The Spamhaus story

November 2012

DENOG4

Prepared by:
Erik Bais
ebais@a2b-internet.com

What do we provide ?

- Registration of IP addresses and AS numbers

- System integration for required infrastructure setup.
  - A2B Internet is a Extreme Networks Gold partner.
  - Consultancy, sales, implementation & management
  - and support

- Provide bandwidth between regional datacenters
  - Both Internet access as vlan's, VMAN's or wavelengths.
  - Also international capacity

- 24 * 7 Monitoring and management of infrastructure.

Ports and services

- A2B Internet provides customers access to the netwerk through netwerk ports.

- Customer can use our IP addresses or request their own registered addresses or move their already obtained own addresses to us.
  - A2B Internet also registrers IP addresses for none-netwerk customers.

- Added service – Provide Extreme Networks equipment and optics.

Currently 14 POP's online in NL & BE

interxion™
Carrier-Neutral Data Centres

NIKHEF

the DATACENTERGROUP

TelecityGroup

DATAONE
RELIABLE DATACENTER FACILITIES

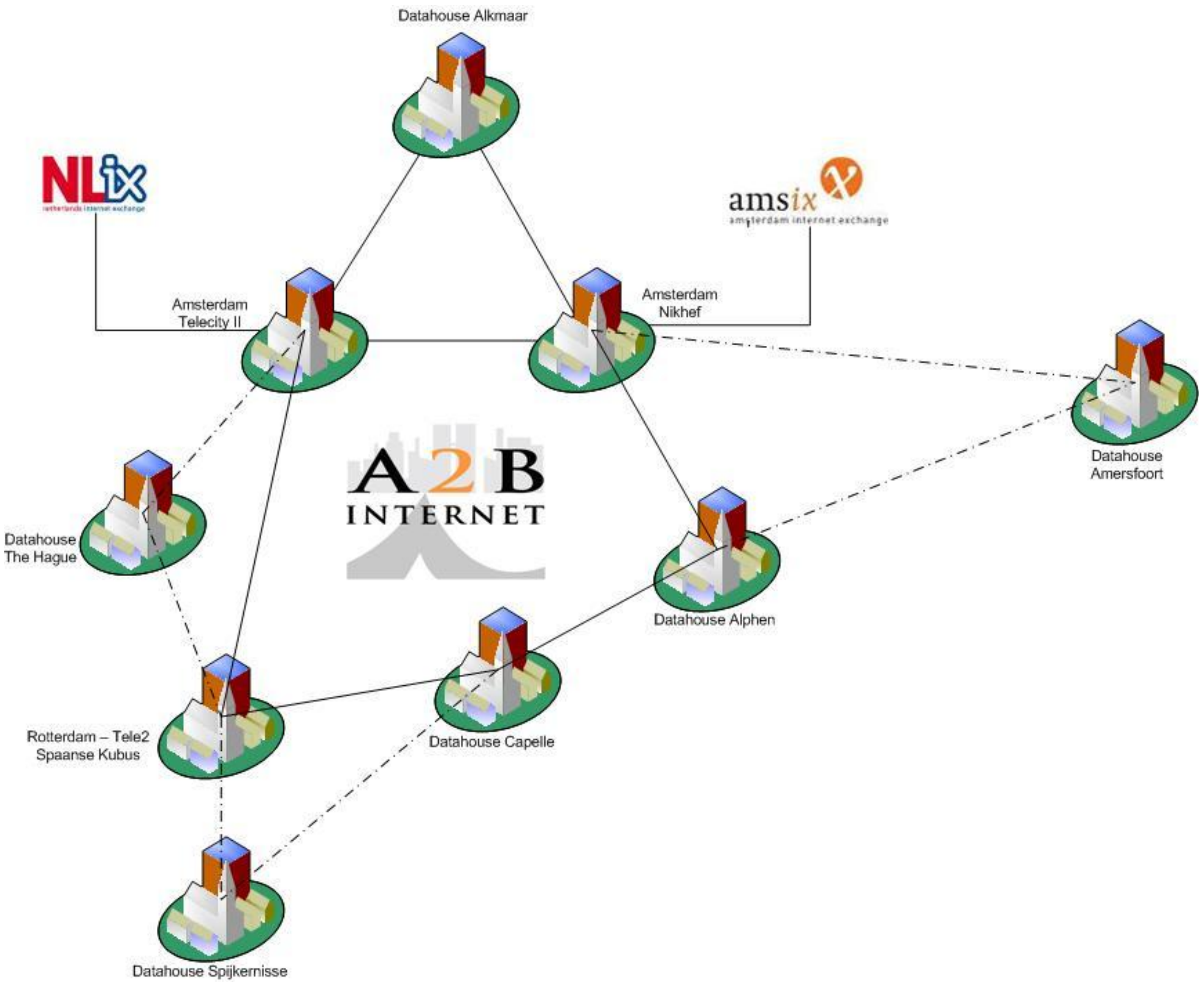
DATA HOUSE
DATACENTER FACILITIES

A2B
INTERNET

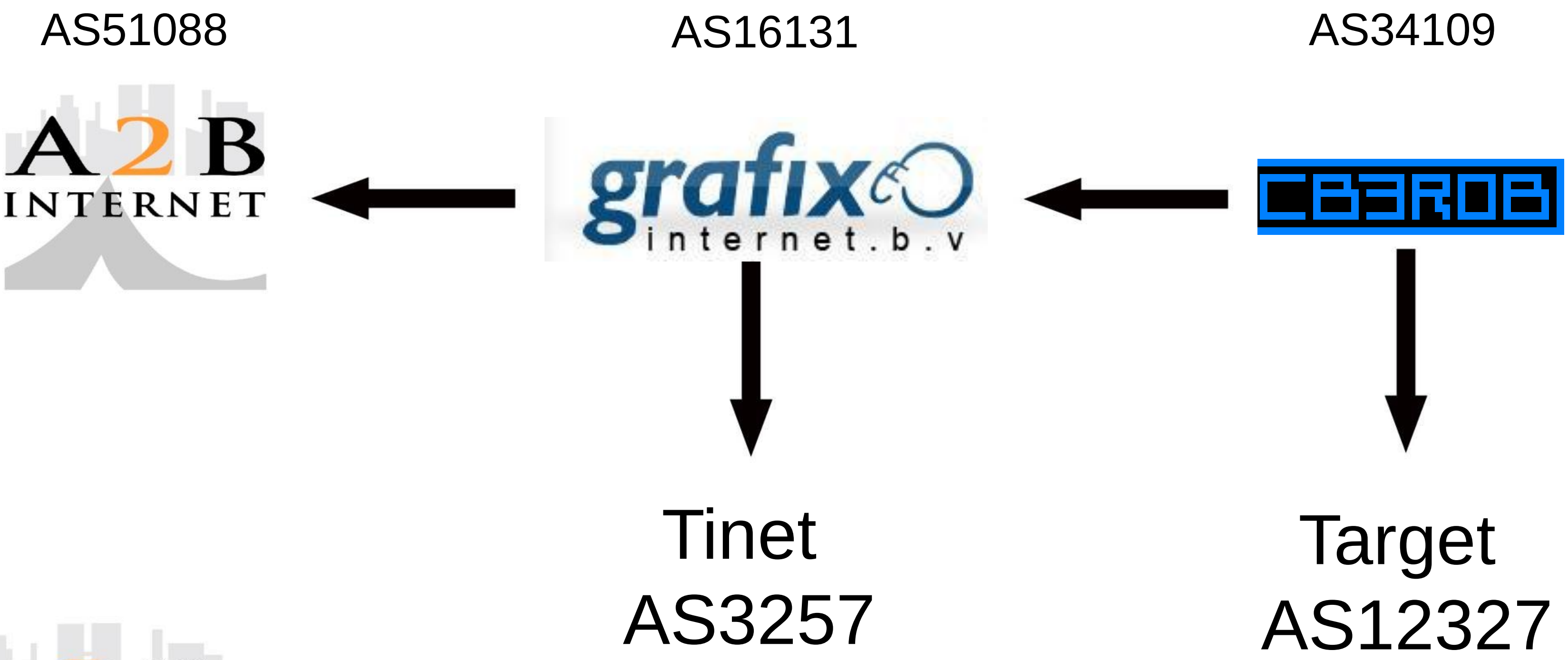
Once upon a time ...

- A2B Internet provided transit to Grafix Internet (AS16131)
- Grafix provided colo services in 2 regional datacenters. (Alphen a/d Rijn & Capelle a/d Ijssel in The Netherlands)
- CB3ROB was a customer of Grafix and used AS16131 as one of their transit providers.
- One of the CB3ROB (transit) customers was the actual target of Spamhaus.

Network map at the time



Transit connections



AS51088

AS16131

AS34109

Tinet
AS3257

Target
AS12327

Impact of the Spamhaus listing

- One of the A2B Internet prefixes (a /21) was completly listed on SBL
- The only IP address in the traceroute from A2B Internet involved was a /30 towards the AS16131 for a BGP session.
- All customers using IP Addresses in the specific prefix were located in the datacenter in Alkmaar. (Not Alphen or Capelle)
- None of the customers listed had anything to do with spam, malware or abuse but could not send any emails.
- The actual target customer didn’t even send emails or hosted any mailservers.

A bit of background.

- CB3ROB is a network provider with some unusual customers ... Like Cyberbunker.
- Typically where most networks focus on local customers, most of CB3ROB their customers are international ‘in-famous’ customers... That require something special...
- Think about reconnecting The Pirate Bay when they were booted offline in Sweden ...
- Or providing (anonymous) VPN services to end-customers or transit to certain goverments ...
- Most of CB3ROB customers are not very liked, and have had experience with peer pressure or RBL’s, DMCA notifications etc. But not spammers ...

Not the usual hoster ...

The story ...

- June 21st 2011 – router interface listed at A2B Internet for routing IDEAR4Business
  - 178.249.152.238/32
  - Problem: routing AS12327 IDEAR4BUSINESS & CB3ROB
- 2 emails send within 24 hrs (first one after 4 hrs) asking for more info.
  - 1 reply received stating:
    - SBL lists spam sources AND SPAM SUPPORT SERVICES. Listing stands.
- October 6th 2011 - Prefix 178.249.152.0/21 listed on SBL.
  - Reason given: No response. Problems continue. Listing adjusted to 178.249.152.0/21
  - Traceroute to http://www.1000cashvip.com

The ‘SBL Removals’ dance ...

- All emails are posted online for review ...
  - http://www.a2b-internet.com/Spamhaus_emails.zip

- A short summary:
  - The sarcastic and un-informative replies show a complete dis-respect for the people that try to resolve the issue.
    - Average mail response was about 12 hrs not including the uninformative replies and semi smart-ass remarks.

- The actual reason for the escallation was :
  - SMS text send from an USA based SMS gateway to US cell numbers to do a credit check at http://www.1000cashvip.com (with an opt-out)

The actual issue for A2B Internet

- The messages were not send to the actual abuser or it's upstream (CB3ROB)
- The upstream of CB3ROB wasn't informed. (Grafix)

- A random prefix was put on SBL to enforce presure to stop routing CB3ROB.

- No usable information was provided about the actual abuse.

- The listing provided details of a traceroute, but nothing usefull like the source of abuse or how the abuse was send.

- Offer to the SBL team to null-route the IP address for the website **wasn't enough ...**

- SH didn't seem to follow any normal procedure for listing spam sources ...

A2B INTERNET

Actions taken ...

- Directly after the SBL dance, a complaint was filed at the Dutch police.

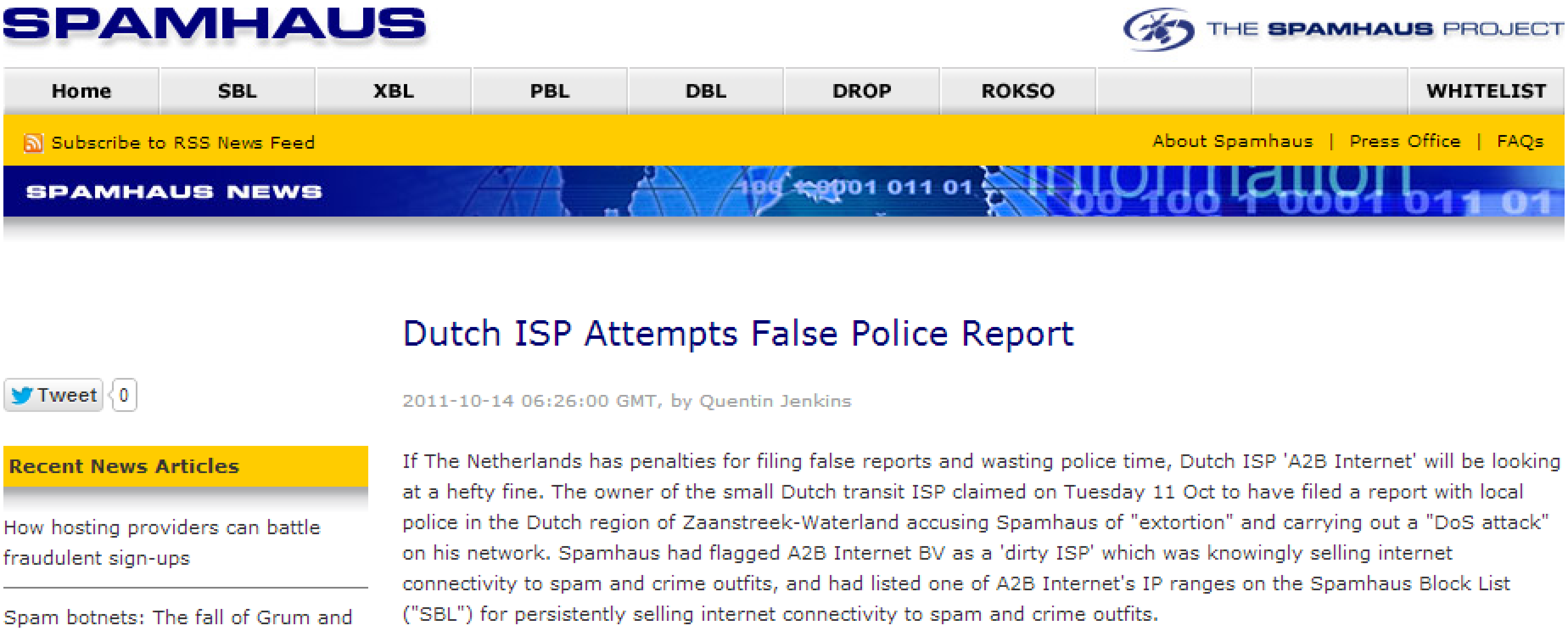
- Prefixes from CB3ROB were dropped by A2B Internet to get the listing removed.
  - As AS16131 (Grafix) also had other transit providers and CB3ROB was connected to the NL-iX, this didn't change the reachability for CB3ROB.

- A reported for a large IT website was picked up the story from Twitter about the police filing and wrote about it on http://www.webwereld.nl

- International websites followed soon on the story after WebWereld.
  - Like The Register Co.UK, TechWeek Europe, SpamReSource, SlashDot.

The media fight starts ...

- Spamhaus noticed the media interest of their action on social media and international IT websites ... And starts to spin their side of the story...



Dutch ISP Attempts False Police Report

2011-10-14 06:26:00 GMT, by Quentin Jenkins

If The Netherlands has penalties for filing false reports and wasting police time, Dutch ISP 'A2B Internet' will be looking at a hefty fine. The owner of the small Dutch transit ISP claimed on Tuesday 11 Oct to have filed a report with local police in the Dutch region of Zaanstreek-Waterland accusing Spamhaus of "extortion" and carrying out a "DoS attack" on his network. Spamhaus had flagged A2B Internet BV as a 'dirty ISP' which was knowingly selling internet connectivity to spam and crime outfits, and had listed one of A2B Internet's IP ranges on the Spamhaus Block List ("SBL") for persistently selling internet connectivity to spam and crime outfits.

Recent News Articles

How hosting providers can battle fraudulent sign-ups

Spam botnets: The fall of Grum and

In the background ...

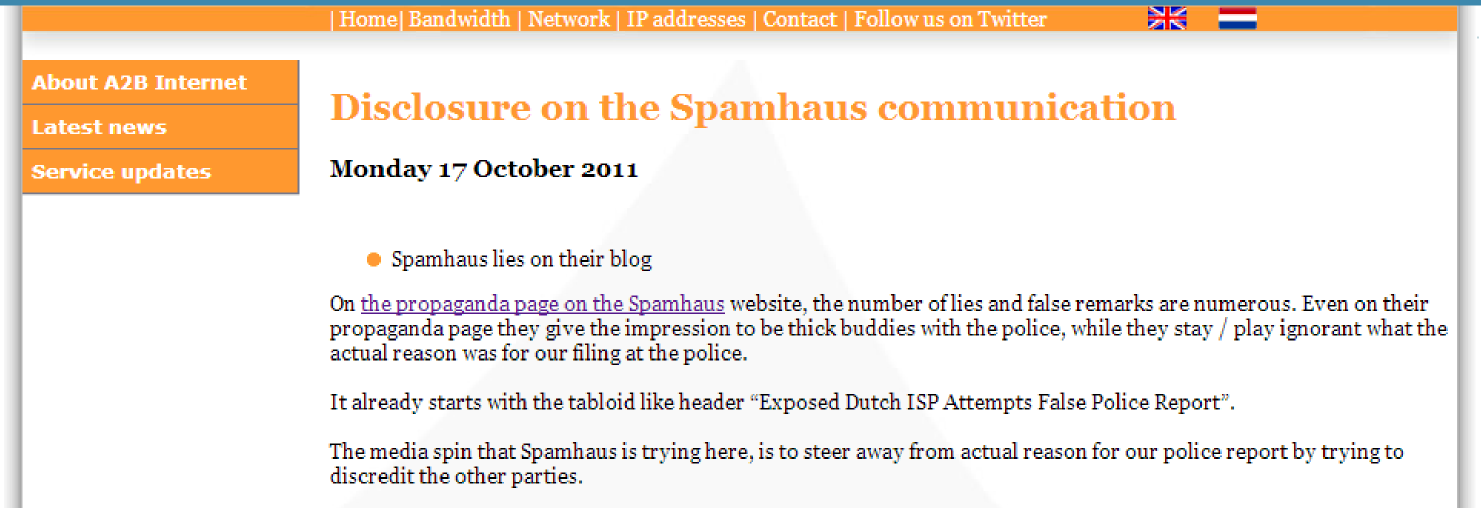
- The Dutch High Tech Crime Unit was contacted to inform them on the situation ... And they asked some people from SH during a converence that same week on this matter, asking what they were thinking ...

- There has a long standing informal (working) relationship between the Dutch HTCU and SH on other matters.

- A2B Internet had direct contacts at the Dutch HTCU and the Dutch Telco Regulator on how to proceed.

  - It was decided to file a report at the police instead of pursueing a civil case, directly after the SBL listing was removed.

The A2B Internet media reply


| Home| Bandwidth | Network | IP addresses | Contact | Follow us on Twitter
About A2B Internet
Latest news
Service updates

Disclosure on the Spamhaus communication

Monday 17 October 2011

- Spamhaus lies on their blog

On the propaganda page on the Spamhaus website, the number of lies and false remarks are numerous. Even on their propaganda page they give the impression to be thick buddies with the police, while they stay / play ignorant what the actual reason was for our filing at the police.

It already starts with the tabloid like header “Exposed Dutch ISP Attempts False Police Report”.

The media spin that Spamhaus is trying here, is to steer away from actual reason for our police report by trying to discredit the other parties.

- Full disclosure of the information about the SBL listing and all communication.

- Including the communication with the CEO of Spamhaus – Steve Lindford.

- The communication with Steve Lindford requested an open discussion about the process, to see if the policy could be adjusted.
  - Suggestion was given at the following RIPE meeting.

Don’t feed the trolls ...

- On Twitter there is an active group of Spamhaus groupies ...
- They re-tweet whatever is originating from the Spamhaus
- Reply to anything that has a #SpamHaus hashtag, as if they have any kind fo authority
- They post online comments like:
  - $ISP is a CyberCrime source
    - also directly to customers tweeting about not being able to email due to a listing
  - Not getting any false positives and Spamhaus is never wrong ...
  - $ISP, You obviously haven't answered complaints by Spamhaus for months and now you want them to react immediately.

Netneutrality

- The effects of Net-Neutrality laws
  - It is not allowed to block, filter, discriminate traffic without reason or cause.
  - The usage of the Spamhaus DROP list, is not allowed.
  - Filtering for violations on an UAP should be ‘proportionate’
- SH’s information providing isn’t sufficient to act upon.
  - Just because they say so, doesn’t make it so ...

The end of RBL’s ?

- RBL’s have been around since the beginning of time ...

- RBL’s are very effective, however their usability comes and goes with their reputation ...

- RBL’s that provide a high rate of false positive or list unrelated prefixes should not be used for blocking spam, but at most for rating spam.
  - Or not be used at all ...

- Entries that are not the source of SPAM have no place on an RBL.
  - Like random prefixes used for pressure or routing interfaces ...

- Reputation is key to a good RBL ...

What did we learn ?

- Spamhaus lists prefixes / complete subnets that are not according to their views ... Regardless if they are a source of spam ...
- Regardless of the ISP's or hosters reputation .... Think about the NIC.AT case.
- Large prefixes are often listed for unclear reasons.
  - http://www.spamhaus.org/sbl/latest/
- A lot of listings on SBL have nothing to do with the SMTP.
- Part of the Spamhaus SBL team is ran by a number of vigilanties with no respect for local laws or normal business policies ...
- Spamhaus is acting as the new MAPS .. Remember what happend to them ?
  - http://yro.slashdot.org/story/00/12/13/1853237/maps-rbl-is-now-censorware-updated

Things to ponder ?

- Are we living in a world where Spamhaus is allowed to act as the internet police ?
  - Without the requirement to provide proof of wrong-doing ?
  - Being judge and executioner on ISP networks reachability ?
  - Allowed to willingly list unrelated prefixes to put presure on transit providers ?
    - If yes, what is next ? Is BGP hijacking of your prefixes allowed ?

Who has the first question ?

Email to: ebais@a2b-internet.com
Or call : +31 - 299 – 707 115