AbuseHelper

call for an open discussion

31st TF-CSIRT meeting Istanbul
16-17 September 2010

Christian Van Heurck: BELNET CERT & CERT.be
David Durveaux: BELNET Services & BEGrid
problem!

- abundance of “sources”
  - clean-mx
  - abusix
  - shadowserver
  - d-shield

- limited resources for “one-on-one”
  - CERT side
  - constituency side
problem!

- correct & valuable info
- overlap of sources
- manual processing / aggregation / triage
- follow-up overhead

- valuable time & resources get lost
conclusion:

- we need to automate
- we need to change our “output”
- what do the others do?
  - CERTS
  - ISP’s
  - constituency / customers
AbuseHelper!

- generic open source framework
- automated incident report processing
- chat-rooms & chat-bots
  - python scripted + XMPP
  - scalable
  - modular
  - fully customizable
  - Debian GNU/Linux - OpenBSD
- flexible input modules
- flexible output modules
AH community

- CERT EE + CERT FI
  - founding fathers

- Clarified Networks
  - management

- BELNET
  - fast growing community …
licensing = open source

- **MIT**
  - default

- **EUPL**
  - CERT EE

- **Google Project Hosting**
  - code.google.com
  - Google terms & conditions
status

- CERT FI
  - in production ???

- CERT EE
  - in production ???

- BELNET CERT & CERT.be
  - POC
  - want to use in production as soon as feasible
  - want to promote collaboration!!!
how can you contribute?

- **resources**
  - coding
  - testing & debugging
  - new modules
  - ideas
  - new sources

- **money**
  - Clarified Networks development
  - Clarified Networks support & training
  - other third parties
BELNET POC

- **INPUT sources**
  - d-shield
  - abusix (IMAP)
  - clean-mx (FEED)
  - shadowserver

- IDS and-or honeypot sources
  - Snort4All (CERT-EE)
BELNET POC

- bots
  - IMAP
  - clean-mx FEED
  - sanitizer
  - historian
  - whois
  - CRM (BELNET CERT)
BELNET POC

- OUTPUT means
  - csv - mail digest
  - store in database

- statistics & dashboard
- integration with RT
- output via web interface
  - dashboard pages for customer
  - ACL
BELNET POC

The network of knowledge
BELNET POC

ABUSIX Mail parsed from 08-13-10: 569
ShadowServer C&C from 08-15-10: 4
ShadowServer Sinkhole 05-28-10: 161
ShadowServer SPAM 08-10-10: 27
DShield events: 2437
live stream from CleanMXReport generated: 67

modest IT resources: VM 1 CPU, 4GB RAM

legal department looked @licensing
names

- Hillar Aareleid (CERT-EE)
- Juhani Eronen (CERT-FI)
- Jani Kenttälä (Clarified Networks)

- David Durveaux (BELNET)
- Harri Sylvander (Funet CERT)
- Christian Van Heurck (BELNET CERT & CERT.be)
URL’s

- http://code.google.com/p/abusehelper/
- https://www.clarifiednetworks.com/AbuseHelper
whish list

- COLLABORATE !!!
- integration with RT
- output module
- share data from IDS, Snort4All, ...

- Virtual Situation Room (CERT-EE)
Thanks for your time 😊