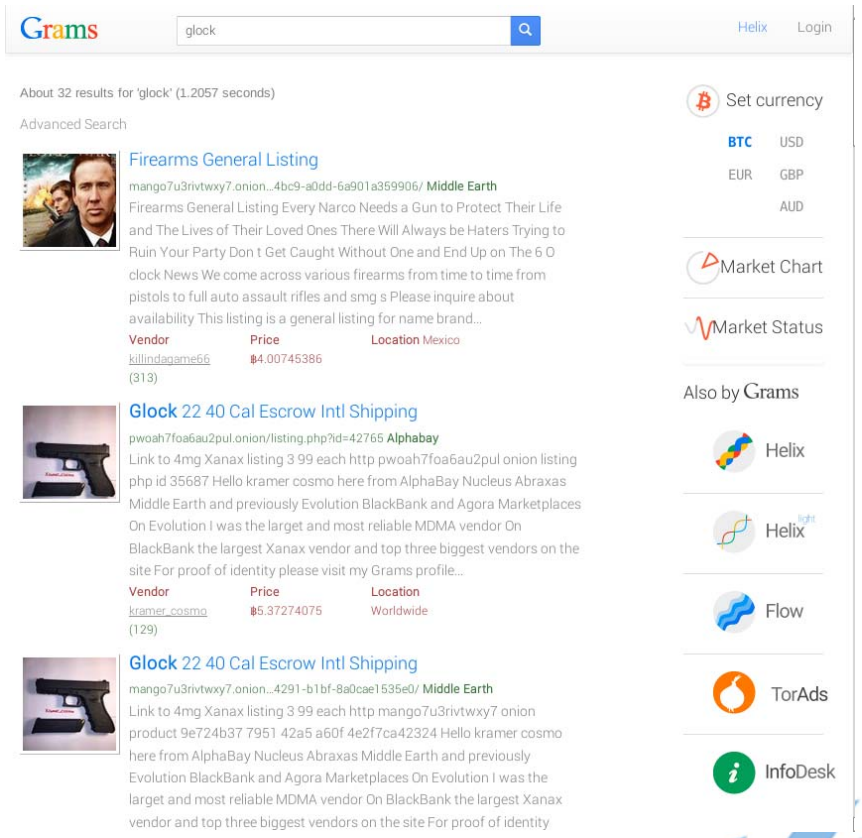
#RSAC


Forum
Virtual Carding
CVV, enroll, bins, ssn, dob, fullz
Sub Forums: Tutorials
Instore Carding
Dumps, plastic, skimmers, documents
Sub Forums: Tutorials
Cardable Sites
Post cardable and other useful links here.
Documents & Data
Scans, Holograms, Labels, Templates
Carding Tools
Tools for carding.
Payment Systems
Perfect Money, Bitcoin, PayPal, Webmoney
Hacking Tutorials
Find/Share Hacking Tutorials And Ebooks
Sub Forums: Ebooks
Exploits & POC
exploits, bugs, 0days, proof of concepts
Hacking Tools
Hacking/exploitation related programs and scripts.
Sub Forums: Wordlist
Botnets & Malwares
Botnet , malwares, crypter, binder, trojan
Sub Forums: Source Codes
Anonimity & Security

Darknet Markets

- Web based markets which enable vendors to advertise their wares and buyers to purchase said wares – in total there are around 4000 vendors
- Often, but not always, illicit stuff like narcotics, hacking services and on some markets, weapons and products/services for undertaking fraud
- Dark Net Markets, when stable, turnover around $20 million dollars a month – mostly in Bitcoin.
- Big markets have included: SR, Atlantis, Sheep, Evolution and Agora
- Currently the biggest market is probably Abraxas.
- Some vendors have their own dedicated web-sites, some trade on forums or via e-mail
- Decentralised markets are in development and coming soon…





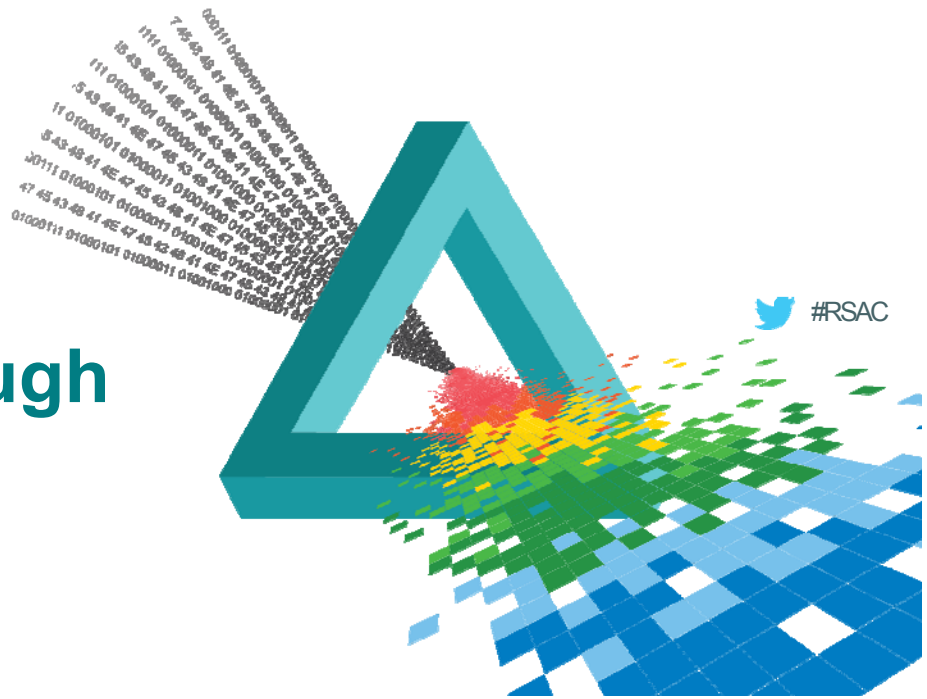
Grams – a DNM search engine

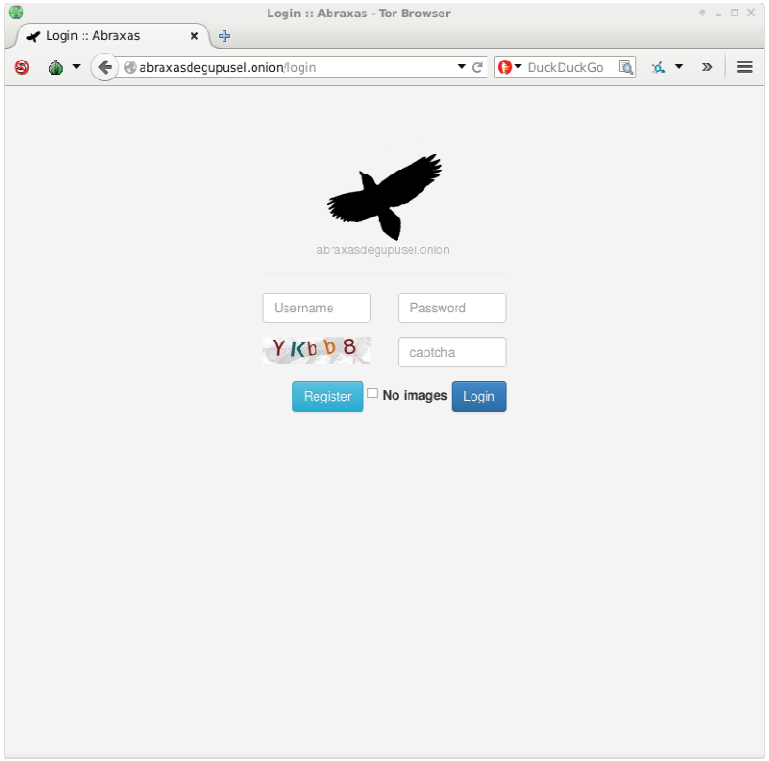
DigitalAssurance

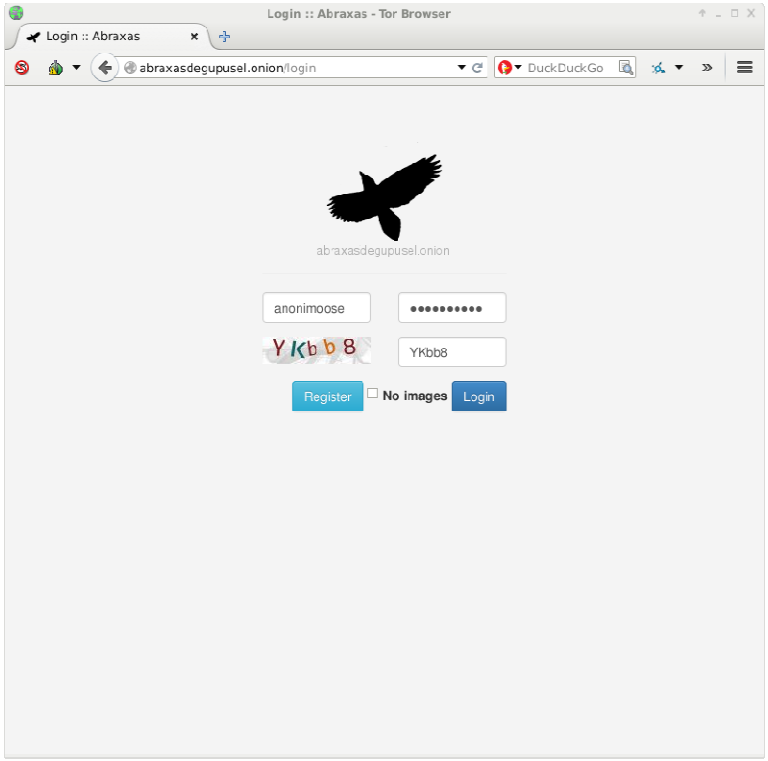
RSAConference2015

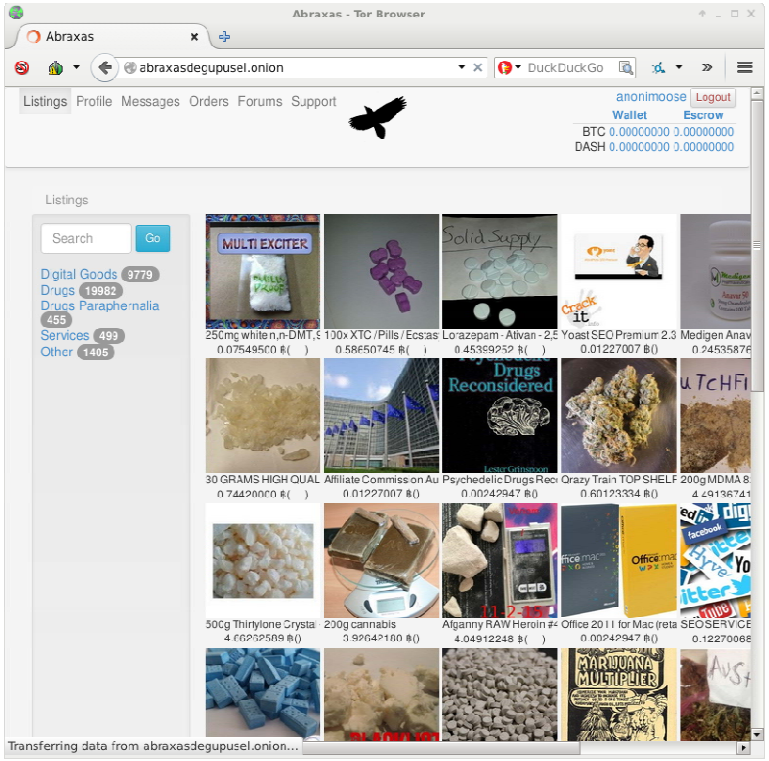
Abu Dhabi | 4–5 November | Emirates Palace

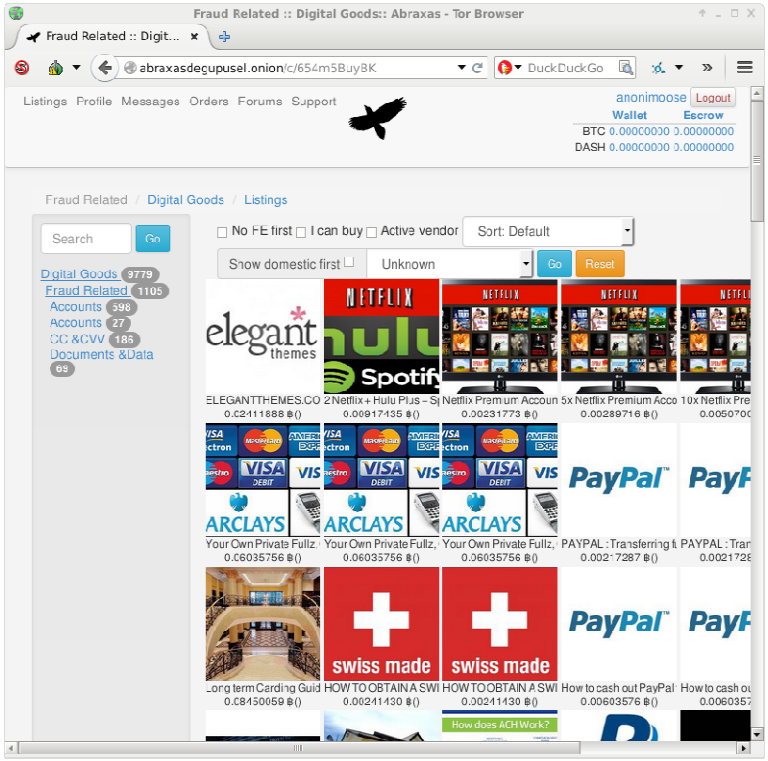
Darknet Market Walkthrough

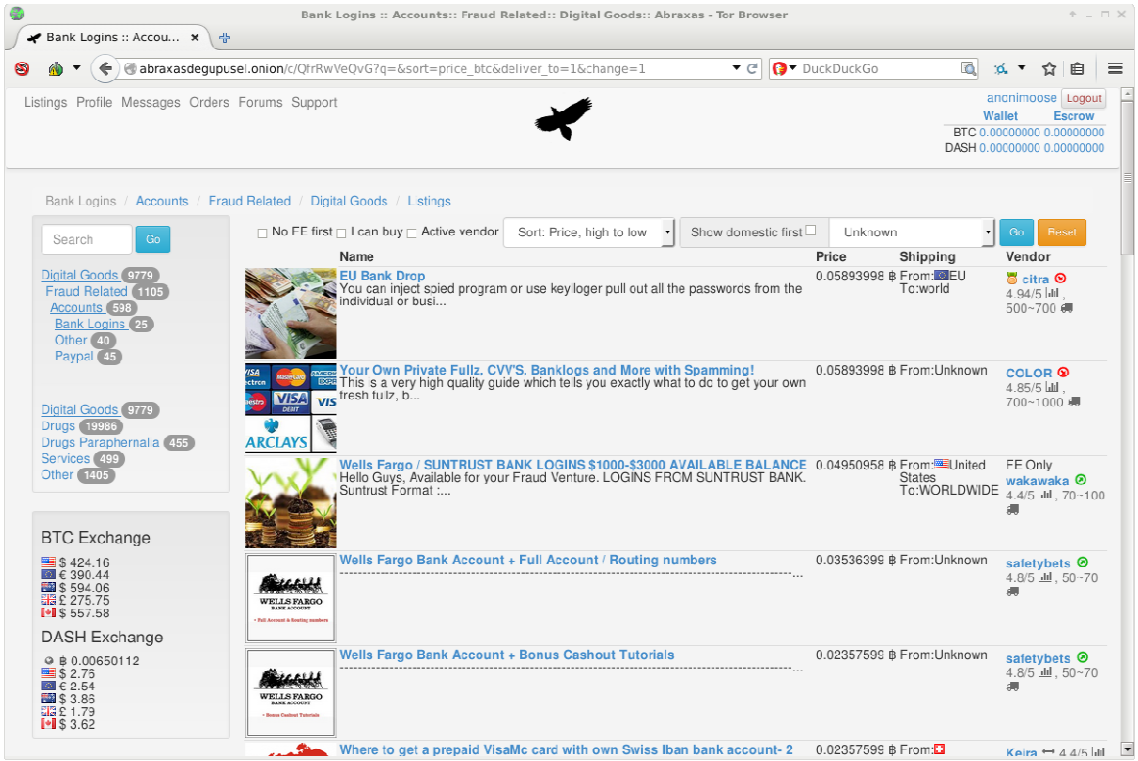


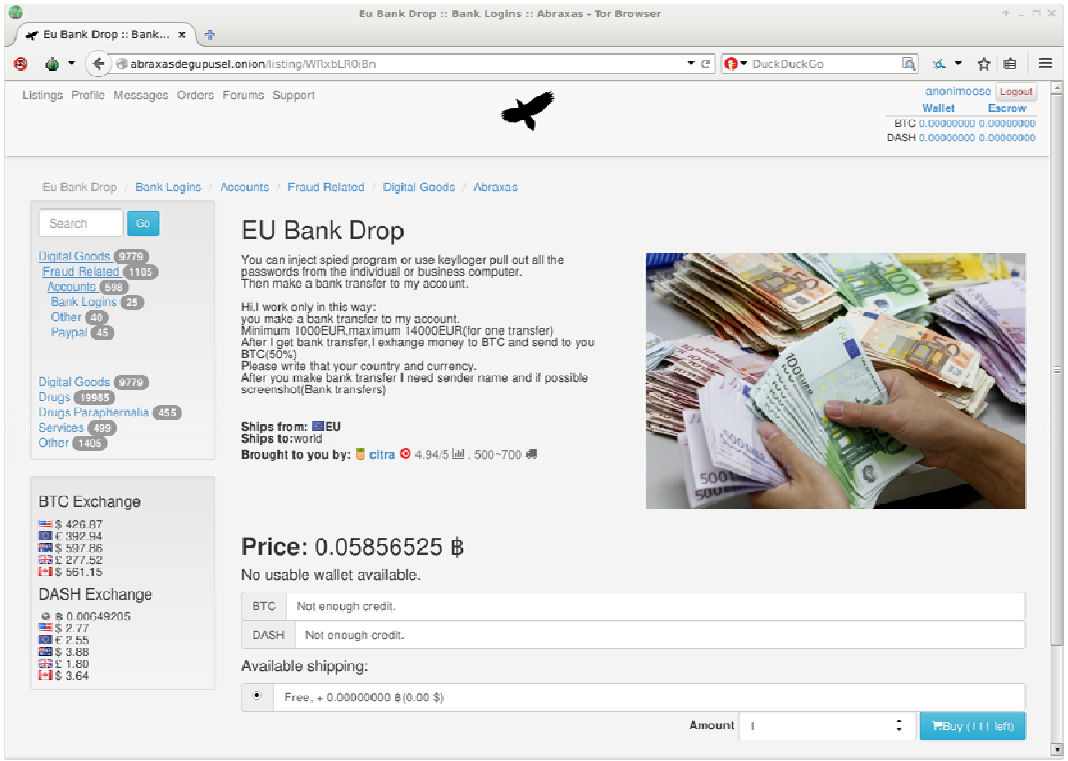

Login :: Abraxas - Tor Browser
Login :: Abraxas
abraxasdeçupusel.onion/login
DuckDuckGo
abraxasdegupusel.onion
Username
Password
captcha
Register
No images
Login

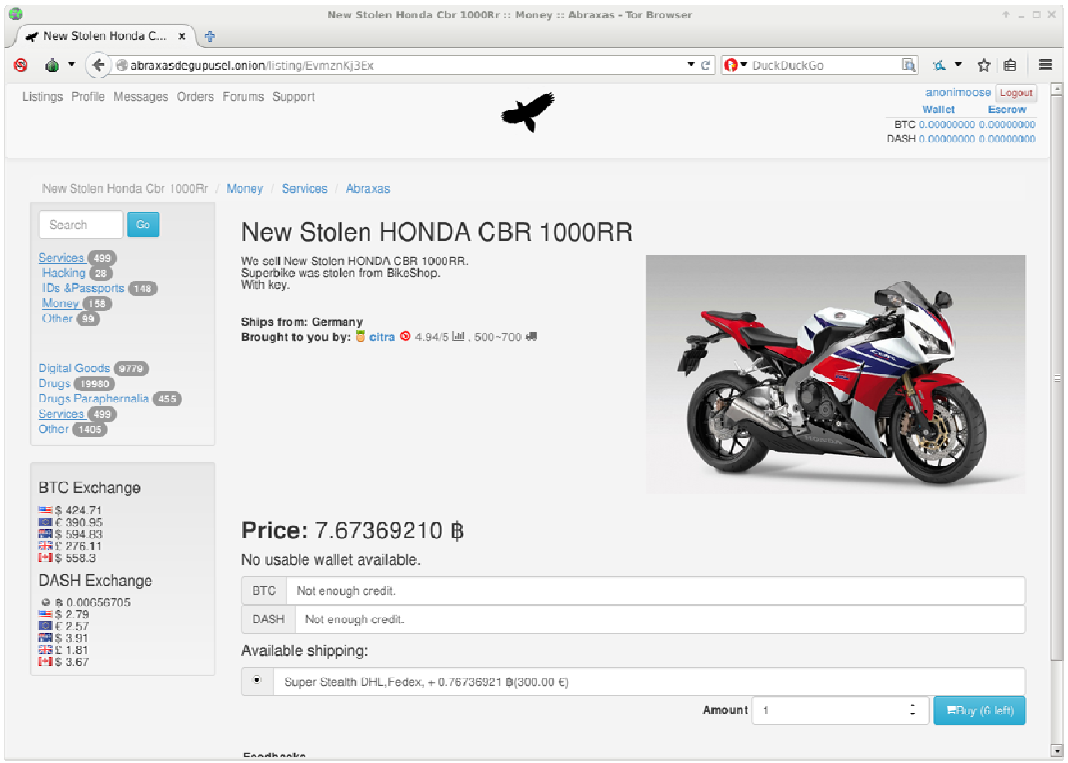

Login :: Abraxas - Tor Browser
Login :: Abraxas
abraxasdegupusel.onion/login
DuckDuckGo
abraxasdegupusel.onion
anonimoose
Ykbb8
Register
No images
Login


Abraxas - Tor Browser
Abraxas
abraxasdegupusel.onion
DuckDuckGo
Listings Profile Messages Orders Forums Support
anonimoose Logout
Wallet Escrow
BTC 0.00000000 0.00000000
DASH 0.00000000 0.00000000
Listings
Search
Go
Digital Goods 9779
Drugs 19982
Drugs Paraphernalia 455
Services 493
Other 1405
MULTI EXCITER
Solid Supply
Drugs Reconsidered
MARIJUANA MULTIPLIER
Transferring data from abraxasdegupusel.onion...


Fraud Related :: Digital Goods:: Abraxas - Tor Browser
Fraud Related :: Digit...
abraxasdecupusel.onion/c/654m5Buy8K
DuckDuckGo
Listings Profile Messages Orders Forums Support
anonimoose Logout
Wallet Escrow
BTC 0.00000000 0.00000000
DASH 0.00000000 0.00000000
Fraud Related / Digital Goods / Listings
Search Go
Digital Goods 9779
Fraud Related 1105
Accounts 398
Accounts 27
CC &CVV 185
Documents &Data 65
No FE first I can buy Active vendor Sort: Default
Show domestic first Unknown Go Reset
elegant themes
NETFLIX
Spotify
ELEGANTTHEMES.CO 2 Netflix + Hulu Plus – Sp Netflix Premium Accoun 5x Netflix Premium Acco 10x Netflix Pre
0.02111888 ฿() 0.00917435 ฿() 0.00231773 ฿() 0.00289716 ฿() 0.0050700
VISA DEBIT
ARCLAYS
Your Own Private Fullz Your Own Private Fullz, Your Own Private Fullz, PAYPAL : Transferring f PAYPAL : Tran
0.06035756 ฿() 0.06035756 ฿() 0.06035756 ฿() 0.002 7287 ฿() 0.0021728
PayPal
swiss made
Long term Carding Guid HOW TO OBTAIN A SWI HOW TO OBTAIN A SWI How to cash out PayPal How to cash ou
0.08450059 ฿() 0.00241430 ฿() 0.00241430 ฿() 0.00603576 ฿() 0.0060357
How does ACH Work?

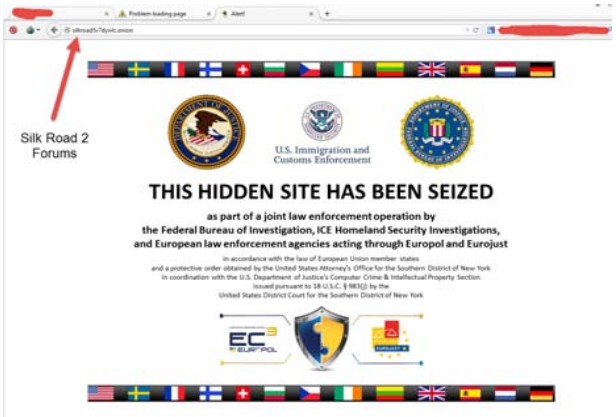

Bank Logins :: Accounts:: Fraud Related:: Digital Goods:: Abraxas - Tor Browser
Bank Logins :: Accou...
abraxasdegupusel.onion/c/QfrRwVeQvG?q=&sort=price_btc&deliver_to=1&change=1
DuckDuckGo
Listings Profile Messages Orders Forums Support
anonimoose Logout
Wallet Escrow
BTC 0.00000000 0.00000000
DASH 0.00000000 0.00000000
Bank Logins / Accounts / Fraud Related / Digital Goods / Listings
Search Go
Digital Goods 9779
Fraud Related 1105
Accounts 538
Bank Logins 25
Other 40
Paypal 45
Digital Goods 9779
Drugs 19986
Drugs Paraphernalia 455
Services 499
Other 1405
BTC Exchange
$ 424.16
€ 390.44
$ 594.06
£ 275.75
$ 557.58
DASH Exchange
Ƀ 0.00650112
$ 2.75
€ 2.54
$ 3.85
£ 1.79
$ 3.62
No FE first I can buy Active vendor
Sort: Price, high to low
Show domestic first
Unknown
Go
Reset
Name
Price
Shipping
Vendor
EU Bank Drop
You can inject spied program or use key loger pull out all the passworcs from the individual or busi...
0.05893998 Ƀ
From: EU To:world
citra 4.94/5, 500~700
Your Own Private Fullz. CVV'S. Banklogs and More with Spamming!
This s a very high quality guide which tells you exactly what to do to get your own fresh fullz, b...
0.05893998 Ƀ
From:Unknown
COLOR 4.85/5, 700~1000
Wells Fargo / SUNTRUST BANK LOGINS $1000-$3000 AVAILABLE BALANCE
Hello Guys, Available for your Fraud Venture. LOGINS FROM SUNTRUST BANK. Suntrust Format :...
0.04950958 Ƀ
From: United States To:WORLDWIDE
FE Only
wakawaka 4.4/5, 70~100
Wells Fargo Bank Account + Full Account / Routing numbers
0.03536399 Ƀ
From:Unknown
safetybets 4.8/5, 50~70
Wells Fargo Bank Account + Bonus Cashout Tutorials
0.02357599 Ƀ
From:Unknown
safetybets 4.8/5, 50~70
Where to get a prepaid VisaMc card with own Swiss Iban bank account- 2
0.02357599 Ƀ
From:
Keira 4.4/5


Eu Bank Drop :: Bank Logins :: Abraxas - Tor Browser
Eu Bank Drop :: Bank...
abraxasdegupusel.onion/listing/WTlxbLR0iBn
DuckDuckGo
Listings Profile Messages Orders Forums Support
anonimoose Logout
Wallet Escrow
BTC 0.00000000 0.00000000
DASH 0.00000000 0.00000000
Eu Bank Drop / Bank Logins / Accounts / Fraud Related / Digital Goods / Abraxas
Search
Go
Digital Goods 9779
Fraud Related 1105
Accounts 598
Bank Logins 25
Other 40
Paypal 45
Digital Goods 9779
Drugs 19985
Drugs Paraphernalia 455
Services 499
Other 1405
BTC Exchange
$ 426.87
€ 392.94
$ 597.86
£ 277.52
$ 561.15
DASH Exchange
฿ 0.00049205
$ 2.77
€ 2.55
$ 3.88
£ 1.80
$ 3.64
EU Bank Drop
You can inject spied program or use keylloger pull out all the passwords from the individual or business computer.
Then make a bank transfer to my account.
Hi,I work only in this way:
you make a bank transfer to my account.
Minimum 1000EUR,maximum 14000EUR(for one transfer)
After I get bank transfer,I exhange money to BTC and send to you BTC(50%)
Please write that your country and currency.
After you make bank transfer I need sender name and if possible screenshot(Bank transfers)
Ships from: EU
Ships to: world
Brought to you by: citra 4.94/5 , 500~700
Price: 0.05856525 ฿
No usable wallet available.
BTC Not enough credit.
DASH Not enough credit.
Available shipping:
Free, + 0.00000000 ฿ (0.00 $)
Amount 1
Buy (11 left)


New Stolen Honda Cbr 1000Rr :: Money :: Abraxas - Tor Browser
New Stolen Honda C...
abraxasdcgupuscl.onion/listing/EvmznKj3Ex
DuckDuckGo
Listings Profile Messages Orders Forums Support
anonimoose Logout
Wallet Escrow
BTC 0.00000000 0.00000000
DASH 0.00000000 0.00000000
New Stolen Honda Cbr 1000Rr / Money / Services / Abraxas
Search
Go
Services 499
Hacking 28
IDs &Passports 148
Money 158
Other 84
Digital Goods 9779
Drugs 19980
Drugs Paraphernalia 455
Services 499
Other 1405
BTC Exchange
$ 424.71
€ 390.95
$ 594.83
£ 276.11
$ 558.3
DASH Exchange
฿ 0.00056705
$ 2.79
€ 2.57
$ 3.91
£ 1.81
$ 3.67
New Stolen HONDA CBR 1000RR
We sell New Stolen HONDA CBR 1000RR.
Superbike was stolen from BikeShop.
With key.
Ships from: Germany
Brought to you by: citra 4.94/5 , 500~700
Price: 7.67369210 ฿
No usable wallet available.
BTC Not enough credit.
DASH Not enough credit.
Available shipping:
Super Stealth DHL,Fedex, + 0.76736921 ฿(300.00 €)
Amount 1
Buy (6 left)

End game

- Darknet markets (and forums) tend to end one of three ways
  - They get seized and shutdown by Police and other law enforcement
  - The sites get “hacked” resulting in the loss of any stored Bitcoin
  - The operators close down gracefully and run with their Bitcoin



Summary

- Darknets (or The Darknet) can be used to host content or services in a way which makes identification of the server location very hard
- Almost any device can host content on the Darknet regardless of underlying IP topology
- Tor is currently the most popular darknet platform
- There are dozens of well organised markets and forums where illegal goods and services can be procured with relative ease
- The barrier to entry for both buyers and sellers of illegal products and services is significantly reduced
- Easy access to skilled “hackers for hire” can be a “force multiplier” for bad actors who are motivated but lack capability

What you can do

- Understand the implications of the rise of the Darknet
  - Develop a contingency plan to minimise impact taking account of the fact that DN hosted content cannot be “taken down”
  - Reconsider the results of risk assessments when taking into account the ability of unskilled threat sources to employ CNE
  - Do not base your policies on the assumption that this is a passing craze
- Identify if your organisations assets are being exploited in the Darknet
  - Make use of the available DN search engines, trading sites and forums to search for references to those assets or engage a competent TI provider to do that for you on an on-going basis
- Assess your networks exposure to exfiltration via the Darknet
  - Evaluate network perimeter controls including both blocking and monitoring
  - Evaluate EUD configuration and controls

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Thank you

Any questions?