Open Source abuse management

by Erik Bais

Talking points

- The history of AbuseIO
- Why AbuseIO
- Features
- Deployment at A2B Internet
- Workflows
- Questions

History of AbuseIO

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

- Plans to open source AbuseReporter as AbuseIO (December 2014) 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)
- Public Benefit Organization for tax deductible donations
- Next release planned for Q1/2016 (January/February)

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
- Complementary to other projects, like the Abuse Information Exchange / AbuseHUB (NL)

Features AbuseIO-4.0

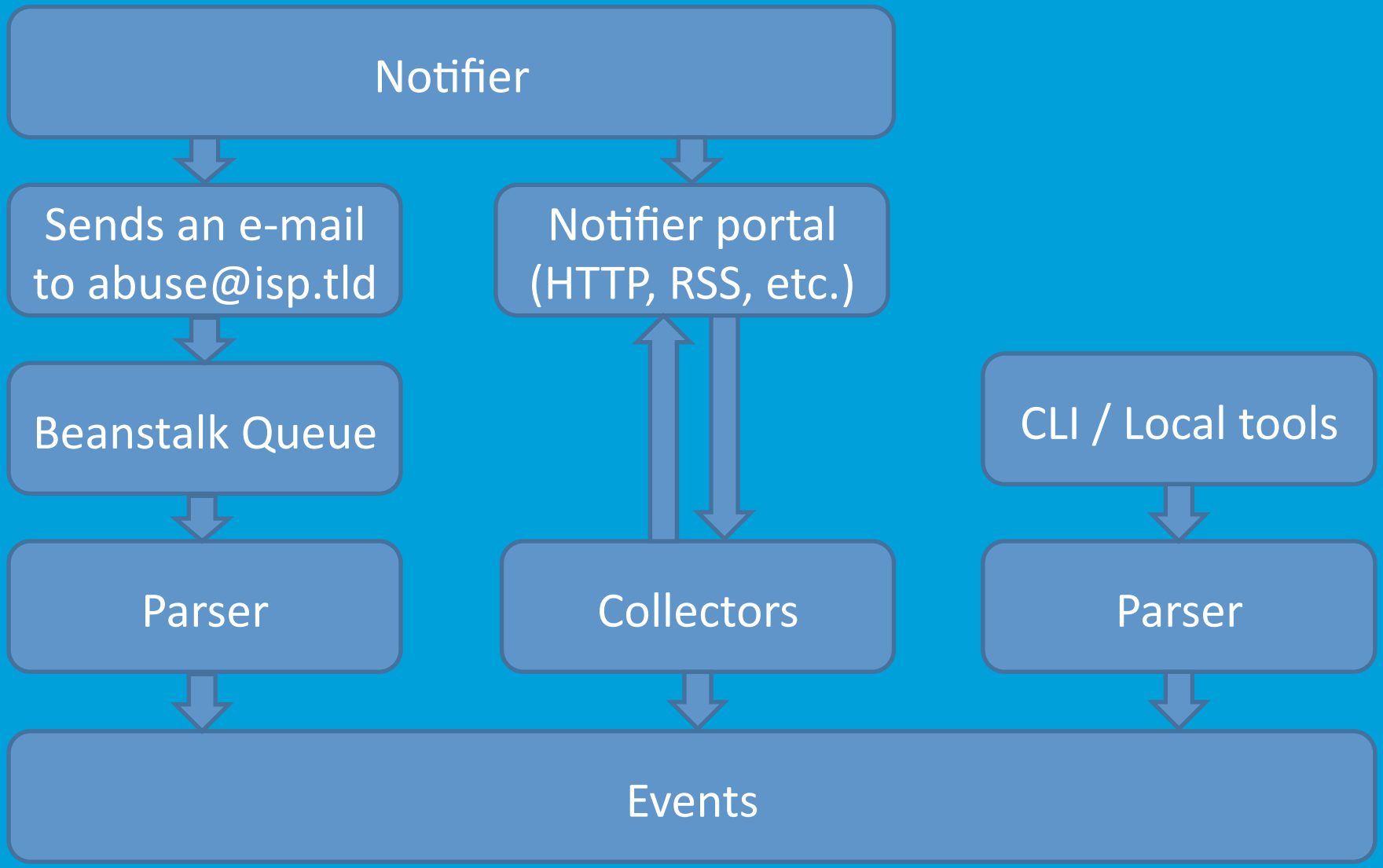
- Just as easy to install as wordpress
- Receive and process incoming abuse events
- Support for nearly all the Notifier feeds available
- Merge related events into a combined report
- Classify and prioritize reports
- Integrate with any IPAM or backend
- Send out near real-time notifications
- Direct IP and Domain owners to a self-help portal
- Hook to external scripts (actions, blackhole, quarantine, etc.)
- Archive and link to original evidence
- Works with IPv4 and IPv6 addresses
- For anyone to use, for FREE!

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

Deployment at A2B Internet

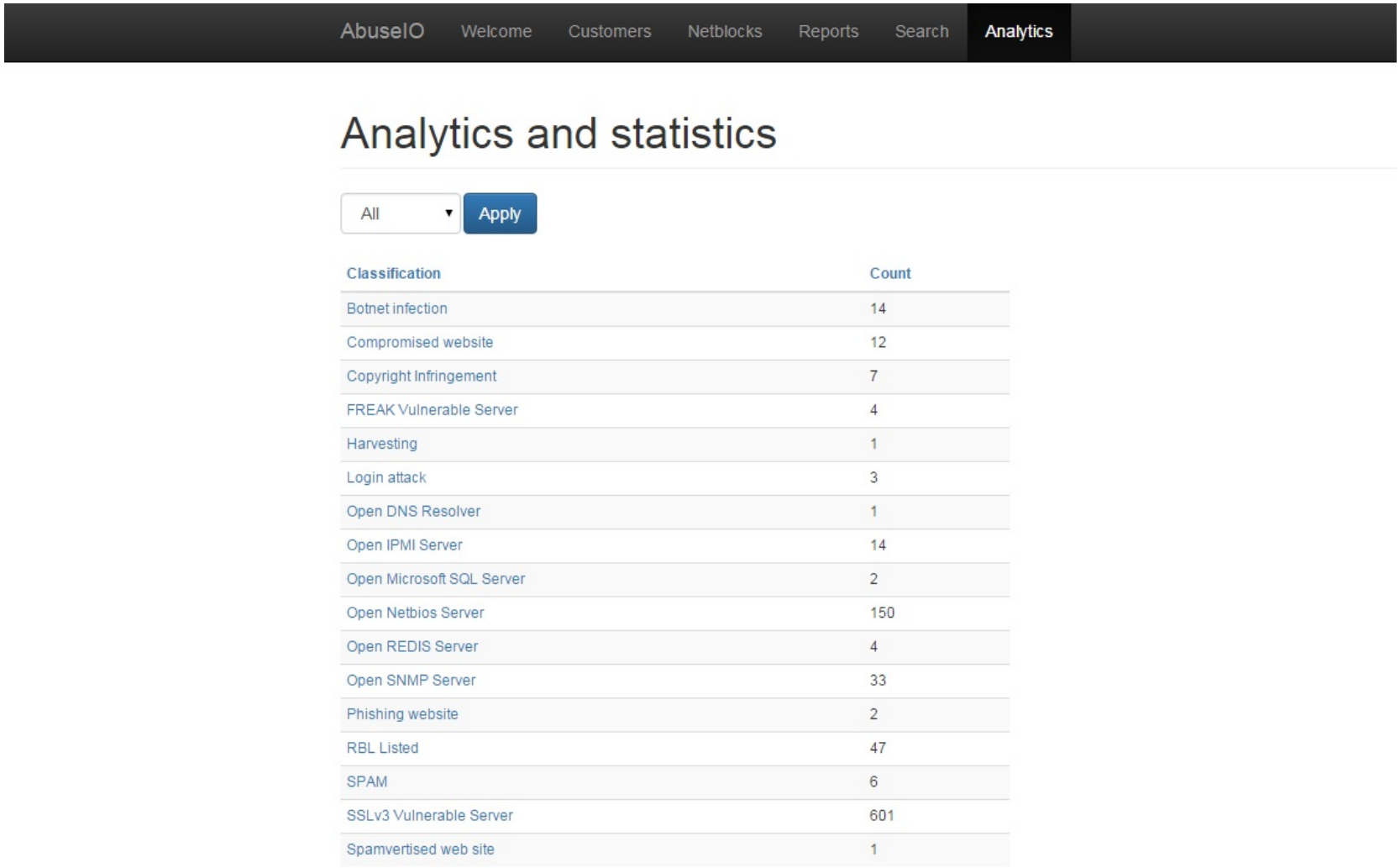
- Saving a LOT of time handling abuse
  - Processing for instance all the Shadowserver reports, all follow-ups by email manually … takes about 2 – 3 hrs if done manually.
- *Uptime of abuse highly reduced*
  - *Quicker insight on the tickets and quicker follow up.*
- *Good overview on abuse matters and the clients are responsible*
  - *All information is in 1 system, including their contact mail address.*
- *We also monitor IP space of LIR customers not in our own network. (Rented IP space and Managed LIR customers)*
- *Very positive response from our customers for the system and the information provided through it.*

Workflow – incoming events

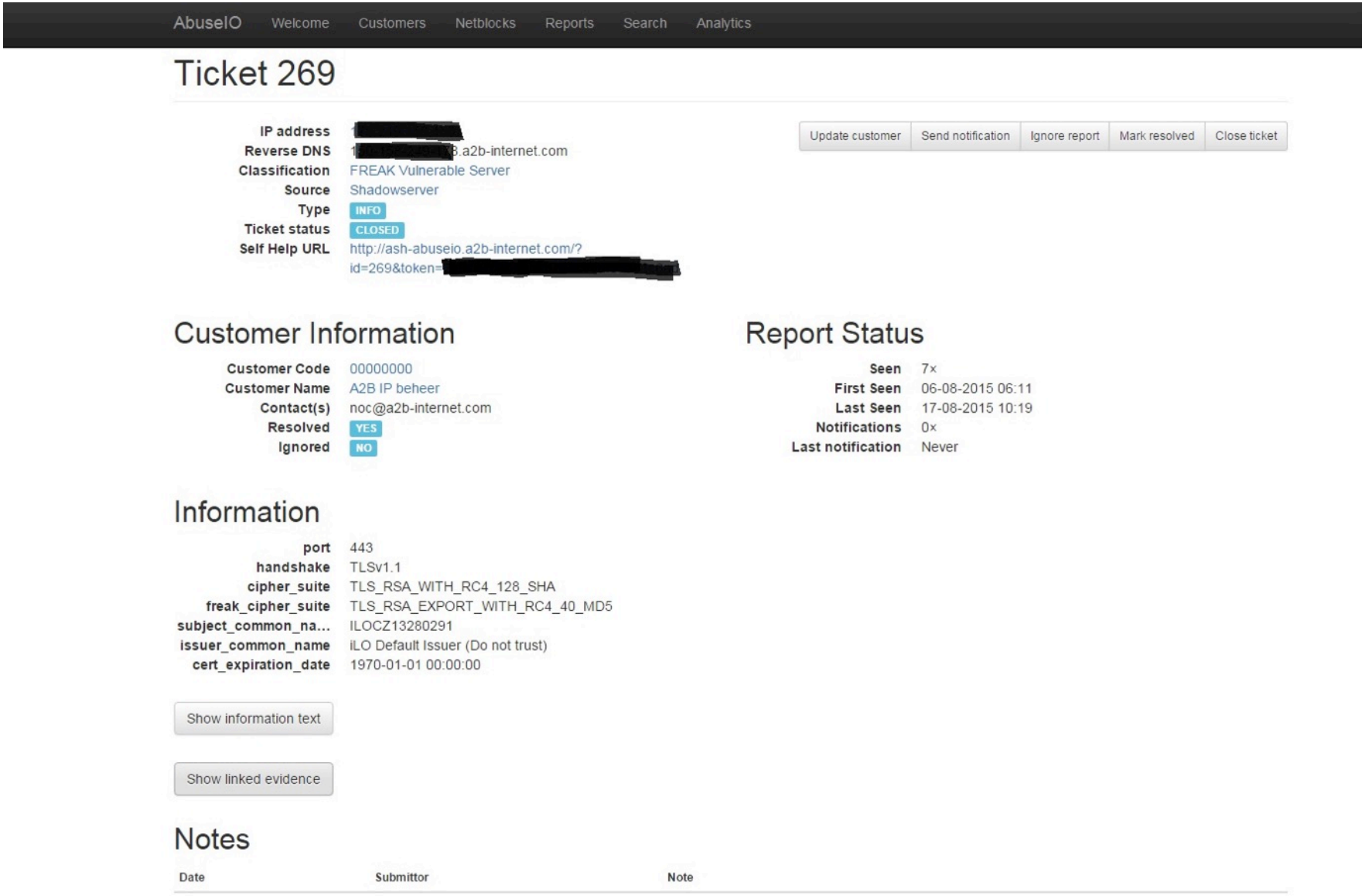


Workflow – handling events

Screenshots



Screenshots



AbuseIO Welcome Customers Netblocks Reports Search Analytics

Ticket 269

Update customer | Send notification | Ignore report | Mark resolved | Close ticket

IP address	[redacted]
Reverse DNS	[redacted].a2b-internet.com
Classification	FREAK Vulnerable Server
Source	Shadowserver
Type	INFO
Ticket status	CLOSED
Self Help URL	http://ash-abuseio.a2b-internet.com/?id=269&token=[redacted]

Customer Information

Customer Code	00000000
Customer Name	A2B IP beheer
Contact(s)	noc@a2b-internet.com
Resolved	YES
Ignored	NO

Report Status

Seen	7×
First Seen	06-08-2015 06:11
Last Seen	17-08-2015 10:19
Notifications	0×
Last notification	Never

Information

port	443
handshake	TLSv1.1
cipher_suite	TLS_RSA_WITH_RC4_128_SHA
freak_cipher_suite	TLS_RSA_EXPORT_WITH_RC4_40_MD5
subject_common_na...	ILOCZ13280291
issuer_common_name	iLO Default Issuer (Do not trust)
cert_expiration_date	1970-01-01 00:00:00

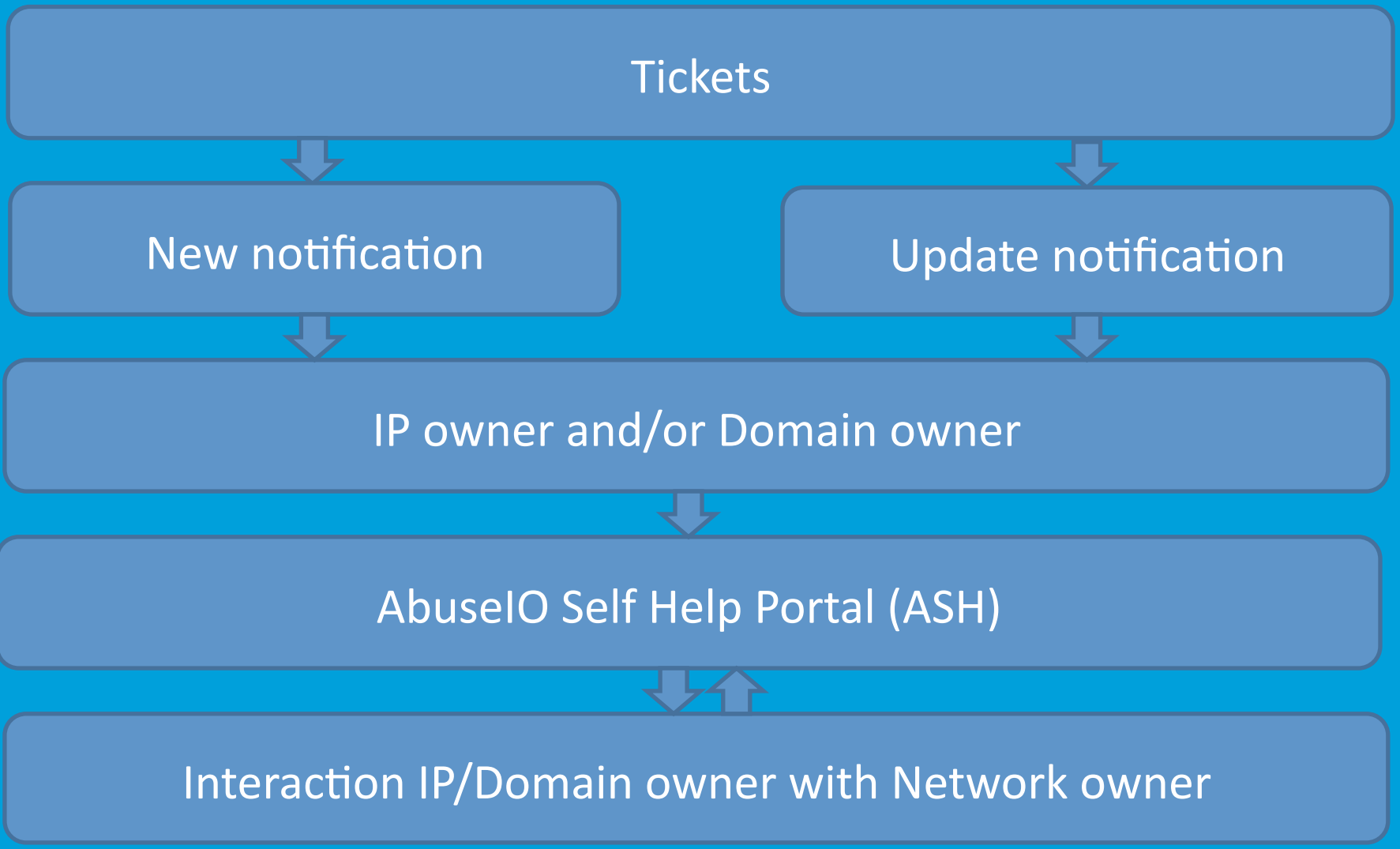
Show information text

Show linked evidence

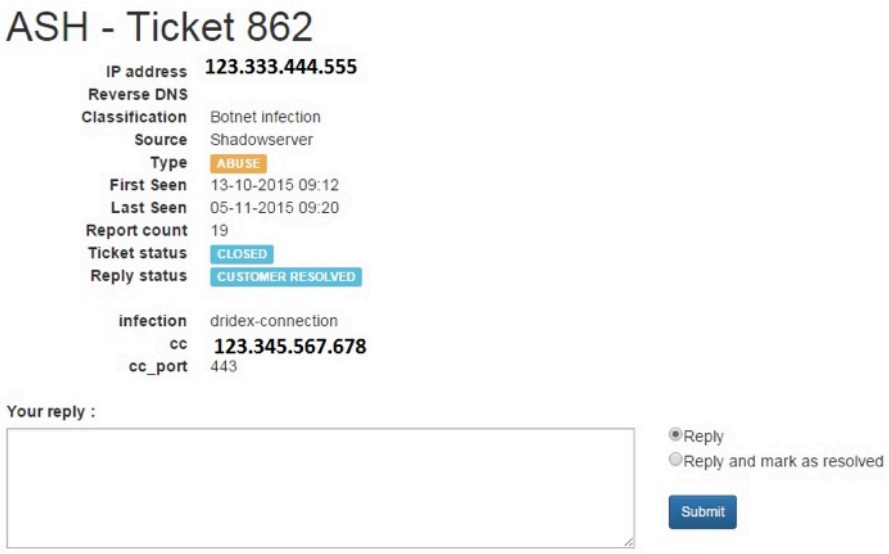
Notes

Date	Submittor	Note

Workflow – outgoing reports



Screenshots



ASH - Ticket 862

IP address	**123.333.444.555**
Reverse DNS	
Classification	Botnet infection
Source	Shadowserver
Type	ABUSE
First Seen	13-10-2015 09:12
Last Seen	05-11-2015 09:20
Report count	19
Ticket status	CLOSED
Reply status	CUSTOMER RESOLVED
infection	dridex-connection
cc	**123.345.567.678**
cc_port	443

Your reply :

Reply
Reply and mark as resolved

Submit

What is a 'Botnet infection'?

Botnet is a portmanteau derived from the words robot and network. Bot refers to a computer program that independently performs automated jobs. Such programs have many legitimate uses; search engines, for example, commonly use bots to catalogue web sites. Unfortunately, bots can also be programmed to perform malicious actions on systems. A botnet is a large group of infected computers connected to each other via the internet. Criminals administering the botnet make sure that the the programs get installed on as many systems as possible. The programs stay under the radar, generally running in the background, and are usually difficult for antivirus software to identify. Once a computer is infected, it can then become part of the botnet through the exploitation of vulnerabilities in software installed on the user's system. There are many avenues for this infection, such as visiting a (generally infected) web site, 'drive-by downloads' (when malware is downloaded and installed on the system without the user's knowledge), and even by simply clicking attachments or links in an e-mail or merely connecting peripherals such as USB sticks or external hard drives to the system.

Why would this be bad?

The IP listed in the report (the system behind it using NAT), has seen participating inside the botnet. With your system in communication with the botnet you can be 99,9% sure it has been compromised. It's hosting malware and is participating in a botnet.

A botnet can be used to steal your personal data, send spam, hack into other computers and launch network attacks. In these examples you are the actual source of these attacks!

Recommended action

This issue needs to be resolved by removing the malicious software. In very persistant infections you will need to reinstall the system to get rid of the infection

Questions

?

More information

Website: https://Abuse.IO
IRC: #abuseio on FreeNode
E-Mail: Info@Abuse.IO
Twitter: @AbuseIO

THANK YOU