VIGILO consult

Running botnets

..and getting away with it

ISD 2013

Cologne/Brühl

Introduction

- Hein Dries- Ziekenheiner
  - Dutch Law (Masters, ICT and Telecom)
  - eLaw Leiden University
  - Dutch ISP association (RIP)
  - Post And Telecommunications Authority (OPTA now ACM)
  - Consultancy

VIGILO consult

Todays subjects

- Dollarrevenue (adware program)
- European law (a lot)
- Dutch law (a little)

VIGILO consult

Dividing that 1/3

- Underground economy
- Case in point: Dollarrevenue

VIGILO consult

Dividing that 2/3

- Dollarrevenue
  - Case

VIGILO consult

Dividing that 3/3

- Analysis
  - What can be enforced under telecoms law?
  - Or the reverse: how can you get away with just about anything?

VIGILO consult

VIGILO consult

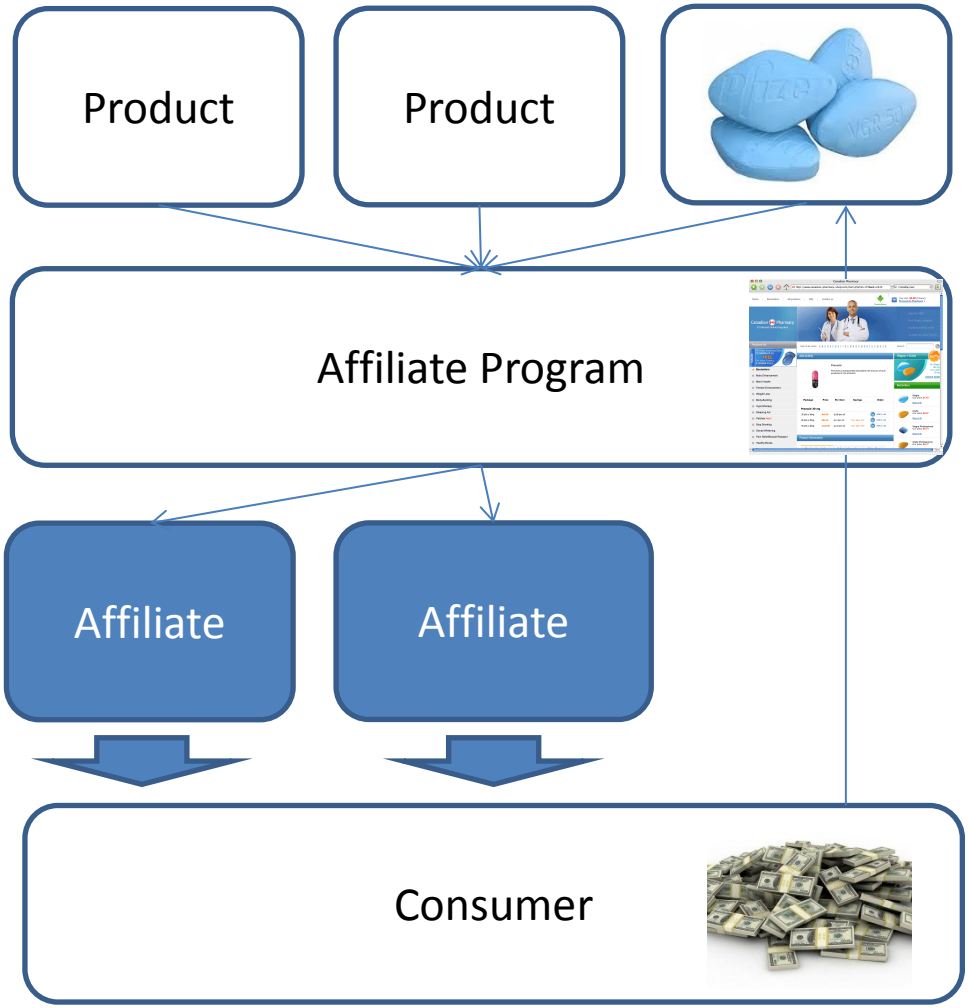
Underground economy

Division of labour

- Increasingly used
- Separation between
  - Product
  - Marketing (Affiliates)
  - Payment processing
  - Technical infrastructure
  - Botnet infrastructure

VIGILO consult

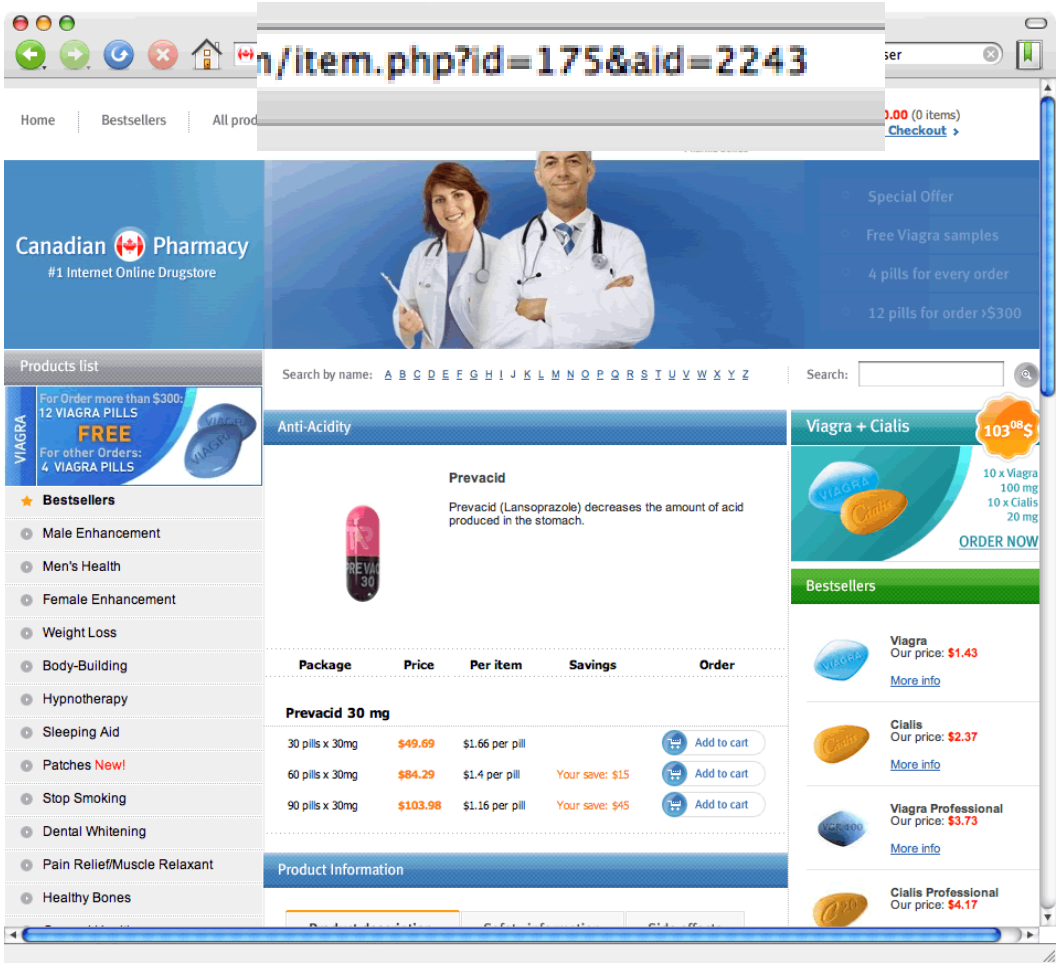
Affiliate marketing



- Affiliates mislead spam or infect consumers
- Transaction: Pay-out
- Affiliates: "create traffic"
- Programs: "sells traffic"

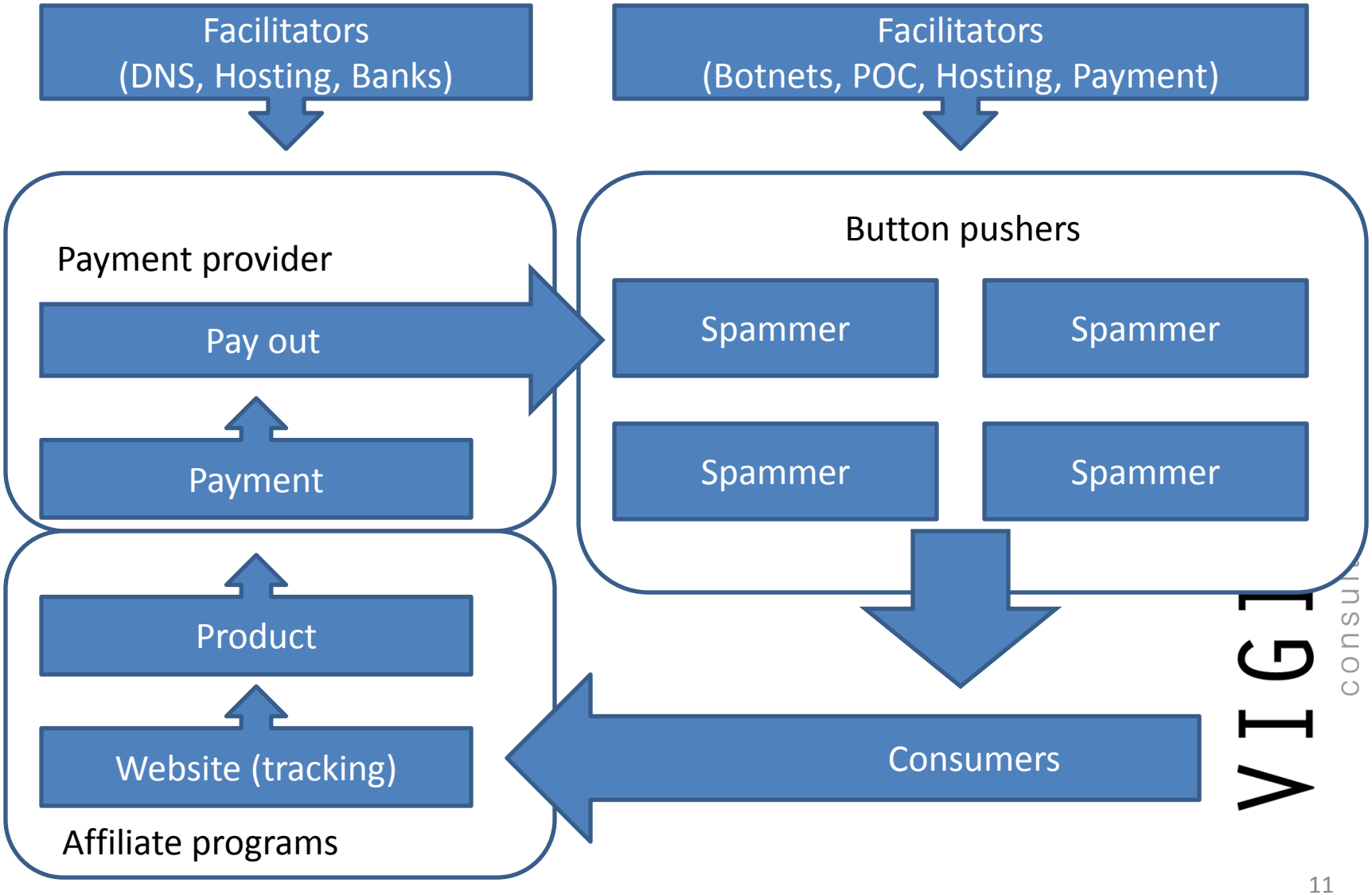
VIGILO consult

Affiliate marketing



VIGILO consult

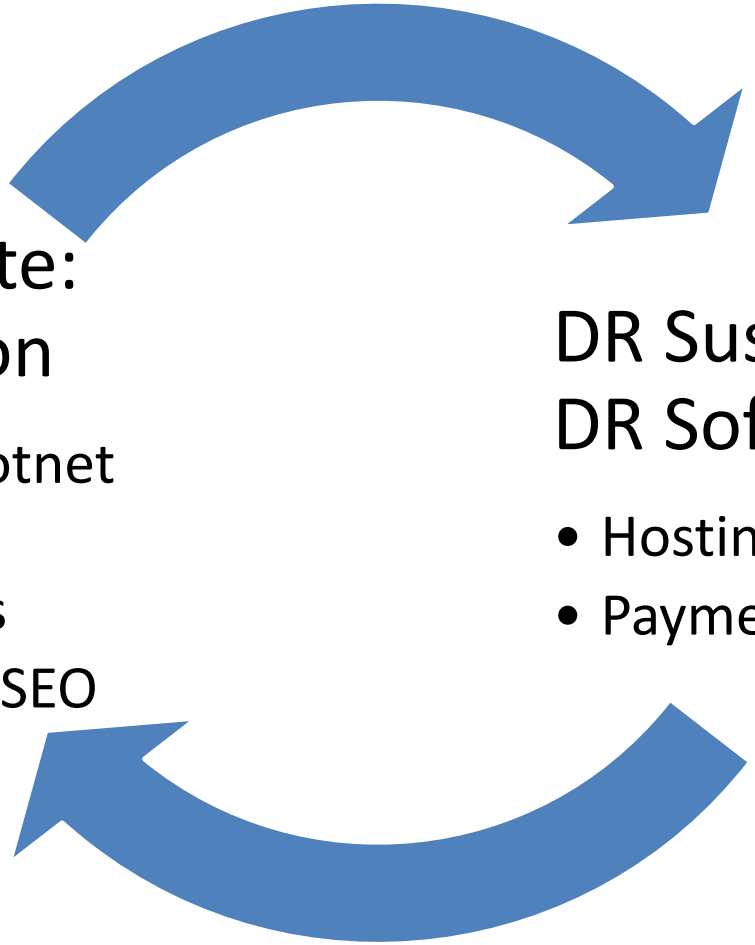
Diagram


Facilitators
(DNS, Hosting, Banks)
Facilitators
(Botnets, POC, Hosting, Payment)
Payment provider
Pay out
Payment
Button pushers
Spammer
Spammer
Spammer
Spammer
Product
Website (tracking)
Affiliate programs
Consumers

Dollarrevenue

VIGILO consult

Result: specialisation and facilitators



DR Affiliate:
Installation

- Herder: Botnet Operation
- Spam: lists
- Websites: SEO

DR Suspects:
DR Software

- Hosting
- Payments

VIGILO consult

International?

- Dollarrevenue:
  - 22M hosts
  - 1 to 2% NL
- Market:

VIGILO consult

International!

Three points

- Division of labour
- Extensive facilitation and specialisation
  - Legal
  - Illegal
- Across International boundaries

VIGILO consult

VIGILO consult

Dollarrevenue

The Law

- Adminstrative Decision on End User Rights and Universal service (4.1 BUDE):
  - Information on what is placed
  - A means to refuse the installation/placement
- Follows from EU telecoms package

  (ePrivacy directive 2002/58/EC)

VIGILO consult

EU Law

- Aims to provide similar protection to ALL consumers in internal market
- “Harmonisation”
- Does not cover enforcement
  - National matter
  - Third pillar (law enforcement)

VIGILO consult

Fine!

- ACM investigates
- November 2007
- Fines 2 individuals and 3 companies a total of € 1.000.000
- Two appeals stages

VIGILO consult

Dollarrevenue & ACM agree:

Not disputed:

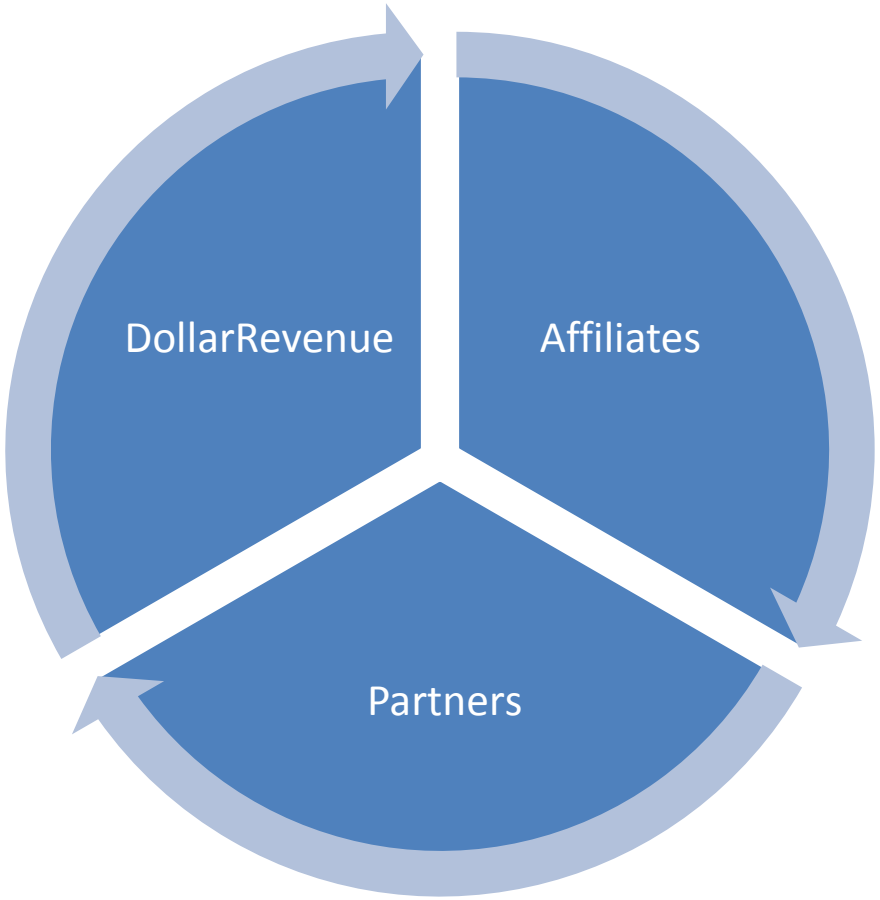
- “Software was placed”
- Staged downloader
  - DollarRevenue Controlled software “bundle”
  - Affiliates placed software using several methods
  - Most of these were illegal – mostly since information was lacking (EULA, ActiveX/Browser warnings are insufficient)

VIGILO consult

But…. Who?

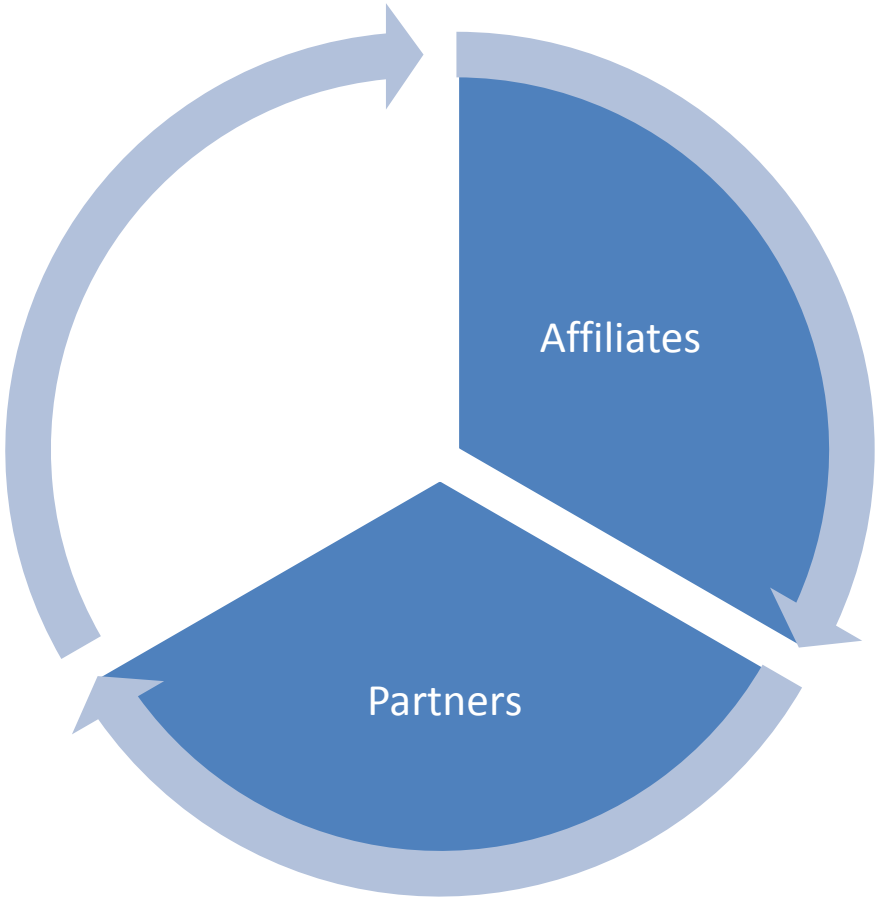
VIGILO
consult

ACM/OPTA



VIGILO consult

DollarRevenue



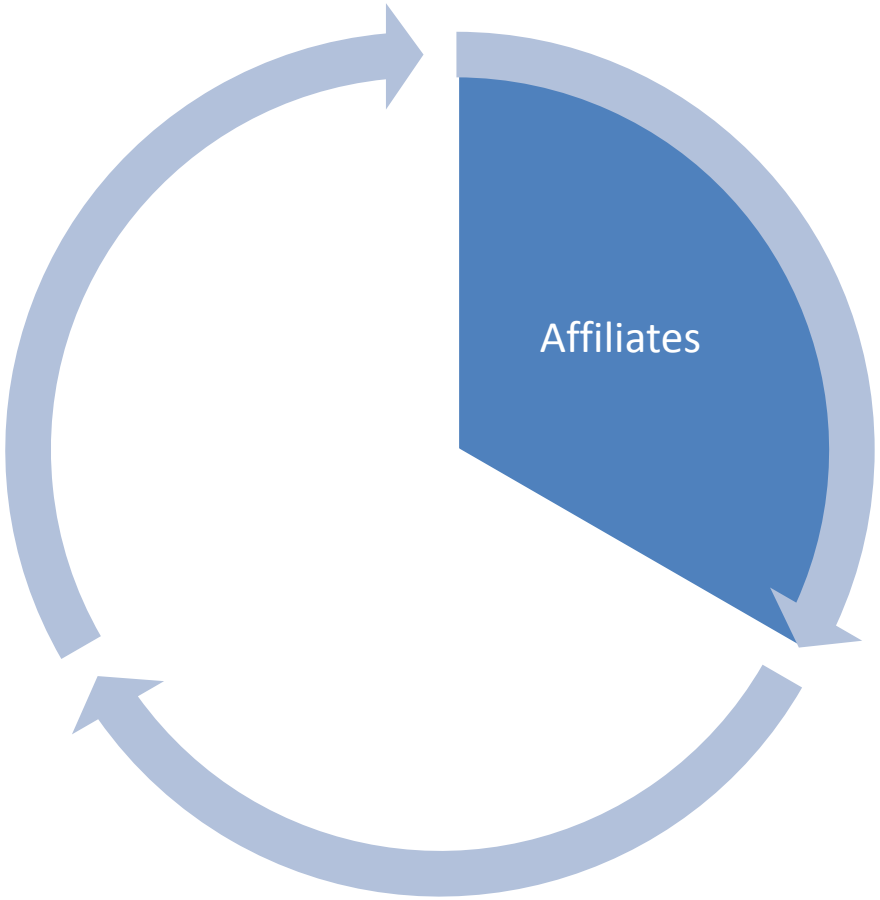
VIGILO consult

What do you think?

- A: Affiliates
- B: Partners
- C: DollarRevenue
- D: All of the above

VIGILO consult

The Court

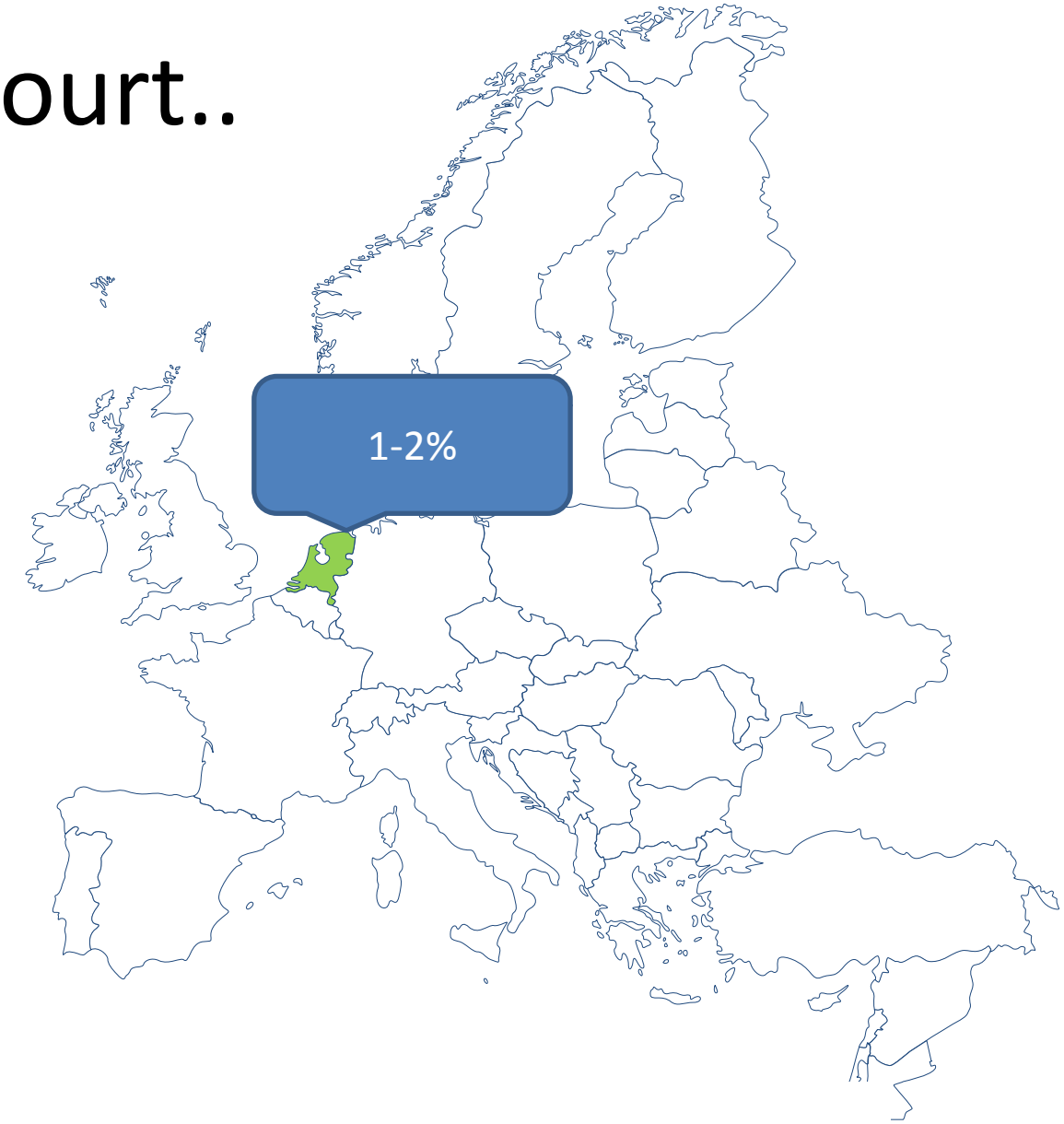


VIGILO consult

And then..

VIGILO consult

The court..



VIGILO consult

VIGILO consult

Analysis

How to…

Gap analysis…

Autoriteit
Consument & Markt

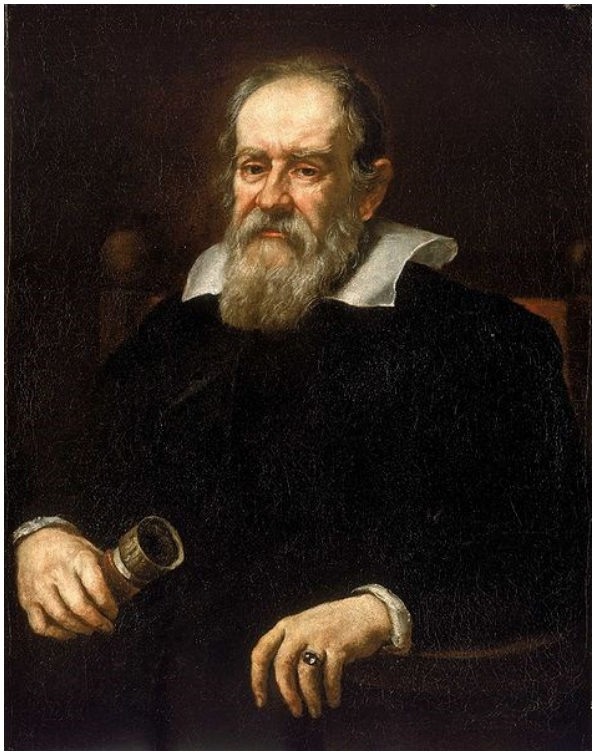
VIGILO
consult

Gap analysis…

- Gap between security measures and criminal enforcement
  - Security: ISO 2700x, PCI DSS, COBIT etc…
  - Criminal enforcement: hacking, computer crime
- Difficulties in addressing facilitators to a crime?
  - Division of labor
  - Specialisation

VIGILO consult

Gap analysis…



VIGILO consult

Issues?

VIGILO
consult

Conclusion

How to… Set up a malware shop in the Netherlands:

- Find many affiliates!
- Make sure they are not from the EU..
- Install abroad (that is .. not in the Netherlands)

- AND: Don’t piss off Dutch police..

VIGILO consult