SPAMHAUS

THE SPAMHAUS PROJECT

ICANN 38 Brussels

SPAMHAUS
THE SPAMHAUS PROJECT

About The Spamhaus Project

- Since 1998, non-profit
- Headquartered in the UK
- 30+ specialists around the world
- DNSBLs: SBL, XBL, PBL and DBL
- DROP
- ROKSO

SPAMHAUS
THE SPAMHAUS PROJECT

Over

1,500,000,000

mailboxes protected using our data

SPAMHAUS
THE SPAMHAUS PROJECT

Fast flux

15 new locations. Every few minutes.

SPAMHAUS
THE SPAMHAUS PROJECT

Traditional bullet-proof hosting

- Located in poorly regulated jurisdictions (China, Brazil, Russia)
- ISP is slow when complaints are received
- Site resolves to a single IP address

Fast flux bullet-proof hosting

- Multiple IP addresses act as a proxy for a conceiled website
- Hosted globally
- They change ***fast***

SPAMHAUS
THE SPAMHAUS PROJECT

Fast flux bullet-proof hosting

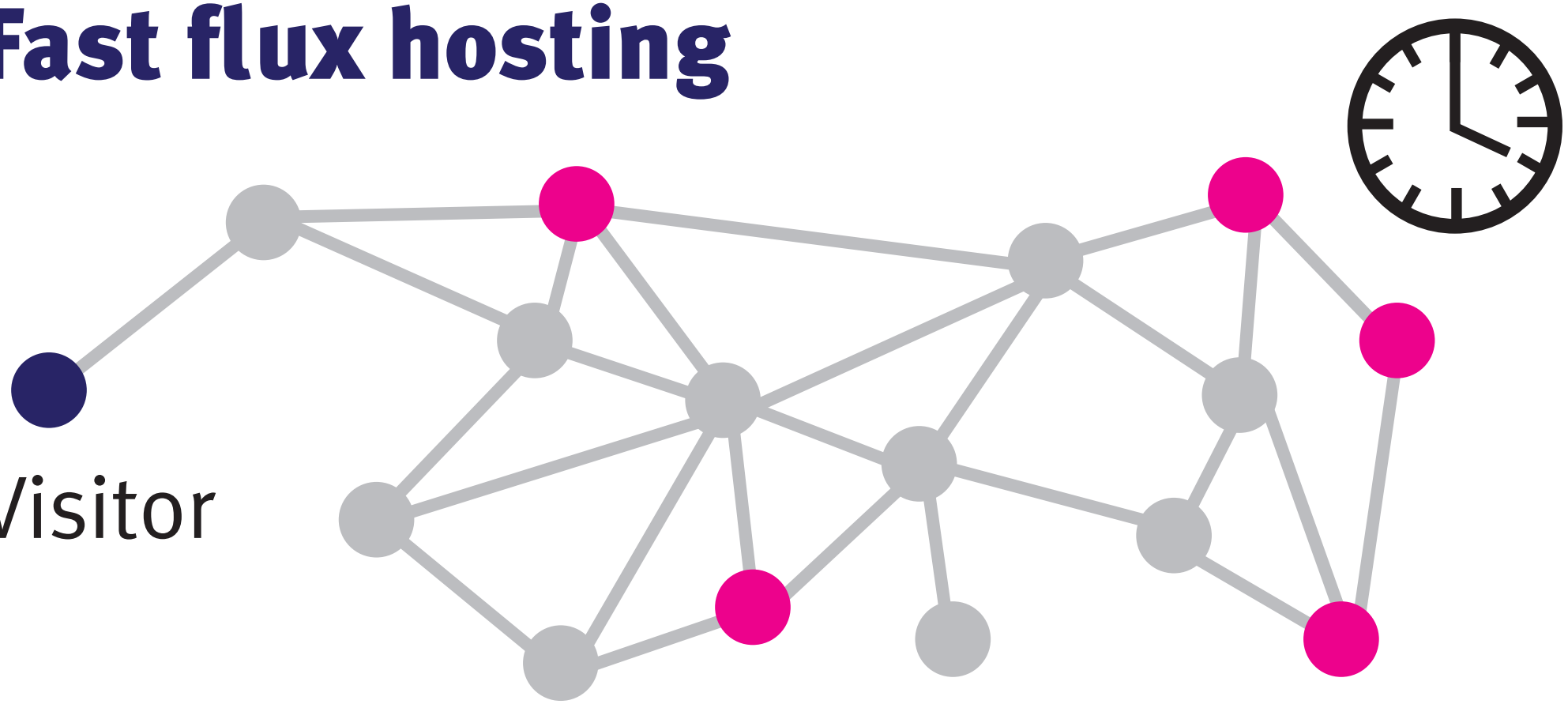
- Multiple IP addresses can also answer for the hidden nameservers of a domain
- This means that abuse mitigation has been moved from the hosting company to the registrar - registrars were never intended to handle this scenario
- Most are not prepared to handle this!

Hosting the worst of the worst

- Counterfeit medicines
- Phishing websites
  (Zeus/Avalanche specifically)
- Mule scams
- Malware downloads

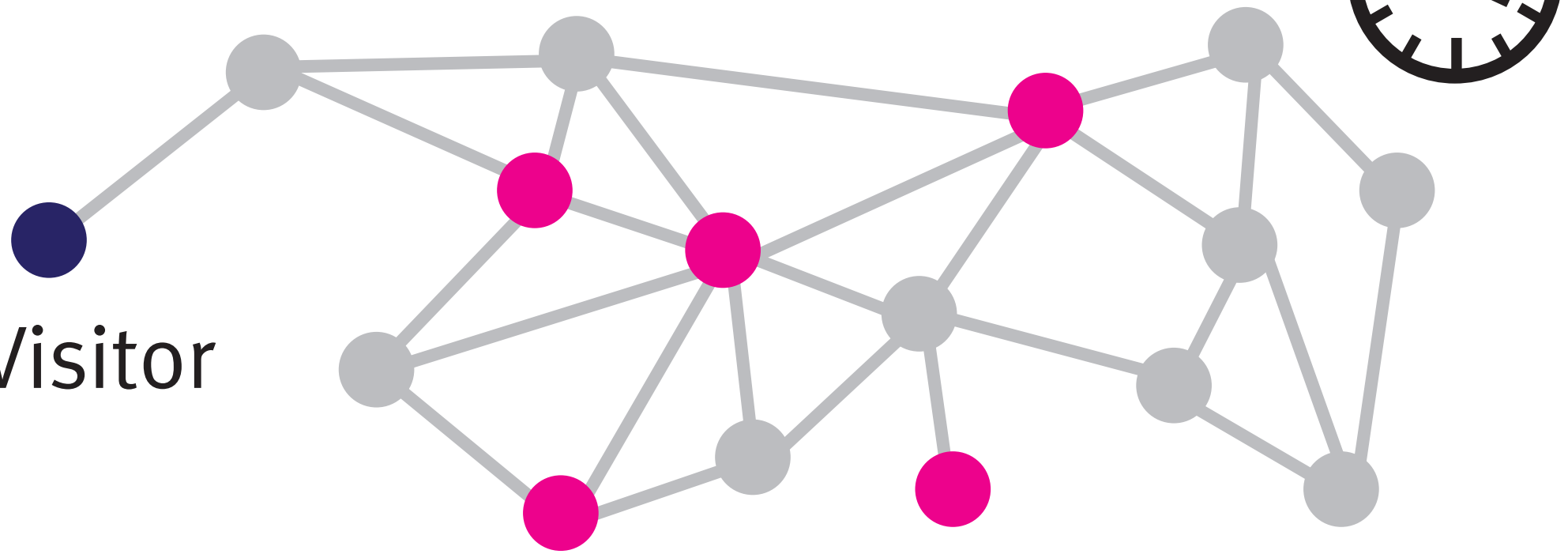
SPAMHAUS
THE SPAMHAUS PROJECT

Fast flux hosting



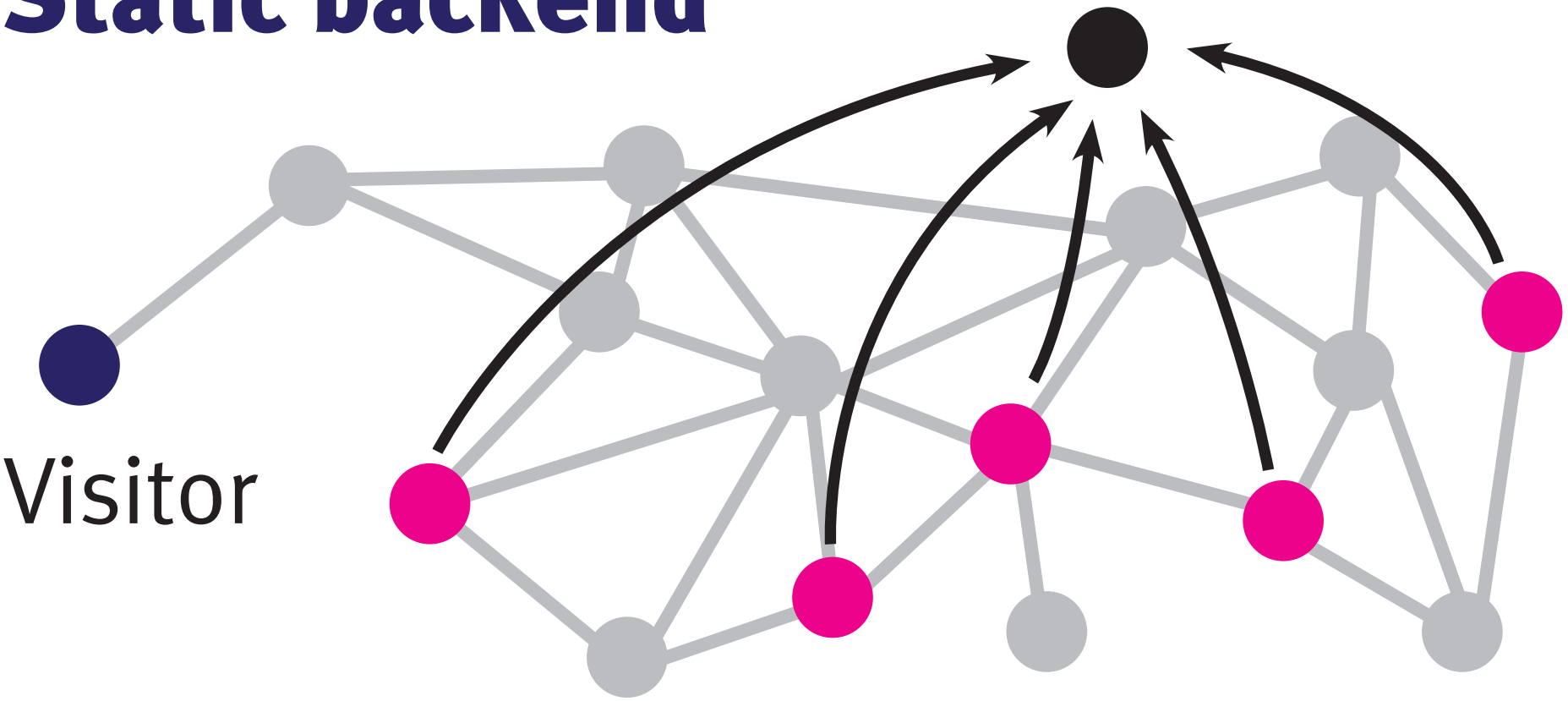
SPAMHAUS
THE SPAMHAUS PROJECT

Fast flux hosting



SPAMHAUS
THE SPAMHAUS PROJECT

Static backend



www.lztalsole.com

SPAMHAUS
THE SPAMHAUS PROJECT

Domain Block List

- New since March 2010
- Standard in latest SpamAssassin
- Usable in any content filter that can check domains against a DNSBL

Main goals

- Provide additional protection against spam that passes IP-based DNSBLs
- Shorten the usable lifespan of spammer controlled domains
- Help registrars and registries protect their investment in the reputation of their brand
- Zero false positives

SPAMHAUS
THE SPAMHAUS PROJECT

What is the input for the DBL?

- Domains, domains, domains
- And some IP addresses as well
- Not only bad domains!

And then?

- DBL engine processes each domain to calculate reputation
- Bad domains are put into the DBL zone
- New zone is built and distributed to worldwide users ***every minute***

What ends up in the zone?

- Domains fully under the control of cybercriminals and spammers
- Used for spam, phishing or malware distribution
- These domains will have either been used in spamvertized URLs or as nameservers, redirectors, reverse DNS, etc.

SPAMHAUS
THE SPAMHAUS PROJECT

Usage in mail filtering

- Extract domain from mailbody or headers
- Lookup on DBL via DNS query
- If listed: discard/score/move email

Some lessons learned (1)

- The big ‘Ruskranian’ spam operations use new domains every few minutes
- So, they consider domains a throw-away resource!
- Makes them very different from regular customers, who tend to be in it for the long run

Some lessons learned (2)

- Some spammers ‘age’ domains: domains are not always used directly after registration
- Aging can be weeks or months, periods of over a year have been seen in the wild

Some lessons learned (3)

- Who considers rogoxxywtrcwph.info to be a legit domain?
- Apparently there is no need to hide

SPAMHAUS
THE SPAMHAUS PROJECT

Some lessons learned (4)

- Speaking of hiding... whois privacy protection is still strongly associated with badness
- 1 in 5 privacy protected domains is used for spam (in any shape or form), phishing or malware distribution.

SPAMHAUS
THE SPAMHAUS PROJECT

Some lessons learned (5)

- Some registrars have over 90% of their sponsored domains listed
- We doubt the legitimacy of these kind of ‘registrars’

SPAMHAUS
THE SPAMHAUS PROJECT

Thank you!

Our team is happy to answer questions either now or after the event!