AbuseHUB: Ramping Up the Fight against Botnets in the Netherlands

Nov 20, 2013

ccNSO meeting @ ICANN48

Cristian Hesselman

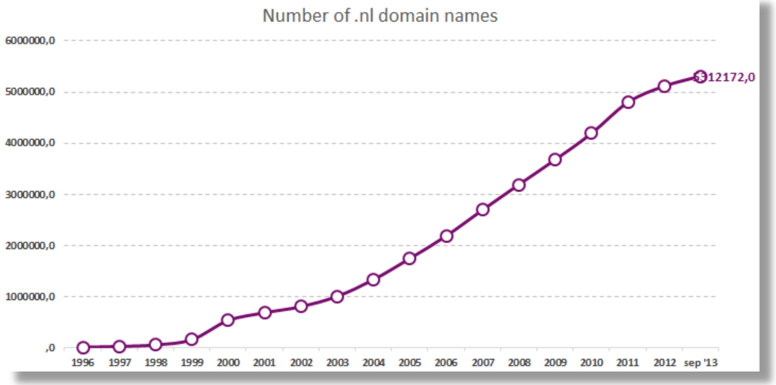
SIDN labs

Internet Research & Innovation

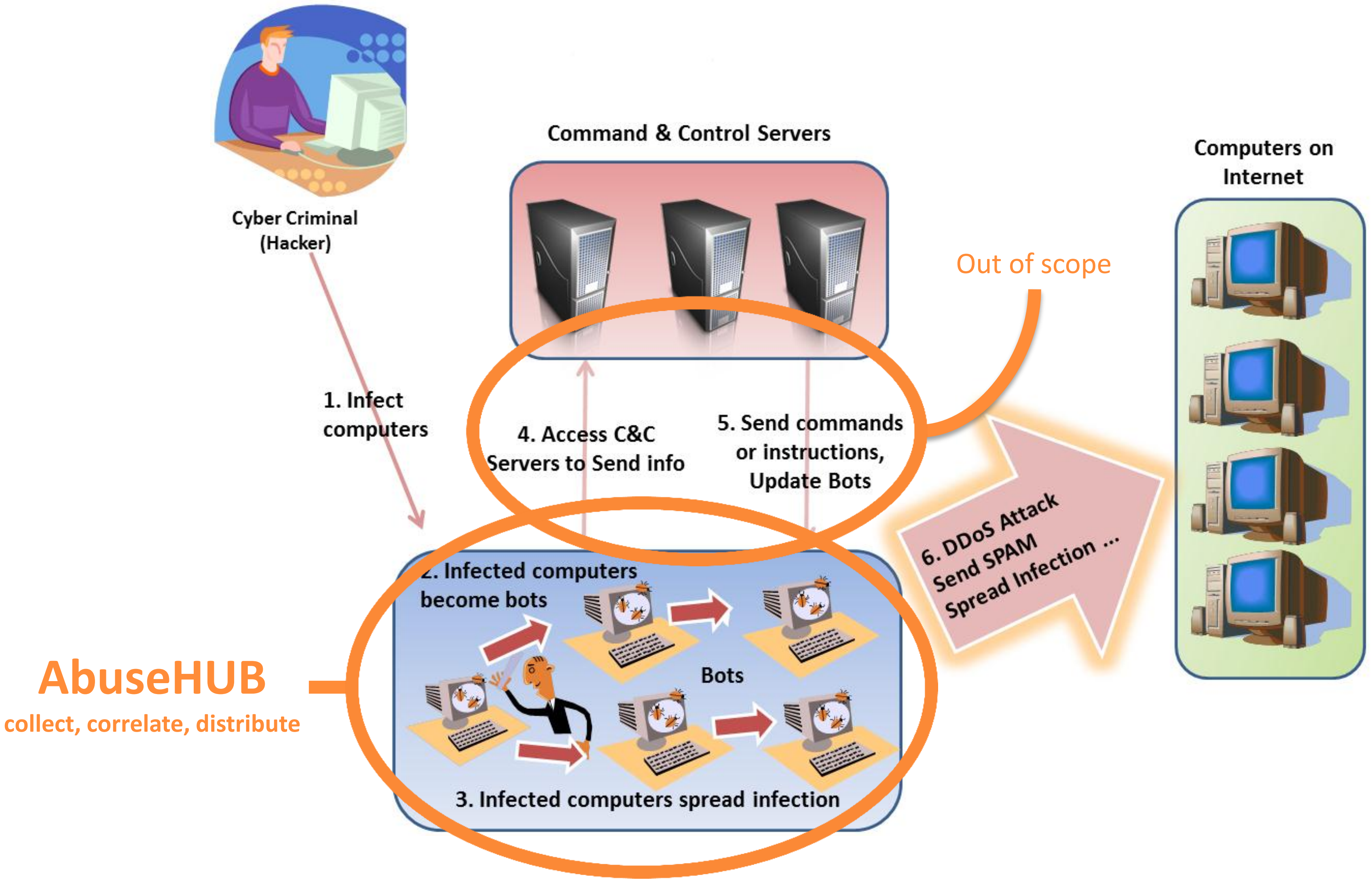
SIDN

SIDN

- Registry for the Netherlands (.nl)
- 5.2M domain names, 1.600 registrars
- Largest DNSSEC zone in the world (1.5M signed)
- RSP for .amsterdam (capital)



Botnet Infections


Cyber Criminal (Hacker)
1. Infect computers
Command & Control Servers
4. Access C&C Servers to Send info
5. Send commands or instructions, Update Bots
Out of scope
Computers on Internet
6. DDoS Attack Send SPAM Spread Infection ...
2. Infected computers become bots
Bots
3. Infected computers spread infection
AbuseHUB
collect, correlate, distribute

Source: http://pineut.wordpress.com/2013/04/13/botnet-aanval-op-wordpress-com/

Abuse Information Exchange

- Legal entity (association) that manages AbuseHUB

- Open cross-industry collaboration for ISPs, ccTLDs, hosting providers, and other infrastructure providers

- Goal: improve fight against botnets in the Netherlands through a national information hub

- Targeted impact: further increased internet security and internet usage

Members

90% of fixed access market | 70% of domain name market

upc ZeelandNet SIDN

solcon SURF NET TELE2

XS4ALL kpn Ziggo

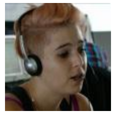
With financial support from:

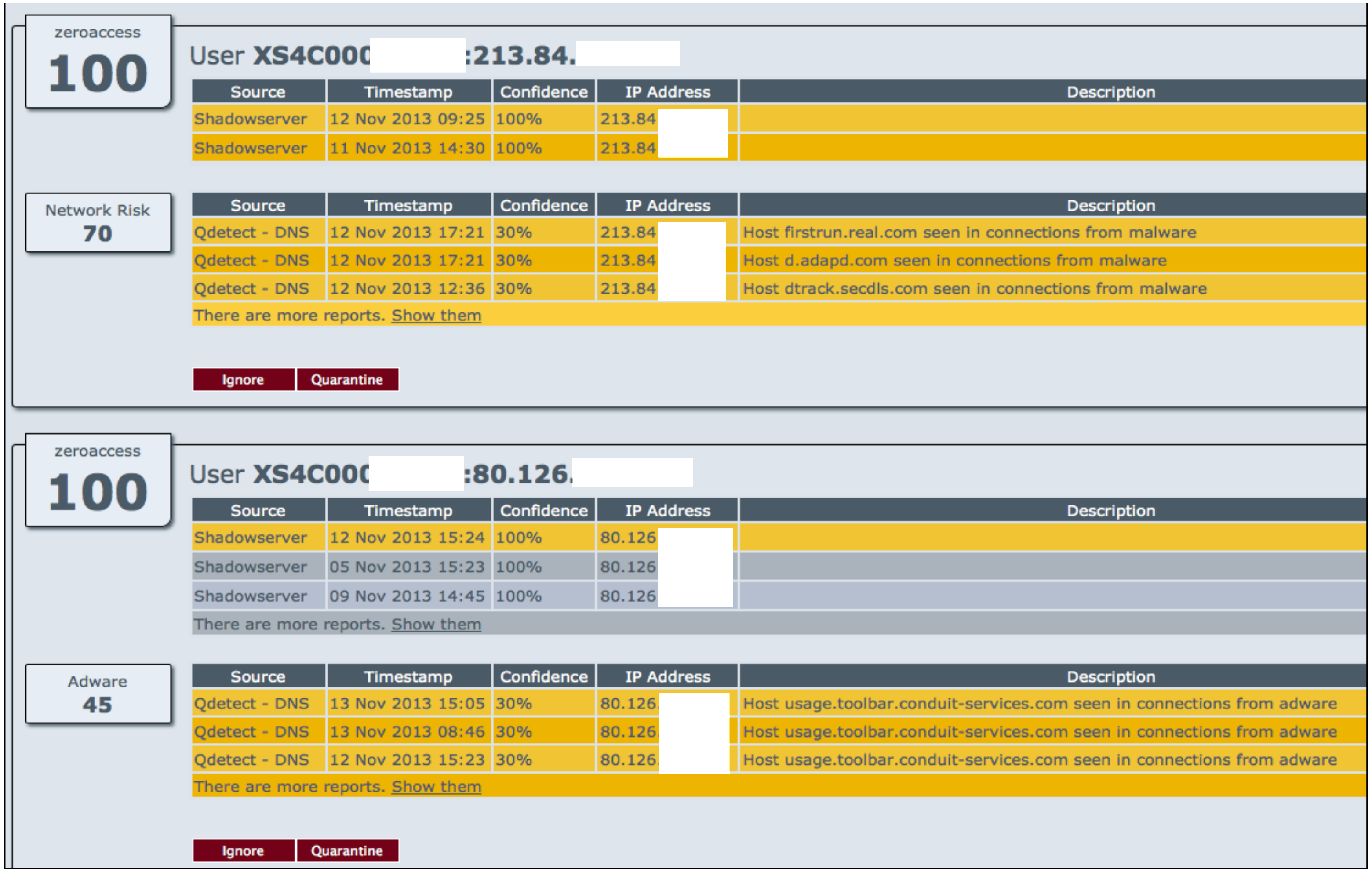
Ministerie van Economische Zaken SIDN

Botnets from a Users' Perspective

RTL News (Netherlands)
Sep 11, 2013
XS4ALL = ISP

Abuse Desk (XS4ALL)





zeroaccess
100

User **XS4C000[redacted]:213.84.[redacted]**

Source	Timestamp	Confidence	IP Address	Description
Shadowserver	12 Nov 2013 09:25	100%	213.84[redacted]	
Shadowserver	11 Nov 2013 14:30	100%	213.84[redacted]	

Network Risk
70

Source	Timestamp	Confidence	IP Address	Description
Qdetect - DNS	12 Nov 2013 17:21	30%	213.84[redacted]	Host firstrun.real.com seen in connections from malware
Qdetect - DNS	12 Nov 2013 17:21	30%	213.84[redacted]	Host d.adapd.com seen in connections from malware
Qdetect - DNS	12 Nov 2013 12:36	30%	213.84[redacted]	Host dtrack.secdls.com seen in connections from malware

There are more reports. Show them

zeroaccess
100

User **XS4C000[redacted]:80.126.[redacted]**

Source	Timestamp	Confidence	IP Address	Description
Shadowserver	12 Nov 2013 15:24	100%	80.126[redacted]	
Shadowserver	05 Nov 2013 15:23	100%	80.126[redacted]	
Shadowserver	09 Nov 2013 14:45	100%	80.126[redacted]	

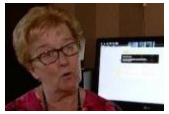
There are more reports. Show them

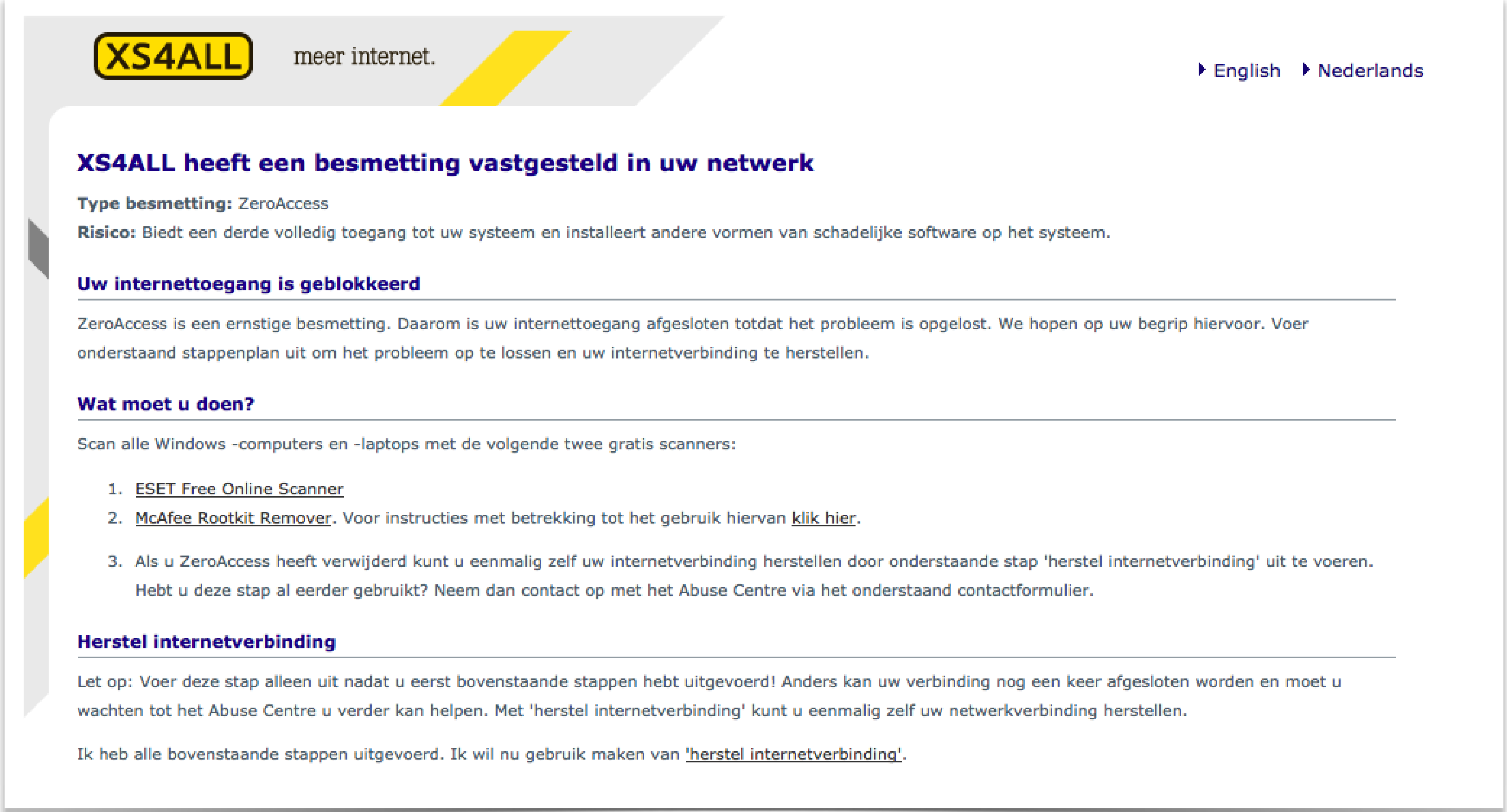
Adware
45

Source	Timestamp	Confidence	IP Address	Description
Qdetect - DNS	13 Nov 2013 15:05	30%	80.126.[redacted]	Host usage.toolbar.conduit-services.com seen in connections from adware
Qdetect - DNS	13 Nov 2013 08:46	30%	80.126.[redacted]	Host usage.toolbar.conduit-services.com seen in connections from adware
Qdetect - DNS	12 Nov 2013 15:23	30%	80.126.[redacted]	Host usage.toolbar.conduit-services.com seen in connections from adware

There are more reports. Show them

Warning Page





XS4ALL heeft een besmetting vastgesteld in uw netwerk

Type besmetting: ZeroAccess

Risico: Biedt een derde volledig toegang tot uw systeem en installeert andere vormen van schadelijke software op het systeem.

Uw internettoegang is geblokkeerd

ZeroAccess is een ernstige besmetting. Daarom is uw internettoegang afgesloten totdat het probleem is opgelost. We hopen op uw begrip hiervoor. Voer onderstaand stappenplan uit om het probleem op te lossen en uw internetverbinding te herstellen.

Wat moet u doen?

Scan alle Windows -computers en -laptops met de volgende twee gratis scanners:

1. ESET Free Online Scanner
2. McAfee Rootkit Remover. Voor instructies met betrekking tot het gebruik hiervan klik hier.
3. Als u ZeroAccess heeft verwijderd kunt u eenmalig zelf uw internetverbinding herstellen door onderstaande stap 'herstel internetverbinding' uit te voeren. Hebt u deze stap al eerder gebruikt? Neem dan contact op met het Abuse Centre via het onderstaand contactformulier.

Herstel internetverbinding

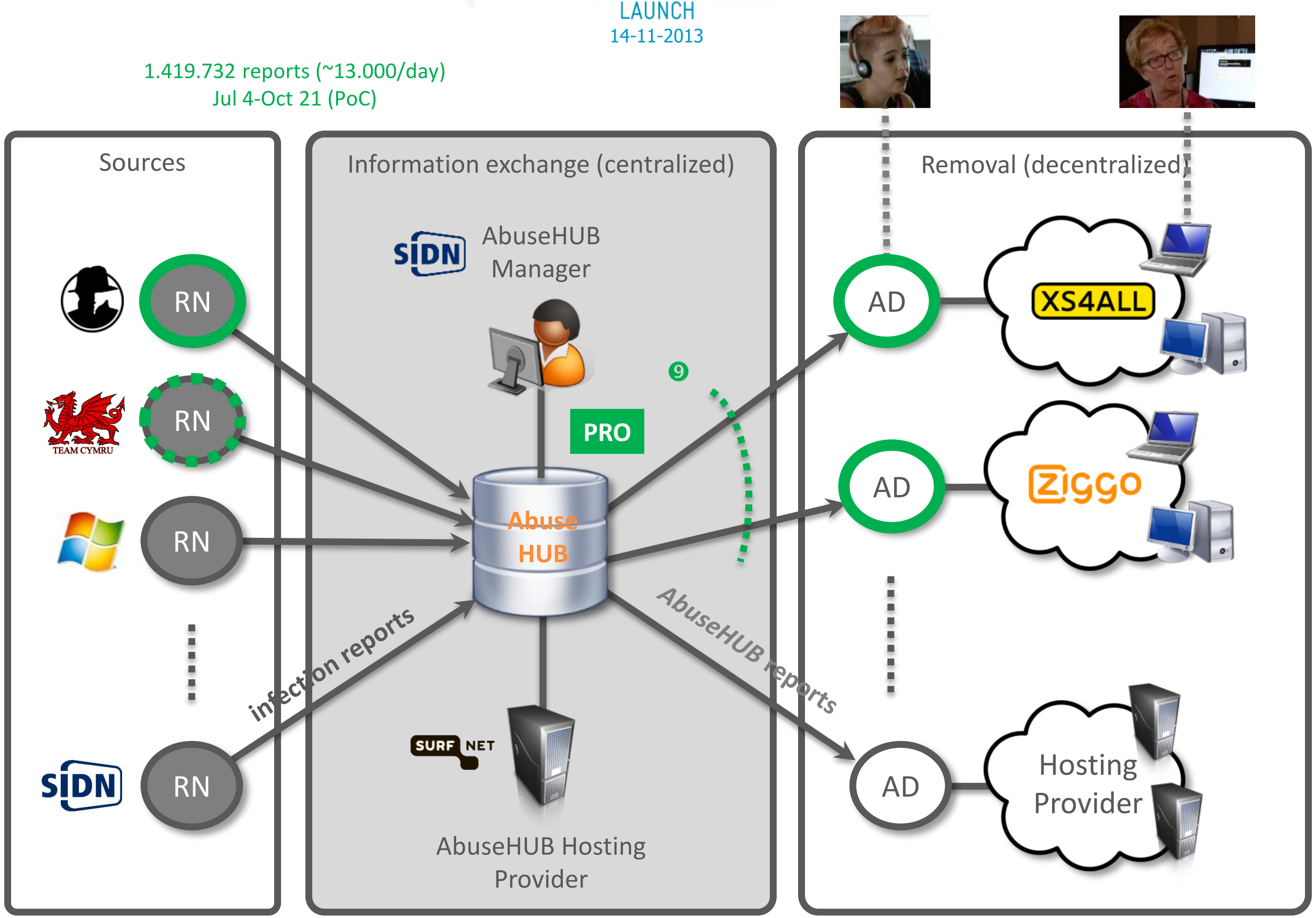
Let op: Voer deze stap alleen uit nadat u eerst bovenstaande stappen hebt uitgevoerd! Anders kan uw verbinding nog een keer afgesloten worden en moet u wachten tot het Abuse Centre u verder kan helpen. Met 'herstel internetverbinding' kunt u eenmalig zelf uw netwerkverbinding herstellen.

Ik heb alle bovenstaande stappen uitgevoerd. Ik wil nu gebruik maken van 'herstel internetverbinding'.

AbuseHUB: Under the Hood

LAUNCH
14-11-2013

1.419.732 reports (~13.000/day)
Jul 4-Oct 21 (PoC)



Added Value

Stakeholder	Expected Impact
Internet users	• Safer and more stable internet experience • Shorter quarantine periods
Members (ISPs and hosting providers)	• Reduced costs (fewer notifiers to manage) • Increased effectiveness through correlation • Increased scale and level of automation • Competitive advantage
Reliable notifiers	• Increased efficiency through one-stop-shop • SIDN: new tool to fight DNS botnets
Ministry of Economic Affairs	• New tool against cybercrime • Contributes to economic growth in the Netherlands • Self-regulating initiative • Sets an example within the EU and elsewhere
Research institutes	• Improved botnet research based on anonymous data

Why Does SIDN Participate?

- Increased value of local internet through increased security
- Strengthens self-regulation of the Dutch internet industry
- New collaborative tool to fight DNS botnets in a collaborative way (as reliable notifier)
- Further improve relations with other industries such as ISPs
- Extends our expertise on abuse handling

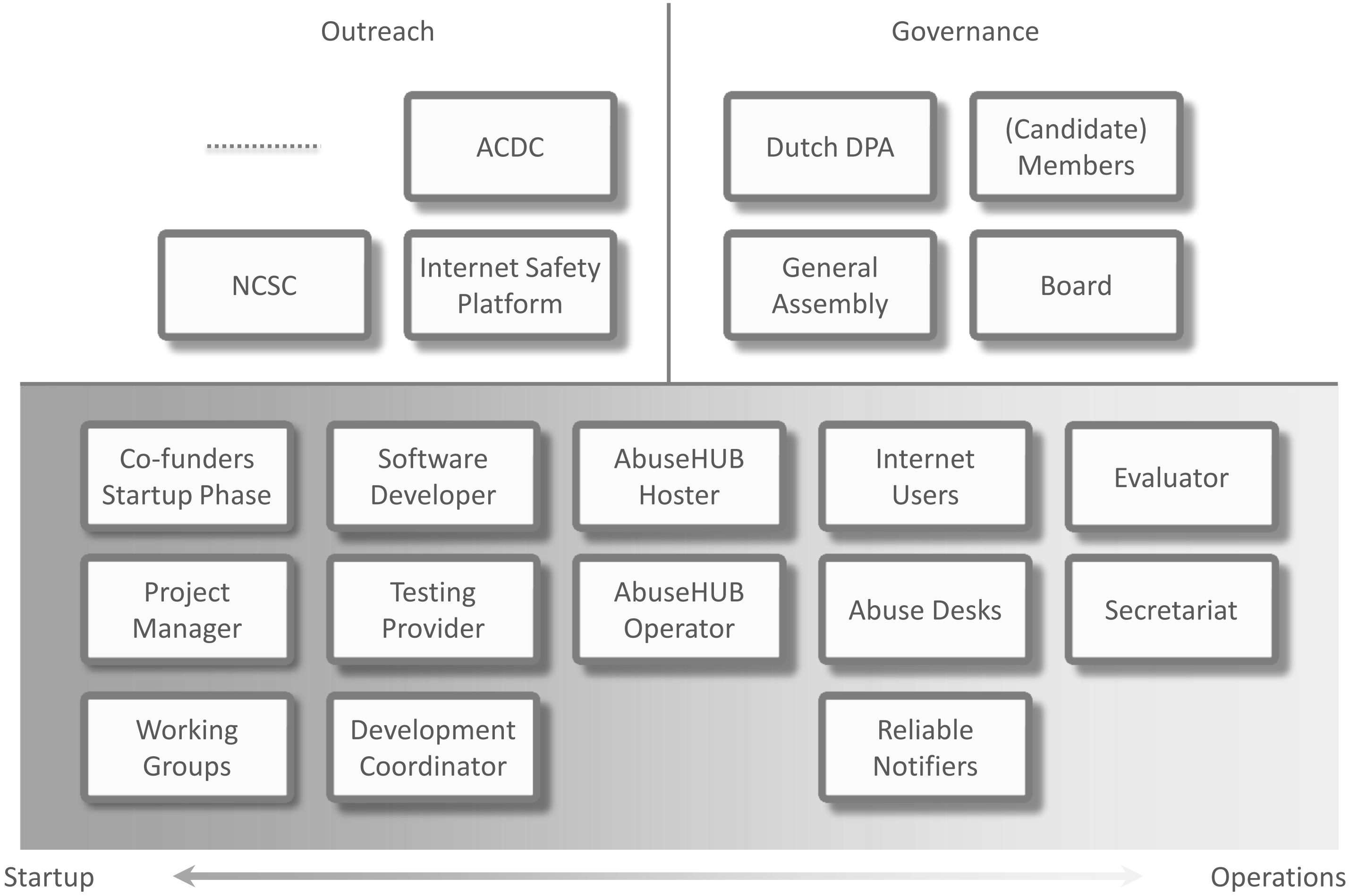
SIDN’s Contribution

- ccTLD that enables a safer internet for the local internet community

- Co-funder of development phase
  - Together with the Dutch Ministry of Economic Affairs
  - Emphasizing an open and cross-industry approach with ISPs, hosting providers, and others

- Active participation in operational phase
  - Roles: notifier of DNS abuse, AbuseHUB operator, and receiver of AbuseHUB reports (member)
  - Board seat (treasurer)

Ecosystem


Outreach
Governance
ACDC
Dutch DPA
(Candidate) Members
NCSC
Internet Safety Platform
General Assembly
Board
Co-funders Startup Phase
Software Developer
AbuseHUB Hoster
Internet Users
Evaluator
Project Manager
Testing Provider
AbuseHUB Operator
Abuse Desks
Secretariat
Working Groups
Development Coordinator
Reliable Notifiers
Startup
Operations

Past, Present, Future

Month	Milestone	
Apr 2012	SIDN decides to cofund the initiative	Preparation
Jul 2012	Business plan approved by founding members	
Jul 2012	Established: the Association Abuse Information Exchange	
Aug 2012	Ministry of Economic Affairs decides to cofund	
Jul 2013	Proof-of-concept live (using “AIRT”)	Development
Jul 2013	Contracted software development company (iBuildings)	
Jul 2013	Kick-off software development phase	
Oct 2013	Production-like testing	
Nov 2013	AbuseHUB version 1 in production (Nov 14)	
Dec 2013	Addition of second reliable notifier	Growth
Dec 2013	Addition of two new members	
Mar 2014	AbuseHUB version 2 in production (correlation)	
Q2 2014	Support for users to de-infect themselves, in collaboration	

Questions?

Cristian Hesselman

Manager SIDN Labs

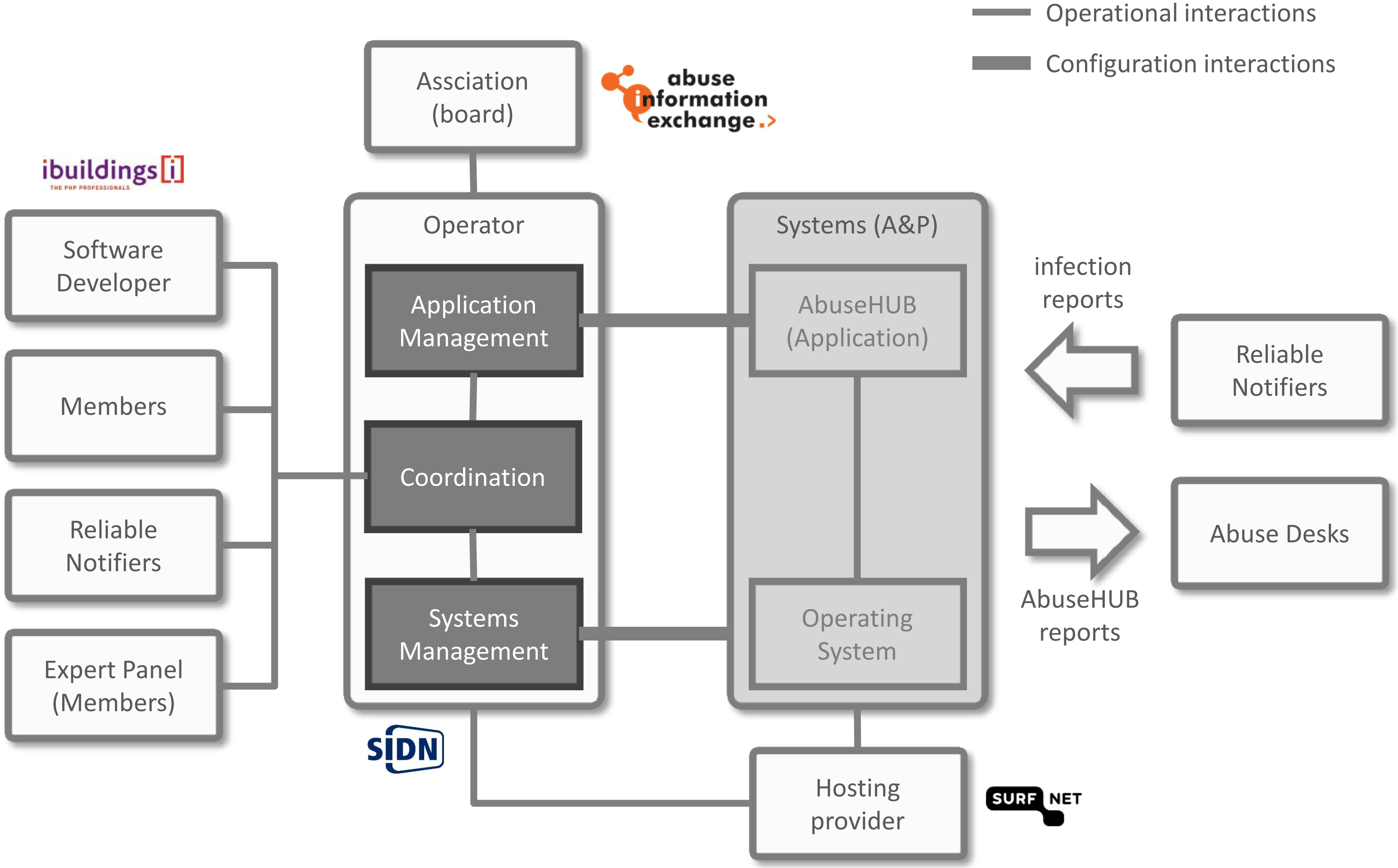
cristian.hesselman@sidn.nl

@hesselma

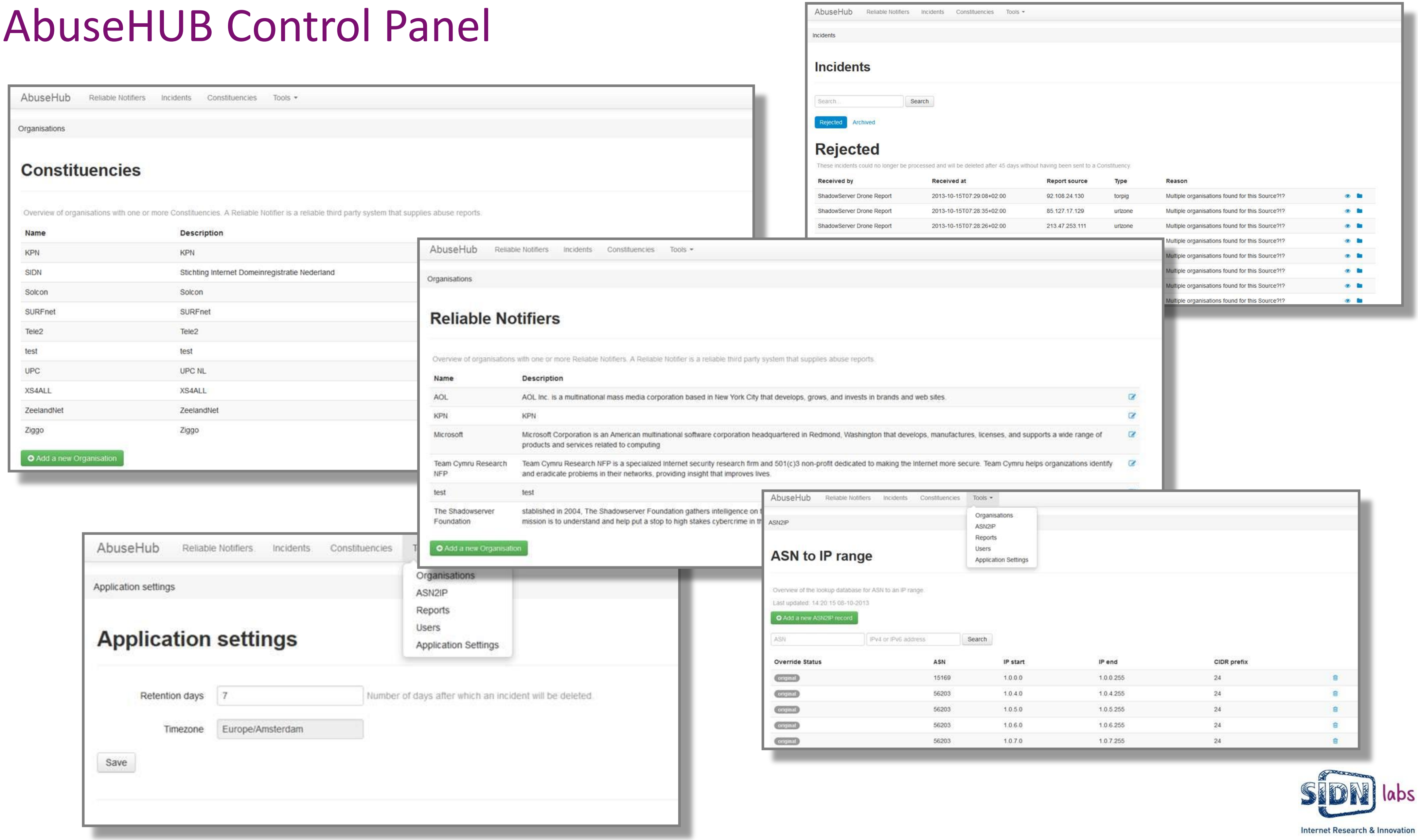
www.sidnlabs.nl

www.abuseinformationexchange.nl

AbuseHUB Operator



AbuseHUB Control Panel



Incidents

Incidents

Rejected

These incidents could no longer be processed and will be deleted after 45 days without having been sent to a Constituency.

Received by	Received at	Report source	Type	Reason
ShadowServer Drone Report	2013-10-15T07:29:08+02:00	92.108.24.130	torpig	Multiple organisations found for this Source?!?
ShadowServer Drone Report	2013-10-15T07:28:35+02:00	85.127.17.129	urlzone	Multiple organisations found for this Source?!?
ShadowServer Drone Report	2013-10-15T07:28:26+02:00	213.47.253.111	urlzone	Multiple organisations found for this Source?!?
				Multiple organisations found for this Source?!?
				Multiple organisations found for this Source?!?
				Multiple organisations found for this Source?!?
				Multiple organisations found for this Source?!?
				Multiple organisations found for this Source?!?

Organisations

Constituencies

Overview of organisations with one or more Constituencies. A Reliable Notifier is a reliable third party system that supplies abuse reports.

Name	Description
KPN	KPN
SIDN	Stichting Internet Domeinregistratie Nederland
Solcon	Solcon
SURFnet	SURFnet
Tele2	Tele2
test	test
UPC	UPC NL
XS4ALL	XS4ALL
ZeelandNet	ZeelandNet
Ziggo	Ziggo

Organisations

Reliable Notifiers

Overview of organisations with one or more Reliable Notifiers. A Reliable Notifier is a reliable third party system that supplies abuse reports.

Name	Description
AOL	AOL Inc. is a multinational mass media corporation based in New York City that develops, grows, and invests in brands and web sites.
KPN	KPN
Microsoft	Microsoft Corporation is an American multinational software corporation headquartered in Redmond, Washington that develops, manufactures, licenses, and supports a wide range of products and services related to computing
Team Cymru Research NFP	Team Cymru Research NFP is a specialized Internet security research firm and 501(c)3 non-profit dedicated to making the Internet more secure. Team Cymru helps organizations identify and eradicate problems in their networks, providing insight that improves lives.
test	test
The Shadowserver Foundation	stablished in 2004, The Shadowserver Foundation gathers intelligence on t mission is to understand and help put a stop to high stakes cybercrime in th

Application settings

Application settings

Retention days: 7 — Number of days after which an incident will be deleted

Timezone: Europe/Amsterdam

ASN2IP

ASN to IP range

Overview of the lookup database for ASN to an IP range.

Last updated: 14:20:15 08-10-2013

Override Status	ASN	IP start	IP end	CIDR prefix
original	15169	1.0.0.0	1.0.0.255	24
original	56203	1.0.4.0	1.0.4.255	24
original	56203	1.0.5.0	1.0.5.255	24
original	56203	1.0.6.0	1.0.6.255	24
original	56203	1.0.7.0	1.0.7.255	24