SPAMHAUS

THE SPAMHAUS PROJECT

RIPE54 - 8TH MAY 2007

Welcome! In the next hour:

- About Spamhaus
- Zombies: problems, current state
- What you can do
  (and how can we help you)
  - PBL

SPAMHAUS
THE SPAMHAUS PROJECT

About Spamhaus

- Founded in late 90's, non-profit
- Headquartered in the UK
- 25+ specialists around the world
- DNSBLs: SBL, XBL and PBL
- ROKSO, DROP
- Corporate research team

SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus SBL

- Spamhaus Block List
- 100% human input
- Static spam sources
- Spam webhosting / DNS
- Other spam support services
- Escalations if needed

SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus SBL

- Take SBL listings seriously (they are not ‘another spam complaint’!)

Spamhaus XBL

- Spamhaus eXploits Block List
- 100% automated input
- Lists illegal 3rd party exploits
- Only /32 listings
- No-questions-asked (but limited) removals

Spamhaus PBL

- Spamhaus Policy Block List
- List ranges that should not do direct-to-MX
- Input by Spamhaus and ISPs (you!)
- More on this later

ZEN: One-stop-shopping

- All zones roled into one
- One query, result shows listing type
- www.spamhaus.org/zen/
- Query zen.spamhaus.org

ROKSO

- Register Of Known Spam Operations
- ~200 spammers, 80% of all spam
- Vetting of customers

SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus DROP

- Don’t Route Or Peer list
- Known rogue networks / IP ranges / ASNs, 100% under spammer control
- Excellent for no-traffic policies and router usage

Spamhaus DROP

- Using DROP makes lots of Botnet C&Cs, rogue DNS servers and web-based exploits ‘drop off the net’
- We’re working on a BGP feed

SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus relations

- ISPs / ESPs / xSPs
- Networks, Registrars and Regulators
- Law enforcement
- Research community

Spamhaus users

- ISPs, ESPs, xSPs, governments, universities, military, etc
- Over 800 million mailboxes protected

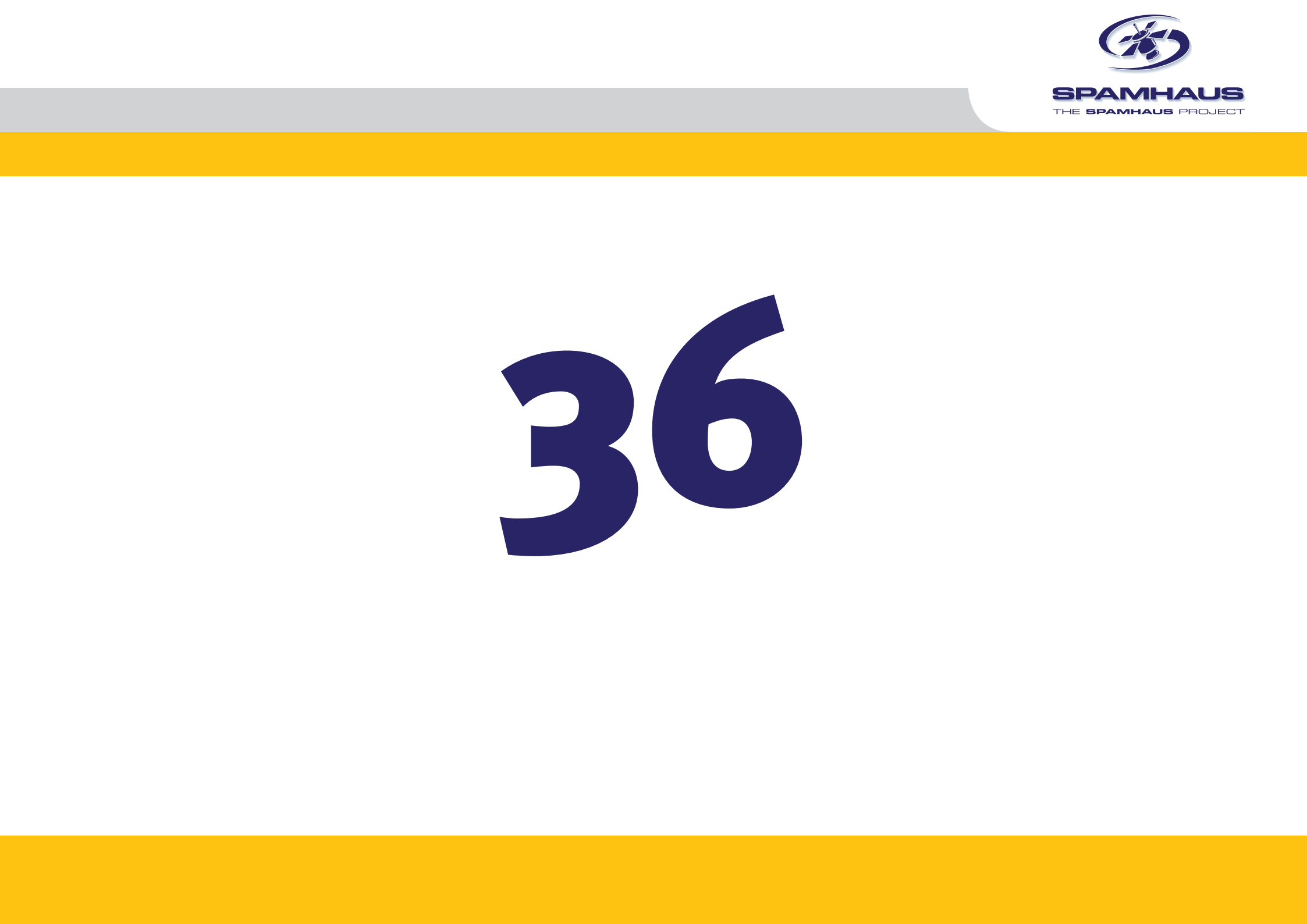
The zombie problem

9825655

SPAMHAUS
THE SPAMHAUS PROJECT

982565

New zombies detected by XBL
on 8th of may 2007 (unique IP addresses)


SPAMHAUS
THE SPAMHAUS PROJECT
36

SPAMHAUS
THE SPAMHAUS PROJECT

36

seconds between infection and first-spam-sent (W32/Warezov)

SPAMHAUS

THE SPAMHAUS PROJECT

Zombies - How do they work?

Attack vectors

- Network scanning (135-139)
- Email viruses (25)
- Webpages / browserexploits (80)
- Social engineering
  - postcard_newyear.jpg.exe,
  - Video codecs

Multi stage

- User installs software
- Software downloads malware
- Malware installs proxy/mailer
- Spam flows
- Other exploits installed (DDOS!)

Evolution

- Proxies
- Private (ACL'ed) proxies
- Mail engines
- Windows 'rootkits'
- P2P for payload retrieval

Evolution

- Proxies
- Private (ACL'ed) proxies
- Mail engines
- Windows 'rootkits'
- P2P for payload retrieval
- What's coming next?

Command & Control (C&C)

- Hosted in ‘dark alleys’
  - Esthost
- Small number of IP addresses causes **lots** of trouble
- Many ISPs do not know that they are hosting a C&C

Command & Control (C&C)

- If C&C locations were known:
  - could you block?
  - would you block?

Zombies -
Have uses apart from mail

'Yambo' webhosting

- HTTP and DNS served on zombies
- Zombie is really a uni-directional proxy
- which proxies to another proxy
- automated blocking
- Linux hosted

Fast Flux hosting

- URL served on 5-10 IP addresses
- Low TTL - 1-5 minutes
- After expiry: new zombies
- DNS fast fluxed too

Fast Flux combatting

- Difficult to track!
- Difficult to shut down
- Port blocking (80 & 53)!
- The only effective point of control is in the hands of the registrar

Zombies - What can you do?

Using traffic patterns

- DNS traffic
- Port 25 outgoing
- But: expensive equipment
- Network may need change

Using feedback loops

- abuse@
- Feedback loops
  - AOL, Outblaze, Hotmail SNDS
- Larger networks willing to share data can contact us for a more effective solution

Why you should care

- Large consumer networks will block parts of your network if high levels of zombie traffic are perceived
- Reputation amongst peers

Spamhaus PBL

The Spamhaus PBL is a DNSBL database of end-user IP address ranges which should not be delivering unauthenticated SMTP email to any Internet mail server except those provided for specifically by an ISP for that customer's use.

The PBL helps networks enforce their Acceptable Use Policy for dynamic and non-MTA customer IP ranges.

SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus Policy Blocklist

- End user ranges
- Two categories:
  - Data by participating ISP
  - Data by Spamhaus
  - Recognizable by DNS response

SPAMHAUS
THE SPAMHAUS PROJECT

Spamhaus Policy Blocklist

- No-questions-asked automated single IP removal

- ISP interface for your managing your own IP ranges

SPAMHAUS
THE SPAMHAUS PROJECT

How not to use PBL

- Do NOT use on smarthosts or SMTP AUTH for your own customers!
- Do NOT use for other than checking IP addresses that hand of to your mailservers (no ‘deep parsing’)

SPAMHAUS
THE SPAMHAUS PROJECT

PBL: A win-win-win opportunity

- Cuts down on bandwith being stolen and damage being done and deliverability problems
- Cuts down the complaints (which frees staff for other things)
- Stops damage to your reputation

www.spamhaus.org/pbl/

SPAMHAUS
THE SPAMHAUS PROJECT

Closing up...

- We must try harder. Problems are getting more serious and harder to solve.
- Balance between prevention of harm and the traditional freedoms of the ‘net

SPAMHAUS
THE SPAMHAUS PROJECT

Closing up...

- Governments are not empowered to solve these problems. They are looking to the industry to implement self-regulation.

Closing up...

- What other data can we provide that would help you protect your network?