Information sharing after botnet take-downs

Martijn van der Heide, KPN-CERT
3 April 2013

What to do after conquering a drop zone?

- **Imagine being offered “vaguely obtained” 750GB worth of stolen data.**
- **How do you go about**
  - **Finding out whose data is in it**
  - **Reaching out to them**
- **Media attention**

“Vaguely obtained”?

- **Highly privileged information:**
  - **Bank statements**
  - **Medical records**
  - **Employee records**
  - **Trade secrets**

- **Can you trust the person who obtained the data?**
- **Wouldn’t one break the law to accept this data?**
  - **Who would you trust with this sort of data anyway?**

- **Securely storing and destroying the data at a later date.**

Finding out whose data is in it

- **Privacy, anyone?**
- **Not all of it is easily identifiable.**
  - **Not always clear what the data actually *is* to begin with!**
  - **If the owner cannot be machine determined, a person may need to look at it.**
- **Problem of scale.**
- **If you find a name, does that data belong to this person or a company?**
  - **Similarly, employees can work from home, or do private things at work.**
- **In case of financial information, can banks play a role?**
  - **They have a relation with the victim and can perhaps help stop any further damage.**

Reaching out

- Who will be in charge of reaching out? The ISP's?
- Determining the relevant ISP is not always so easy.
- If you just have IP addresses, how about dynamic allocations?

- What will you tell the victim?
  - Will they understand what is going on?
  - Be careful not to look phishy yourself!
  - The age of the data is also relevant - "Data may have been stolen from your company 6 months ago" is not a good message to send.

- Authenticating the owner.
  - Anyone can claim to be such and such and obtain juicy information.
  - Who is accountable if data falls in the wrong hands?

- How to securely hand over the relevant data?

Media attention

- **Botnet take-downs are not that uncommon.**
- **This work is generally done without public visibility (which is good).**

- **But now, the media get involved.**
  - **PR nightmare.**
  - **Integrity goes out the window.**
  - **Government gets the blame for not doing enough, even though it is highly unclear what they could have done…**

Thank you for your attention