Monitoring Internet Background Radiation

What The Hack 2005

Liempde, The Netherlands

Hendrik Scholz
hscholz@raisdorf.net
http://www.wormulon.net/

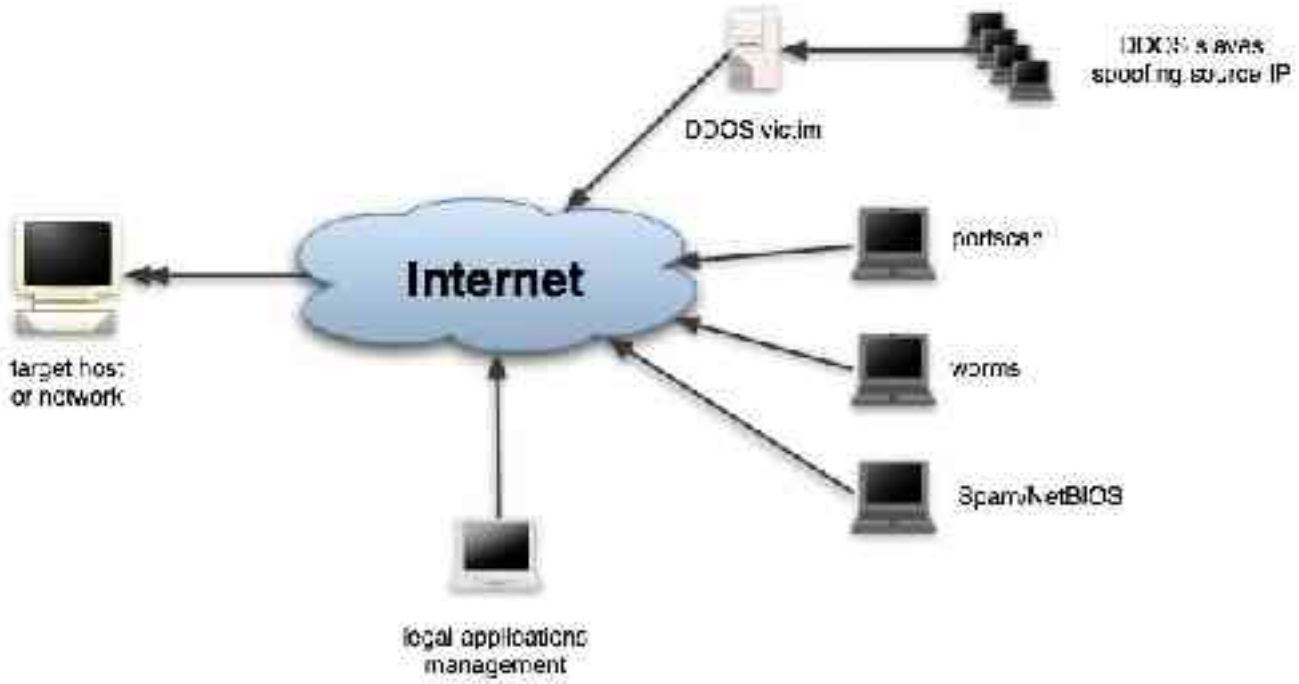
Agenda

- What is Internet Background Radiation?
- Traffic Analysis
  - applications, sources, ..
- Conclusions

Internet Background Radiation

- nonproductive traffic, i.e.
  - portscans
  - worms
  - backscatter from spoofed packets
  - from misconfiguration
- easily visible when snooping on an otherwise unused IP address

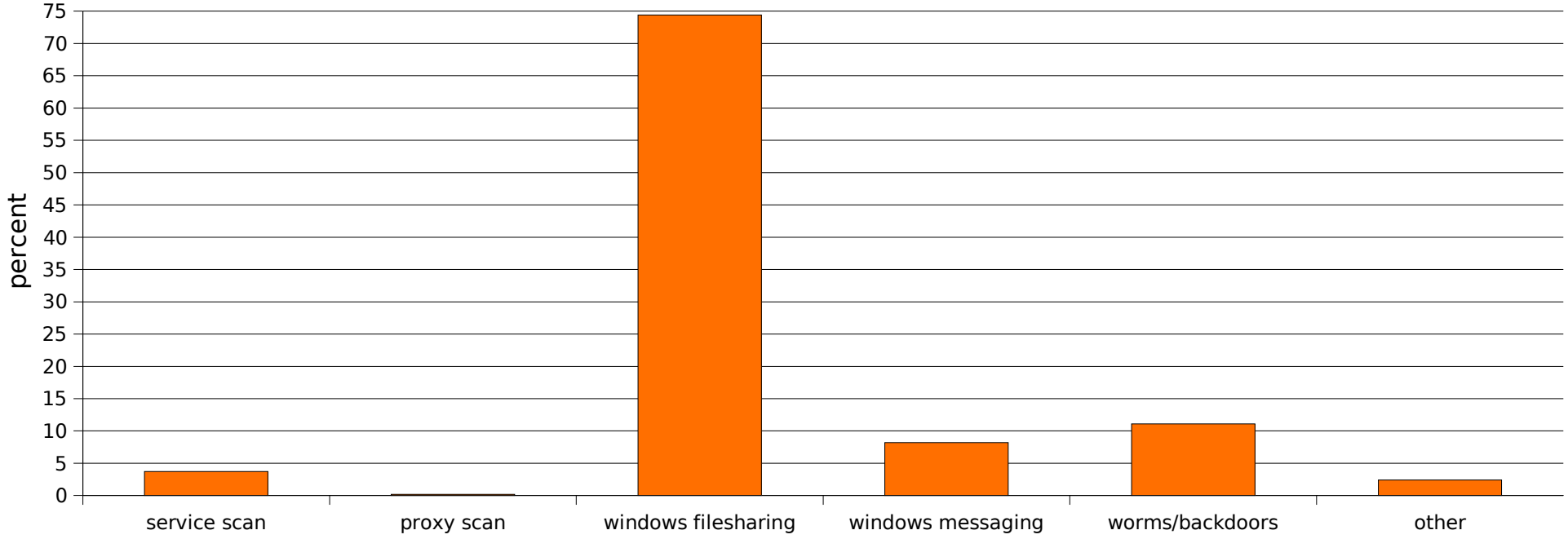
Test Setup


DDOS victim
Internet
target host
or network
portscan
worms
SpamNetBIOS
local application
management

Expectations

- lots of portscans
- worms
- DDOS backscatter
- spoofed IP percentage?
- how much volume?

First Results



- Volume: ~1.5Bytes/s per IP (root server IP)
- Volume and patterns depend on network
  - dialup, root server, NNTP environment

Analysis: NetBIOS

- Windows Messenger Service
- common URLS

  ms-repair.net, msrepair.net, www.fixwinregister.com, ww.fixwinregister.com, www.regcleaner32.com, disinfect-me.com, msreg.com, msrepair.net, regeditpro.com, www.pcregfix.com, fixmyreg.com, fixyourreg.com, ...

- just a few source IP addresses were used (!)

Analysis: NetBIOS (2)

- same IP, different TTL values
  - spoofing?
  - two groups: TTL class 128 & 64
- IP ID matching trick didn't work
  - most IP IDs 0
- sources: 90% 'Shanghai Global Network Inc'
  - 61.129.0.0/16 and 61.152.156.0/22

Analysis: Bogons

- bogon space: unallocated/unused networks
- bogon packet: packet pretending to be from a bogus network
- often generated when spoofing IP addresses
- Filtering via ACL on igress/egress routers
- Your mileage may vary due to constant changes!
- not a single bogon hit my .de traffic sink
- more info: http://www.cymru.com/Bogons/

Analysis: Worms

- 10-15% worms and backdoor checks
- some worms exploit bugs in others
  - W32.Dabber exploiting W32.Sasser FTP server
- SQL slammer
  - 900+ days old but still active
- limited variety: 20 different breeds
- some worms die within days, i.e. Dumaru/Nibu

Analysis: Backscatter

- TCP RST
  - very few packets
  - zero IP ID, window size, seq. numbers, ...
- ICMP errors
  - less than one packet per day
  - host unreachable from intermediate routers

Analysis: What else?

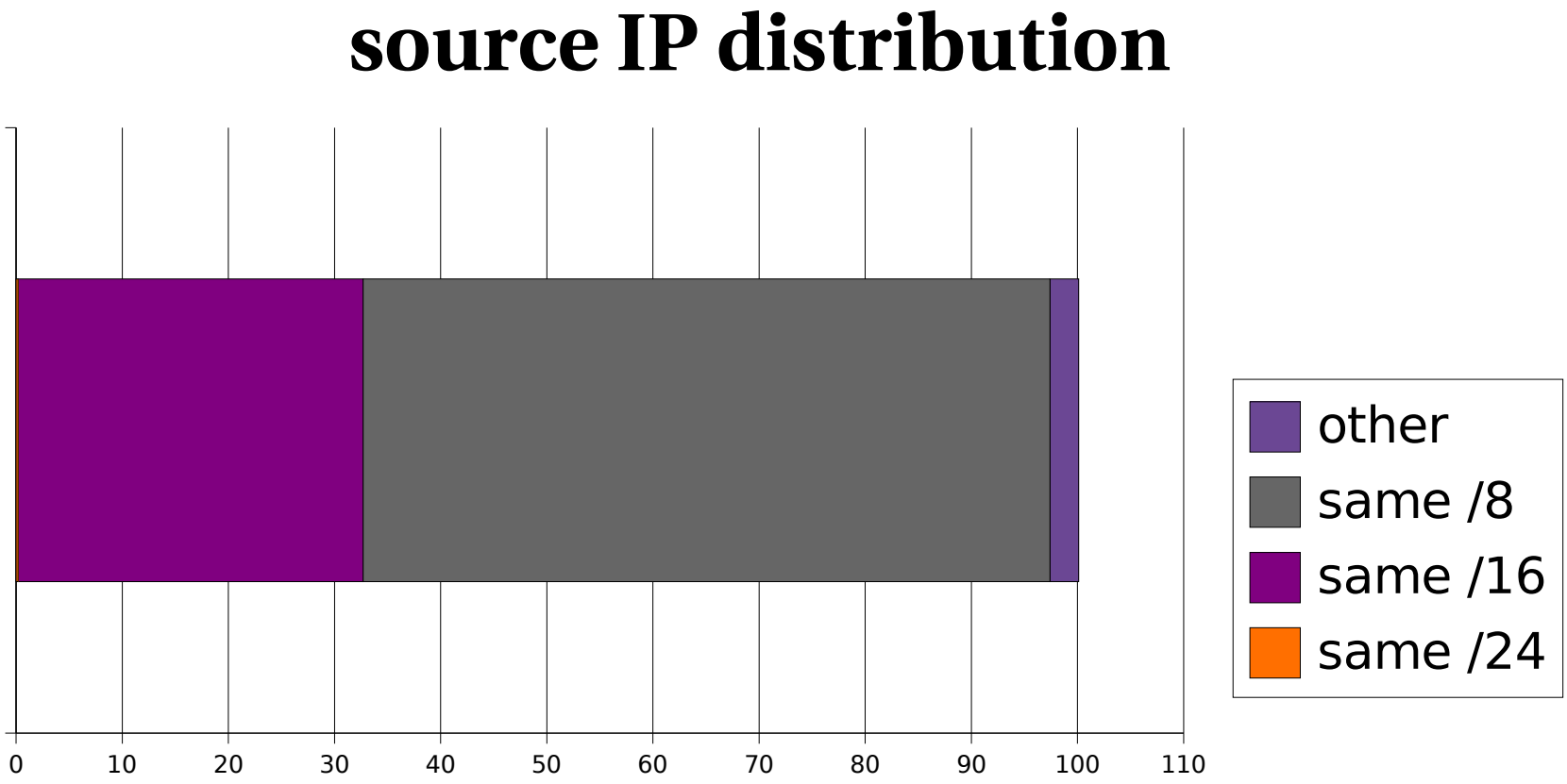
- legal management
  - i.e. Check for new hosts, open ports, ...
- few real portscans with >1 port
- unknown destination port 27585

```
22:03:04.773450 IP (tos 0x0, ttl 106, id 23990, offset 0, flags [none], length: 40)
    203.90.128.75.7777 > 81.169.xxx.xxx.27585: R [tcp sum ok] 0:0(0) ack 28991 win 0
10:11:26.035685 IP (tos 0x0, ttl  29, id 61998, offset 0, flags [none], length: 40)
    219.129.239.4.80 > 81.169.xxx.xxx.27585: R [tcp sum ok] 0:0(0) ack 28991 win 0
16:58:17.810513 IP (tos 0x0, ttl 109, id 63974, offset 0, flags [none], length: 40)
    219.129.239.4.80 > 81.169.xxx.xxx.27585: R [tcp sum ok] 0:0(0) ack 28991 win 0
19:01:16.102343 IP (tos 0x0, ttl 105, id 23739, offset 0, flags [none], length: 40)
    59.148.232.144.80 > 81.169.xxx.xxx.27585: R [tcp sum ok] 0:0(0) ack 28991 win 0
22:33:44.889381 IP (tos 0x0, ttl 108, id 27619, offset 0, flags [none], length: 40)
    61.156.38.36.27016 > 81.169.xxx.xxx.27585: R [tcp sum ok] 0:0(0) ack 28991 win 0
```

Analysis: Distance

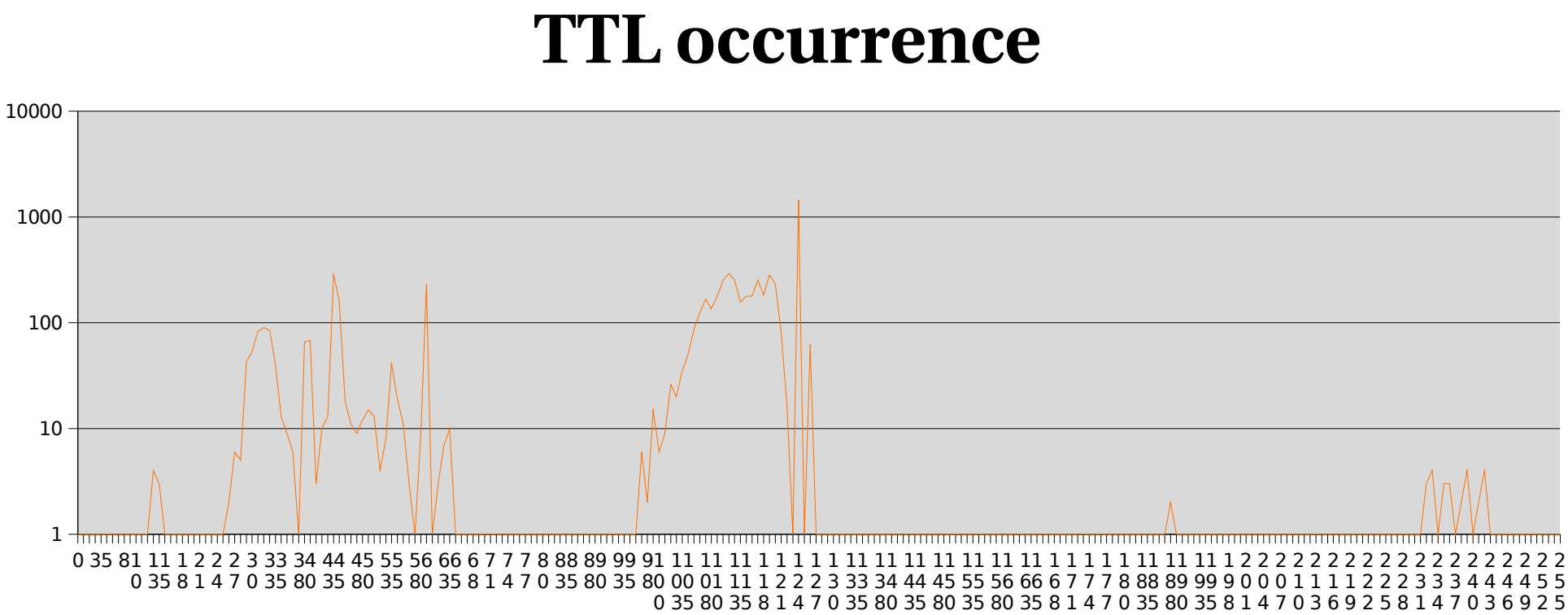
- Where is that stuff coming from?
- Speed depends on
  - network topology, connections
  - distance in hops
- script kiddie/worm paradigm:
  - similar IP address -> nearby
  - nearby -> faster download/worm propagation

Analysis: Distance (2)



- virtually everybody is from the same /16

Analysis: Distance (3)



- peak at 4 hops due to 'SkyDSL' proxies
- average distance 8-20 hops

Traffic Sink Setup

- use libpcap to save traffic to disk
  - source code available on request
- set up IP filter to prevent any answer packets
- post-process data and mask out known traffic
- nice tools: capsinfo (Ethereal), ngrep

snort vs. honeypot vs. traffic sink

- traffic sink
  - no additional traffic
  - no security issues
  - less information
- active solution (honeypot)
  - harder to maintain
  - in-depth info on payload/communication
- snort
  - identify/filter out known traffic

Conclusion

- way less traffic than expected
- filtering on ISP side DOES matter
- mostly boring Windows stuff

Who is paying for the traffic?

Q&A

Questions?

hscholz@raisdorf.net

http://www.wormulon.net