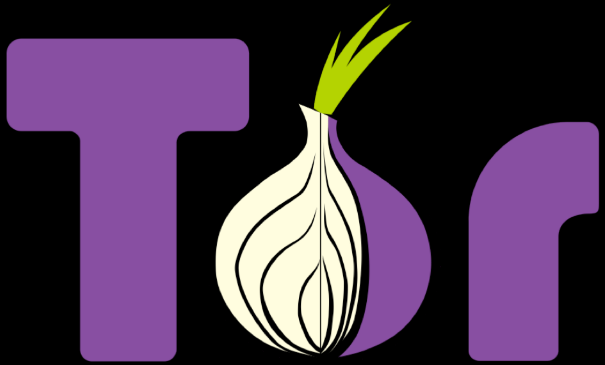
Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web

Seunghyeon Lee [†‡], Changhoon Yoon[†], Heedo Kang[†], Yeonkeun Kim[‡], Yongdae Kim[‡], Dongsu Han[‡], Sooel Son[‡], Seungwon Shin[†‡]

[†]S2W LAB Inc.

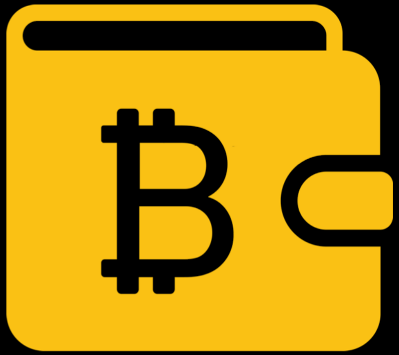
[‡]KAIST

Anonymity services



Dark Web

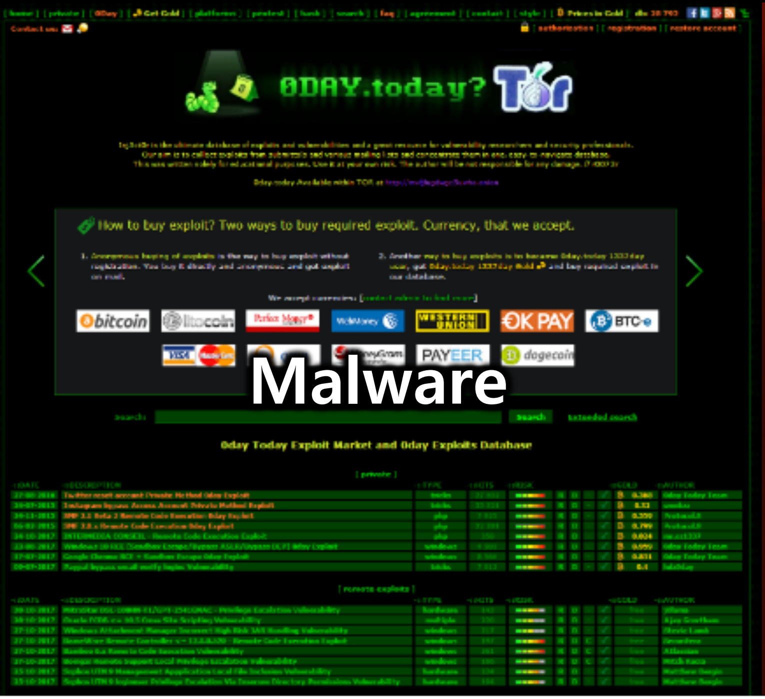
- **Tor hidden services**
  - Strong anonymity guarantees via Tor
  - Anonymous and untraceable network
  - Special software to access (i.e., Tor browser)



Cryptocurrency

- **A blockchain-based digital currency**
  - Cryptographic currency
  - Strong pseudonymity (almost anonymous)
  - Mostly unregulated and unverifiable

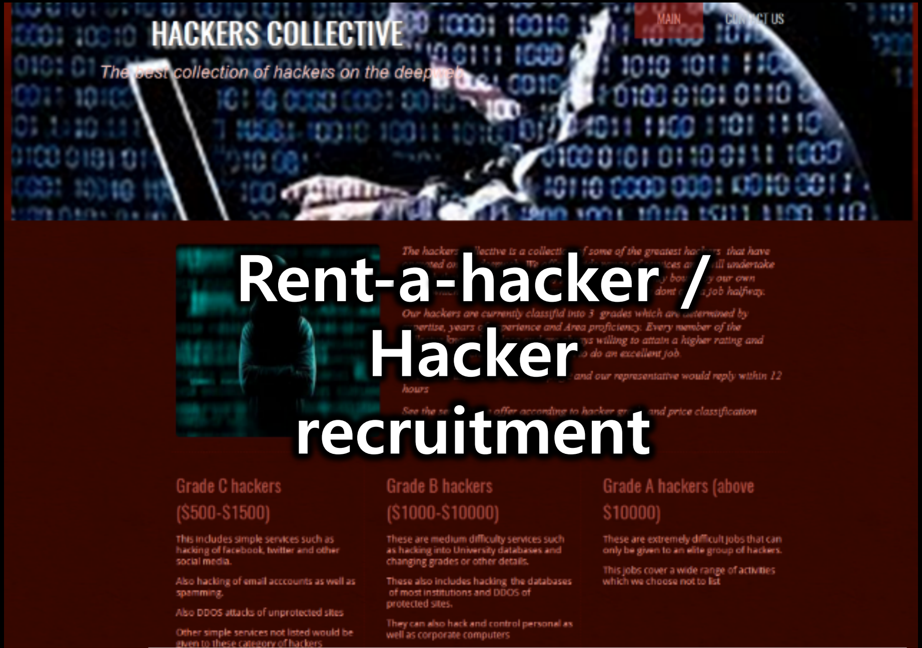
Illicit trades on the Dark Web



How to buy exploit? Two ways to buy required exploit. Currency, that we accept.

0day Today Exploit Market and 0day Exploits Database

Malware



The best collection of hackers on the deep web

Rent-a-hacker /
Hacker
recruitment

Grade C hackers ($500-$1500)

This includes simple services such as hacking of facebook, twitter and other social media.

Also hacking of email acccounts as well as spamming.

Also DDOS attacks of unprotected sites

Other simple services not listed would be given to these category of hackers

Grade B hackers ($1000-$10000)

These are medium difficulty services such as hacking into University databases and changing grades or other details.

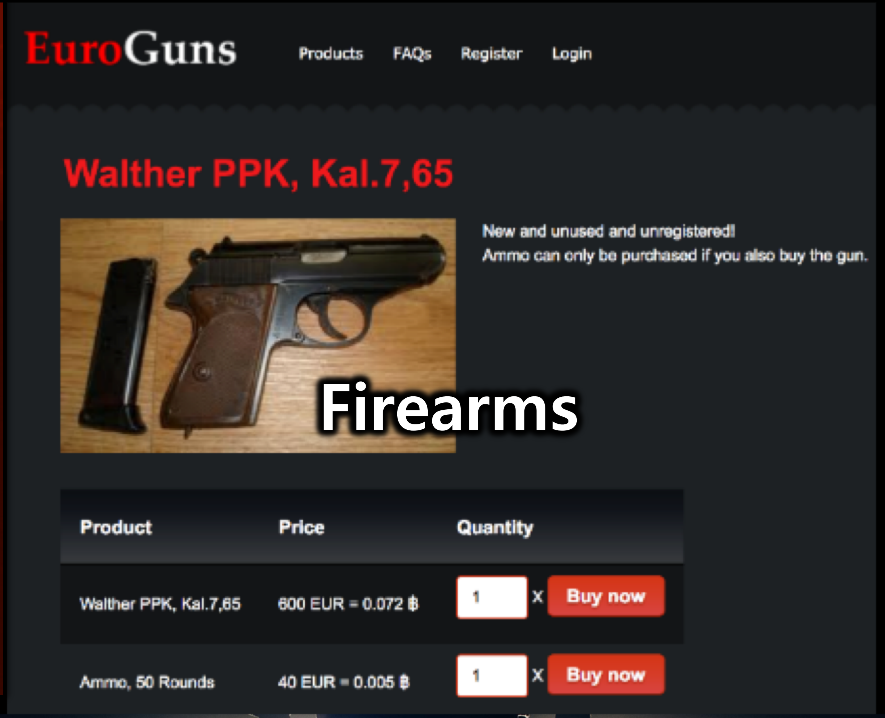
These also includes hacking the databases of most institutions and DDOS of protected sites.

They can also hack and control personal as well as corporate computers

Grade A hackers (above $10000)

These are extremely difficult jobs that can only be given to an elite group of hackers.

This jobs cover a wide range of activities which we choose not to list

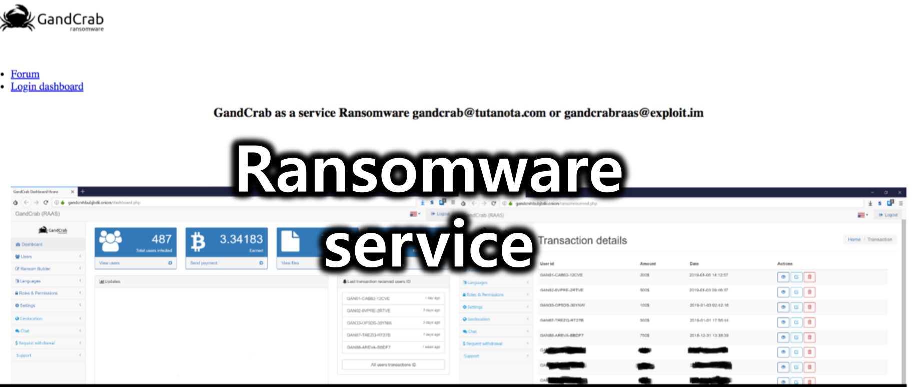


Walther PPK, Kal.7,65

New and unused and unregistered!
Ammo can only be purchased if you also buy the gun.

Firearms

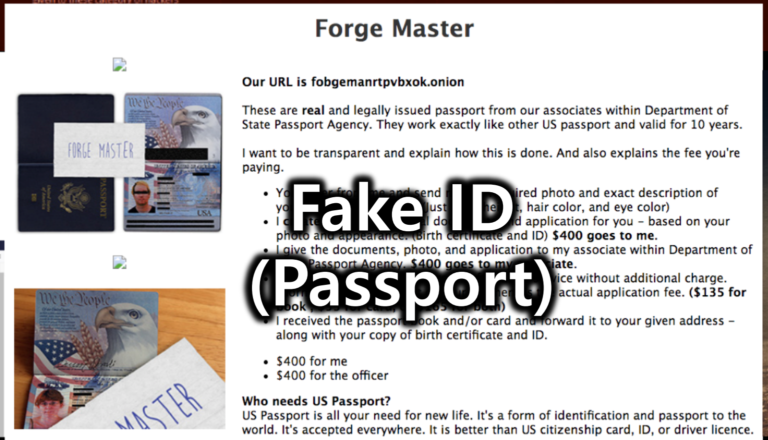
Product	Price	Quantity
Walther PPK, Kal.7,65	600 EUR = 0.072 ฿	1 x Buy now
Ammo, 50 Rounds	40 EUR = 0.005 ฿	1 x Buy now



- Forum
- Login dashboard

GandCrab as a service Ransomware gandcrab@tutanota.com or gandcrabraas@exploit.im

Ransomware
service



Forge Master

Our URL is fobgemanrtpvbxok.onion

These are **real** and legally issued passport from our associates within Department of State Passport Agency. They work exactly like other US passport and valid for 10 years.

I want to be transparent and explain how this is done. And also explains the fee you're paying.

- Yo[illegible] from me and send [illegible]ired photo and exact description of yo[illegible] (Just [illegible] hei[illegible]t, hair color, and eye color)
- I c[illegible]l do[illegible]d application for you – based on your photo and appearance. (Birth certificate and ID) **$400 goes to me**.
- I give the documents, photo, and application to my associate within Department of [illegible] Passport Agency. **$400 goes to my [illegible]iate.**
- [illegible]ice without additional charge. [illegible] actual application fee. **($135 for book [illegible])**
- I received the passport book and/or card and forward it to your given address – along with your copy of birth certificate and ID.

- $400 for me
- $400 for the officer

Who needs US Passport?
US Passport is all your need for new life. It's a form of identification and passport to the world. It's accepted everywhere. It is better than US citizenship card, ID, or driver licence.

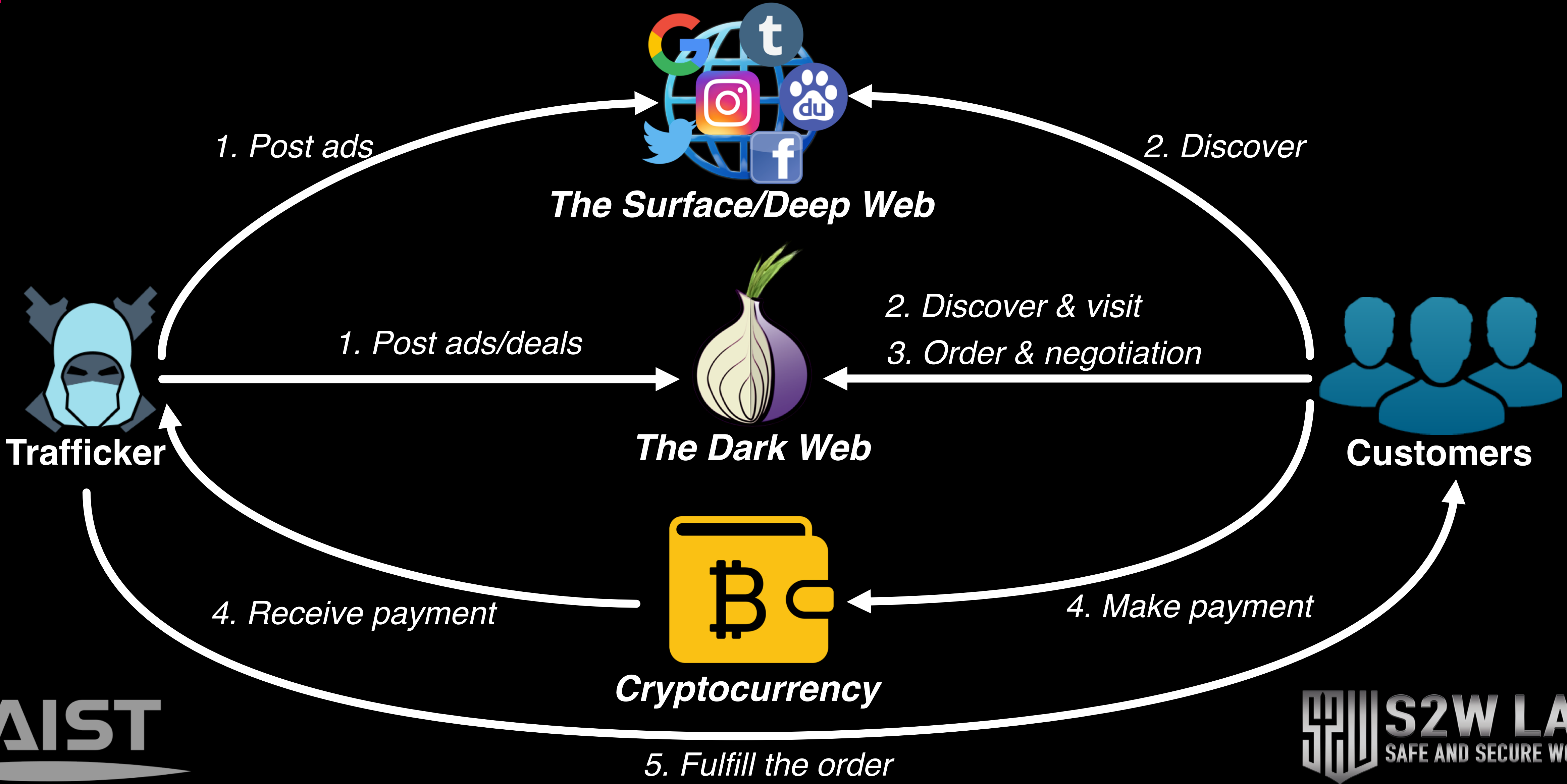
Fake ID
(Passport)

HITMAN SICARIO THE PROFESSIONAL HITMAN SERVICE / WE DO NOT HIRE HITMAN ANY MORE SO PLEASE DO NOT APPLY NETWORK SLOTS ARE FULL

Welcome to the Best Hitman Service in the Dark Web

Hitman
services

The procedures of an underground illegal trade



KAIST

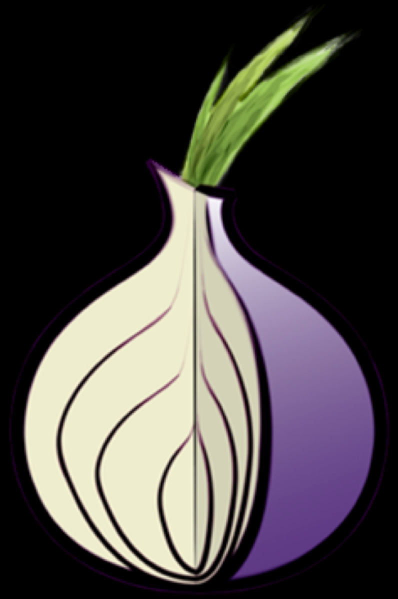
S2W LAB
SAFE AND SECURE WORLD

Research Questions

- **How badly is cryptocurrency being abused on the Dark Web ?**
  - ***Perform large-scale analysis on the Dark Web.***

- **How can we investigate and analyze cryptocurrency abuses on the Dark Web ?**
  - ***Investigate the perpetrators' online & financial activities.***

Challenge: Limited Dark Web data accessibility



The SURFACE WEB

- Searchable (via Google, Bing, etc.) data
- Most of the known websites

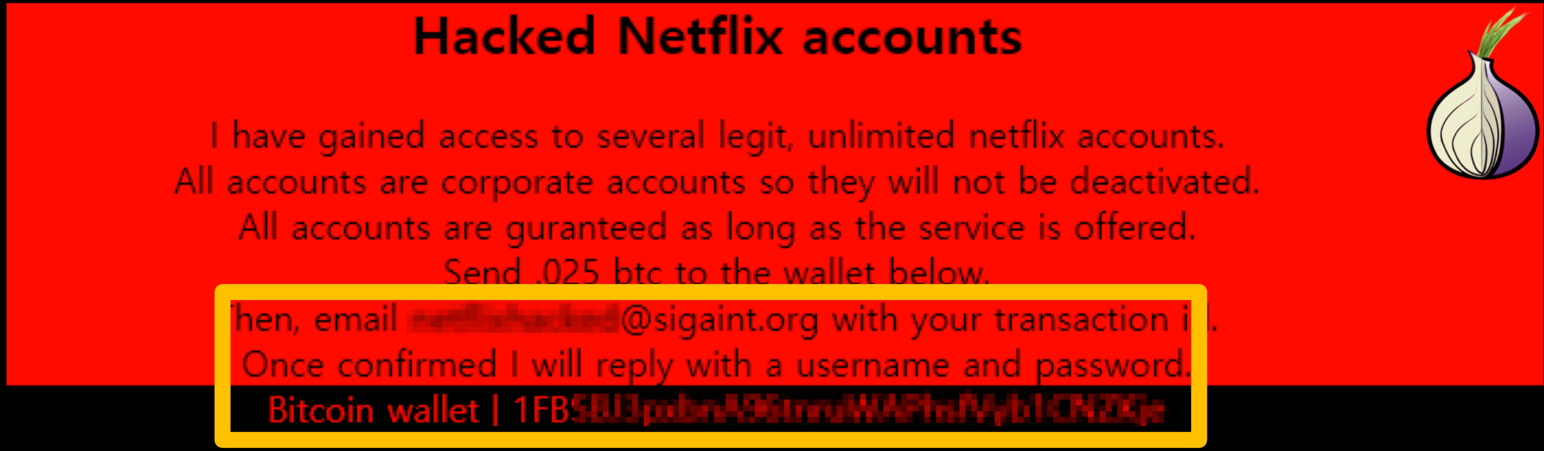
The DARK WEB

- No Dark Web search engines with extensive coverage (i.e., Poor-indexed websites)
- Highly volatile contents

Challenge: Lack of evidence

I will **conceal evidence** that possibly reveals our entire illegal business!

Hacked account selling



Hacked Netflix accounts

I have gained access to several legit, unlimited netflix accounts.
All accounts are corporate accounts so they will not be deactivated.
All accounts are guranteed as long as the service is offered.
Send .025 btc to the wallet below.
hen, email [redacted]@sigaint.org with your transaction i .
Once confirmed I will reply with a username and password.
Bitcoin wallet | 1FB[redacted]

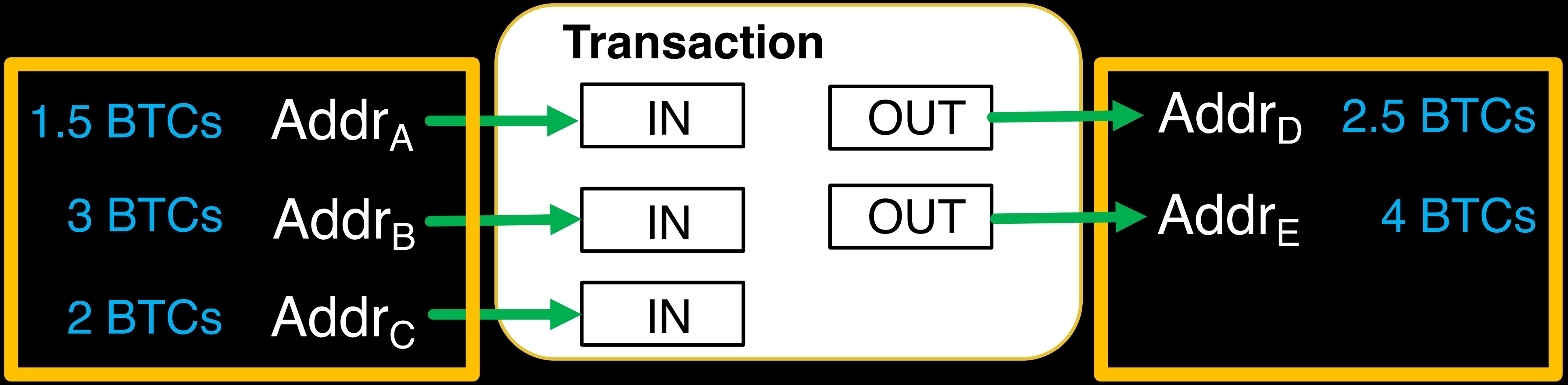
Using privacy-oriented services *(e.g., SIGAINT*)*

*SIGAINT is a Tor hidden service offering secure email services

Challenge: Obscure cryptocurrency money flows

2. Lack of ownership information

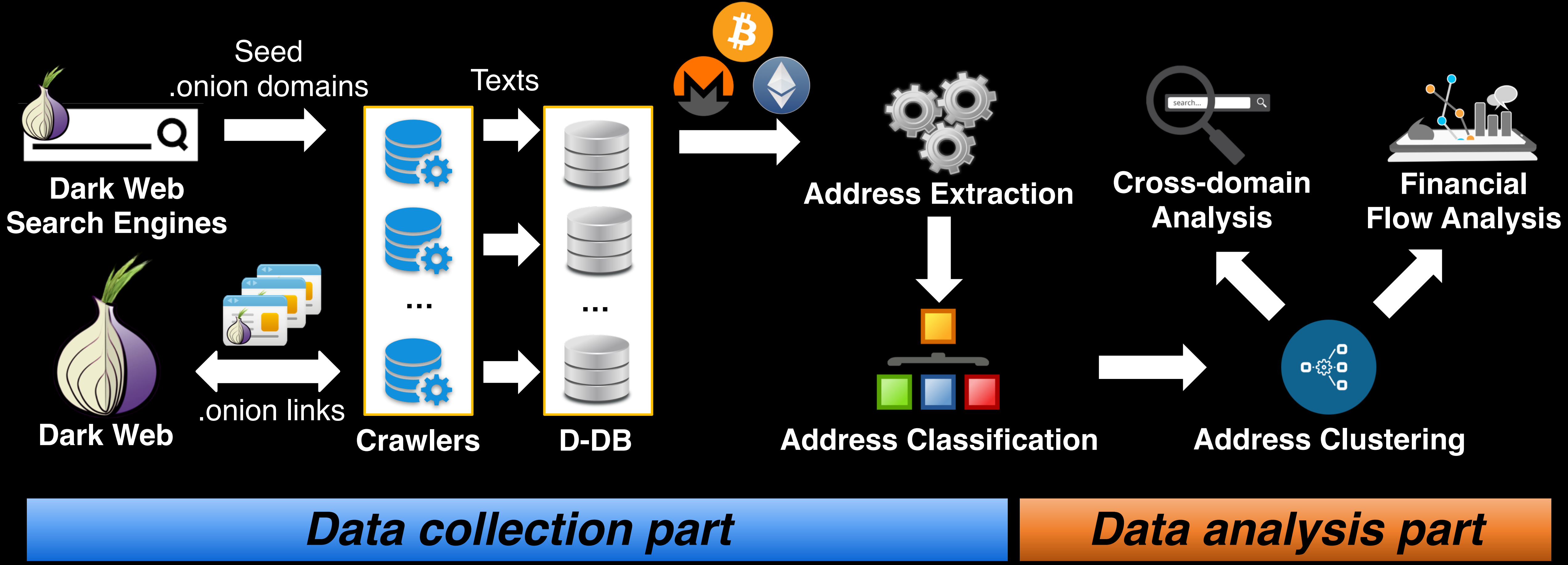
➔ Who receives funds?



1. Lack of explicit links

➔ How much BTCs are transferred to each output?

MFScope: Dark Web and cryptocurrency analysis framework



Crawling the Dark Web

- Seed 10k *.onion* addresses from
  - Ahmia[*]
  - FreshOnions[**]

Category	Count
# of dark websites	36,864
# of dark webpages	27,665,572
Data collection period	Jan 2017 ~ March 2018 **(15 months)**

Our data collection

[*] Ahmia, https://ahmia.fi

[**] FreshOnions, http://zlal32teyptf4tvi.onion

Extracting cryptocurrency addresses

- Extract addresses with each **regex** from dark webpages
  - Bitcoin, Ethereum, and Monero
- Filter invalid addresses are
  - Cryptographically invalid
  - Having no transactions
  - Extracted from Blockchain mirror sites

	Bitcoin	Ethereum	Monero	Total
# dark websites	2,886	180	121	3,187
# dark webpages	1,579,047	4,743	4,410	1,588,200
# addresses	9,906,129	649	38,440	9,945,218
# final addresses	**5,440**	**50**	**61**	**5,551**

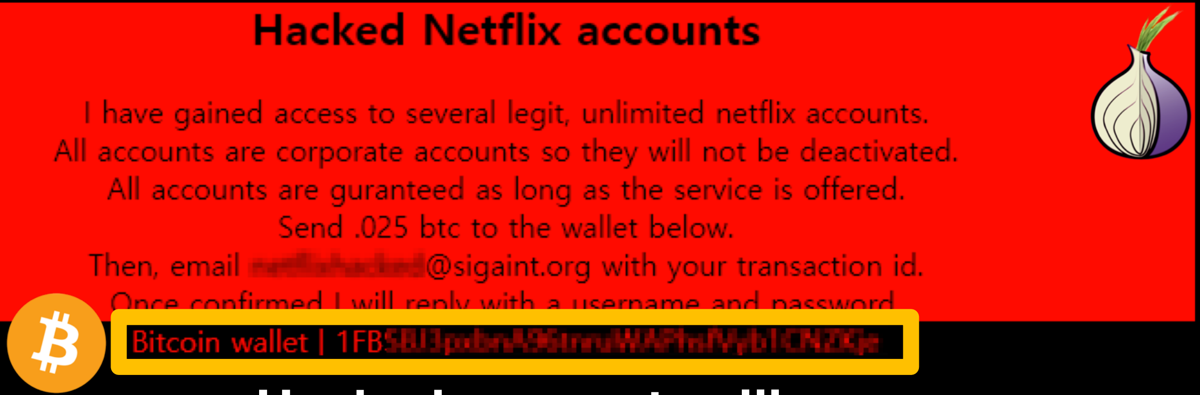
The statistics of cryptocurrency addresses

Classifying Bitcoin addresses

Is this Bitcoin address for promoting **illicit goods or services**?

Security researchers

Vote (%)	Category
~ 20%	*Legitimate*
20% ~ 70%	*Possible illicit*
70% ~	*Illicit*

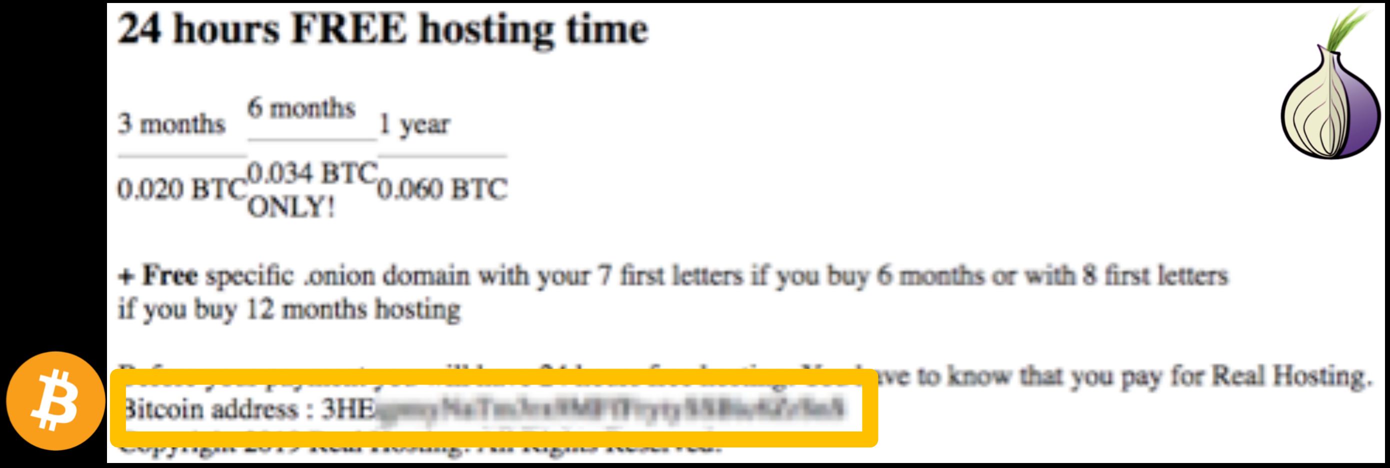


Hacked Netflix accounts

I have gained access to several legit, unlimited netflix accounts.
All accounts are corporate accounts so they will not be deactivated.
All accounts are guranteed as long as the service is offered.
Send .025 btc to the wallet below.
Then, email [redacted]@sigaint.org with your transaction id.
Once confirmed I will reply with a username and password.

Bitcoin wallet | 1FB[redacted]

Hacked account selling



24 hours FREE hosting time

3 months	6 months	1 year
0.020 BTC	0.034 BTC ONLY!	0.060 BTC

+ **Free** specific .onion domain with your 7 first letters if you buy 6 months or with 8 first letters if you buy 12 months hosting

ve to know that you pay for Real Hosting.
Bitcoin address : 3HE[redacted]

Hosting service

Classifying Bitcoin addresses

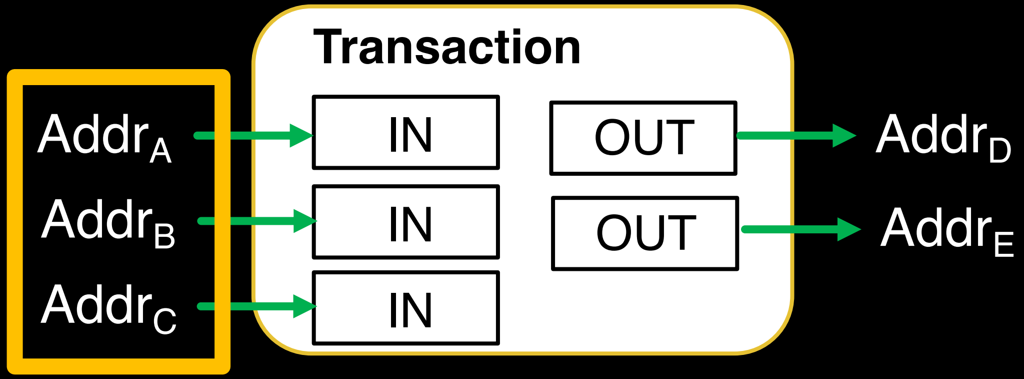
Category	Count	Ratio
Legitimate addresses	*884*	*16.25%*
Possible illicit addresses	*4,471*	***83.75%***
Illicit addresses	*85*	
Total	*5,440*	*100.00%*

Cryptocurrency distribution over the Dark Web

- Legitimate addresses
  - Donation, escrow, identification, etc.
- 85 seed illicit addresses
  - Abuse, counterfeit, drug, weapons, etc.

Demystifying perpetrators: Address clustering

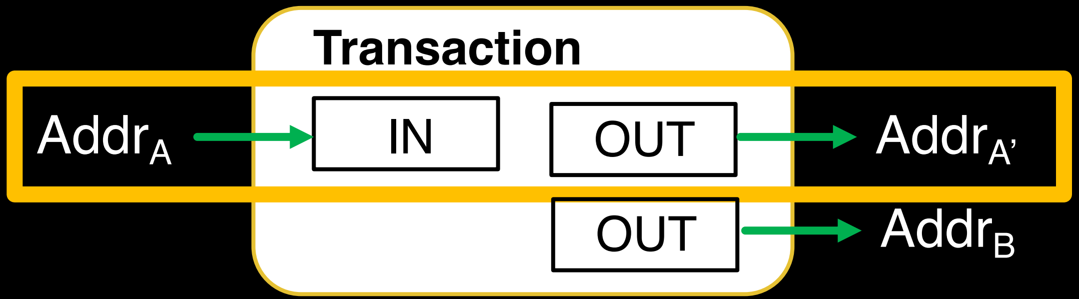
MI (Multi-input) heuristic



A sender should have corresponding private keys

→ Addr_A, Addr_B, $\text{Addr}_C \subset$ sender's addresses

CA (change address) heuristic



A wallet software generates a new address to receive the remainder

→ Addr_A, $\text{Addr}_{A'} \subset$ sender's addresses

The volumes of perpetrator’s Bitcoin

Category	**# addrs**			**BTC (USD) received**** [MI heuristic only]	**BTC (USD) sent** [MI heuristic only]	**Lifetime** (TX_{first} – TX_{last})
	Seed	MI	MI + CA*			
Abuse	15	486	539	3,416 ($3,862,983)	3,416 ($3,863,185)	19/03/2015-30/04/2018
Account selling	6	60	201	2 ($1,811)	2 ($2,298)	03/03/2016-24/12/2017
Card dumps	6	205	833	2,323 ($9,935,313)	2,323 ($9,938,336)	17/11/2014-30/04/2018
Counterfeit	2	23	27	0.49 ($1,129)	0.49 ($1,142)	25/02/2017-05/07/2017
Drug	4	18	26	5,245 ($14,124,499)	5,245 ($14,373,916)	19/07/2014-13/12/2017
Investment scam	29	2,025	204	32,428 ($151,438,331)	32,421 ($151,816,053)	04/09/2013-30/04/2018
Membership	8	95	247	29 ($85,481)	29 ($92,185)	14/11/2016-23/01/2018
Service	8	113	861	59 ($60,141)	59 ($59,206)	18/07/2014-29/04/2018
Weapon	1	42	754	46 ($32,964)	46 ($33,028)	18/07/2014-29/04/2018
Others	6	9	22	65 ($32,043)	65 ($32,434)	14/07/2015-03/01/2018
Total	**85**	**3,029**	**2,044**	**43,422 ($179,317,131)**	**43,415 ($179,954,158)**	04/09/2015-30/04/2018

* The super clusters are excluded

** The amount is based on the trading currency of BTC to USD

Demystifying perpetrators: Cross-domain analysis

- Cryptocurrency address as a keyword
- Google search API

Category	**Seed**	**MI**	**MI+CA**	**Total**
Tor proxy	38	38	45	121
Community	35	59	20	114
Sales	17	27	9	53
Media	10	17	5	32
Archive	4	12	6	22
Miscellaneous	1	3	4	8
Unavailable	8	17	6	31
Total	**113**	**173**	**95**	**381**

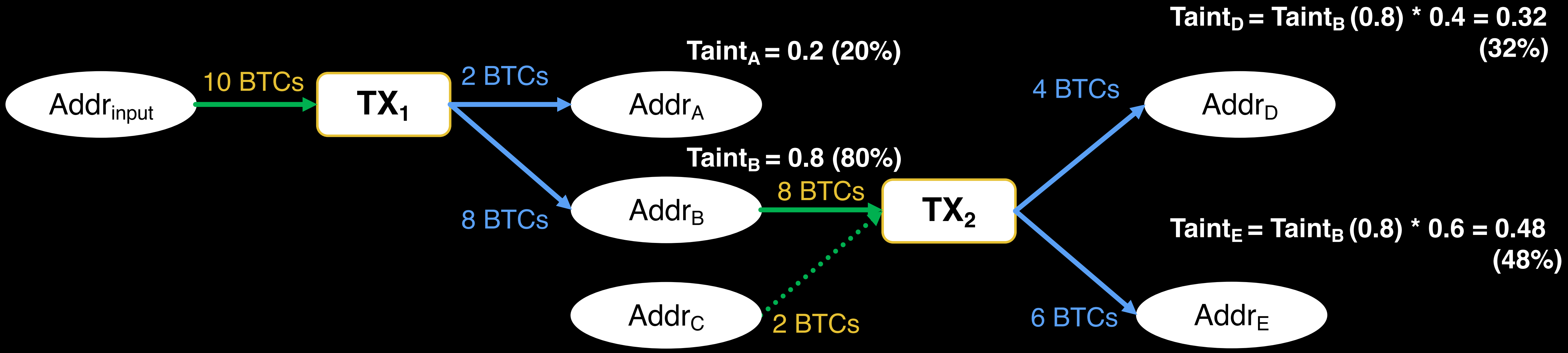
The statistics of cross-referencing results (# pages)

The search results include

real-world identities (profile)
personal interests
complaints (fraud reports)
service feedback
another illicit business

➔ Help us understand the perpetrators

Taint-based cryptocurrency flow analysis



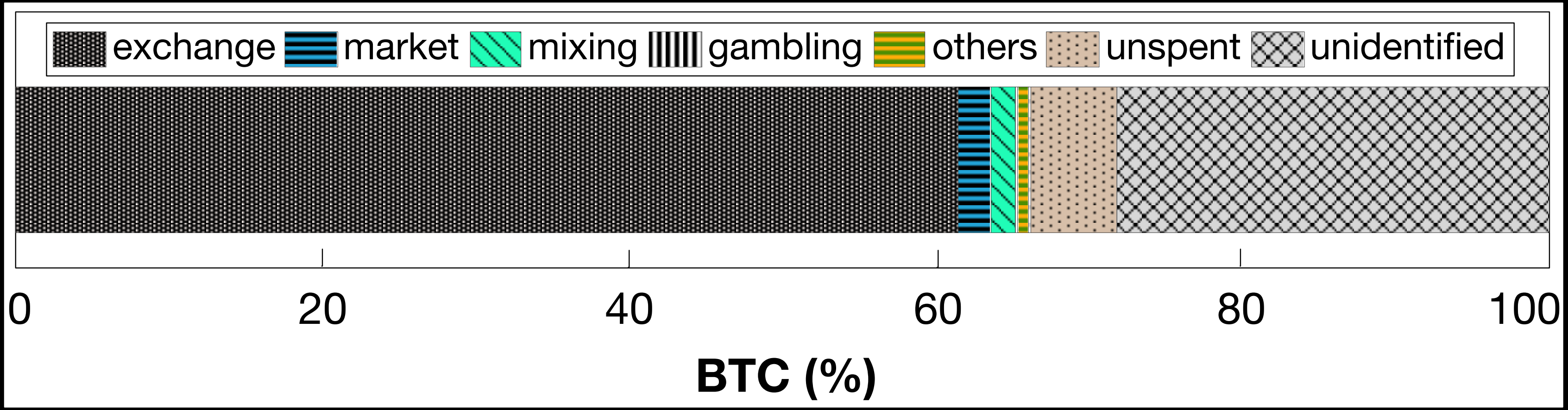
Stop conditions

1. Unspent output
2. Bitcoin service address*
3. Threshold (i.e., # of transaction)

* WalletExplorer provides ownership information about known Bitcoin services

Perpetrator’s black money operation

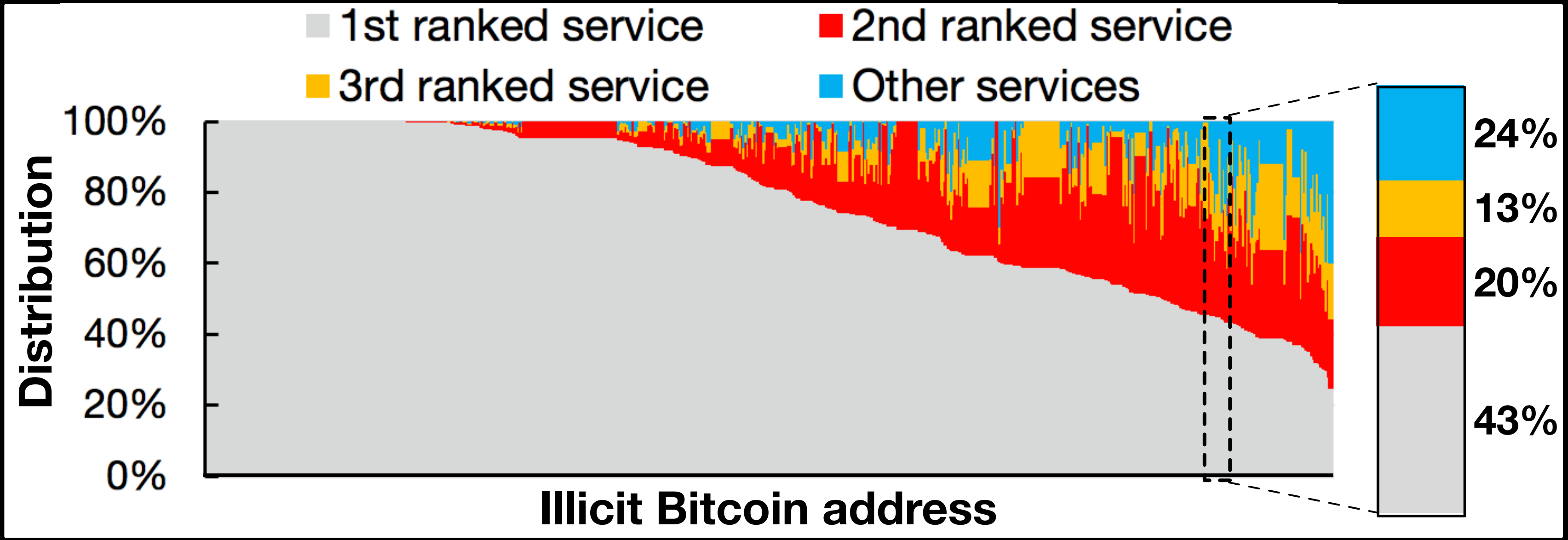
61.4 % has flown into ”exchange”



Distribution of the entire illicit Bitcoins

Perpetrators prefer to exchange illicit funds into ***alt-coins or traditional currencies***

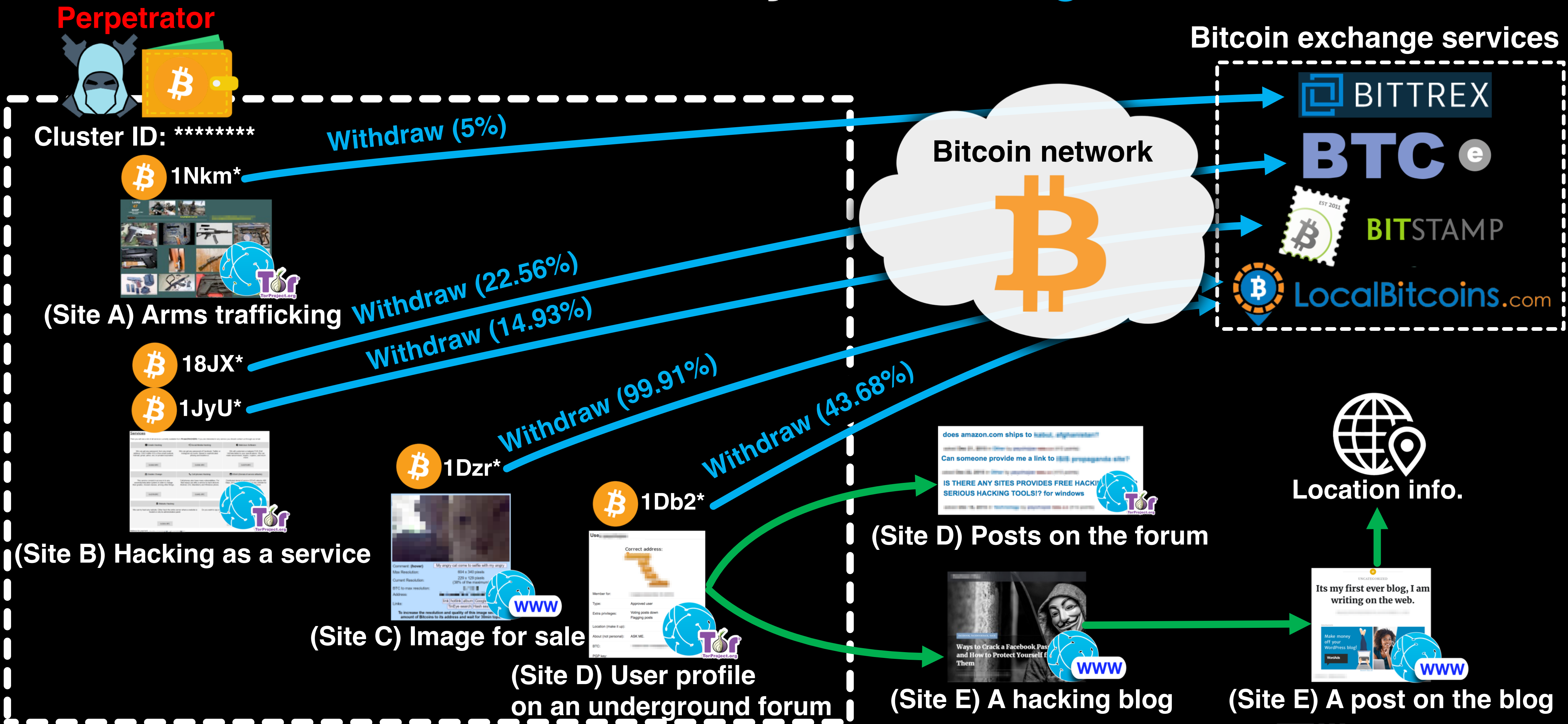
Service distribution per cryptocurrency account



Service usage per each illicit address

A large sum of their money to ***one particular service*** rather than ***diversifying their expenditure***

Case study: trafficking



does amazon.com ships to [redacted]

[redacted]

Can someone provide me a link to [redacted]

[redacted]

IS THERE ANY SITES PROVIDES FREE HACKI SERIOUS HACKING TOOLS!? for windows

[redacted]

Ways to Crack a Facebook Pas and How to Protect Yourself f Them

UNCATEGORIZED

Its my first ever blog, I am writing on the web.

Make money off your WordPress blog!

WordAds

Conclusion

- Cryptocurrency abuses in the Dark Web are pervasive.
- We should think about the dark side of anonymity services.

Don't be relieved;
few evidence could reveal
what you did in the Dark Web.

KAIST

S2W LAB SAFE AND SECURE WORLD