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
Todays subjects

• Dollarrevenue (adware program)
• European law (a lot)
• Dutch law (a little)
Dividing that 1/3

- Underground economy
- Case in point: Dollarrevenue
Dividing that 2/3

• Dollarrevenue
  • Case
Dividing that 3/3

• Analysis
  • What can be enforced under telecoms law?
  • Or the reverse: how can you get away with just about anything?
Underground economy
Division of labour

• Increasingly used
• Separation between
  • Product
  • Marketing (Affiliates)
  • Payment processing
  • Technical infrastructure
  • Botnet infrastructure
Affiliate marketing

- Affiliates mislead spam or infect consumers
- Transaction: Pay-out
- Affiliates: “create traffic”
- Programs: “sells traffic”
Affiliate marketing
Diagram

Facilitators (DNS, Hosting, Banks)

Payment provider

Pay out

Payment

Product

Website (tracking)

Affiliate programs

Facilitators (Botnets, POC, Hosting, Payment)

Button pushers

Spammer

Spammer

Spammer

Spammer

Consumers
Dollarrevenue

I will call these “partners”

Affiliate network

Dollarrevenue

Affiliates

Makes Downloader

Install Software

Provides Ads

VIGILO consult

12
Result: specialisation and facilitators

DR Affiliate:
Installation
• Herder: Botnet Operation
• Spam: lists
• Websites: SEO

DR Suspects:
DR Software
• Hosting
• Payments
International?

- Dollar revenue:
  - 22M hosts
  - 1 to 2% NL
- Market:

<table>
<thead>
<tr>
<th>DollarRevenue payouts:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>$ 0.30</td>
</tr>
<tr>
<td>Canada</td>
<td>$ 0.20</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>$ 0.10</td>
</tr>
<tr>
<td>China</td>
<td>$ 0.01</td>
</tr>
<tr>
<td>Other countries</td>
<td>$ 0.02</td>
</tr>
</tbody>
</table>
International!
Three points

• Division of labour
• Extensive facilitation and specialisation
  • Legal
  • Illegal
• Across International boundaries
The Law

• Administrative 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)
EU Law

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

- ACM investigates
- November 2007
- Fines 2 individuals and 3 companies a total of €1.000.000
- Two appeals stages
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)
But.... Who?
DollarRevenue
What do you think?

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

Diagram: A cycle with one section labeled "Affiliates".
And then..
The court..
Analysis

How to...
Gap analysis...
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
Gap analysis...
Issues?
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..