Risky Business?

Investigating the Security Practices of Vendors on an Online Anonymous Market using Ground-Truth Data

Jochem van de Laarschot and Rolf van Wegberg

Delft University of Technology

Introduction to online anonymous markets

Security on online anonymous markets

Hansa Market

Capturing security practices

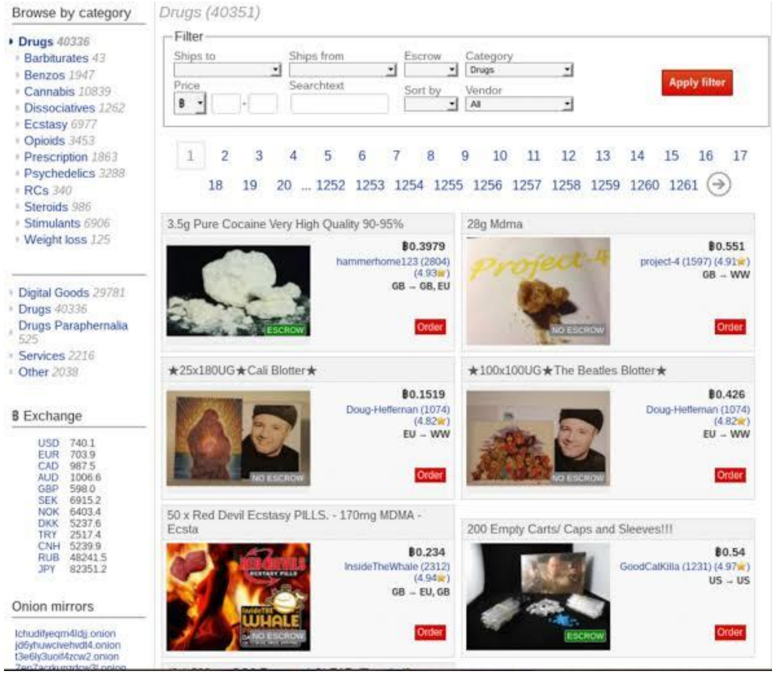
Our approach

Results

Take-aways

Online anonymous markets

Platforms that facilitate the pseudonymous trade of illicit physical goods and digital items.



Browse by category

- **Drugs** *40336*
  - Barbiturates *43*
  - Benzos *1947*
  - Cannabis *10839*
  - Dissociatives *1262*
  - Ecstasy *6977*
  - Opioids *3453*
  - Prescription *1863*
  - Psychedelics *3288*
  - RCs *340*
  - Steroids *986*
  - Stimulants *6906*
  - Weight loss *125*

- Digital Goods *29781*
- Drugs *40336*
- Drugs Paraphernalia *525*
- Services *2216*
- Other *2038*

฿ Exchange

USD	740.1
EUR	703.9
CAD	987.5
AUD	1006.6
GBP	598.0
SEK	6915.2
NOK	6403.4
DKK	5237.6
TRY	2517.4
CNH	5239.9
RUB	48241.5
JPY	82351.2

Onion mirrors

lchudifyeqm4ldjj.onion
jd6yhuwcivehvdt4.onion
t3e6ly3uoif4zcw2.onion

Drugs (40351)

Filter

Ships to ▾ | Ships from ▾ | Escrow ▾ | Category: Drugs ▾
Price: ฿ ▾ [ ] - [ ] | Searchtext [ ] | Sort by ▾ | Vendor: All ▾

Apply filter

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
18 19 20 ... 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 →

3.5g Pure Cocaine Very High Quality 90-95%
฿0.3979
hammerhome123 (2804) (4.93★)
GB → GB, EU
ESCROW
Order

28g Mdma
฿0.551
project-4 (1597) (4.91★)
GB → WW
NO ESCROW
Order

★25x180UG★Cali Blotter★
฿0.1519
Doug-Heffernan (1074) (4.82★)
EU → WW
NO ESCROW
Order

★100x100UG★The Beatles Blotter★
฿0.426
Doug-Heffernan (1074) (4.82★)
EU → WW
NO ESCROW
Order

50 x Red Devil Ecstasy PILLS. - 170mg MDMA - Ecsta
฿0.234
InsideTheWhale (2312) (4.94★)
GB → EU, GB
NO ESCROW
Order

200 Empty Carts/ Caps and Sleeves!!!
฿0.54
GoodCatKilla (1231) (4.97★)
US → US
ESCROW
Order

Physical goods

Digital cybercrime items

Introduction to online anonymous markets

Security on online anonymous markets

Hansa Market

Capturing security practices

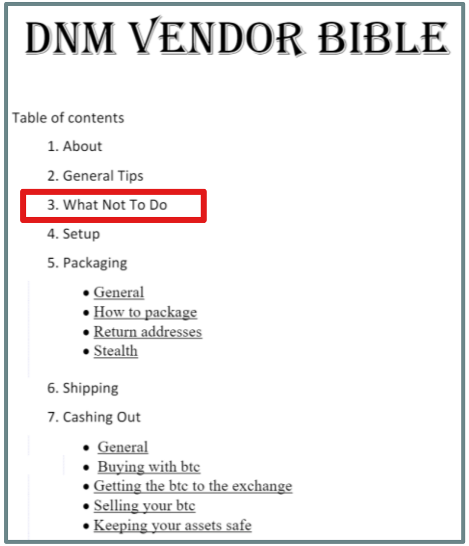
Our approach

Results

Take-aways

Easy access to OPSEC guides

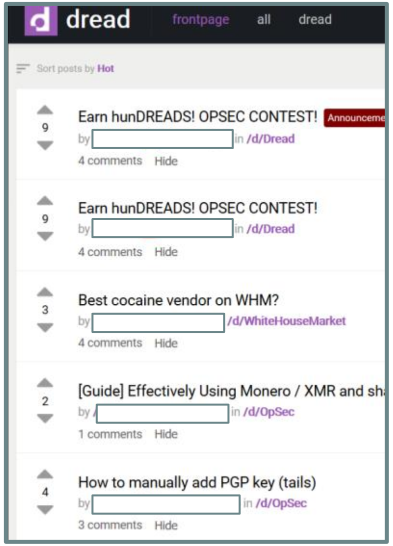
Given that 'Operational Security' (OPSEC) techniques are frequently shared in the underground community…



DNM VENDOR BIBLE

Table of contents

1. About
2. General Tips
3. What Not To Do
4. Setup
5. Packaging
   - General
   - How to package
   - Return addresses
   - Stealth
6. Shipping
7. Cashing Out
   - General
   - Buying with btc
   - Getting the btc to the exchange
   - Selling your btc
   - Keeping your assets safe



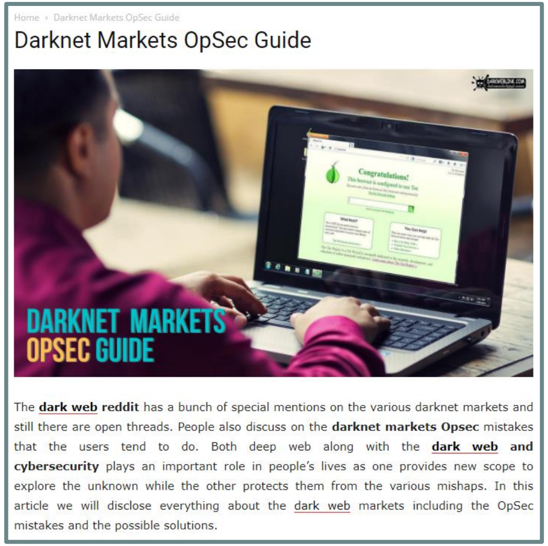
9 Earn hunDREADS! OPSEC CONTEST! Announceme
by [redacted] in /d/Dread
4 comments Hide

9 Earn hunDREADS! OPSEC CONTEST!
by [redacted] in /d/Dread
4 comments Hide

3 Best cocaine vendor on WHM?
by [redacted] /d/WhiteHouseMarket
4 comments Hide

2 [Guide] Effectively Using Monero / XMR and sh
by / [redacted] in /d/OpSec
1 comments Hide

4 How to manually add PGP key (tails)
by [redacted] in /d/OpSec
3 comments Hide



Home › Darknet Markets OpSec Guide

Darknet Markets OpSec Guide

The **dark web reddit** has a bunch of special mentions on the various darknet markets and still there are open threads. People also discuss on the **darknet markets Opsec** mistakes that the users tend to do. Both deep web along with the **dark web** and **cybersecurity** plays an important role in people's lives as one provides new scope to explore the unknown while the other protects them from the various mishaps. In this article we will disclose everything about the dark web markets including the OpSec mistakes and the possible solutions.

TU Delft

Introduction to online anonymous markets

Security on online anonymous markets

Hansa Market

Capturing security practices

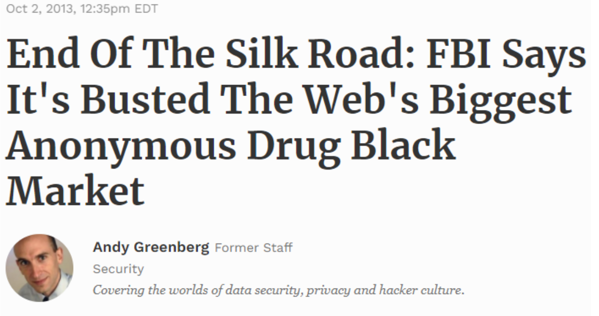
Our approach

Results

Take-aways

Law enforcement

… and given the increasing amount of scrutiny by law enforcement …



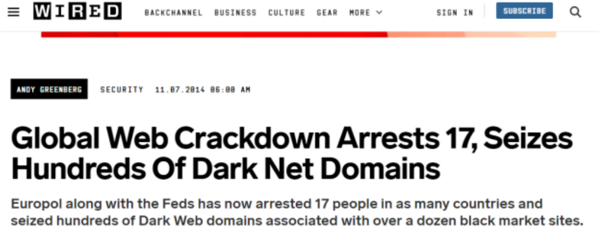
Oct 2, 2013, 12:35pm EDT

End Of The Silk Road: FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market

Andy Greenberg Former Staff

Security

Covering the worlds of data security, privacy and hacker culture.



ANDY GREENBERG SECURITY 11.07.2014 06:00 AM

Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains

Europol along with the Feds has now arrested 17 people in as many countries and seized hundreds of Dark Web domains associated with over a dozen black market sites.

Introduction to online anonymous markets

Security on online anonymous markets

Hansa Market

Capturing security practices

Our approach

Results

Take-aways

TUDelft

Prevalence of (in)secure practices

… we should expect that poor security practices are rare among the users that are active on these markets.

However, cybercriminals do not always achieve maximum security:

- the inevitable trade-off between security and efficiency of operations
- ‘Perfect security’ is not economically viable: security comes at a cost

So, how prevalent are poor security practices among online anonymous market vendors?

To find out, we capture certain security practices on a single market: Hansa Market.

Hansa Market

Dutch law enforcement allowed us restricted access to the Hansa Market back-end database.

Introduction to online anonymous markets

Security on online anonymous markets

Hansa Market

Capturing security practices

Our approach

Results

Take-aways

Hansa Market

- Active September 2015 – July 2017.
- ~1750 vendors,
- ~400.000 regular members,15% active
- 1000-8000 daily visitors
- Estimated revenue $33M

Back-end database

- User administration
- Listings (advertisements)
- Orders
- Connection logs

TU Delft

Introduction to online anonymous markets

Security on online anonymous markets

Hansa Market

Capturing security practices

Our approach

Results

Take-aways

Capturing security practices

Additionally, we leveraged *Have I Been Pwnd*, *Grams* and *Chainalysis*.

- **Have I Been Pwnd**, a database of leaked passwords.
  - 10B+ leaked passwords, of which 573M are unique
  - SHA1-hashes are publicly available
- **Grams**, a “Google for darknet markets”.
  - The search engine indexed listings and vendors
  - Shut down in December 2017, through law enforcement access to offline copy
- **Chainalysis,** a blockchain analysis service.
  - Provides context to raw blockchain data
  - Mainly makes use of co-spend clustering heuristics
  - Chainalysis is able to estimate which bitcoin addresses are controlled by – for example – bitcoin exchanges

Approach

Our two-step approach to measuring the prevalence of insecure practices across different types of vendors.

Introduction to online anonymous markets

Security on online anonymous markets

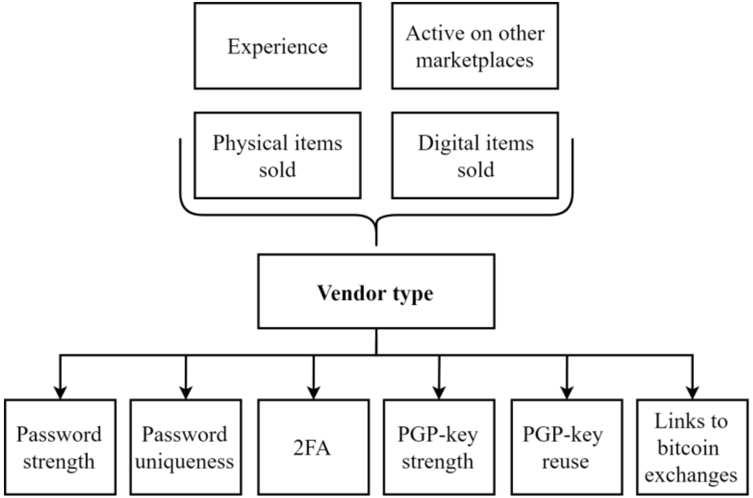
Hansa Market

Capturing security practices

Our approach

Results

Take-aways



1. We **identify characteristics** of vendors and **cluster vendors** that have similar characteristics into distinct ‘**vendor types**’ using latent profile analysis.
2. We **capture** the security practices in our data and **measure the prevalence** of **poor security** practices **across vendor types**.

TUDelft

Introduction to online anonymous markets

Security on online anonymous markets

Hansa Market

Capturing security practices

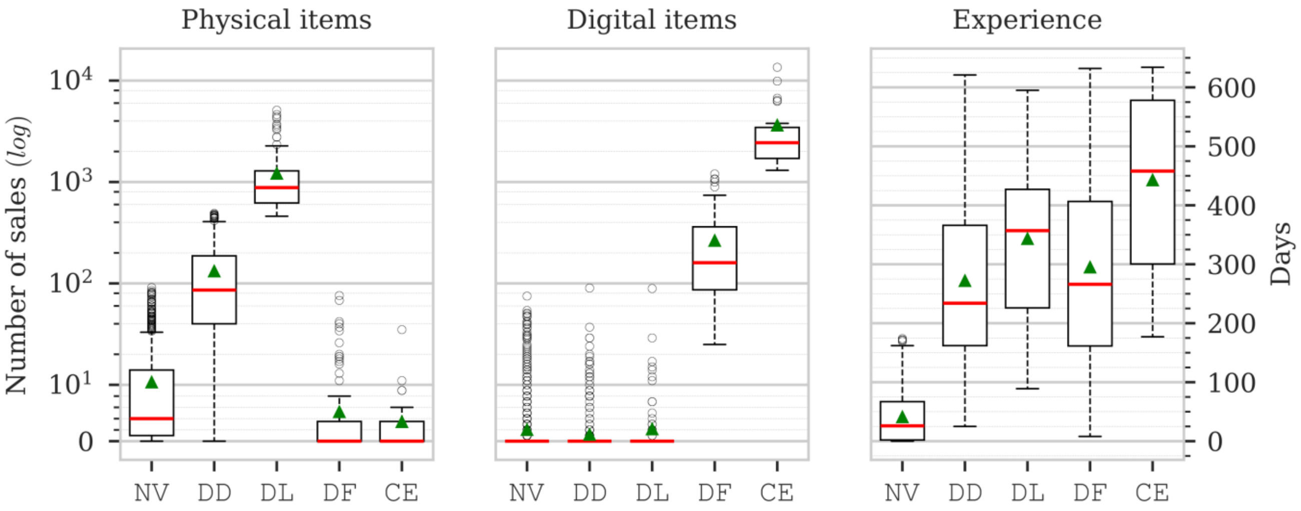
Our approach

Results

Take-aways

Resulting vendor types

The LPA results in a 5-cluster model which clearly differentiates between different types of vendors.



NV - Novices, DD - Drug Dealers, DL - Drug Lords, DF - Digital Fraudsters, CE - Cybercrime Elites

Introduction to online anonymous markets

Security on online anonymous markets

Hansa Market

Capturing security practices

Our approach

Results

Take-aways

Measuring security practices

We capture six security practices of vendors that are active on Hansa Market.

Password strength: zxcvbn.
On average: $10^{14.7}$ estimated guesses, median: $10^{10.5}$ guesses.

Password uniqueness: hibp matching.
185 vendors (17.1%) logged in with a password we could match.

2FA-usage: hansa back-end
Of the total vendor population, only 60.5% used 2FA.

PGP-key adoption and key-strength: GnuPG
~100% adoption, few weak keys.

Reuse of PGP-keys over multiple markets: Grams matching

265 out of 908 matched.

The traceability of their cash-out to bitcoin exchanges: *Chainalysis*
14% of the bitcoin addresses are managed by known online financial service providers.

Introduction to online anonymous markets

Security on online anonymous markets

Hansa Market

Capturing security practices

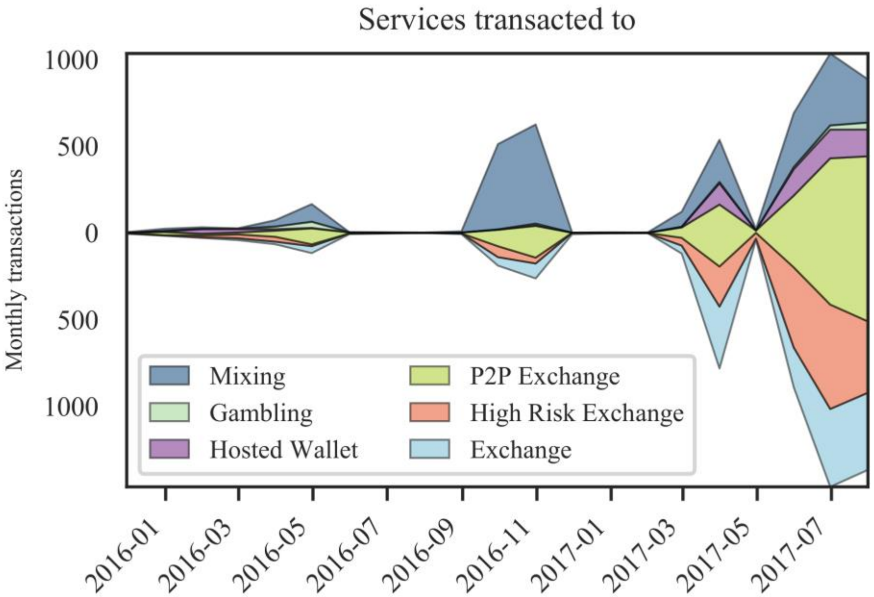
Our approach

Results

Take-aways

Traceability of cash-outs

About 10% of the vendors on Hansa Market can be easily linked to a central bitcoin exchange.



TU Delft

Security across vendor types

Comparing Novices, Drug Dealers, Drug Lords, Digital Fraudsters and Cybercrime Elites

Introduction to online anonymous markets

Security on online anonymous markets

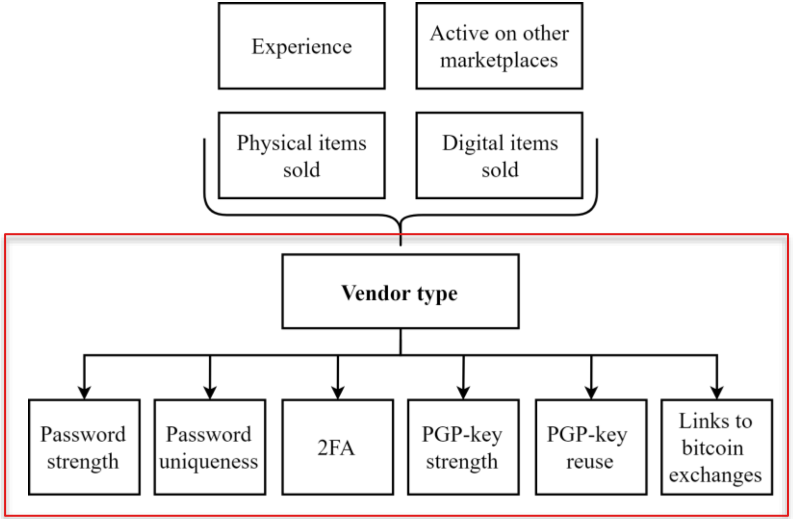
Hansa Market

Capturing security practices

Our approach

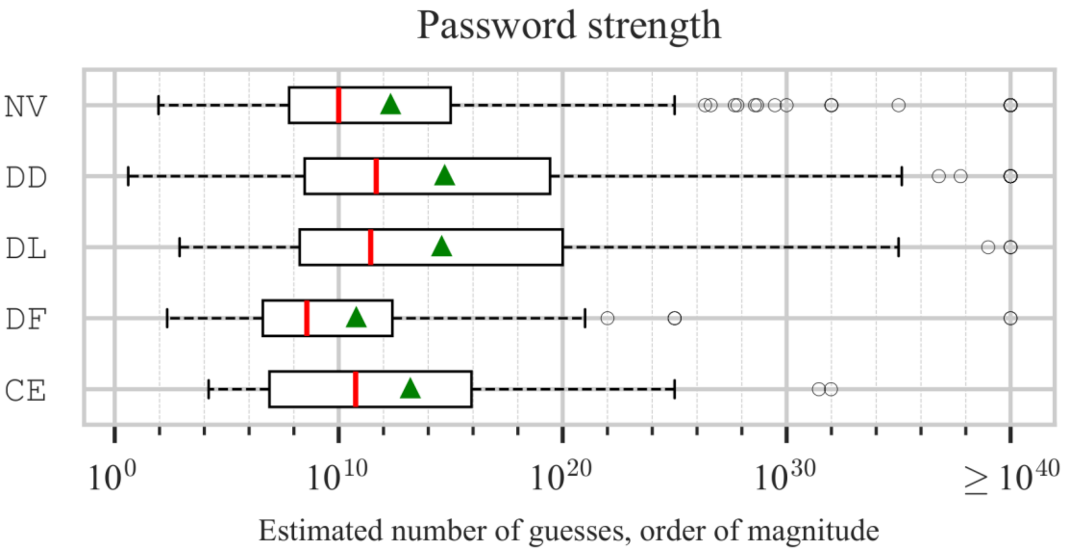
Results

Take-aways



Password strength

Passwords of Drug Lords and Drug Dealers are (significantly) stronger, Digital Fraudsters score low.



Introduction to online anonymous markets

Security on online anonymous markets

Hansa Market

Capturing security practices

Our approach

Results

Take-aways

TU Delft

Introduction to online anonymous markets

Security on online anonymous markets

Hansa Market

Capturing security practices

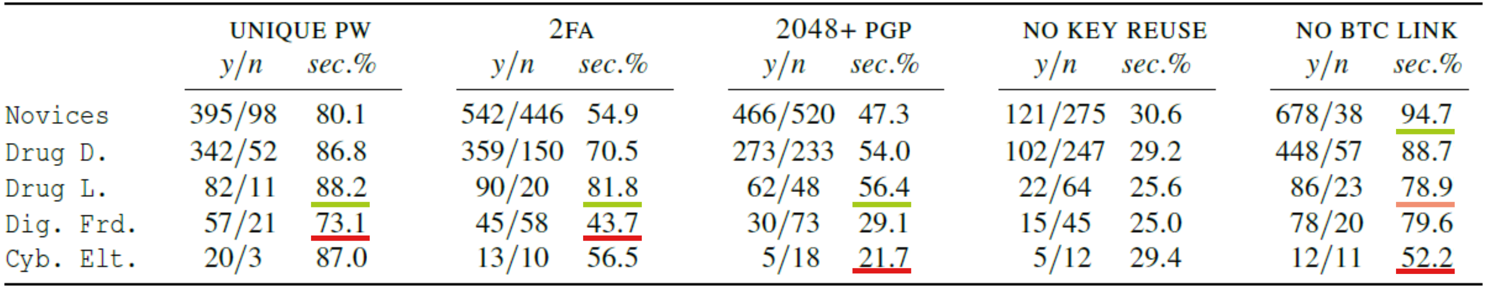
Our approach

Results

Take-aways

Security across vendor types

Vendors selling digital cybercrime items are more likely to have insecure practices.



	UNIQUE PW		2FA		2048+ PGP		NO KEY REUSE		NO BTC LINK	
	y/*n*	*sec.%*	*y*/*n*	*sec.%*	*y*/*n*	*sec.%*	*y*/*n*	*sec.%*	*y*/*n*	*sec.%*
Novices	395/98	80.1	542/446	54.9	466/520	47.3	121/275	30.6	678/38	94.7
Drug D.	342/52	86.8	359/150	70.5	273/233	54.0	102/247	29.2	448/57	88.7
Drug L.	82/11	88.2	90/20	81.8	62/48	56.4	22/64	25.6	86/23	78.9
Dig. Frd.	57/21	73.1	45/58	43.7	30/73	29.1	15/45	25.0	78/20	79.6
Cyb. Elt.	20/3	87.0	13/10	56.5	5/18	21.7	5/12	29.4	12/11	52.2

Take-aways

We found surprising patterns in the security practices of vendors.

- Vendors that specialize in selling digital cybercrime items make ‘mistakes’ in their digital security the most often, while vendors belonging to clusters of successful drug dealers tend to have the best digital security.

- Many vendors – including the highly successful ones – make the mistake of initiating traceable cash-outs to mainstream bitcoin exchanges.

Introduction to online anonymous markets

Security on online anonymous markets

Hansa Market

Capturing security practices

Our approach

Results

Take-aways

TUDelft

Contact

Jochem van de Laarschot	[firstname]vandelaarschot@gmail.com
Rolf van Wegberg	r.s.vanwegberg@tudelft.nl

TU Delft