




Kippo -> SSH Honeypot

Beyond the SSH Bruteforce Attacks



Agenda

- What is Kippo?
 - What does it offer?
 - File structure / config and tty replays
 - Demo
 - Other code developments
- 



What is Kippo?

Kippo is a open source project hosted at the Google Code project build by Upi Tamminen.

NOT MY CODE/PROJECT!


<http://code.google.com/p/kippo/>

Database scripts by Dave De Coster






What is Kippo?

- Kippo is a “medium interaction” SSH honeypot
 - designed to log the entire shell interaction performed by the attacker.
 - Based on Python
 - Under heavy development
 - Always checkout the latest svn builds for added features.
- 




What does it offer?

- Out of the box...
 - Fake shell that looks like debian 5
 - Fake filesystem with the ability to add/remove files
 - Possibility of adding fake file contents so the attacker can “cat”
 - Eg. /etc/passwd, /etc/hosts, /proc/cpuinfo etc
 - Possibility to add fake command output
 - Eg. /sbin/ifconfig, vi, ssh, useradd, apt-get, etc
- 




What does it offer?

- TTY Session logs stored for easy replay with original timings
 - Saves files downloaded with wget for later analysis (De Costers scripts do this!)
 - Writes attack data into sql (svn release only)
 - Plays tricks with the mind!
 - ssh pretends to connect somewhere
 - exit doesn't really exit...
 - Apt-get install pretends to install stuff
- 



What does it offer?

- Information about the attacker
 - SSH agent used (Putty, libssh, version etc)
 - p0f-db (Passive OS fingerprinting)
 - Possible GEO location
 - Timings, general knowledge, bot or human?
 - » Dave De Coster will show the interesting parts I'm just here for the fun :-)
- 



File structure / config and tty replays

- Demo....






More on replays / other code

Want to see more of these funny replays?

- <http://iwatchedyourhack.org> →
 - You hack – we laugh
 - » Adrian Wiesmann

 - Some cool developments by others
 - Markus Koetter → xmpp code
 - Kees Trippelwitz → SurfIDS code
- 

SSH Attacks: Beyond the Login



THE UNIVERSITY
of
WISCONSIN
MADISON

Dave De Coster

- How can we look at the data without watching the ttylog?
- Look at more data at once
- World view
- Interesting things that can be learned



- Provides an overview and details of what happened.
- General stats:
 - Every IP that contacted kippo and info
 - OS info (if available)
 - Number of connections from AS, Country, etc.



- Detailed Output

- All commands that were entered
 - Were they successful?
 - Broken out by category
- All passwords that were entered
 - Success and Failures
- Most common usernames and passwords
- How long it took someone to login
 - And how many passwords they tried
 - Is it a bot? I take a guess

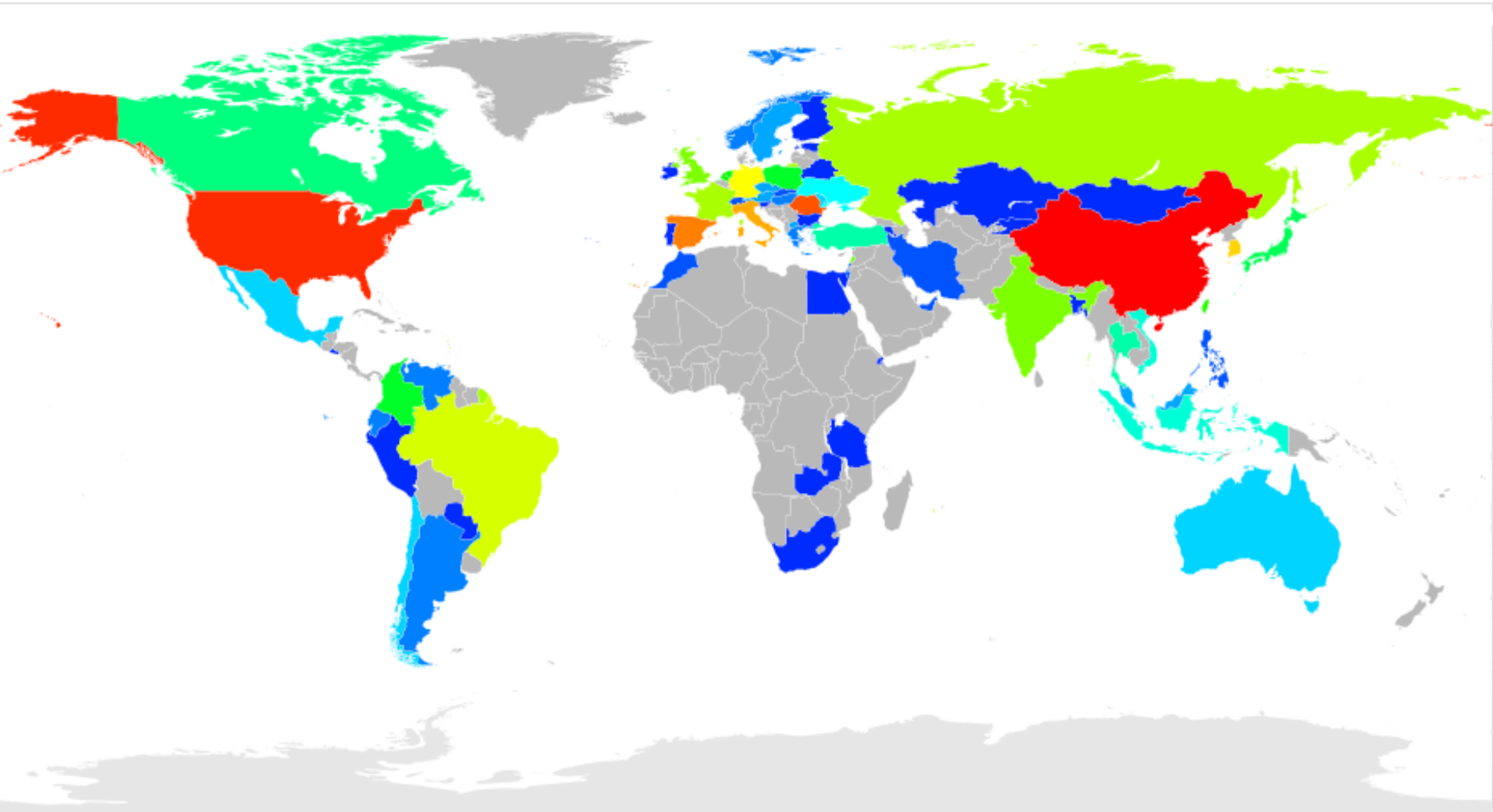


That's a lot of data!

How about a birds eye view?



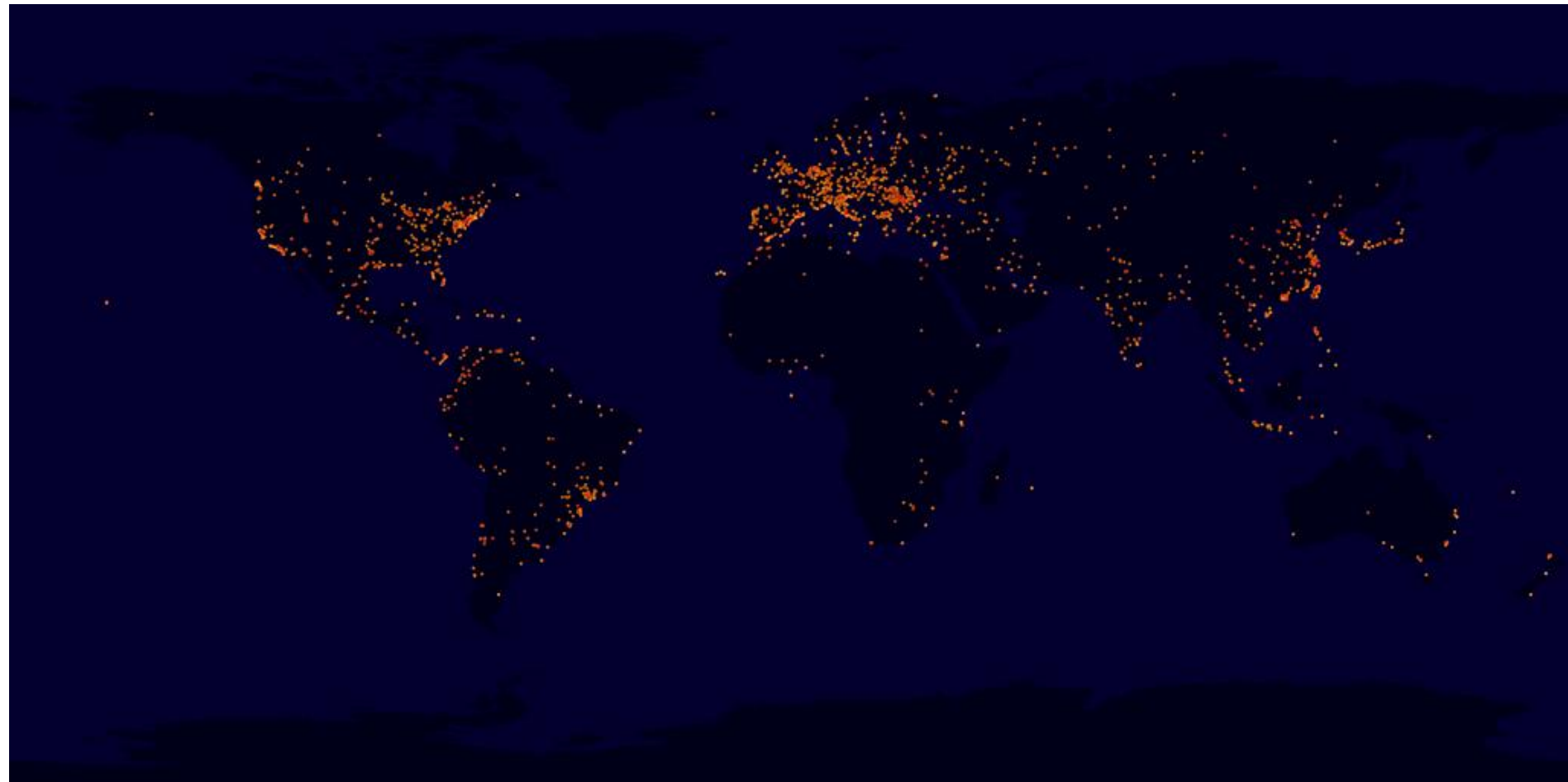
THE UNIVERSITY
of
WISCONSIN
MADISON



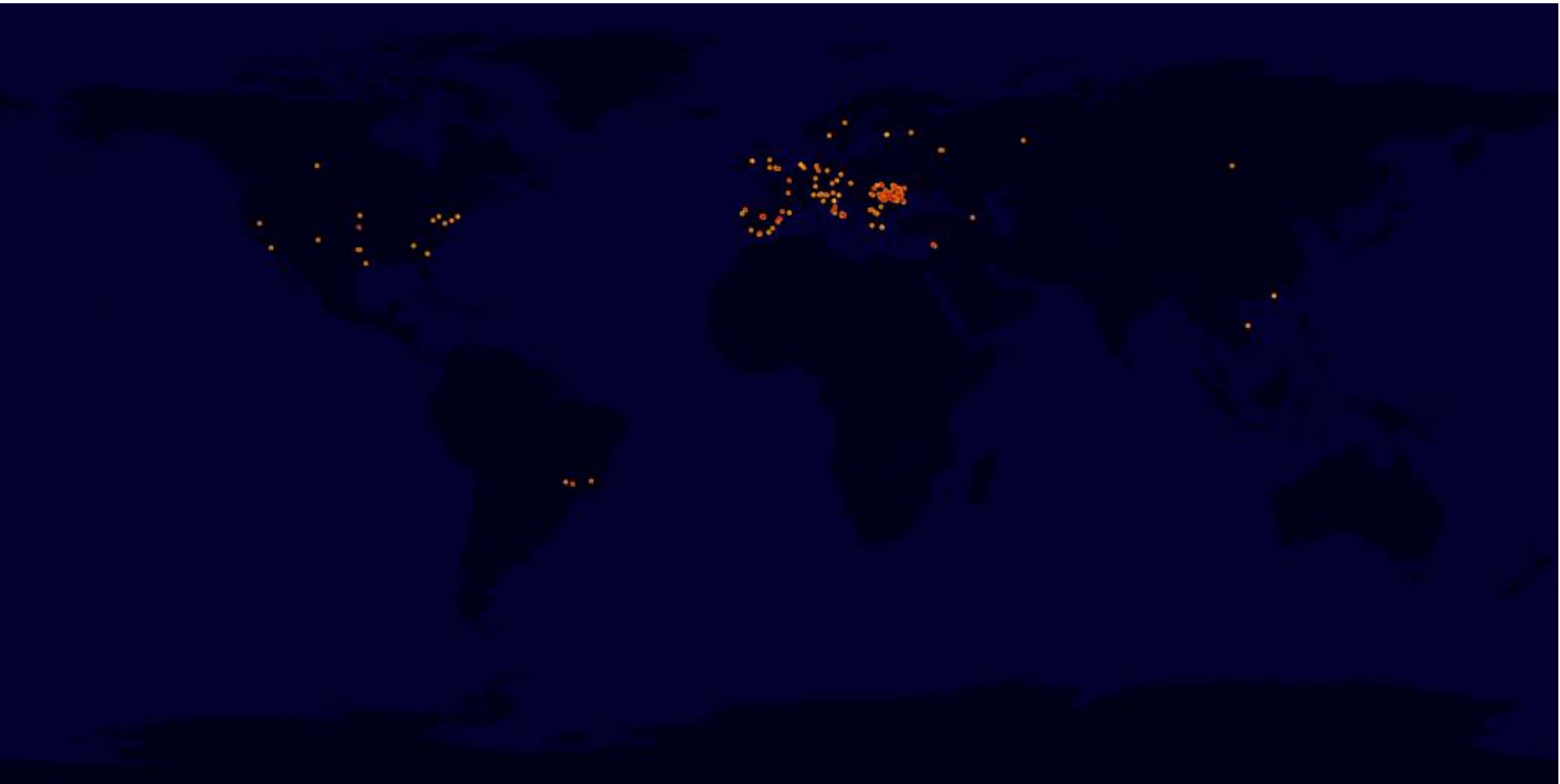
That's neat, but where in those blobs of color are these attacks coming from?



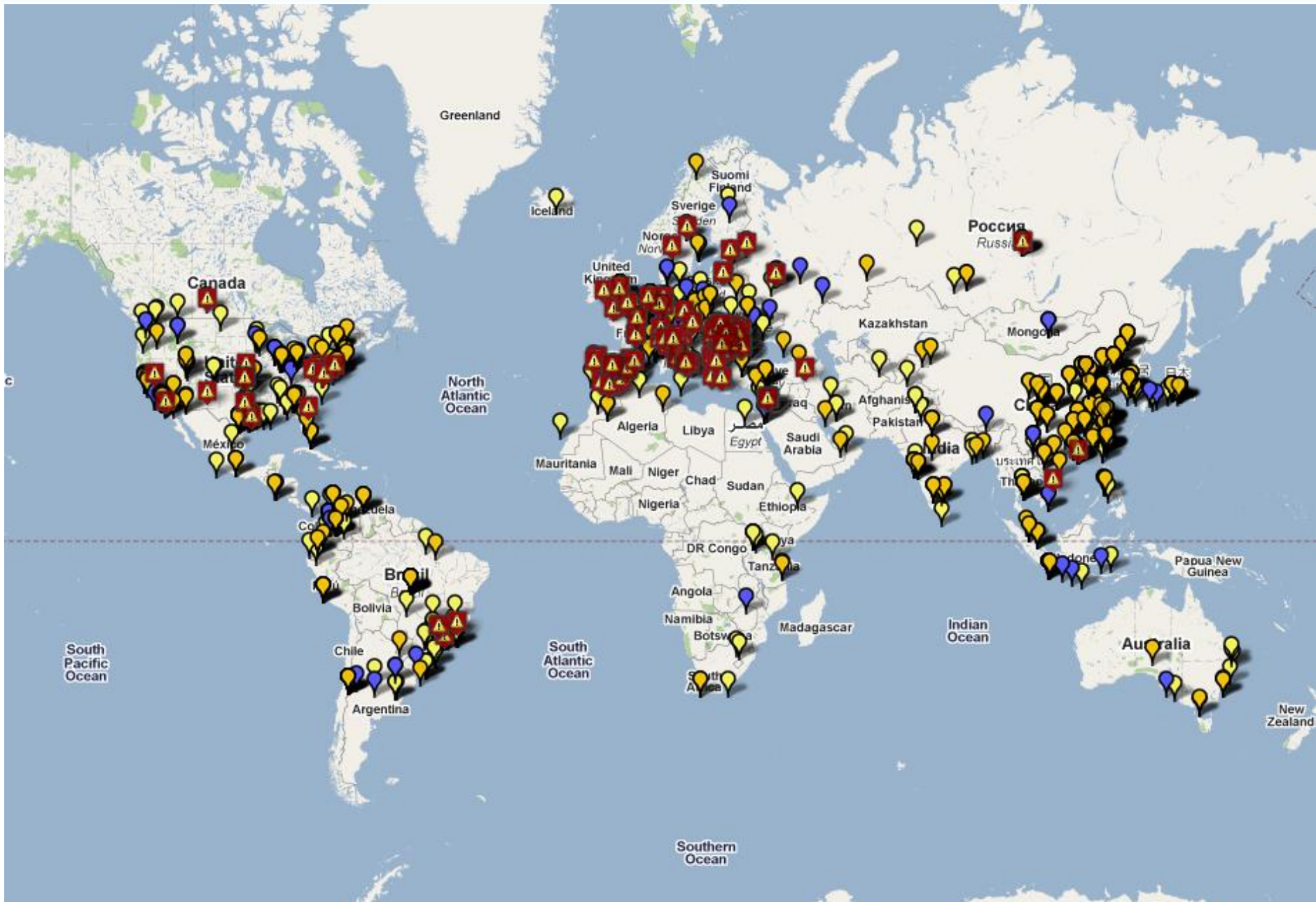
All IPs that connected



Only the IPs that entered a command



Google Maps – IPs by Category



That is awfully cluttered.

Wouldn't it be nice if we
could zoom in?



THE UNIVERSITY
of
WISCONSIN
MADISON

Google Maps – IPs by Category (cont.)

We can!



Google Maps – IPs by Category (cont.)



Google Maps – IPs by Category (cont.)



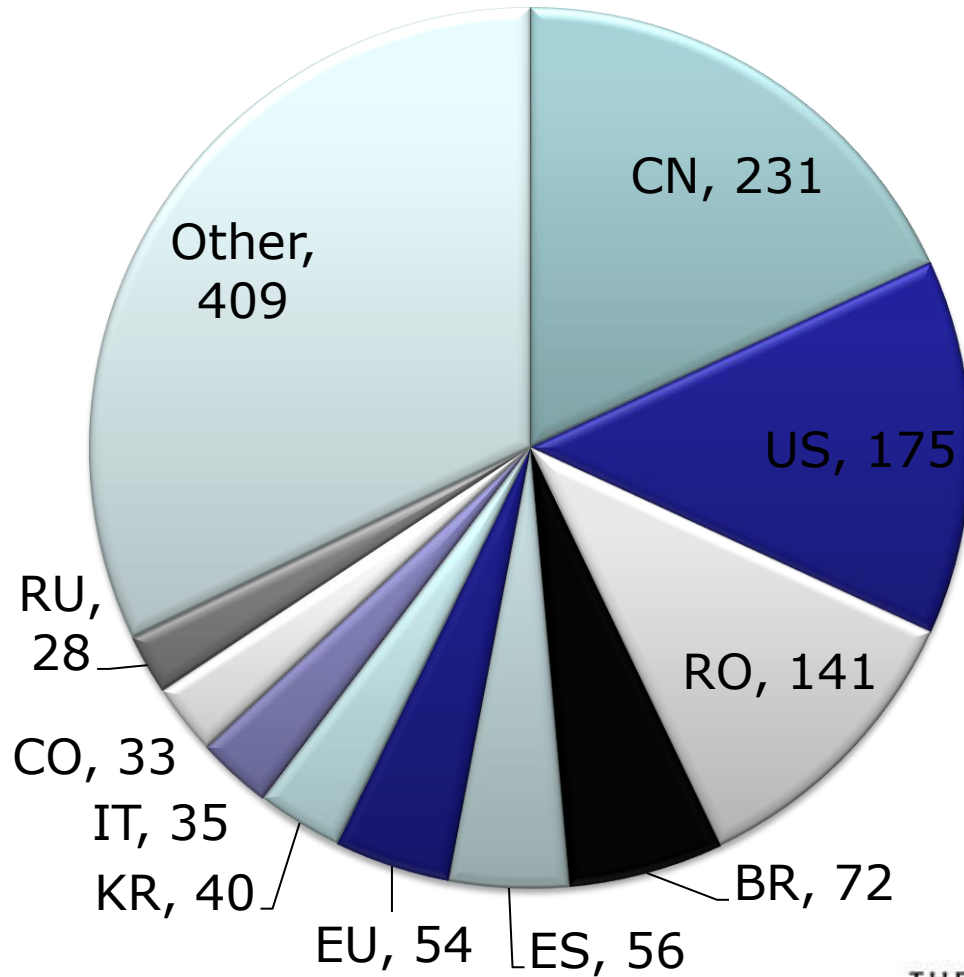
What Can We Learn from this Data?

- The obvious stuff
 - “Top 10” lists
 - Whose contacting the honeypot?
 - What is the most common username?
 - What is the most common password?



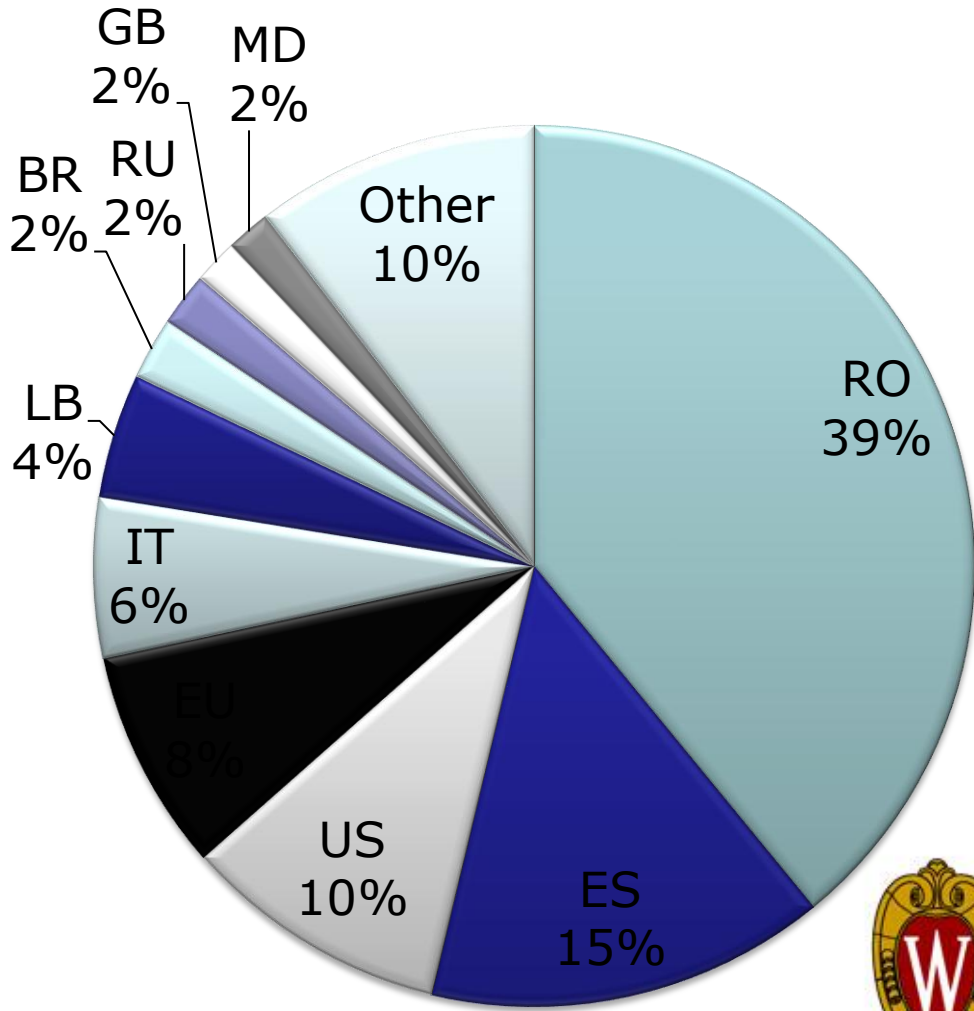
All Connections by Country

Country	Count
CN	231
US	175
RO	141
BR	72
ES	56
EU	54
KR	40
IT	35
CO	33
RU	28
Other	409



Only Those That Entered Commands

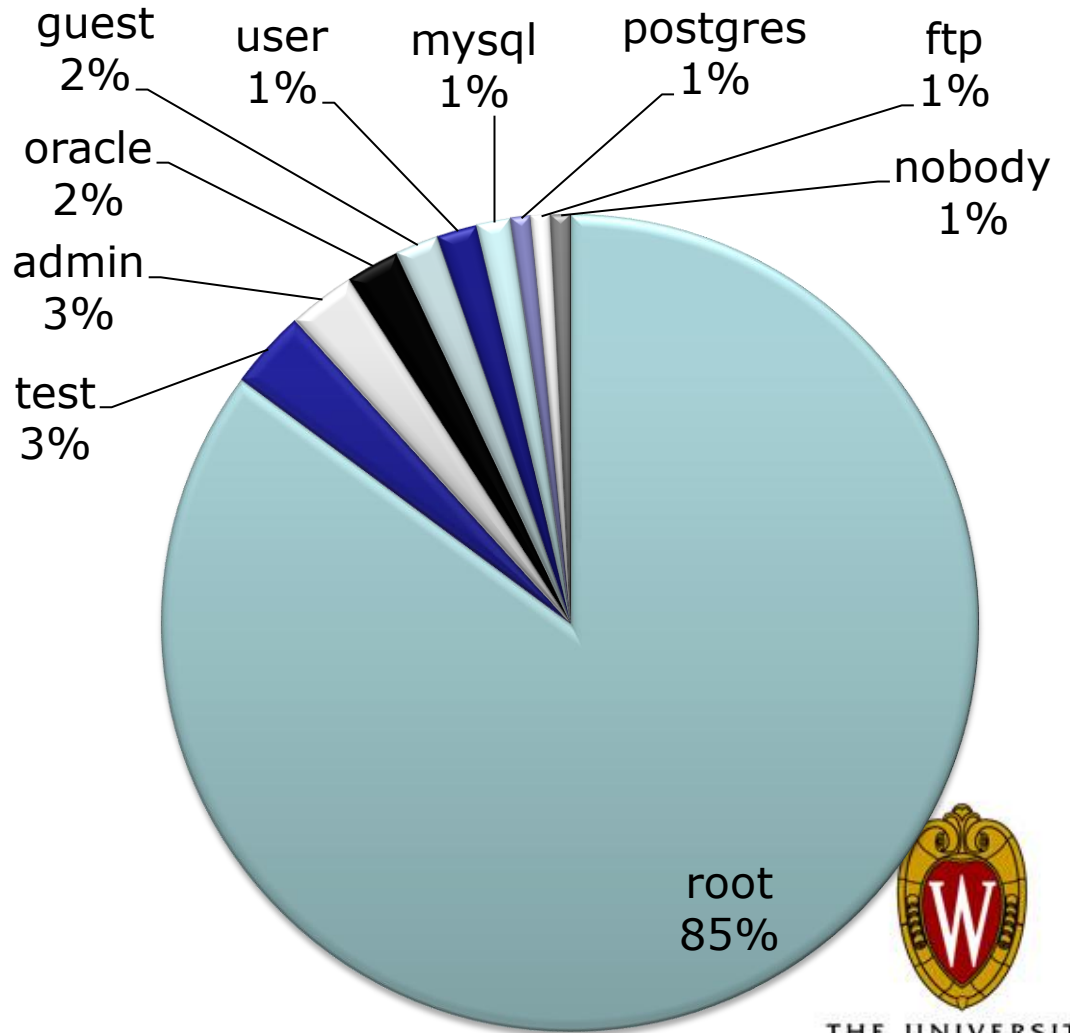
Country	Count
RO	120
ES	45
US	30
EU	25
IT	18
LB	14
BR	7
RU	6
GB	5
MD	5
Other	32



THE UNIVERSITY
of
WISCONSIN
MADISON

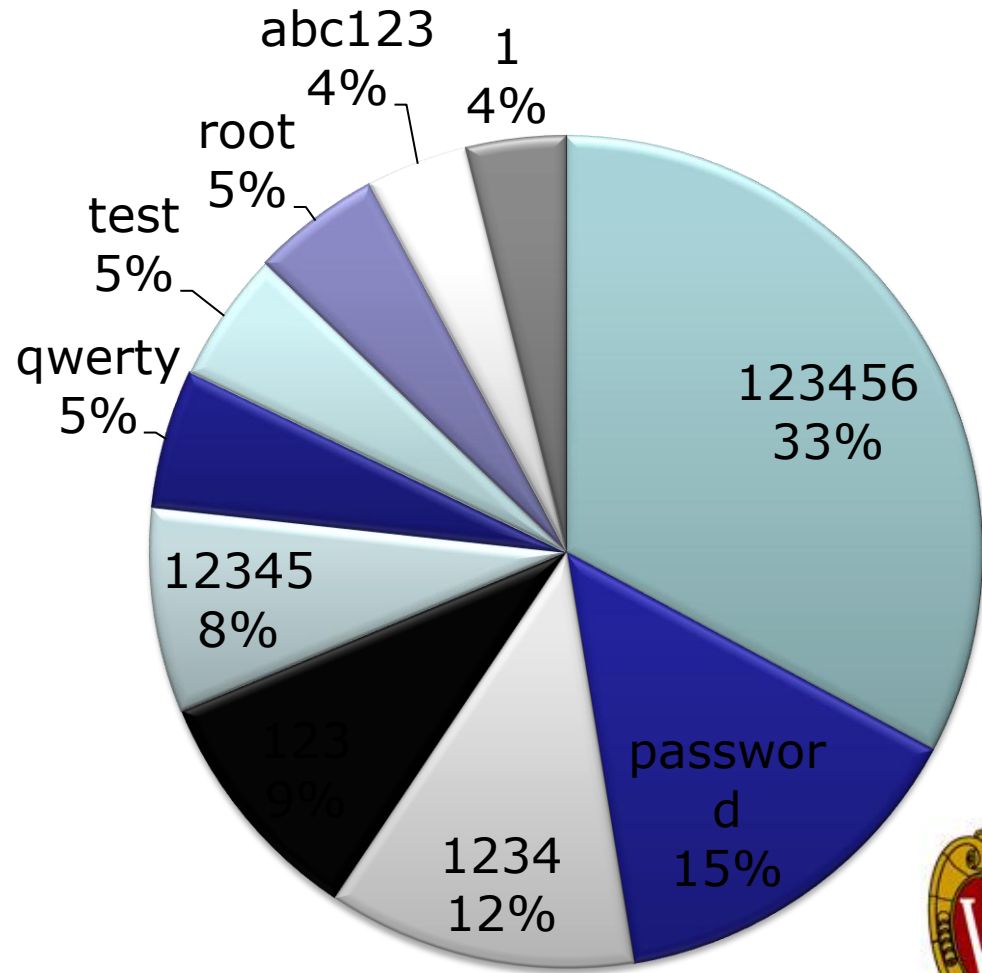
Most Common Username

Username	Count
root	141794
test	5186
admin	4402
oracle	3509
guest	2872
user	2652
mysql	2223
postgres	1332
ftp	1283
nobody	1265
Other	302891



Most Common Password

Password	Count
123456	13115
password	5805
1234	4785
123	3738
12345	3170
qwerty	2143
test	2031
root	2010
abc123	1573
1	1537
Other	429240



THE UNIVERSITY
of
WISCONSIN
MADISON

What Can We Learn from this Data?

- More interesting questions to ask:
 - What ssh clients are the miscreants using?
 - What OS are they using?
 - What are they downloading?
 - Where are they downloading it from?
 - Are there actually people at the keyboard?

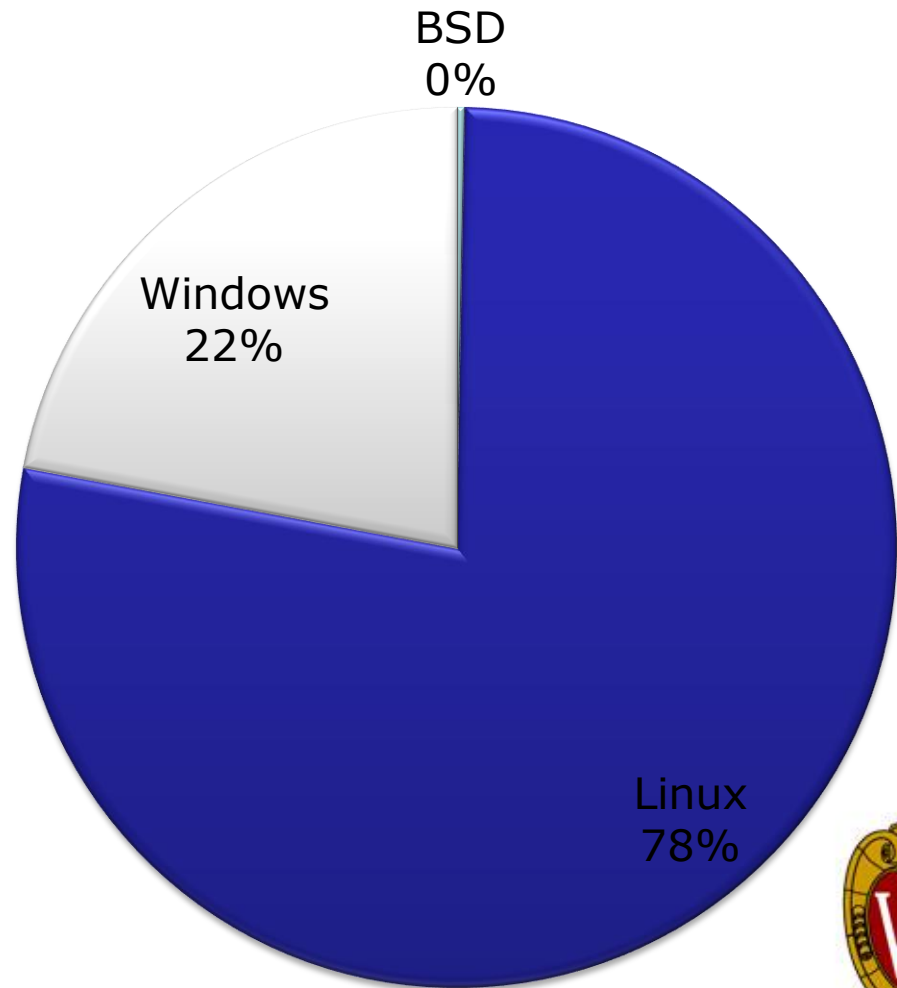


**Most of the interactive attacks
are from Windows systems**



Most Common OS Used

OS	Count
BSD	4
Linux	1038
Windows	295
Total	1337



THE UNIVERSITY
of
WISCONSIN
MADISON

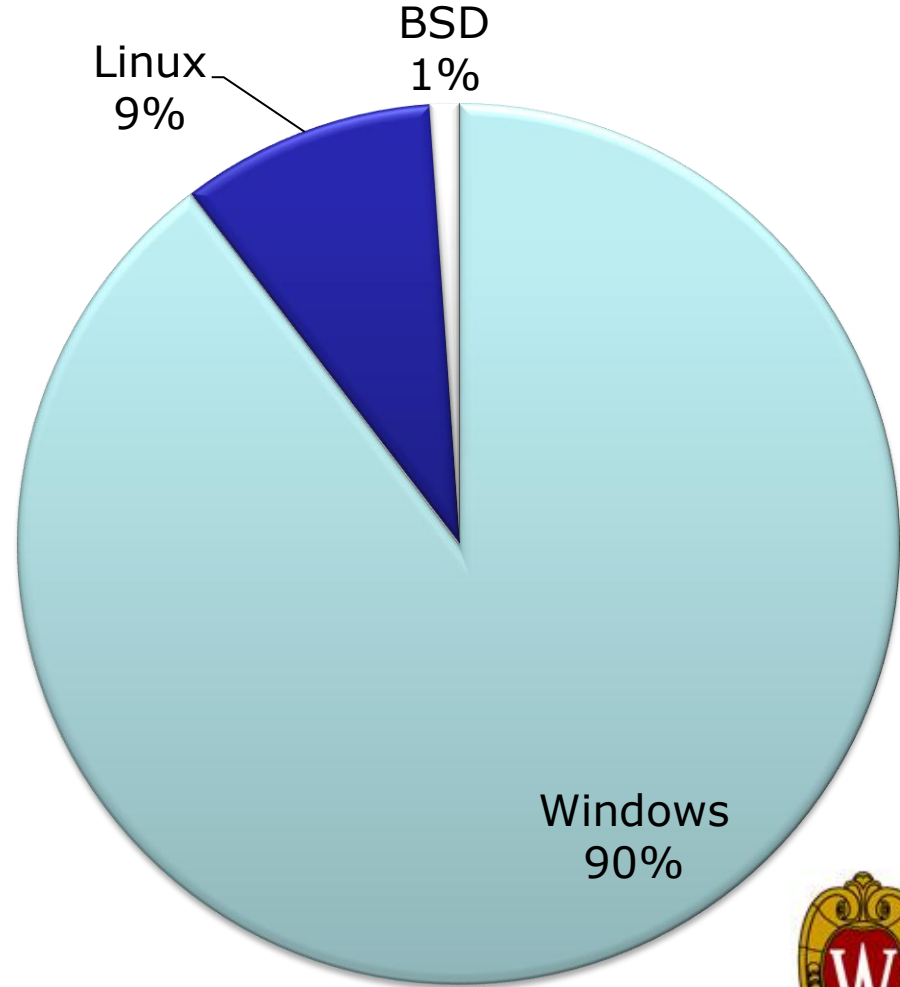
SSH Client Types – All Connections

Client	Count
SSH-2.0-libssh-0.1	559
SSH-2.0-libssh-0.4.3	360
SSH-2.0-PuTTY_Release_0.60	290
SSH-2.0-WinSCP_release_x	74
SSH-2.0-PuTTY_Release_0.5x	31
SSH-2.0-libssh-0.11	21
SSH-2.0-PuTTY_Snapshot_20xx	14
SSH-2.0-dropbear_0.47	11
SSH-2.0-OpenSSH_x	5
SSH-2.0-libssh2_1.0	3
SSH-1.99 (Windows)	1
SSH-2.0-1.89 sshlib: Tunnelier 4.36	1
Total	1370



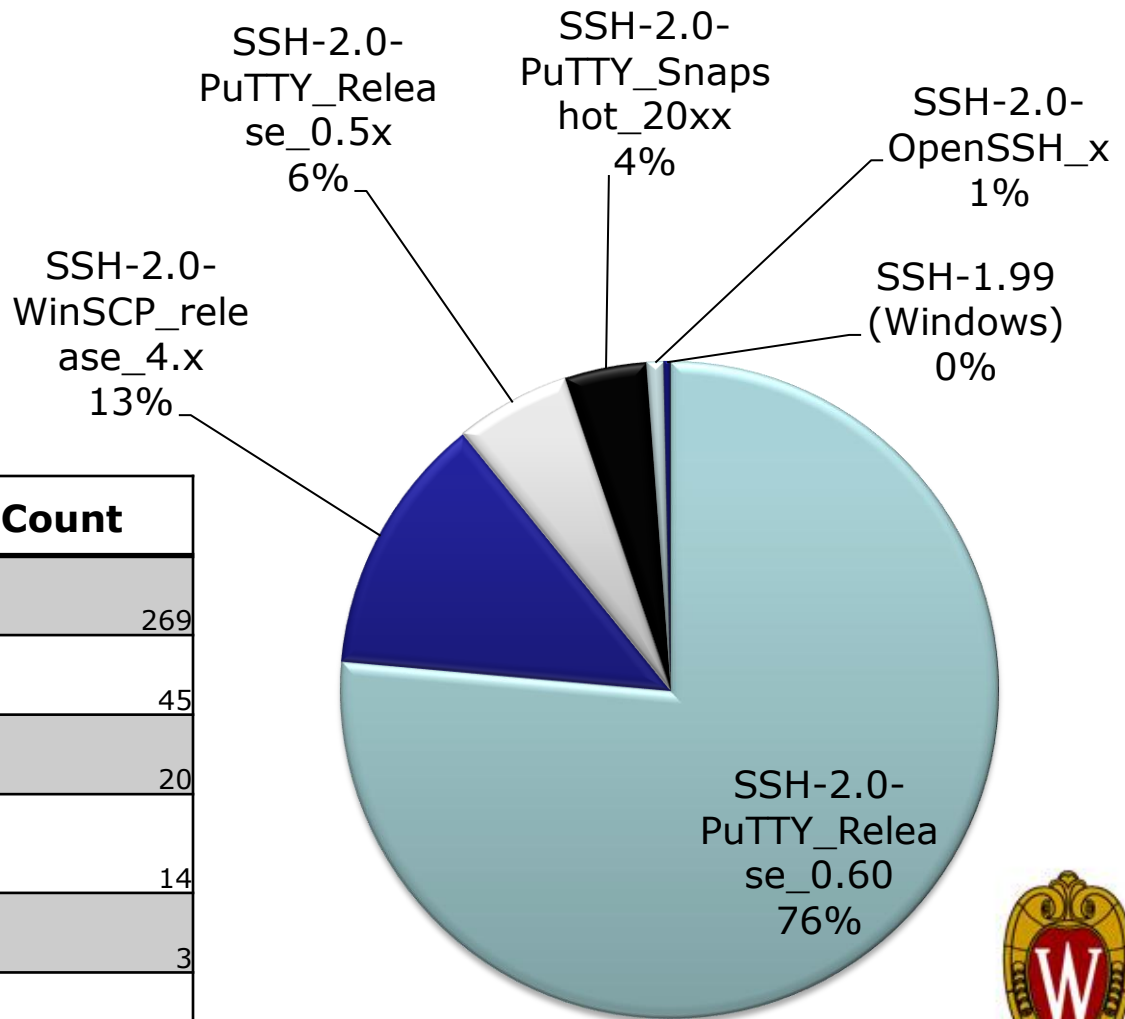
Most Common OS – All Hosts Entered Commands

OS	Count
Windows	259
Linux	27
BSD	3
Total	289



THE UNIVERSITY
of
WISCONSIN
MADISON

SSH Client Types – All Entered Commands



Client	Count
SSH-2.0-PuTTY_Release_0.60	269
SSH-2.0-WinSCP_release_4.x	45
SSH-2.0-PuTTY_Release_0.5x	20
SSH-2.0-PuTTY_Snapshot_20xx	14
SSH-2.0-OpenSSH_x	3
SSH-1.99 (Windows)	1
Total	352



What tools are these people downloading?

Downloads

799 attempted downloads

675 with data

75 W2Ksp3.exe

89 variants of psybnc

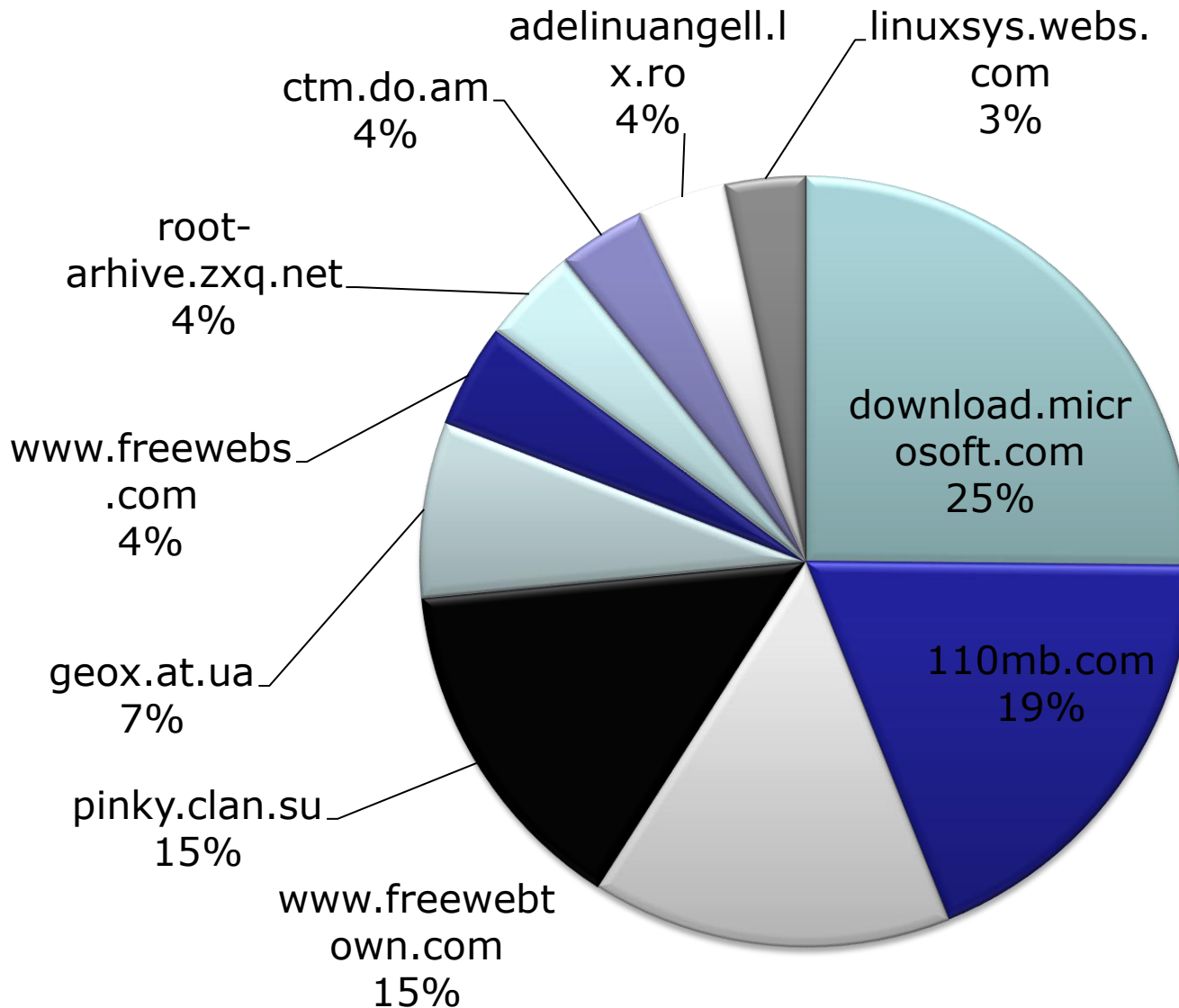
84 variants of go.sh

25 variants of udp.pl



THE UNIVERSITY
of
WISCONSIN
MADISON

Where are they getting these files from?



Where are they getting these files from?

URL	Total
download.microsoft.com	75
110mb.com	56
www.freewebtown.com	45
pinky.clan.su	43
geox.at.ua	22
www.freewebs.com	13
root-arhive.zxq.net	12
ctm.do.am	11
adelinuangell.lx.ro	11
linuxsys.webs.com	10



- Are the bots in control?
 - Probably not.
 - More often than not, IP's that brute force a login do not enter any commands on the honeypot (tend to be linux hosts – probably go.sh)
 - On the other side, IP's that enter commands typically do not have more than 2 failed login attempts. (tend to be windows and putty)



- 708 ttylogs where something interacted
 - 213 hit "DEL"
 - 136 hit "^C"
 - 234 unique hosts hit either ^C or DEL

I know at least 33% of the attacks have humans behind them.

(This is probably low)



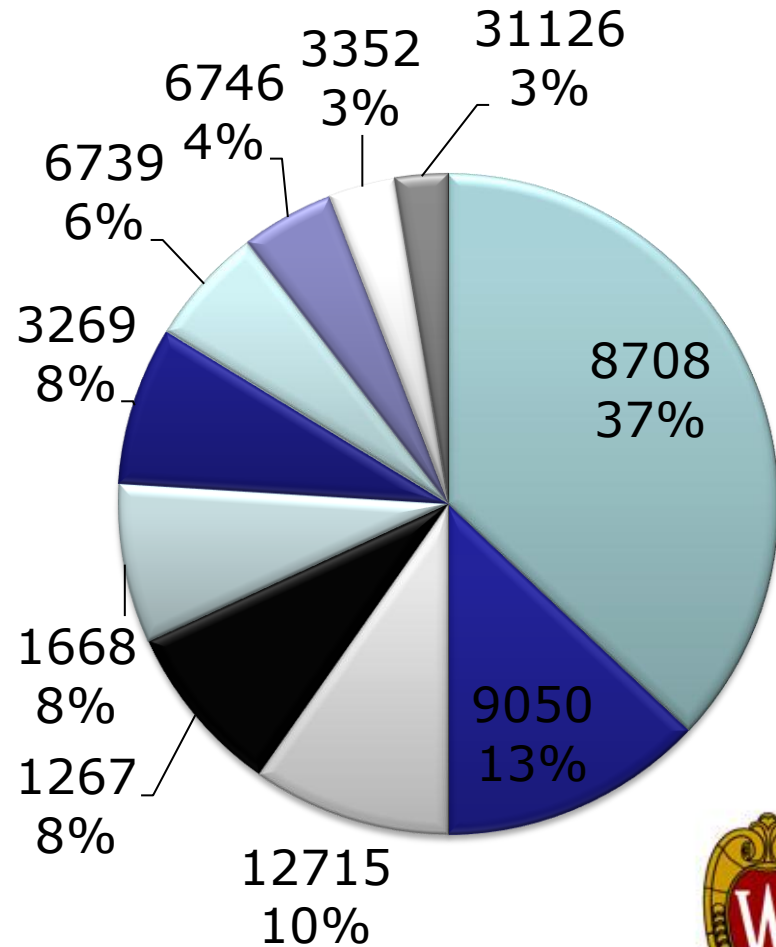
Bots don't use backspace

The “non-bots”



'non-bot' originating AS's

AS	Count
RDSNET RCS & RDS S.A. (AS 8708)	57
RTD ROMTELECOM S.A (AS 9050)	20
JAZZNET Jazz Telecom S.A. (AS 12715)	15
ASN-INFOSTRADA Infostrada S.p.A. (AS 1267)	13
AOL-ATDN AOL Transit Data Network (AS 1668)	12
ASN-IBSNAZ Telecom Italia S.p.a. (AS 3269)	12
ONO-AS Cableuropa - ONO (AS 6739)	9
ASTRAL UPC Romania Srl, Romania (AS 6746)	7
TELEFONICA-DATA-ESPANA TELEFONICA DE ESPANA (AS 3352)	5
SODETEL-AS SODETEL SAL (AS 31126)	4



'non-bot' SSH Client

SSH Client	Total
SSH-2.0-PuTTY_Release_0.60	203
SSH-2.0-PuTTY_Release_0.5x	18
SSH-2.0-PuTTY_Snapshot_20xx	9
SSH-2.0-OpenSSH_4.3	3
SSH-2.0-OpenSSH_3.9p1	1

Probable OS	Total
Windows	168
No Info	33
Linux (NAT)	23
BSD	2
Linux	2

'non-bot' Top Commands

Command	Total
ls -a	473
w	437
ls	404
uname -a	212
cat /proc/cpuinfo	149
chmod +x *	149
cd ..	137
cd /var/tmp	136
wget http://download.microsoft.com/download/win2000platform/SP/SP3/NT5/EN-US/W2Ksp3.exe	119
wget	105



**Next time you see a *nix system
download a file from microsoft.com,
take a closer look**

Thank You for Listening

“The Daves”

Dave Woutersen
&
Dave De Coster

