SPAMHAUS

THE SPAMHAUS PROJECT

UKNOF6 - 19TH JANUARY 2007

Welcome! In the next 30 minutes:

- About Spamhaus
- Zombies - How bad is the problem?
- Zombies - How do they work?
- Zombies - Have uses apart from mail
- Zombies - What can you do?
- Is there a solution?

SPAMHAUS
THE SPAMHAUS PROJECT

About Spamhaus

- Founded in late 90's, non-profit
- Headquartered in the UK
- 25+ specialists around the world
- DNSBLs: SBL and XBL
- 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 XBL

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

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
THE SPAMHAUS PROJECT

Spamhaus relations

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

SPAMHAUS

THE SPAMHAUS PROJECT

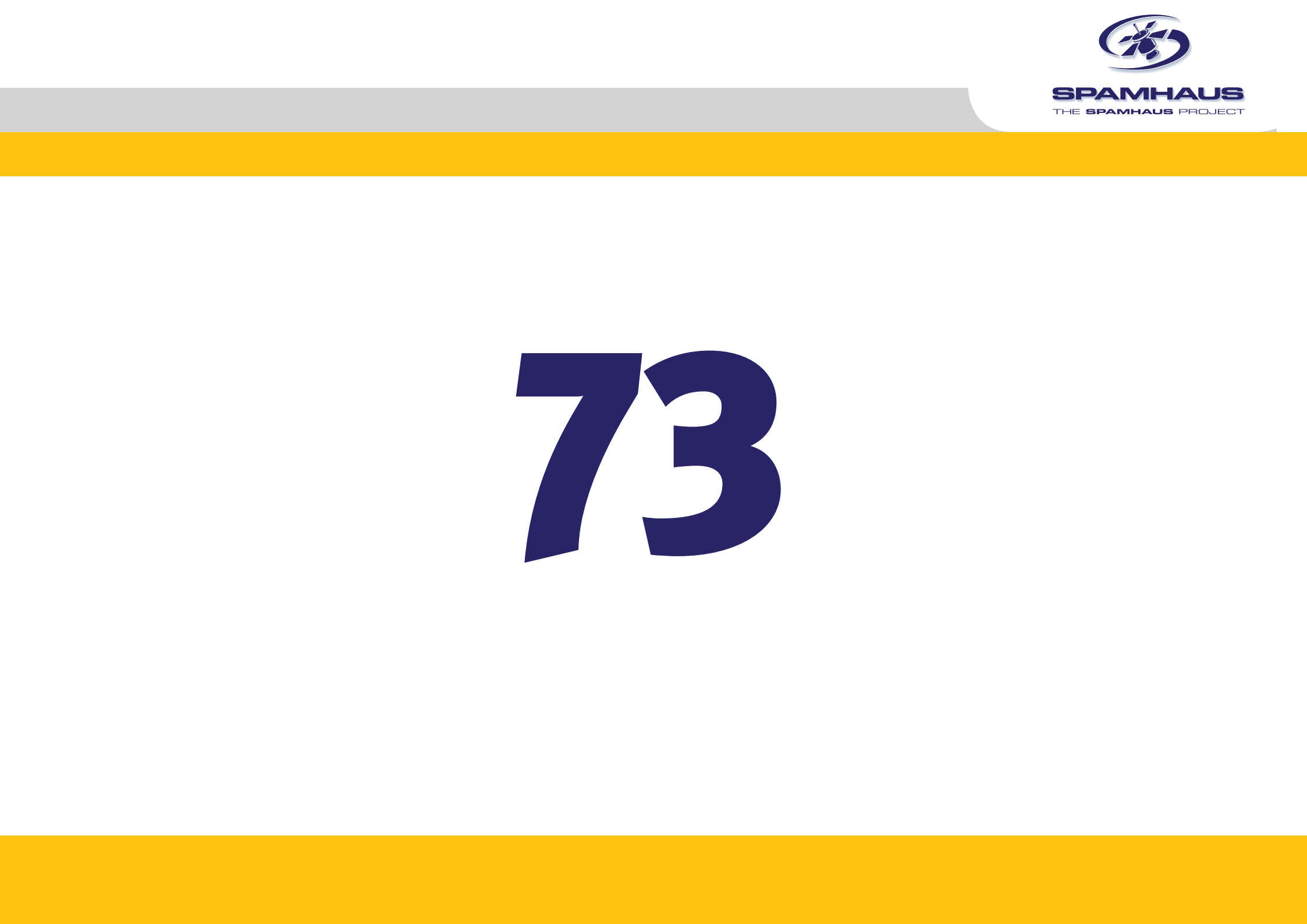
Zombies - How bad is the problem?

7638O9

SPAMHAUS
THE SPAMHAUS PROJECT

763809

New zombies detected by XBL
on 14th of january 2007


SPAMHAUS
THE SPAMHAUS PROJECT
73

SPAMHAUS
THE SPAMHAUS PROJECT

73

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

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)

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’
- Small number of IP addresses causes **lots** of trouble
- Many ISPs do not know one when they have one

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 IP addresses
- Low TTL - 5 minutes
- After 5 minutes: 5 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

SPAMHAUS

THE SPAMHAUS PROJECT

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, Earthlink
- Larger networks 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

THE SPAMHAUS PROJECT

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 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’)

www.spamhaus.org/pbl/

SPAMHAUS
THE SPAMHAUS PROJECT

Closing up...

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