Feedback from the first AbuseHelper workshop

Christian Van Heurck
CERT.be
AbuseHelper workshop feedback

What?

When?

Where?

Who?
AbuseHelper workshop feedback

1st workshop on AbuseHelper

2-3-4 May 2011

@Belnet new offices

CERT.be – CERT.EE – CERT.FI
Funet CERT – DFN-CERT – Govcert.nl
MILCERT – BIPT – Clarified Networks
CIRCL
AbuseHelper workshop feedback

What did we talk about?

Only talking?

http://abusehelper.be
AbuseHelper workshop feedback

Usage:

Whois bots
Screaming experts
VSRoom
Combine Bot
MongoDB
RT-IR (REST API)
AbuseHelper workshop feedback

General:

Capabilities – symantics
  - collab
  - david.durvaux@cert.be

How do we get data in and out?
  - VSRoom – dashboard – X(ARF)
  - Megatron
  - RFC

Quality of the data?
  - BGP-ranking
  - community of screaming experts?

Legal issues!!!
AbuseHelper workshop feedback

General:

Keeping track of information:
- RT-IR
- database: SQL – MongoDB – Cassandra ???
- wiki?

Create community
- working group
- meetings 2 x year?
- TRANSITS ???
- list of existing bots
- live demo @next TF-CSIRT
- event in September in Stockholm (before T-sec)

SHARE DATA!!!!
AbuseHelper workshop feedback

Other points:

Data mining?
Fordrop?
Research – student thesis @Belnet?
Codenomcion
Megatron
Taranis
myCERT.be

- Demo!
myCERT.be
AbuseHelper workshop feedback

Thanks!!!

christian.vanheurck@cert.be

david.durvaux@cert.be

contact@clarifiednetworks.com

http://abusehelper.be