Better safe and private

SURFNET DEVELOPS CODES OF CONDUCT

- Rogier Spoor TNC 2014

History and background

Botnet handling proces
- Reliable source -> notification SURFcert
- Alert constituents
- Institutes clean devices
- Incidentally: sinkholing
- No knowledge about “which data got stolen”

Internet changed
- Must be very reliable, secure
- Interest are high -> academic hospitals, IP research
- In some cases persons need to know which data got “stolen”
- Process of “return stolen data” doesn’t exist

Problems
- Who owns stolen data?
- How to process stolen data?
- EU privacy legislation doesn’t help

Polbelka case

- Pobelka botnet case – extreme sensitive data
- Somebody send email “I can deliver the data”
- Police/NCSC didn’t have procedure
- Can we accept the data? Privacy, criminal law
- How reliable is the data?
- How can we process it?
- How reliable is the source? How did he get it?
- He is a convicted cybercriminal, how can we deal this?

Our approach

- Alert institutes “stolen data” is available
- Interested institutes can ask for data
- Three months limit -> after destroy data
- Security Officer institutes connected with source
- We didn’t get the data, only connecting people

Questions

- How do we know the SO has a mandate?
- Does the institute have privacy regulations
- How are they processing the data?

Lessons learned Pobelka

- Importance of returning data differs (academic hospitals vs education)
- Data unstructured, somebody has to figure out
- Value data only after viewing
- Policies of institutes differ (private internet usage)
- Data handling process within institutes is brand new
- Is the SO the right person?
- Due to VPN -> home data was available
- Check for patient data -> difficult to automate
- Legal (privacy, criminal law) many questions
- Ethics

Steps taken

- Requests to actively participate in botnet takedowns
- Need policy
- Expert opinion papers Criminal law and Privacy law
- Round table sessions with security community
- Share knowledge about experiences
- Policies

Expert opinion criminal law .nl

- Difficult to state if anti-botnet action is illegally. ->depends contract, codes of conduct, state of technique , potential damage, costs, (im) possibilities of various actors to intervene, how society looks at intervention by private actors, Guiding principles of subsidiarity

- Proportionality - the threat of the possible damage caused by the botnet justifies the degree of intervention in computers and data from others.

- For each type of action, and in any context, should be considered whether it is necessary that SURFnet or an affiliated institution performing this action (to the police, antivirus providers or end users about instead of)

Opinion Privacy .NL -1-

- The importance of increasing the security of the Internet can justify processing of some personal data
- Processing and transmission of botnet data are limited to "specified, explicit and legitimate purposes” The goal must be defined in advance and reported

Opinion Privacy -2-

For botnet data restrictive goals:

- warning concerned that their computer is infected by a botnet;
- alerting parties that may be arising from actions by the botnet possible disadvantage;
- that relevant information is provided to relevant third parties, including the institutions connected to SURFnet and other ISPs that victims can warn in this light;
- taking measures to reduce the activity of botnets.

The data must not be kept longer than necessary for the goals that have been identified, Be it must be anonymised. In addition, data that is not relevant for the intended purpose will be removed.

Opinion Privacy -3-

- SURFnet may provide the data to the affiliated institutions. Limit the duty of care SURFnet and affiliated institutions to their own people circle.
- To defend is that the whole data set is transferred to the competent investigating authority -> improve Internet safety
- SURFnet and affiliated institutions may warn internal victims
- When processing the botnet data applies as possible pseudonymisation and anonymisation of data occurs.
- Tune policies with ISPs, DPA and the Consumer and Market Authority.

Policy takedown

Botnet takedown

- After determining obvious importance / impact liaise with ncsc / police / justice
- Any third party inform / warn
- Security contacts report about upcoming takedown.
- Perform Takedown
- Any available data privacy -> importance / impact pathway
- Hand over any data to police
- Report takedown deliver to ncsc / police / justice

Policy returning data

Define "interest" and impact

- Guidelines to weigh the importance and impact
- Sometimes see data to determine impact on procedure
- Review by external committee in doubt
- If sufficient interest, formulate goals and DPA reporting

When receiving or making available of data

- After determining importance / impact as much as possible automated anonymisation / filter
- *Age data is important to distinguish between user and IP link. Old data "justifies" deliver more data.*
- *Or computer or person should be identified*
- Procedurally initially only ip and / or computer name with timestamp and generic interpretation make available.
- Hand data if certain requirements are met to specific contact
- Data breach notification
- Destroy data

Questions

?