



Zombie Alert

Assessing legitimacy of P2P botnet mitigation techniques

Outline

Research question

“What type of entities can – under which conditions – crawl a peer-to-peer botnet given the current European and national data protection and criminal law legal frameworks?”

Methodology

- Literature review
- Functional analysis of relevant doctrine and case law
- Comparative legal study

Intelligence gathering on botnets

Crawling: modus operandi

Crawling P2P Botnets

- P2P Botnet:

“A botnet where bots connect to other bots to exchange C&C traffic, eliminating the need for centralised servers”

- Rossow et. al

- Crawling:

An automated iterative process of visiting bots, requesting their respective lists of known peers and enumerating the links between those peers.

The crawling technique

- Objectives
 - Assess the size of a botnet
 - Identify infected machines
- Preconditions
 - Detailed technical knowledge of botnet malware
 - An initial list of infected computers/peers
 - Knowledge of the communication protocol

Botnet mitigation by private sector and individuals

Privacy issues related to Crawling

- Data Protection issues
 - Processing of personal data
 - Legitimation grounds
- Confidentiality of communications
- Unauthorized surveillance

Agent who is not part to a communication

- Individuals
 - Legitimacy?
 - Potential offences
- ISPs
 - Legal duty to ensure security
 - Contractual obligations
- Security Companies
 - Legitimacy?
 - Legitimate interest of a third party: conditions may apply

Conditions may apply

- Security Companies
 - Restricted collection and distribution to ISPs
 - Additional safeguards
 - Concrete impact assessment: gains vs. losses
 - Sensitivity of the data processed
 - Potential harm to the lives of individuals (and why not organisations?)
 - Use of Article 7(f) as required by A29WP in Opinion 06/2014

Agent who is part to a communication

Legitimate interest vs. Third Parties involved

- Individuals
 - Potential offences
- ISPs
 - Legal duty to ensure security - Reinforced
 - Contractual obligations - Reinforced
- Security Companies
 - Legitimate interest of a third party

Right to Self-Defence?




Botnet crawling in a criminal investigation

4 distinct issues

1. Botnet crawling as a possible offence

Crawler exploits vulnerability caused by botnet malware

- 
- Hacking (BE) or Computer Intrusion (NL)
 - Illegal data/system interference
 - Hacking tools / Malware

Low threshold for criminalisation!



Legitimising ground needed

Possible legitimising grounds for LE

- Intrusive surveillance
- Systematic surveillance
- Network search

Intrusive surveillance

- The power to secretly enter a private place to observe
- Not a home (BE & NL) or office of a doctor or a lawyer (BE)
- Nothing can be seized

Systematic surveillance

- Paradoxically deemed more intrusive than intrusive surveillance
- Systematic observation of people, their presence or conduct or items, places or circumstances
- Systematic character follows from:
 - the duration of the observation;
 - the use of technical means;
 - the international nature of the observation;
 - the involvement of specialised units (BE)

Network search

- More tailored to the digital context
- Allows the extension of an initial search in a computer system to connected systems
- **However:**
not usable in the context of botnet crawling due to access right restriction

2. Crawling is done covertly

- Some botnets can detect and hinder crawling

➡ Need for secrecy

- Covert action by LE implies significant impact on a person's fundamental rights

➡ Adequate legal basis needed

- Both types of surveillance are covert investigatory powers with solid legal roots

3. Crawler as a 'technical means'

- **Remark:**
Surveillance powers were created with the physical world in mind
- Intrusive surveillance => focuses on a 'private place'
- Systematic surveillance => accessing internet always involves technical means?

Intrusive surveillance

- Belgium

Two questions:

- Can a private computer be considered a private place, not part of the home?
- Can crawling be qualified as using technical means?

➡ To both questions: yes

Intrusive surveillance

- The Netherlands

2 arguments against application in virtual world:

- Human rights argument
- Legal technical argument

Systematic surveillance

- Systematic nature of crawling
 - Using technical means
 - International character
 - Undertaken by specialised units
- Technical means in cyberspace:
crawler as specialised software
- Relationship with intrusive surveillance: 2 different phases

4. Crawling knows no borders

- Crawling is borderless, but LE competences are not
- Should territoriality be reinterpreted for cyberspace?

“What you can see in Belgium, takes place in Belgium”



Probably internationally unacceptable

Conclusion

- Crawling by private sector and individuals have different consequences. ISPs seem to be able to use this technique, while individuals should to be prevented from such and most security companies are likely to be unable to legitimize their actions.
- Crawling by LE seems impossible within the currently applicable legal framework, yet reasons why differ between jurisdictions



Thank you

karine.esilva@law.kuleuven.be
ruben.roex@kuleuven.be