CCDCOE

Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Legal Aspects of Fighting Botnets – The Estonian Perspective

09. March 2011

Lauri Aasmann

CCD COE 2011

- Not too long ago…

  - negative effect on available bandwidth due to DDoS and spam

- Today's reality

  - increasing theft of credit card and online banking credentials (malware incorporates credential harvesting functionality)

  - extortion of money with the threat of large-scale DoS attacks against enterprises;

  - politically motivated DDoS attacks

  - cyber espionage

Trends

- Operating and renting out botnets is taking the shape of professional business
  - marketing campaigns
  - mergers (e.g. Zeus and SpyEye)
  - Technical support provided for malware products
  - End-user training is offered in various courses in cybercrime (Cash Paradise University)
  - Custom extensions available for existing products
- Increased malware quality due to a trend towards actual software development process
- Licensing schemes are used to control in which way the software is used
- Evolution - open-source software, construction kits, specialized botnets

Examples of countermeasures

- Removal of the Command & Control (C&C) server renders the entire botnet useless
  - possible if there is only one server, location known
  - Cooperation of ISP necessary

- Sinkholing - redirecting traffic meant for C&C server to other locations
  - Location of C&C server is known but takedown not possible
  - Works also in the other direction, i.e. malicious traffic from infected hosts can be redirected

Examples of mitigation methods in case of DDoS

- Increasing the connection bandwidth
- Disconnecting several links to cut off certain attack source addresses
- Packet filtering at firewalls according to certain traffic patterns

Inspection of Traffic and Packet Data

- First step to detect and characterize botnet traffic (used on daily basis by providers of vital services - banks, power plants, mobile phone networks etc.)

- a number of legal constructs involved - most notably, **privacy**, **unauthorized surveillance** and **confidentiality of communication** concerns

Inspection of Traffic and Packet Data - Perspective of breaching administrative law (1/2)

- According to EU Data Protection Directive, IP addresses may be considered personal data and are therefore subject to personal data processing requirements
  - principle of legality *(personal data shall be collected only in an honest and legal manner)*
  - principle of purposefulness *(personal data shall be collected only for the achievement of determined and lawful objectives, and they shall not be processed in a manner not conforming to the objectives of data processing)*
- The issue of considering IP address as personal data has been debated with no final position
  - the majority of legal researchers, including Article 29 Working Party (an independent EU Advisory Body on Data Protection and Privacy established by Article 29 of the Data Protection Directive), has concluded that unless the data correspond to users that **cannot be identified**, one will have to treat all IP information as personal data

Inspection of Traffic and Packet Data - Perspective of breaching administrative law (2/2)

- Considering IP as personal data, the stakeholder capturing and analysing the traffic, under Section 10 of the Personal Data Protection Act, would need the consent of the data subject
  - Exceptions in case of criminal proceedings or to fulfil legal obligations related to national security and society's well-being
- To eliminate legal risks related to monitoring and analysing the traffic from ISP's point of view, a consent from the data subject needs to be obtained, e.g. by including respective provisions in service level and user agreements and terms of use of its information services and networks

Inspection of Traffic and Packet Data - Perspective of breaching criminal law (1/2)

- Unauthorized surveillance (Estonian Penal Code Section 137)
  - *§ 137 (1) A person without the lawful right to engage in surveillance who observes another person in order to collect information relating to such person shall be punished by a pecuniary punishment or up to 3 years' imprisonment.*

- Distinction must be made whether this technique is used by the actual owner of a computer connected to a botnet (e.g. citizen) or with the help of a third party (e.g. ISP, CERT)
  - listening or recording the communication of the parties by a party of the communication cannot be regarded as unauthorized surveillance (Estonian Supreme Court's Criminal Chamber's judgement from 26.03.2009 No 3-1-1-5-09)

- Based on general theory of criminal law (although not backed by court practice yet) to the extent the purpose of analysing traffic data has to do with technical aspects of countering botnets and is not about collecting information about one specific intruder, the provision of 137 of Penal Code does not apply

Inspection of Traffic and Packet Data - Perspective of breaching criminal law (2/2)

- § 156. Violation of confidentiality of messages
  - (1) *Violation of the confidentiality of a message communicated by a letter or other means of communication is punishable by a pecuniary punishment*

- Message = content
- Making message available for any other person not an addressee = confidentiality violation
- Can not be applied in case of strict traffic and packed data inspection

Takedown of Command & Control Infrastructure

Taking down an identified C&C server by an ISP or by an order of a law enforcement agency (authorized takedown)

- CERT does not have the authority to order a C&C server takedown
- An ISP can decide to restrict access to certain resources in accordance with its general security mandate (limitations of consumer protection, user agreements etc. may apply)
- Only in case of a request by a law enforcement agency (police, court) the service provider is obliged to restrict access to its services
  - *Police and Border Guard Act § 7^{13} - Control action and application of administrative coercive measure*

  (1) In case of danger to or violation of public order the police has the right to oblige the person responsible for public order to remove the danger or eliminate the violation of public order and notify the person of the application of administrative coercive measures pursuant to subsection 2 or 3 of this section if the person does not perform the duty within the term set in the notification

Using force (other than authorized) to take down C&C server or take over a botnet (1/6)

If administrative law creates opportunities for lawful takedown of C&C infrastructure, then criminal law provides for opportunities to hold persons, who illegally do or try to do the same thing, accountable

- *§ 206. Interference in computer data*

(1) Illegal alteration, deletion, damaging or blocking of data or programmes within computer systems, or illegal uploading of data or programmes into computer systems is punishable by a pecuniary punishment or up to three years of imprisonment.

- *§ 207. Hindering of operation of computer system*

(1) Illegal interference with or hindering of the operation of a computer system by way of uploading, transmitting, deleting, damaging, altering or blocking of data is punishable by a pecuniary punishment or up to three years of imprisonment.

- *§ 217. Unlawful use of computer system*

(1) Unlawful access to a computer system by way of removal or circumvention of a code, password or other protective measure is punishable by a pecuniary punishment or up to 3 years' imprisonment.

Using force (other than authorized) to take down C&C server or take over a botnet (2/6)

- Self defence and necessity (§ 28 and 29 of the Penal Code)
  - In order to appeal for cyber self-defence, it has to be ascertained whether the person taking over a C&C server combated a direct or immediate unlawful attack against his or another person's legal rights, whether the means used in self-defence were appropriate and proportional in light of the attack and whether or not the limits of self-defence were exceeded
  - Necessity plays a role when the countermeasures also affect and damage third persons not involved in the attack or threat – e.g. the ignorant owners of the infected machines – and there is no other way to eliminate the danger

Using force (other than authorized) to take down C&C server or take over a botnet (3/6)

- **Takeover of Botnets Using the Botnets' Infrastructure**
  - Gaining control over the botnet's infrastructure by pretending to be the botmaster
  - existing functionality of the botnet can be used, e.g. removing the malware from the infected hosts or replacing it with a new piece of software (without accessing the infected machines directly with the exception of the mentioned C&C server
  - Additionally § 208 - *Dissemination of spyware, malware or computer viruses* may apply

(1) Dissemination of spyware, malware or computer viruses is punishable by a pecuniary punishment or up to 3 years' imprisonment.

Using force (other than authorized) to take down C&C server or take over a botnet (4/6)

- **Takeover of Botnets by Accessing the Infected Hosts**
  - *a researcher giving commands to infected hosts without the need to take over the C&C server or the infrastructure*
  - *possible due to vulnerabilities in the infected hosts*
  - *legal risks are the same as in case of takeover of botnet using their C&C servers (§206 - Interference in computer data; §207 - Hindering of operation of computer system; §208 - Dissemination of spyware, malware or computer viruses)*

Using force (other than authorized) to take down C&C server or take over a botnet (5/6)

- **Remote Disinfection**
  - *Taking over at least parts of a botnet enables disinfect the infected computers remotely*
  - *Remote software execution on the infected computers is implied and therefore side effects are possible*
  - *Even though the intent of the actor reflects the wish to help the owner of the infected machine and is thereby good willed, the provisions of 206 (Interference in computer data), 207 (Hindering of operation of computer system), 208 (Dissemination of spyware), 217 (Unlawful use of computer system) and/or 156 (*Violation of confidentiality of messages*) in Penal Code do not expressis verbis prescribe a motive, aim or any other subjective element that would preclude liability*

Using force (other than authorized) to take down C&C server or take over a botnet (6/6)

- **Automated Disinfection**
  - In addition to remote disinfection, an automated disinfection routine (a "white worm") could be created.
  - Such a white worm would act autonomously, similarly to a malicious worm, but would automatically disinfect hosts without any intended damage to the system
  - From a criminal law point of view, the same offences as to manual disinfection (provisions of 206, 207, 208, 217 and/or 156 in Penal Code) are taken into consideration
    - unlawfulness is determined by physical conduct, not whether the intentions of the actor were ill- or good-willed
  - *Preparation of computer-related crime (§ 216[1] of the Penal Code)*
    - *Self-defence and necessity not applicable*

Preparation of a Computer related Crime (§ *216[1]*)

- *(1) A person who, for the purposes of committing the criminal offences provided in §§ 206, 207, 208, 213 or 217 of this Code prepares, possesses, disseminates or makes available in any other manner a* ***device***, ***program***, ***password***, ***protective code*** *or* ***other data*** *necessary for accessing a computer system, or uses, disseminates or makes available in any other manner the information necessary for the commission of the criminal offences specified in this section shall be punished by a pecuniary punishment or up to three years of imprisonment*

CCDCOE
Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Questions?

CCDCOE
Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Thank you!

Lauri.Aasmann@ccdcoe.org