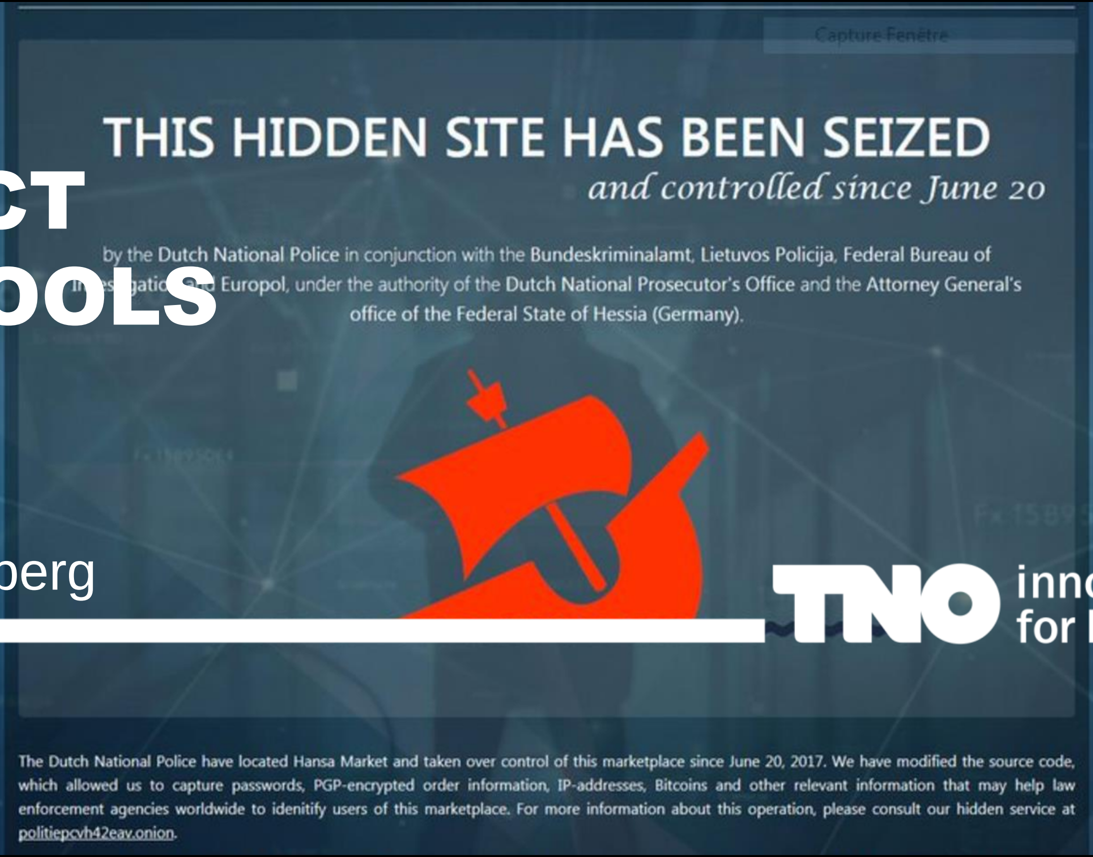
PROJECT DARKTOOLS

Rolf van Wegberg



Capture Fenêtre

THIS HIDDEN SITE HAS BEEN SEIZED

and controlled since June 20

by the Dutch National Police in conjunction with the Bundeskriminalamt, Lietuvos Policija, Federal Bureau of Investigation and Europol, under the authority of the Dutch National Prosecutor's Office and the Attorney General's office of the Federal State of Hessia (Germany).

The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source code, which allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help law enforcement agencies worldwide to idenitify users of this marketplace. For more information about this operation, please consult our hidden service at politiepcvh42eav.onion.

TNO innovation for life

PROJECT DARKTOOLS

- Capability building for INTERPOL member countries on dark net policing:
- *Dark Web Capability Roadmap* – (third-party) solutions mapped to specific capabilities
- *Dark Web Crawling* – ‘state of the onion'
- *Blockchain Analytics* – ‘follow the crypto’
- *Dissemination* – research output and (law enforcement) training

PROJECT DARKTOOLS

- Capability building for INTERPOL member countries on dark net policing:
- *Dark Web Capability Roadmap* – (third-party) solutions mapped to specific capabilities
- ***Dark Web Crawling* – ‘state of the onion’**
- *Blockchain Analytics* – ‘follow the crypto’
- *Dissemination* – research output and (law enforcement) training

TNO DARKWEB RESEARCH PROGRAM

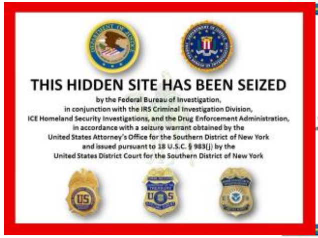
- Applied scientific research following a four stage process:
- *Monitoring the Dark Web* – longitudinal measurements since 2012
- *Sense-making* – from measurements into insights
- *Actionable intelligence creation* – evidence-based interventions
- *Dissemination* – research output and (law enforcement) training

MEASURING THE IMPACT OF INTERVENTIONS

- Types of interventions
- Effect-types
- Crime displacement?
- Desistance?
- Prevention?

INTERVENTIONS

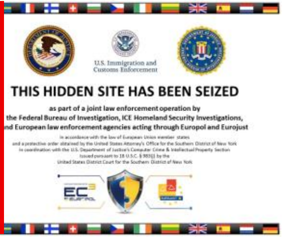
Operation Marco Polo



THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

Operation Onymous



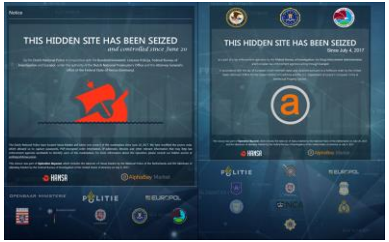
U.S. Immigration and Customs Enforcement

THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

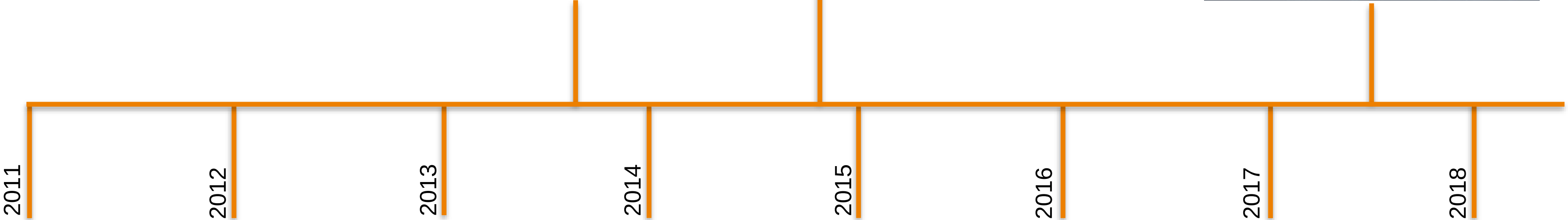
Operation Bayonet



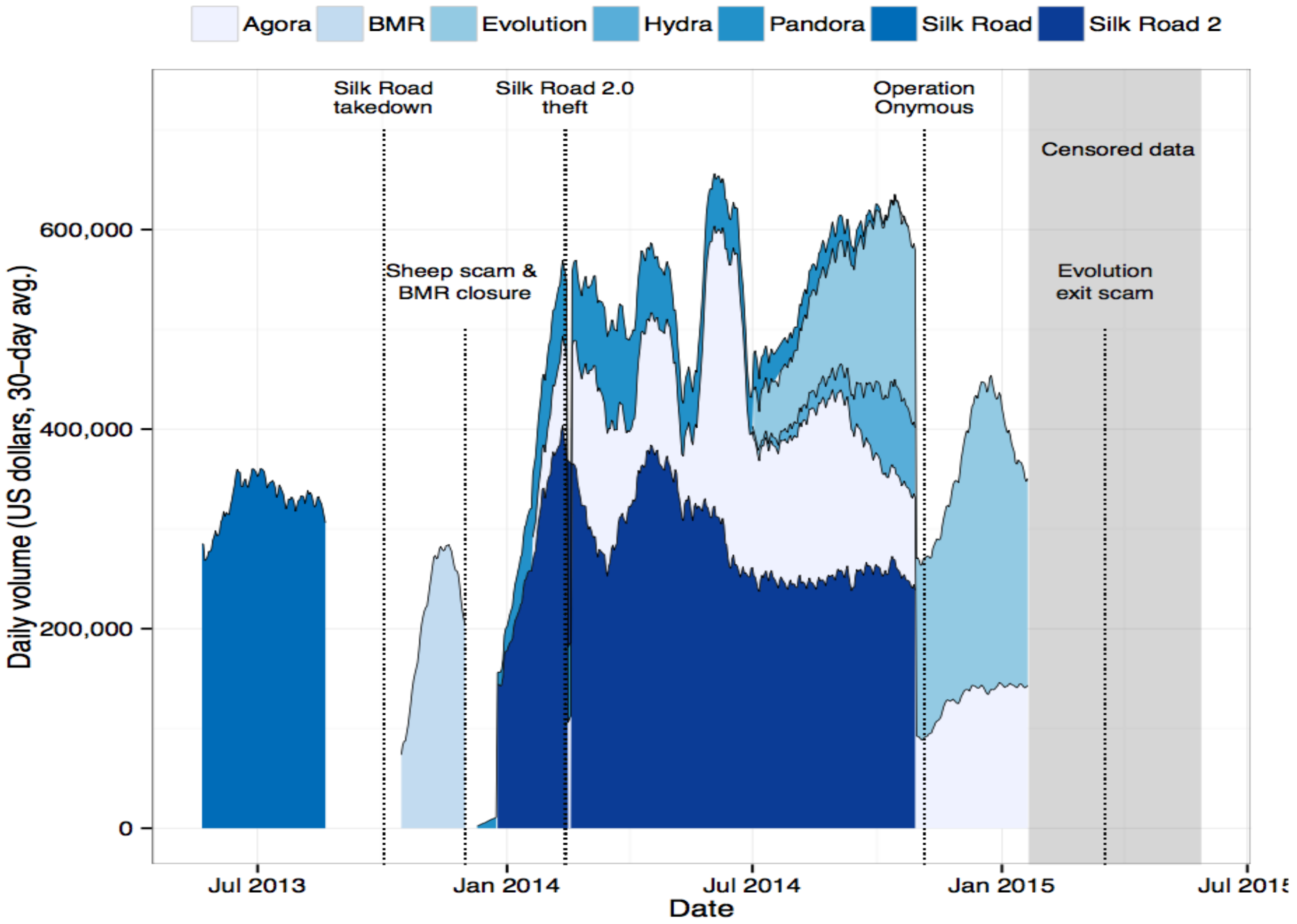
Notice

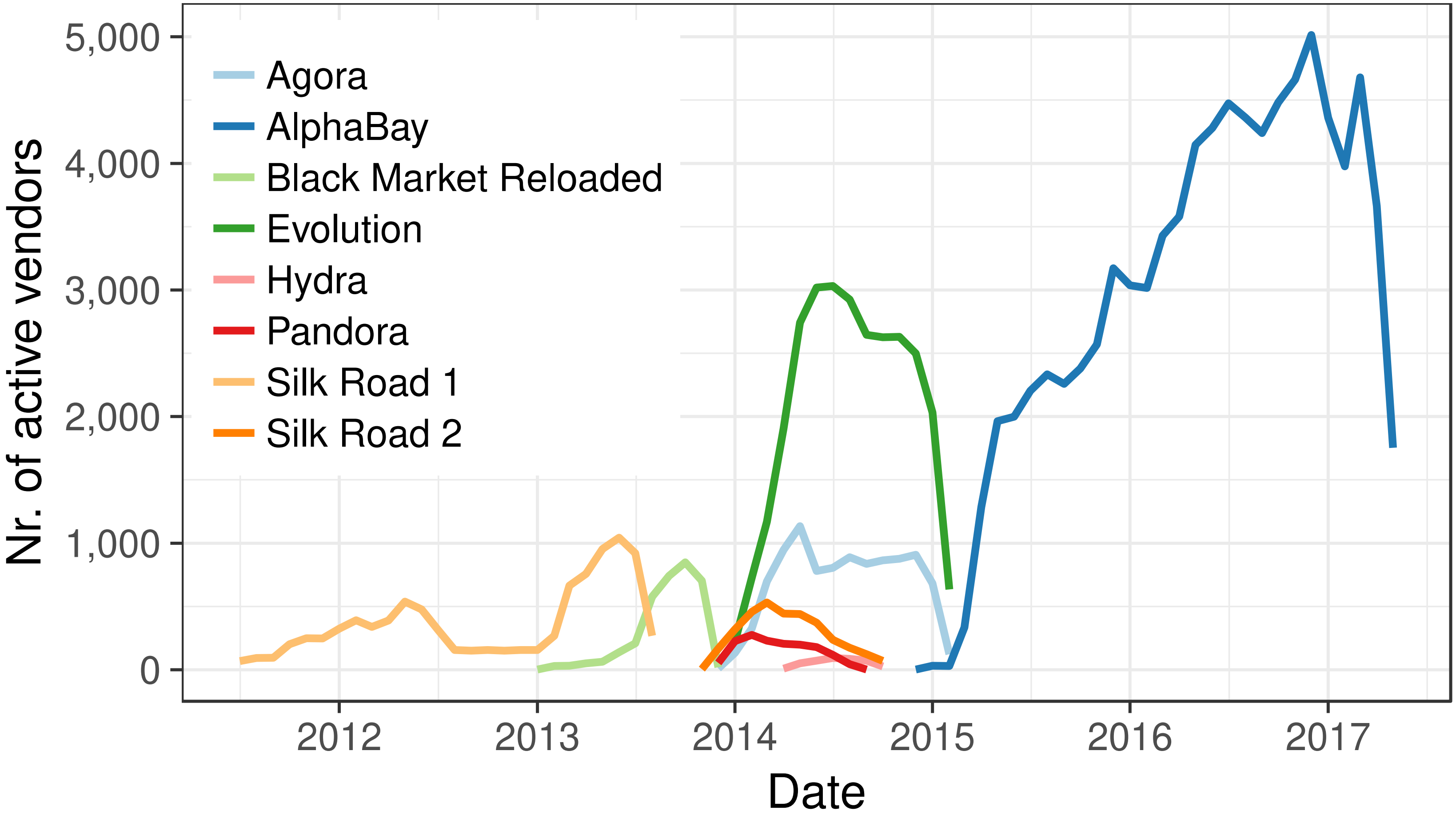
THIS HIDDEN SITE HAS BEEN SEIZED
and controlled since June 20

THIS HIDDEN SITE HAS BEEN SEIZED
Since July 4, 2017



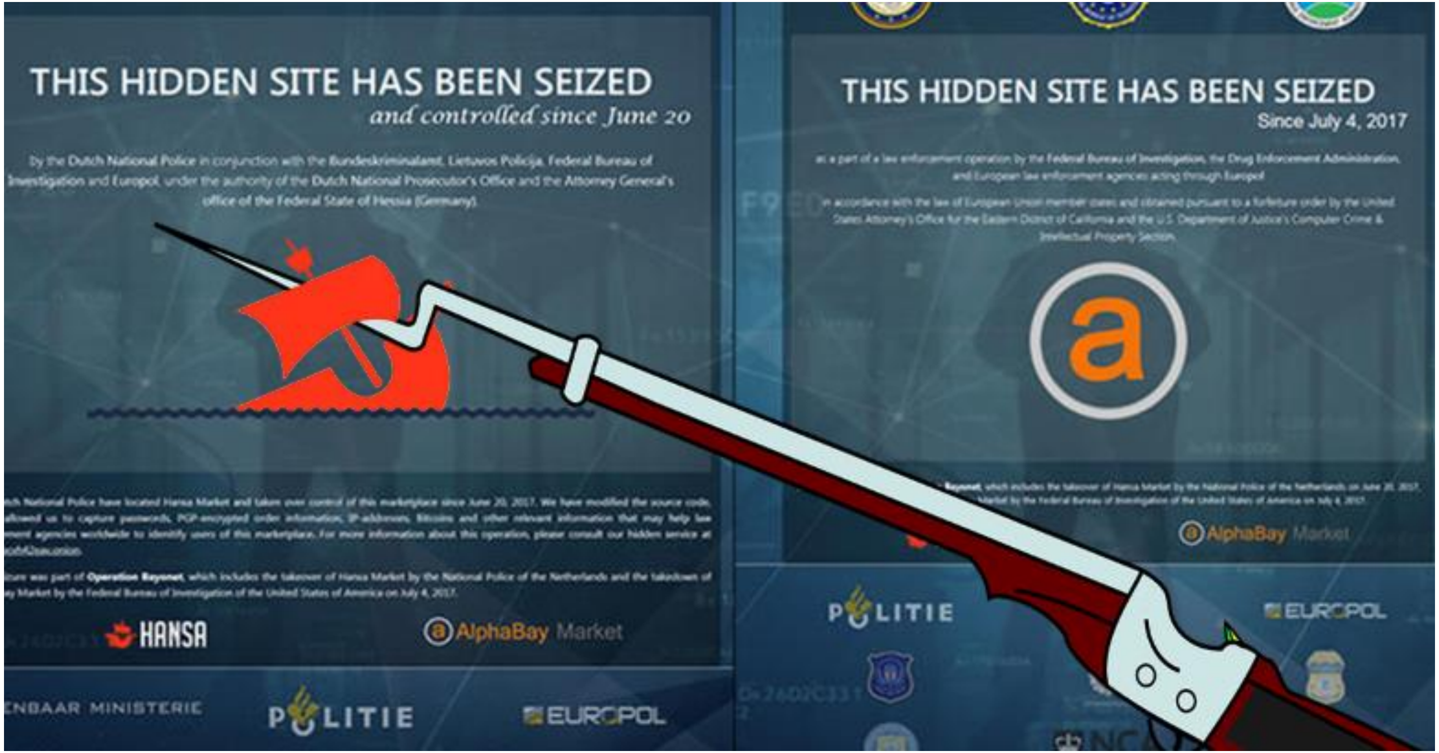
SOSKA & CHRISTIN (2015)





Agora
AlphaBay
Black Market Reloaded
Evolution
Hydra
Pandora
Silk Road 1
Silk Road 2
Nr. of active vendors
5,000
4,000
3,000
2,000
1,000
0
2012
2013
2014
2015
2016
2017
Date

OPERATION BAYONET



THIS HIDDEN SITE HAS BEEN SEIZED
and controlled since June 20

by the Dutch National Police in conjunction with the Bundeskriminalamt, Lietuvos Policija, Federal Bureau of Investigation and Europol, under the authority of the Dutch National Prosecutor's Office and the Attorney General's office of the Federal State of Hessia (Germany).

tch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source code, allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help law ment agencies worldwide to identify users of this marketplace. For more information about this operation, please consult our hidden service at ohf42sac.onion.

izure was part of **Operation Bayonet**, which includes the takeover of Hansa Market by the National Police of the Netherlands and the takedown of ay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.

THIS HIDDEN SITE HAS BEEN SEIZED
Since July 4, 2017

as a part of a law enforcement operation by the Federal Bureau of Investigation, the Drug Enforcement Administration, and European law enforcement agencies acting through Europol

in accordance with the law of European Union member states and obtained pursuant to a forfeiture order by the United States Attorney's Office for the Eastern District of California and the U.S. Department of Justice's Computer Crime & Intellectual Property Section.

Bayonet, which includes the takeover of Hansa Market by the National Police of the Netherlands on June 20, 2017, Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.

MEASURING THE IMPACT OF OPERATION BAYONET

- Distinction between Operation Bayonet and previous interventions
- Crime displacement as intended effect – sting-operation
- New methodology – vendor angle
- Investigating business continuity management of (reputable) vendors

MEASUREMENTS ON DREAM MARKET

- Dump of usernames, registration dates and user type (July – September 2017)
  - Filtering on newly registered vendors (*n=220*)

- Cross-check on Grams (vendor-search engine) - information on historic vendor ‘behavior’
  - PGP-key
  - Previous activity on markets
  - Username(s)

USERBASE OF DREAM MARKET

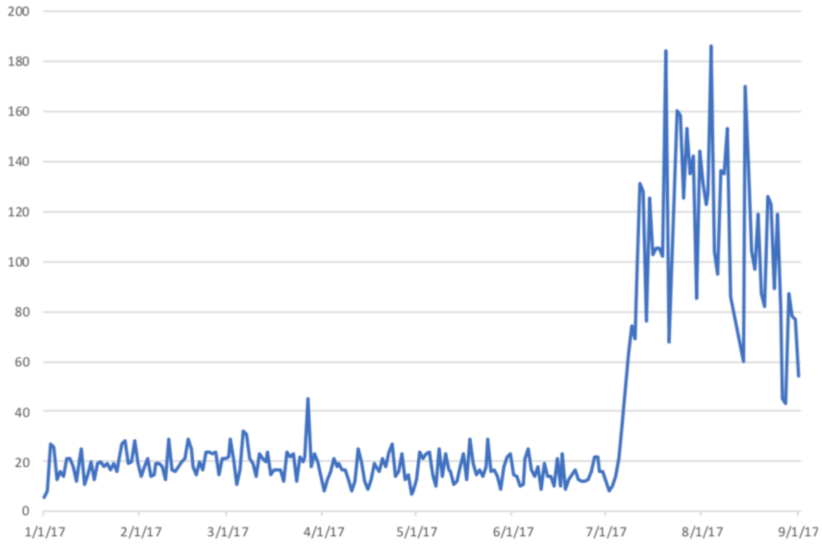


Figure 1: Daily new users on Dream Market in 2017

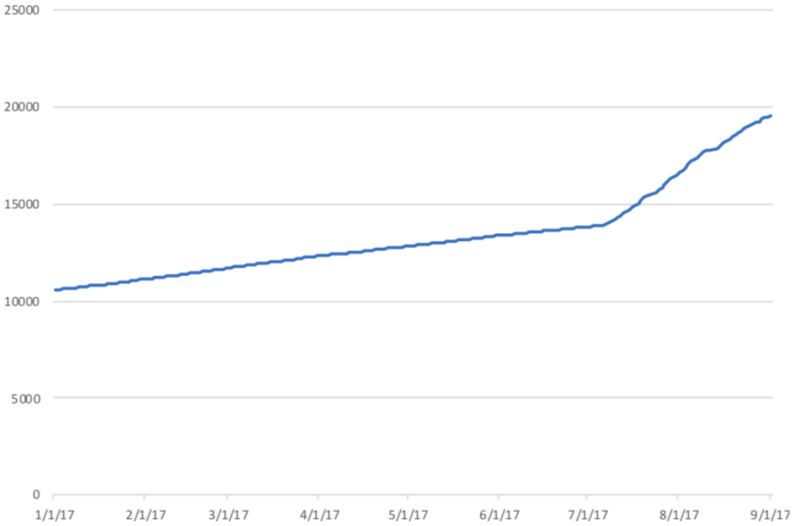


Figure 2: Users on Dream Market in 2017

MIGRATION PATTERNS TO DREAM MARKET

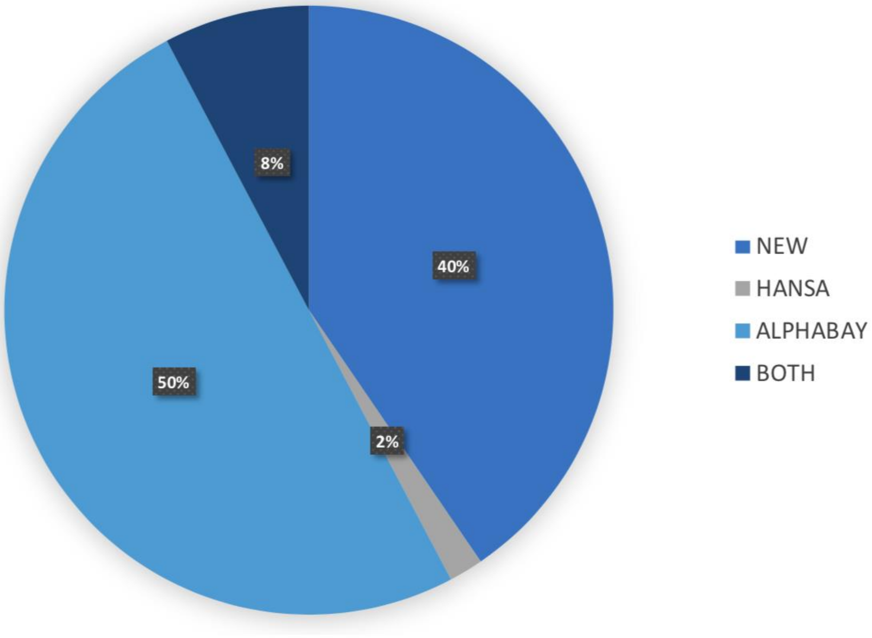


Figure 3: Breakdown of newly registered vendors on Dream Market (*n=220*)

MIGRATION OVER TIME

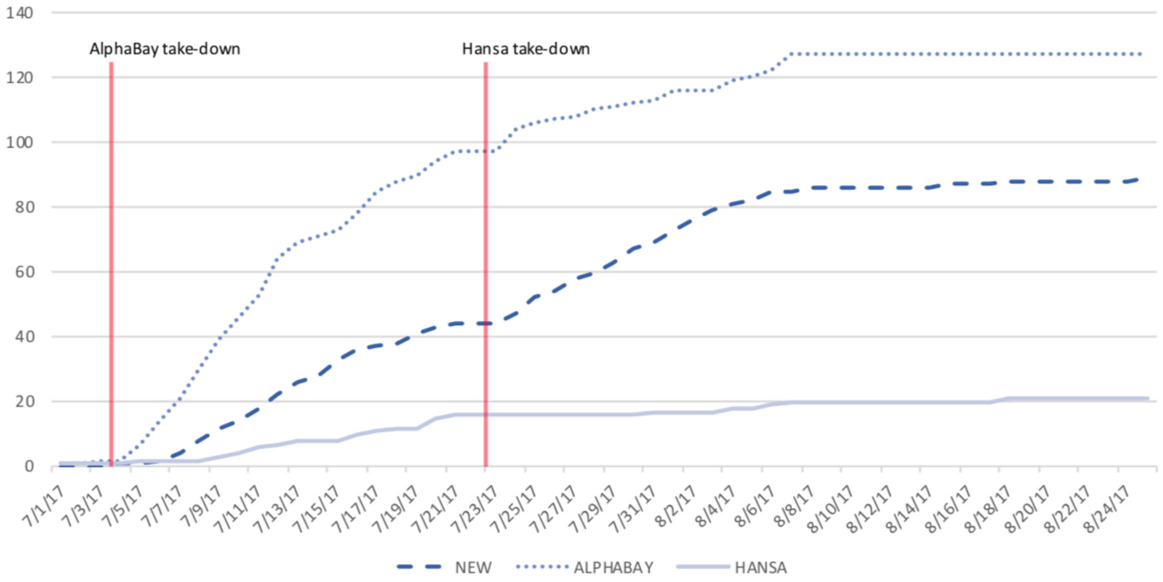


Figure 5: Cumulative number of newly registered vendors on Dream Market per origin on date (*n=220*)

CHANGES IN VENDOR BEHAVIOR?

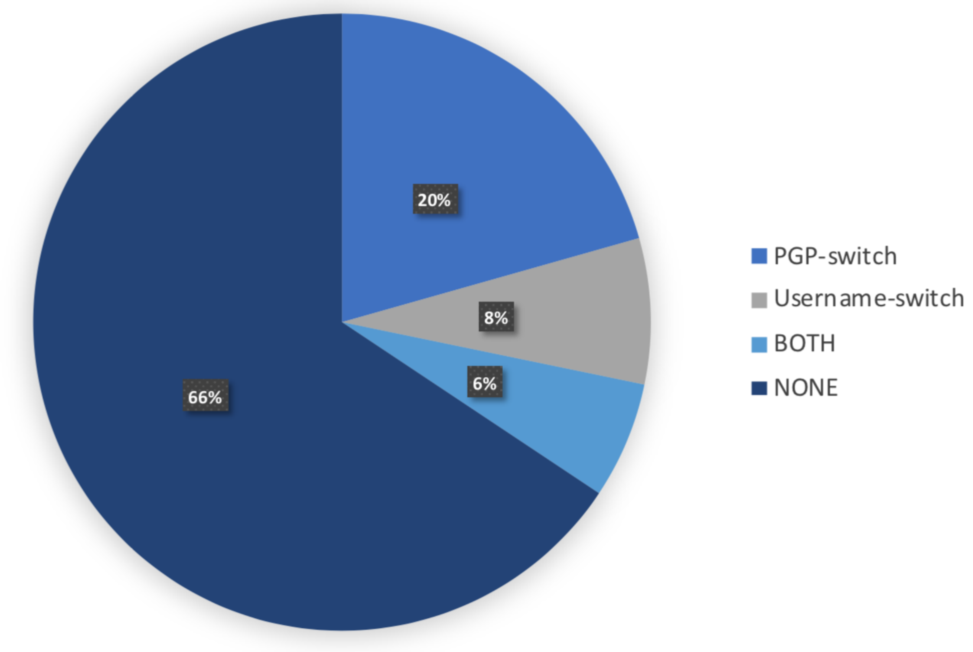


Figure 4: Breakdown of evasive strategies of migrated vendors to Dream Market (*n=131*)

CHANGES IN VENDOR BEHAVIOR OVER TIME

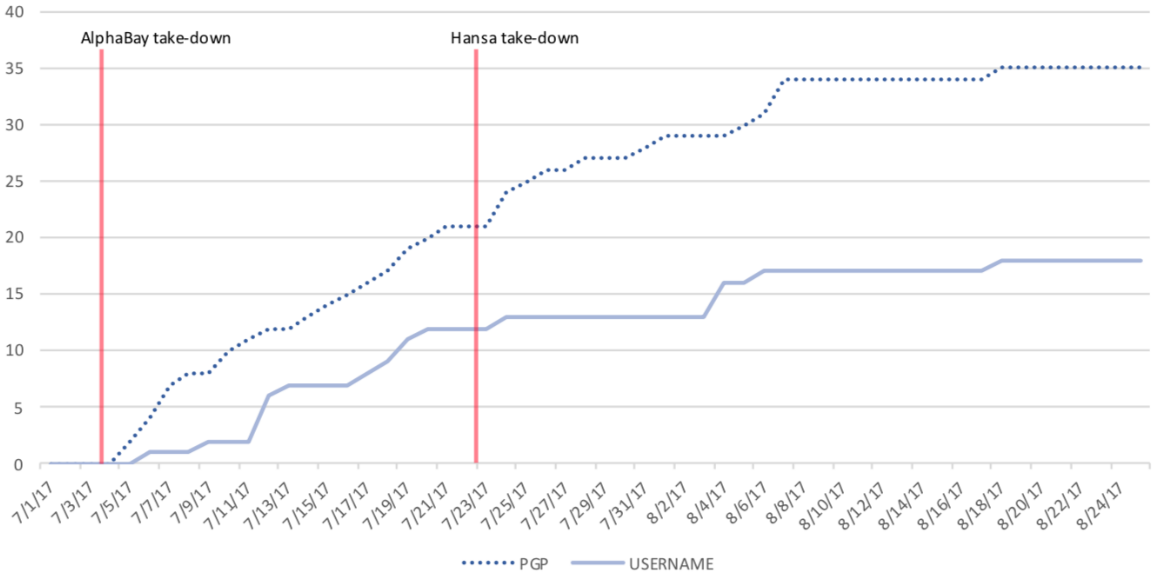


Figure 6: Cumulative number of evasive measures by newly registered vendors on Dream Market on date (*n=53*)

TAKE-AWAYS

- New methodology – inherent limitations (comparability, reproducibility, generalizability)
- Changes in vendor behavior
- First look into incentives stemming from reputation and business continuity-management

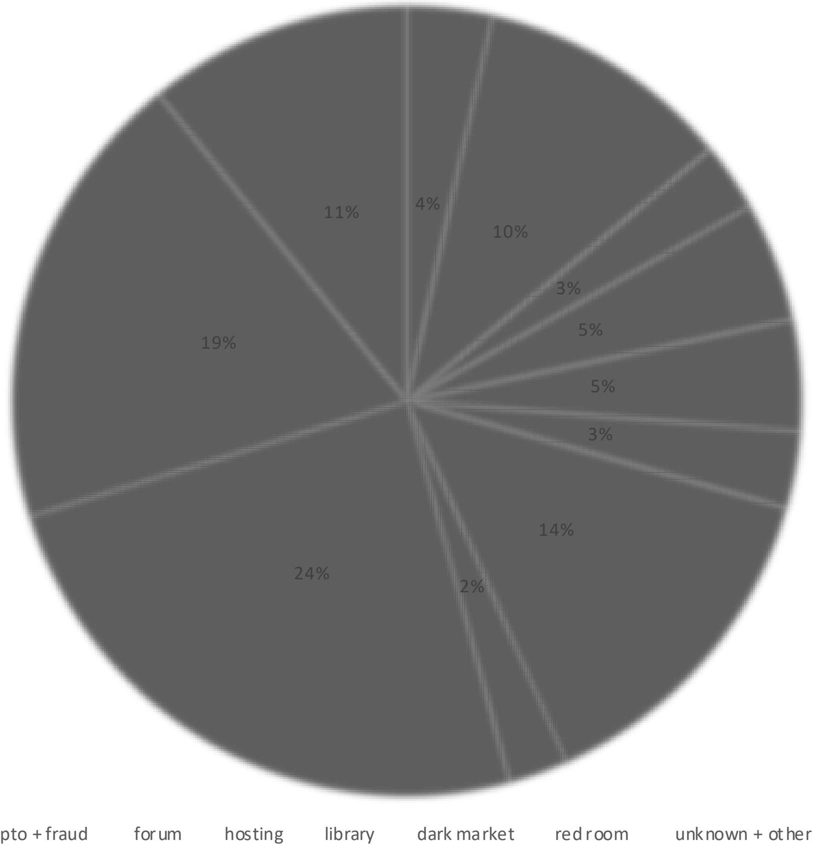
BEYOND – STATE OF THE ONION

- Fragmentation in the dark market ecosystem – single vendor shops

- Significant portion of ‘banned products’ have niche platforms:
  - Child sexual abuse
  - Red rooms

- Significant portion of (cybercrime) ‘facilitators’:
  - Hosting
  - Wiki/forums

New .onions scraped in 2019 week X (n=286)



OUTLOOK

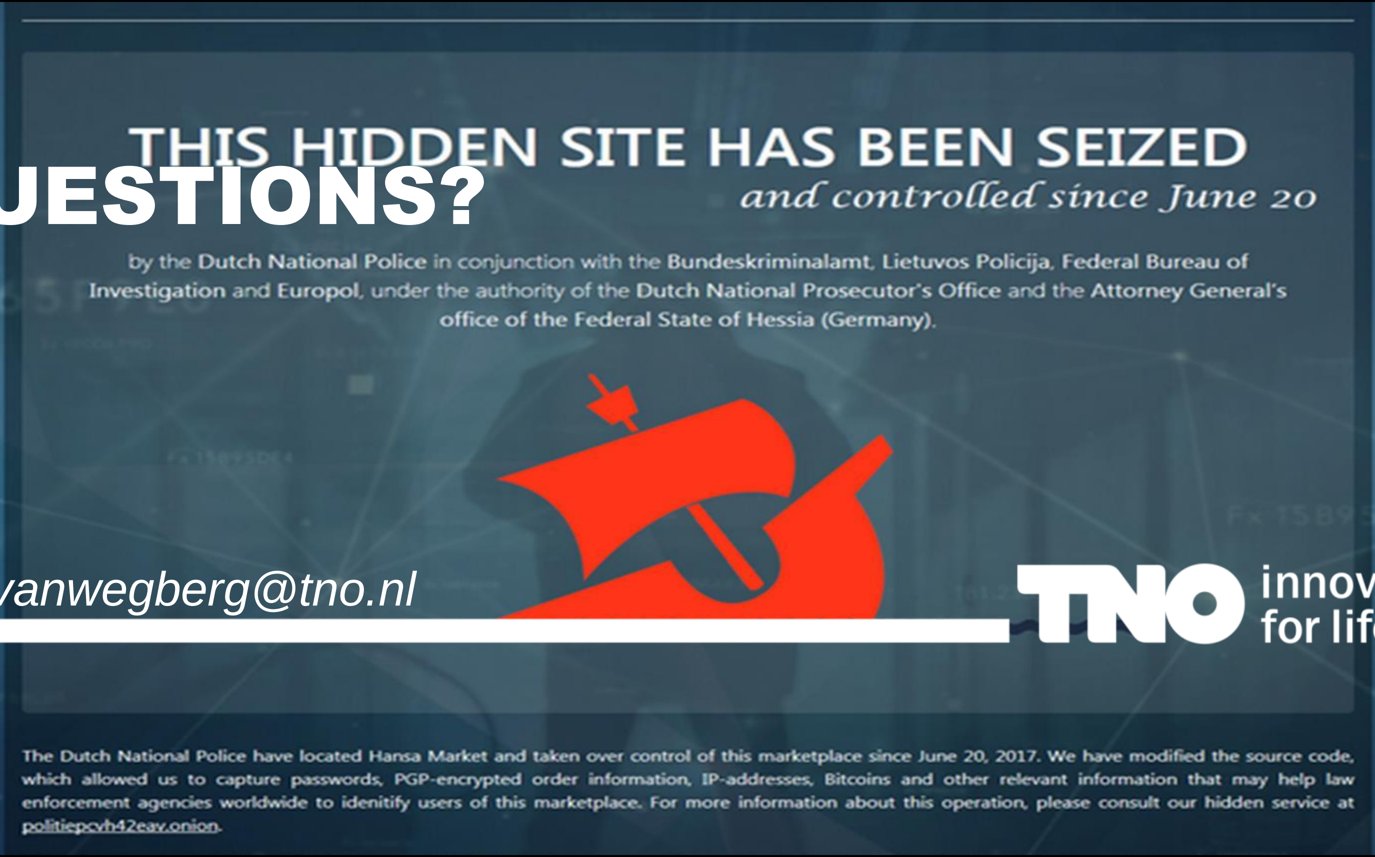
- Interventions aimed at criminal ‘capabilities’:

1. Technologies, e.g., bitcoin mixers

2. Anonymity, e.g., infiltration and/or undercover activities

3. Security, e.g., misconfigurations in .onion domains

QUESTIONS?



THIS HIDDEN SITE HAS BEEN SEIZED

and controlled since June 20

by the Dutch National Police in conjunction with the Bundeskriminalamt, Lietuvos Policija, Federal Bureau of Investigation and Europol, under the authority of the Dutch National Prosecutor's Office and the Attorney General's office of the Federal State of Hessia (Germany).

The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source code, which allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help law enforcement agencies worldwide to idenitify users of this marketplace. For more information about this operation, please consult our hidden service at politiepcvh42eav.onion.

rolf.vanwegberg@tno.nl

TNO innovation for life