ABUSE.IO

Open Source abuse management
for network operators

About me

Bart Vrancken

- Engineer with BIT B.V. (NL/AS12859)
- Handling incoming abuse events since 2009
- White hat hacker (WoonVeilig, KPN, Wehkamp, …)
- Volunteer lifeguard / first responder

Talking points

- The history of AbuseIO
- Why AbuseIO
- Current production release
- Features
- Workflow
- Screenshots
- Upcoming release
- Questions

History of AbuseIO

- In-house developed and deployed at BIT.NL
  - Spamcheck (Version 1.0 - 2009 - 2011)
  - AbuseReporter (Version 2.0 - 2011 - 2014)

- Plans to open source AbuseReporter as AbuseIO (December) quickly followed by support from Tilaa and Tele2
- First release of AbuseIO (Version 3.0 - April)
- Started the AbuseIO non-profit foundation (May)
- Development started on the next release (June)
- AbuseIO was granted a fund by SIDN Fonds (August)

Why AbuseIO

- Currently known software that have the same (or less) features is very expensive
- Freely available software is unnecessarily complex, time consuming and mostly used by CERT’s which have an entirely different scope then an ISP would have
- Smaller ISP’s are still manually processing the data feeds which causes unneeded delay until the abuse matter is resolved
- Most hosting companies with a small group of personnel don’t have the time or resources to handle most of their abuse matters
- Most end-users WANT to fix the problem! However they lack the expertize to solve it and the reporting ISP does not have the time to assist every end-user in resolving the matter

Version 3.0 – April 2015

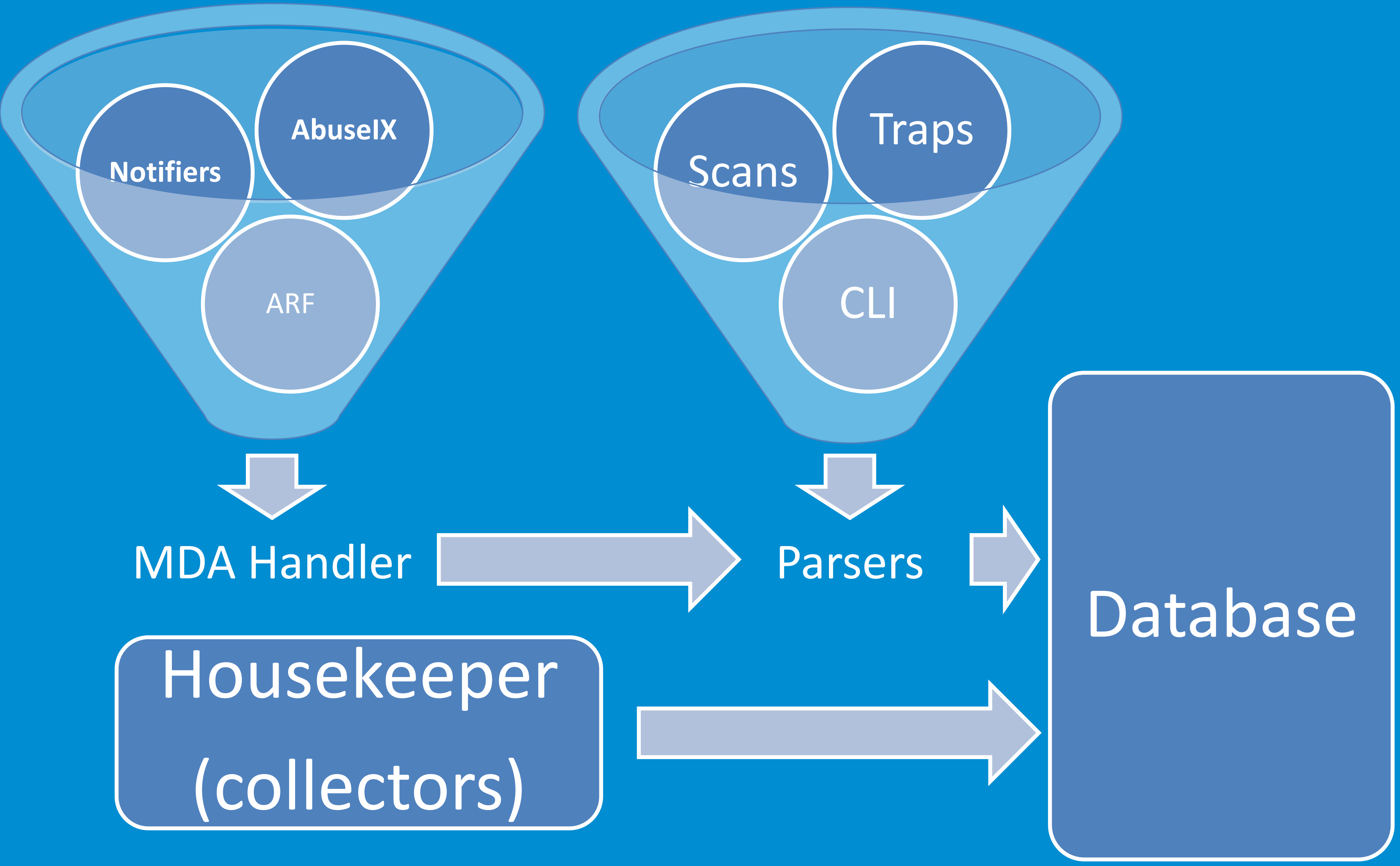
- Converting AbuseReporter which was specifically built for BIT
- Developed in collaboration with Providers and hosting companies based on feeds that are commonly used and freely available
- Fast growing user and development community
- Free to use (GPLv2) open source software with an ‘one size fits all’ solution, but can be modified for any specific use case
- Very low system requirements : a Raspberry PI will suffice to handle 500.000 events a day

With AbuseIO providing the right tooling for free, the Internet providers, hosting companies, network operators and end-users will have no excuse anymore in letting abuse run wild in their networks

Features

- Receive and process incoming abuse events into reports
- Support to process any ARF formatted message
- Support for all the major Feeds like Shadowserver, Google, C-SIRT, SpamCop, AbuseIX, Netcraft, SpamExperts and many more!
- Merge related events into a combined report
- Classify and prioritize each report based on Feed configuration
- Integrate with any IPAM or use a local customer database
- Send out near real-time notifications to end-users and them to a self help portal for more information and troubleshooting of the issue with the ability to reply to the ISP
- Hook to external scripts, e.g. tooling to quarantine a host
- Archive and link to original evidence for future reference
- Works with IPv4 and IPv6 addresses

Workflow – incoming events



AbuseIX

Notifiers

ARF

Traps

Scans

CLI

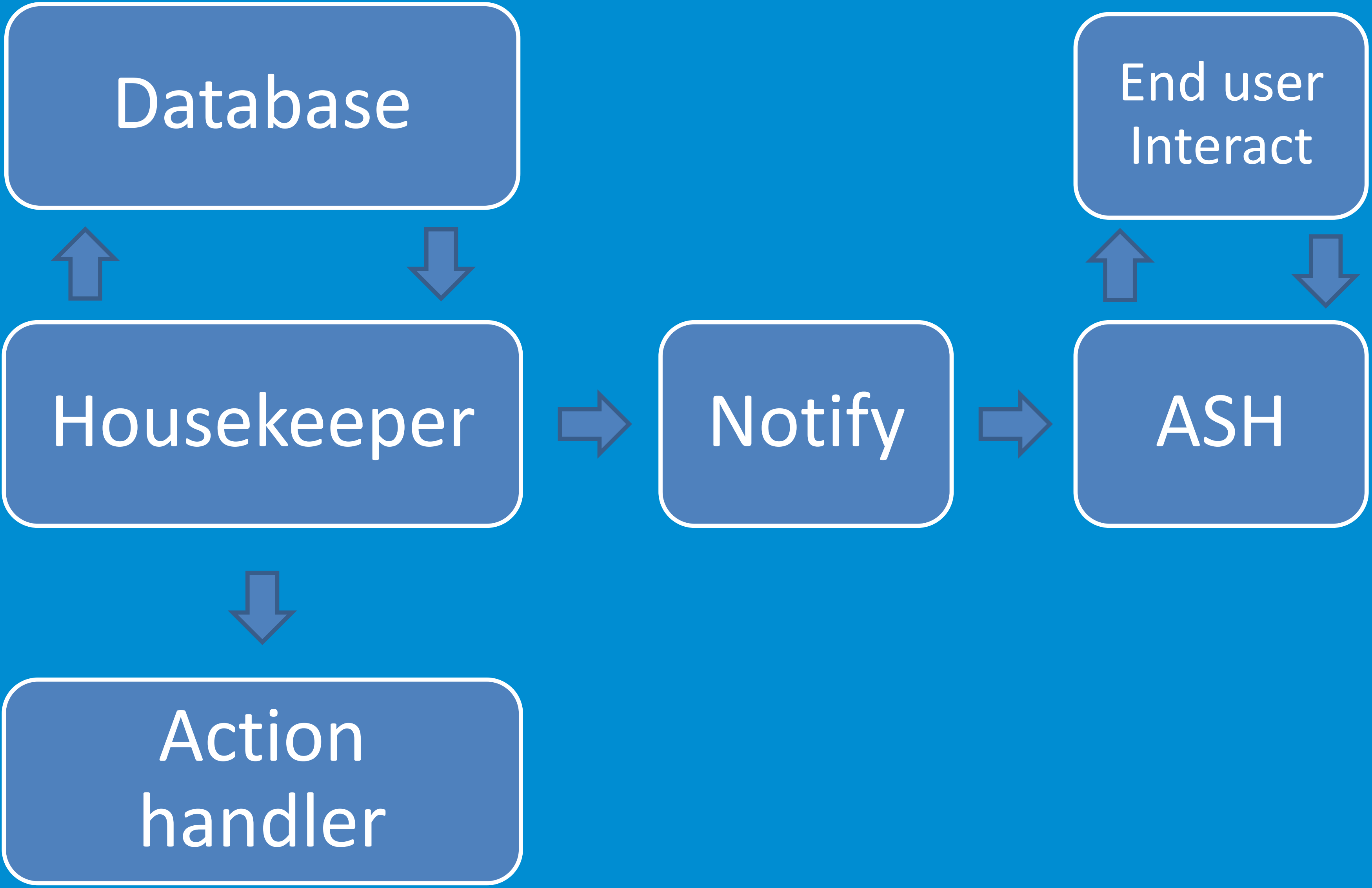
MDA Handler

Parsers

Database

Housekeeper (collectors)

Workflow – outgoing reports



Database

End user Interact

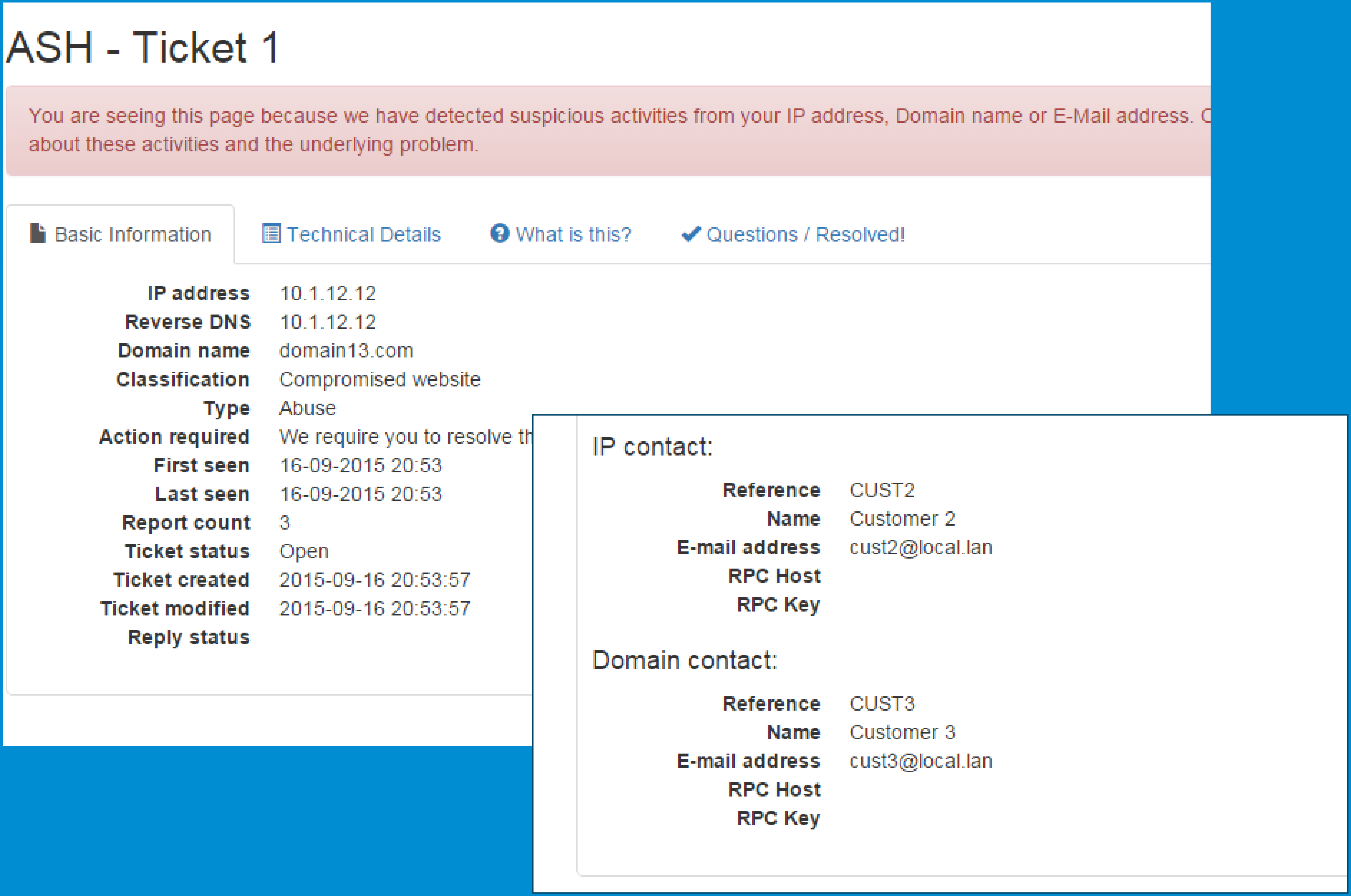
Housekeeper

Notify

ASH

Action handler

Screenshots (4.0)



ASH - Ticket 1

You are seeing this page because we have detected suspicious activities from your IP address, Domain name or E-Mail address. C about these activities and the underlying problem.

IP address	10.1.12.12
Reverse DNS	10.1.12.12
Domain name	domain13.com
Classification	Compromised website
Type	Abuse
Action required	We require you to resolve th
First seen	16-09-2015 20:53
Last seen	16-09-2015 20:53
Report count	3
Ticket status	Open
Ticket created	2015-09-16 20:53:57
Ticket modified	2015-09-16 20:53:57
Reply status	

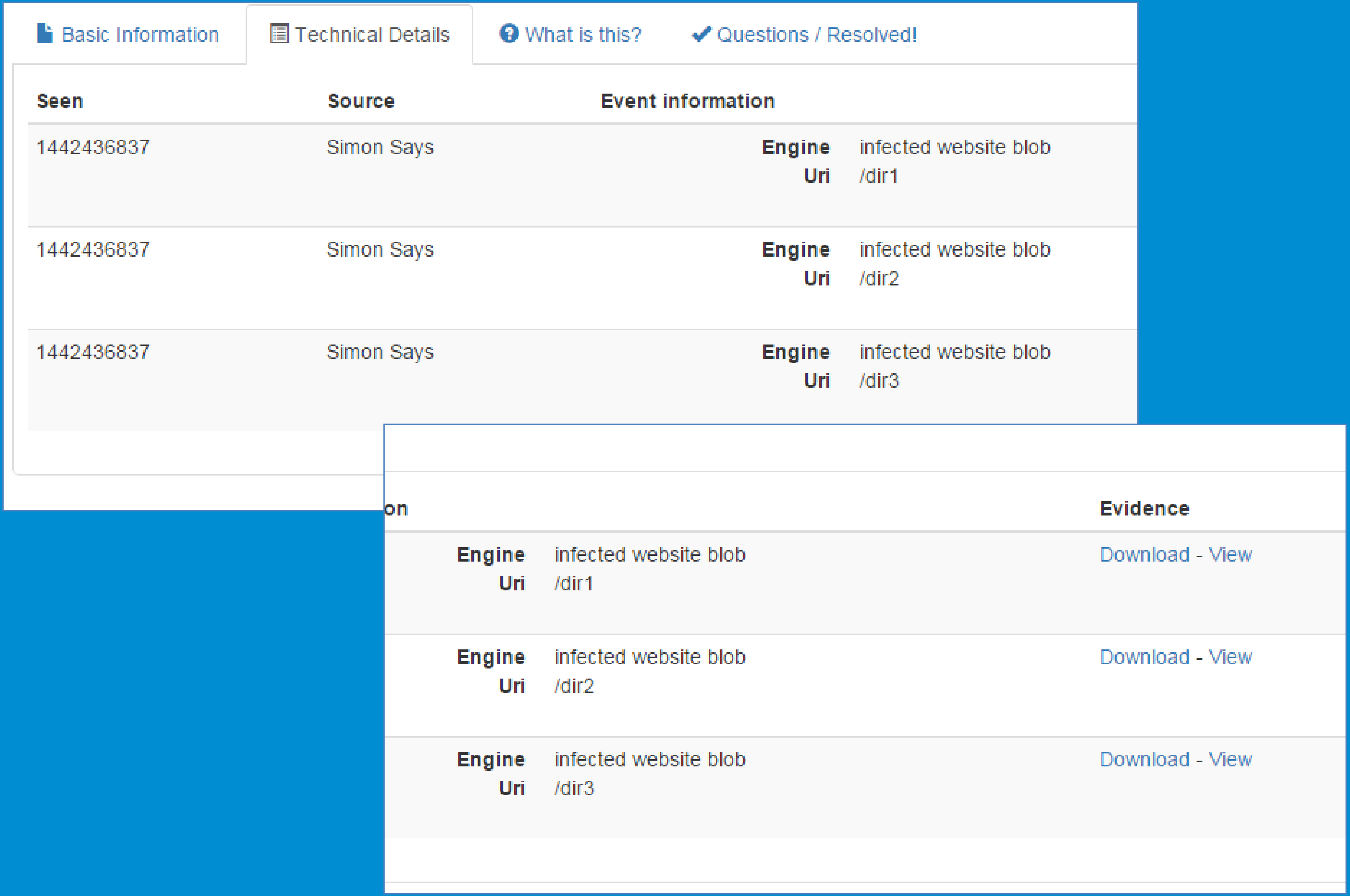
IP contact:

Reference	CUST2
Name	Customer 2
E-mail address	cust2@local.lan
RPC Host	
RPC Key	

Domain contact:

Reference	CUST3
Name	Customer 3
E-mail address	cust3@local.lan
RPC Host	
RPC Key	

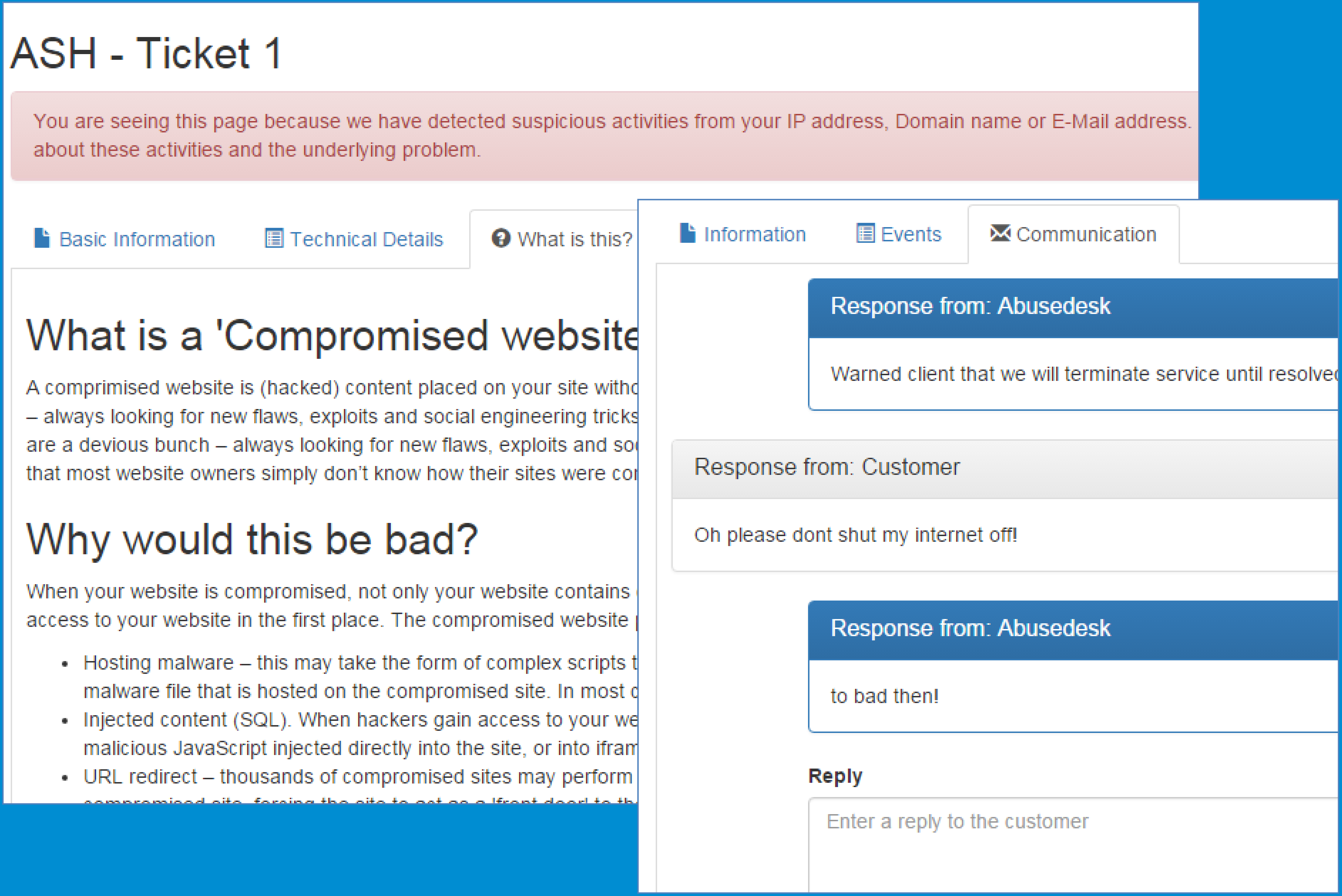
Screenshots (4.0)



Seen	Source	Event information
1442436837	Simon Says	**Engine** infected website blob **Uri** /dir1
1442436837	Simon Says	**Engine** infected website blob **Uri** /dir2
1442436837	Simon Says	**Engine** infected website blob **Uri** /dir3

on	Evidence
Engine infected website blob **Uri** /dir1	Download - View
Engine infected website blob **Uri** /dir2	Download - View
Engine infected website blob **Uri** /dir3	Download - View

Screenshots (4.0)



ASH - Ticket 1

You are seeing this page because we have detected suspicious activities from your IP address, Domain name or E-Mail address. about these activities and the underlying problem.

What is a 'Compromised website

A comprimised website is (hacked) content placed on your site witho – always looking for new flaws, exploits and social engineering tricks are a devious bunch – always looking for new flaws, exploits and so that most website owners simply don't know how their sites were co

Why would this be bad?

When your website is compromised, not only your website contains access to your website in the first place. The compromised website

- Hosting malware – this may take the form of complex scripts t malware file that is hosted on the compromised site. In most c
- Injected content (SQL). When hackers gain access to your we malicious JavaScript injected directly into the site, or into ifram
- URL redirect – thousands of compromised sites may perform compromised site, forcing the site to act as a 'front door' to th

Response from: Abusedesk

Warned client that we will terminate service until resolved

Response from: Customer

Oh please dont shut my internet off!

Response from: Abusedesk

to bad then!

Reply

Enter a reply to the customer

Current plans and development

- The current code works, but it needs the touch of a few skilled developers converting it in a template and MVC styled software
- Adding more parsers with a goal to support all known feeds
- Downstream support for resellers that handle their own Abuse with the ability to provide a ‘result’ upstream to the hosting ISP
- JSON-RPC for external tooling like local honeypots as well as inter-ISP relaying of abuse events using trusted exchange keys
- Ideally defining a exchange format to receive abuse events in such a manner they are complete, but still easily parse-able for the ISP
- Implementing support for domains (shared hosting)
- More extensive analytics and reporting options
- More detailed roadmap on our website and GIT pages
- A Technical committee is being formed to guide and keep up the development to the needs of battling abuse

Questions

?

More information

Website: https://Abuse.IO

IRC: #abuseio on FreeNode

E-Mail: Bart@Abuse.IO

Twitter: @AbuseIO

THANK YOU