CERT.be

cert-fi

Funet CERT

CERT Eesti
Computer Emergency Response Team

AbuseHelper Lightning talk

5 slides in 5 minutes

Hillar Aarelaid – CERT.ee
David Durvaux – CERT.be
Jussi Eronen – CERT.fi
Harri Sylvander – Funet CERT

Why AbuseHelper

- You receive that sort of information every day:

```
Reported-From: autogenerated@blocklist.de
Category: abuse
Report-Type: login-attack
Service: apacheddos
Version: 0.1
User-Agent: Fail2BanFeedBackScript blocklist.de V0.1
Date: Wed, 08 Jun 2011 12:55:17 +0200
Source-Type: ip-address
Source: 87.ab.cd.ef
Port: 80
Report-ID: 1121000@blocklist.de
Schema-URL: http://www.x-arf.org/schema/info_0.1.0.json
Attachment: text/plain
Timezone +0200 (CEST)
Lines containing IP:87.ab.cd.ef in /var/log/apache/pucorp.org.log

ddos-domain.tld 87.ab.cd.ef - - [08/Jun/2011:12:55:17 +0200] "GET
/pacfig.txt HTTP/1.1" 403 1898 "-" "WinHttp-Autoproxy-
Service/5.1 »
```

Why AbuseHelper (2)

- Processing these mails by hand is:

1. Time consuming
2. Not an exciting job
3. Doesn’t have any added value

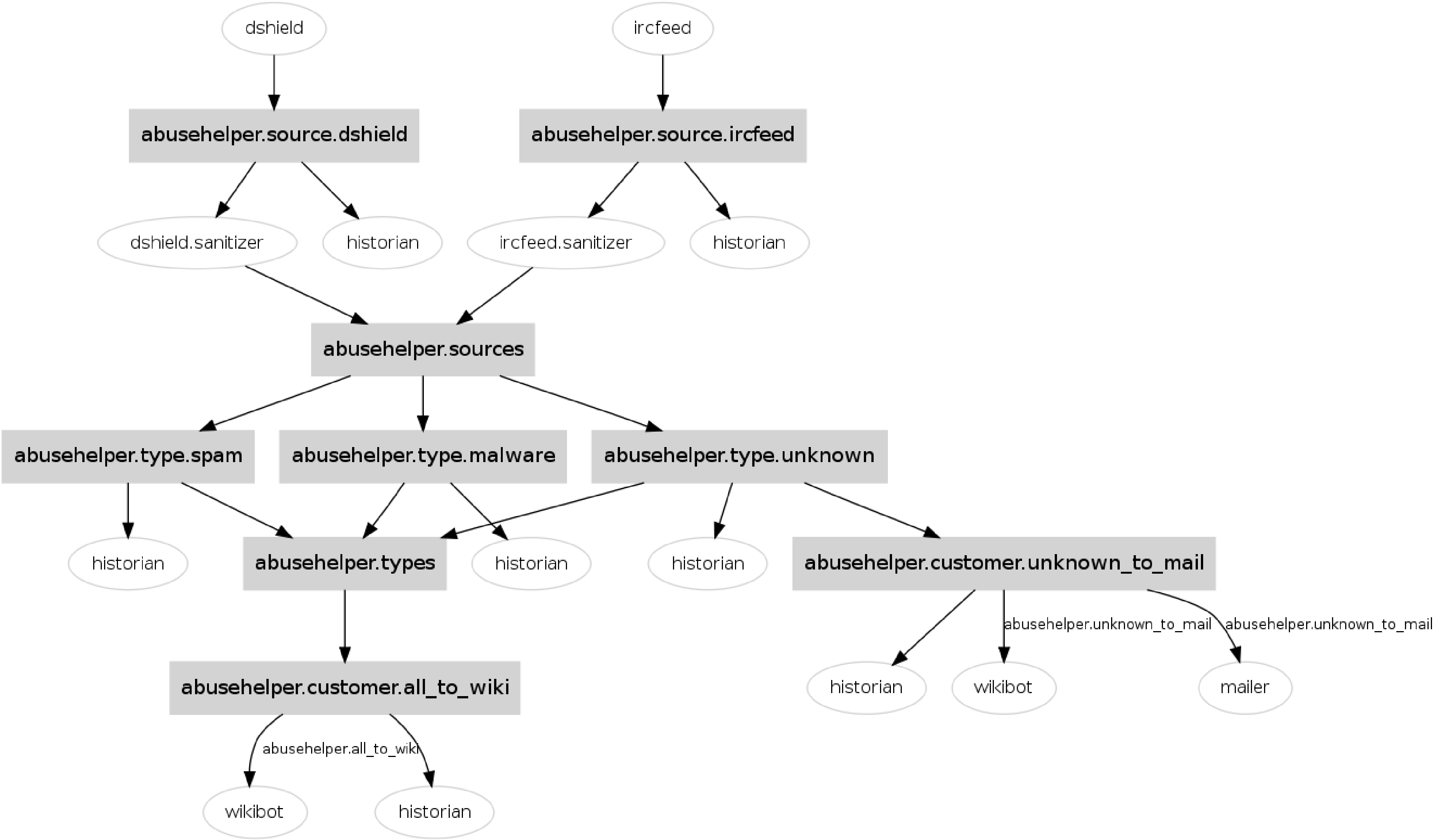
- There are a few “standard” formats in use by the main sources

  - ShadowServer
  - CleanMX
  - AbusIX
  - Dshield
  - …

What is AbuseHelper

- AbuseHelper is a distributed flexible framework to
  - Read information from various sources
    - Mail
    - Chat systems
    - Web servers
    - …
  - Process and enrich this information
  - Send reports following defined workflow to
    - Mail
    - Wiki systems
    - Ticketing systems (RT-IR)
    - …

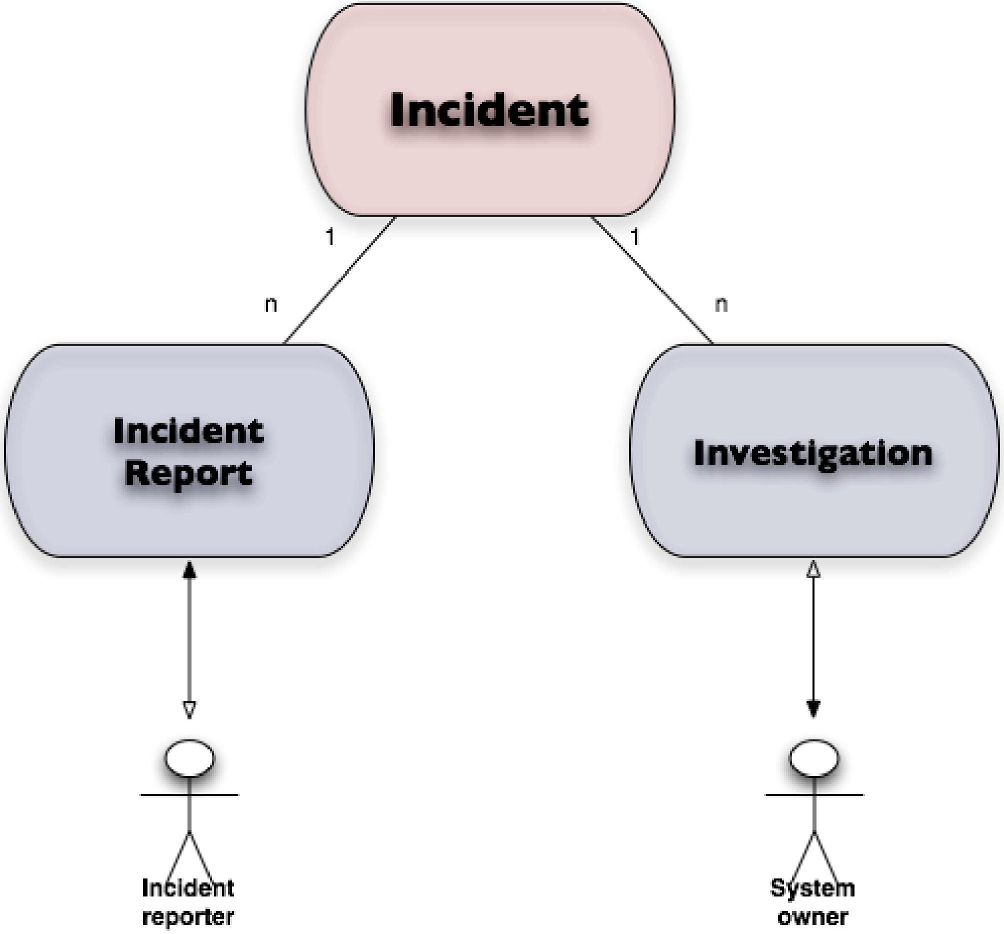
Sample workflow



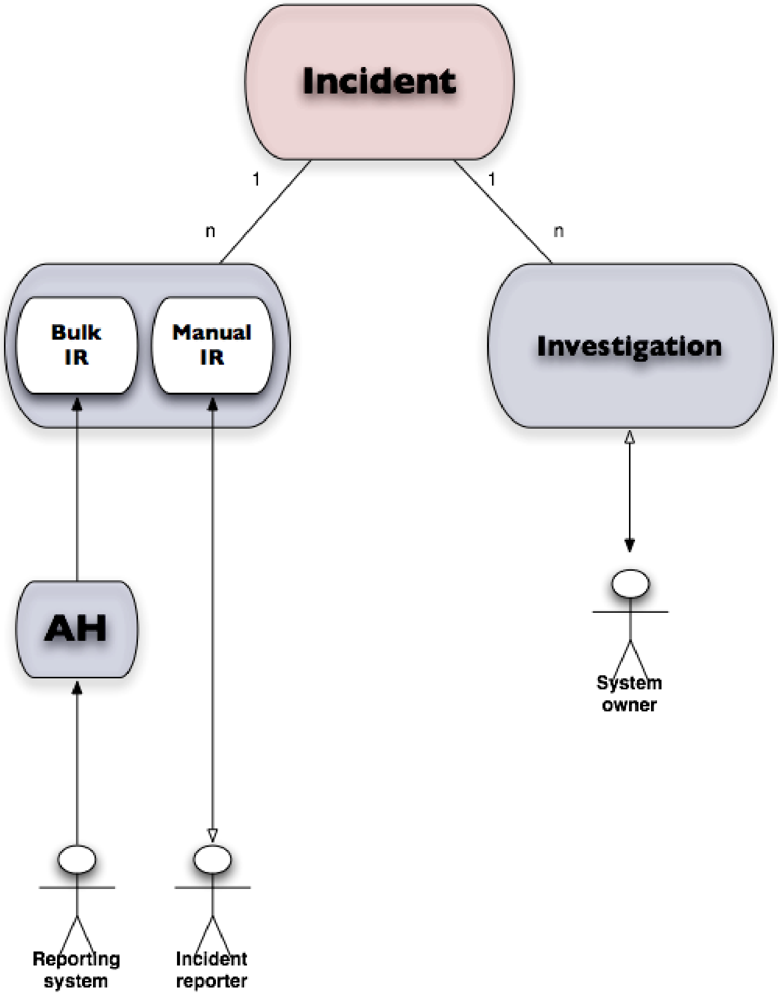
AbuseHelper + RT-IR ⇒ FTW!

- AbuseHelper is great for automated forwarding of "bulk incident" data, but we (Funet CERT) wanted
  - a feedback loop (email)
  - one system for storing historic data and stats
- For us, this meant integrating AH with RT-IR

RT-IR workflow (now)



RT-IR workflow with AbuseHelper



RtirBot

- Uses RT’s REST API
- Creates Incident Reports from AbuseHelper events
- Links IRs to existing Incidents or creates a new Incident
- Will launch investigations for communicating with 3rd parties (not implemented yet)
- Should be in production at Funet CERT in July

Conclusion

- AbuseHelper helps to process large amount of incident notifications

- Integration possible with a long list of other projects to create a complete toolbox
  - BGP ranking (Luxembourg)
  - Passive DNS (Austria / Luxembourg / Estonia)
  - HoneySpider (Netherlands)
  - …

- Possibility to collaborate with CERT community automatically and in real-time…

Questions & Answers

Thanks for your attention.

Feel free to contact us at

cert@cert.be

cert@cert.funet.fi