No Budget Threat Intelligence:

Tracking Malware Campaigns on the Cheap

Presented by:
Andrew Morris

tyvm

Thanks for being here at 10:00 am when you're all hungover

./whoami

Andrew Morris

Security Consultant at Intrepidus/iSEC
part of NCC Group

Background in Offense

Twitter - @andrew___morris
Email - andrew@morris.guru
PGP - FFB1 47C1 326E A063
Github - andrew-morris

Background - Background on threat intelligence, why you should care, previous work

Infrastructure (TL;DR) - Sensor and management. architecture, log management, ***cheap*** hosting

Discovery & Investigation - Analyzing sensor data, securing malware samples, reverse engineering

Automation - Animus system, publishing reports, mass scanning for infrastructure, publishing signatures

Defensive Thoughts - Hardening machines, leveraging data, implementing firewall rules, sharing IOCs

Roadmap

- **Background**
- Infrastructure (TL;DR)
- Discovery & Investigation
- Automation
- Defensive Strategies
- Roadmap

What are we covering today?

- Quick threat intelligence primer
- Setting up *cheap* honeypot sensors
- Examining attacks being executed on the open Internet
- Managing and aggregating data
- Locating, analyzing, and reverse engineering malware artifacts
- Emulating malware traffic
- Tracking DDOS targets
- Automating C2 discovery
- Reporting data

Threat Intelligence

INTREPIDUS GROUP
MOBILE SECURITY

the short version

Threat == bad guys

Intelligence == predicting the future

Threat + Intelligence == studying bad guys to predict what they will do (often to defend yourself)

Conventional Threat Intelligence

- Study bad guys to develop IOCs
- Deploy agents on endpoints
- Alert on anomalous behavior
  - Once is bad, but not that bad
  - Twice is REALLY bad
- And more!

but why tho

A/V is so 2005

Threat intelligence is so 2015

- Today I'm discussing bad guys that target the open Internet
- Not terribly smart
- SSH default creds, JMX console, shellshock, MS08_067 on open Internet, etc

INTREPIDUS GROUP
MOBILE SECURITY

Not talking about these guys

INTREPIDUS GROUP
MOBILE SECURITY

Today, we're mostly talking about these guys

- Background
- **Infrastructure (TL;DR)**
- Discovery & Investigation
- Automation
- Defensive Strategies
- Roadmap

Honeypots

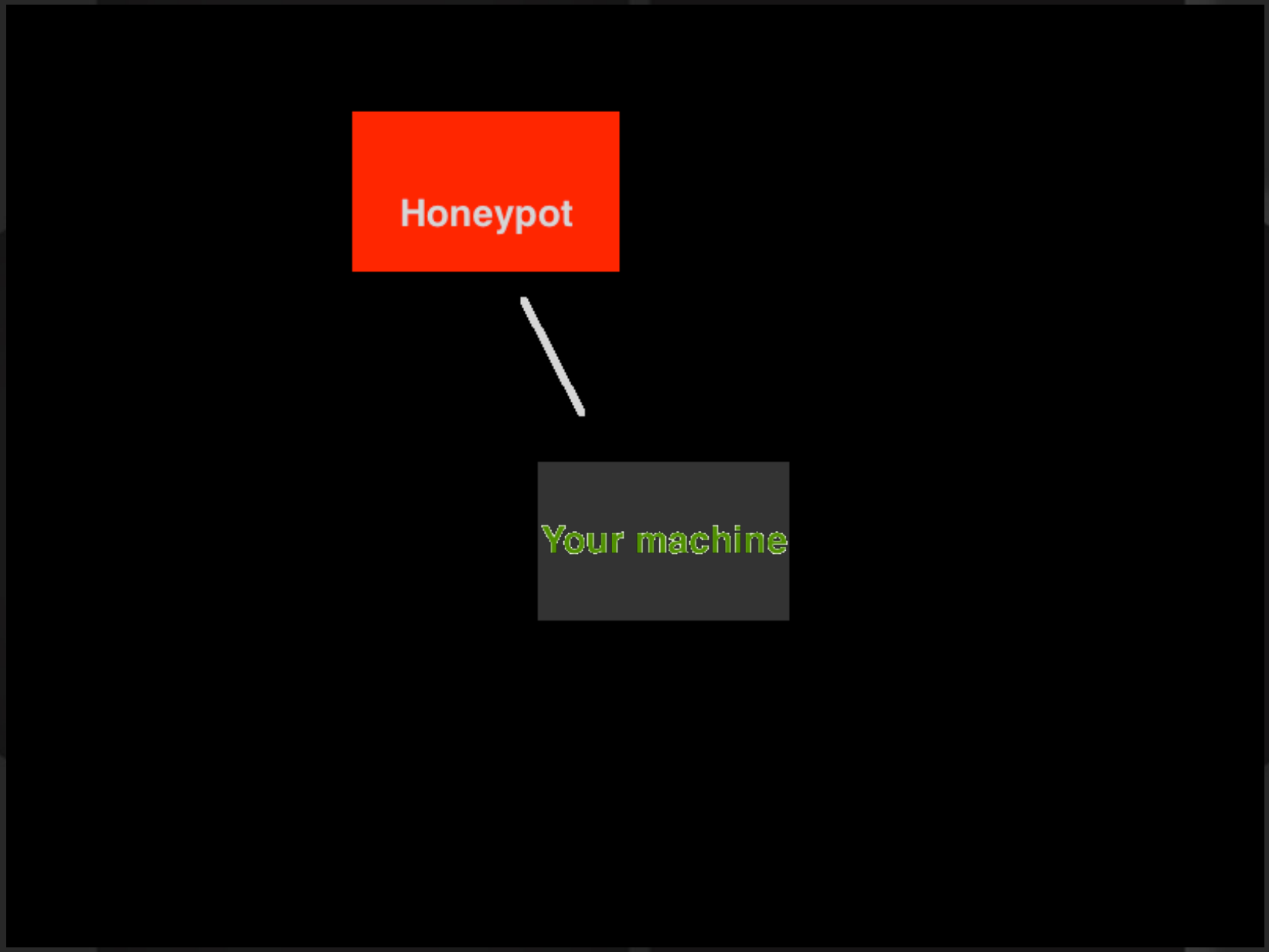
tl;dr

Infrastructure

- I set up lots of cheap honeypots
  - Mostly Kippo
  - Some Dionaea
  - Empty Apache server
- Centrally manage/aggregate data
  - MHN (managed honey network)
- Cheap hosting
  - Cloud at Cost
  - AWS free tier

Kippo

- I use lots of Kippo
- Medium-interaction SSH honeypot
- Logs bad guy terminal sessions for playback
- Can configure which credentials you want to allow
- Logs username, password, source IP address, SSH library version, commands executed, etc
- Hooks fake wget command to download malware samples
- Unrelated- I wrote a Metasploit module which identifies Kippo instances externally



No budget architectural diagrams

MHN

- Managed Honey Network
- Developed by Threatstream
- Developer is awesome for answering all of my dumb ass questions
- Open source
- Allows you to deploy honeypots easily
- Aggregate data
- API is awesome (but undocumented)
- Mnemosyne is also awesome

Attack Stats

Attacks in the last 24 hours: **74,668**

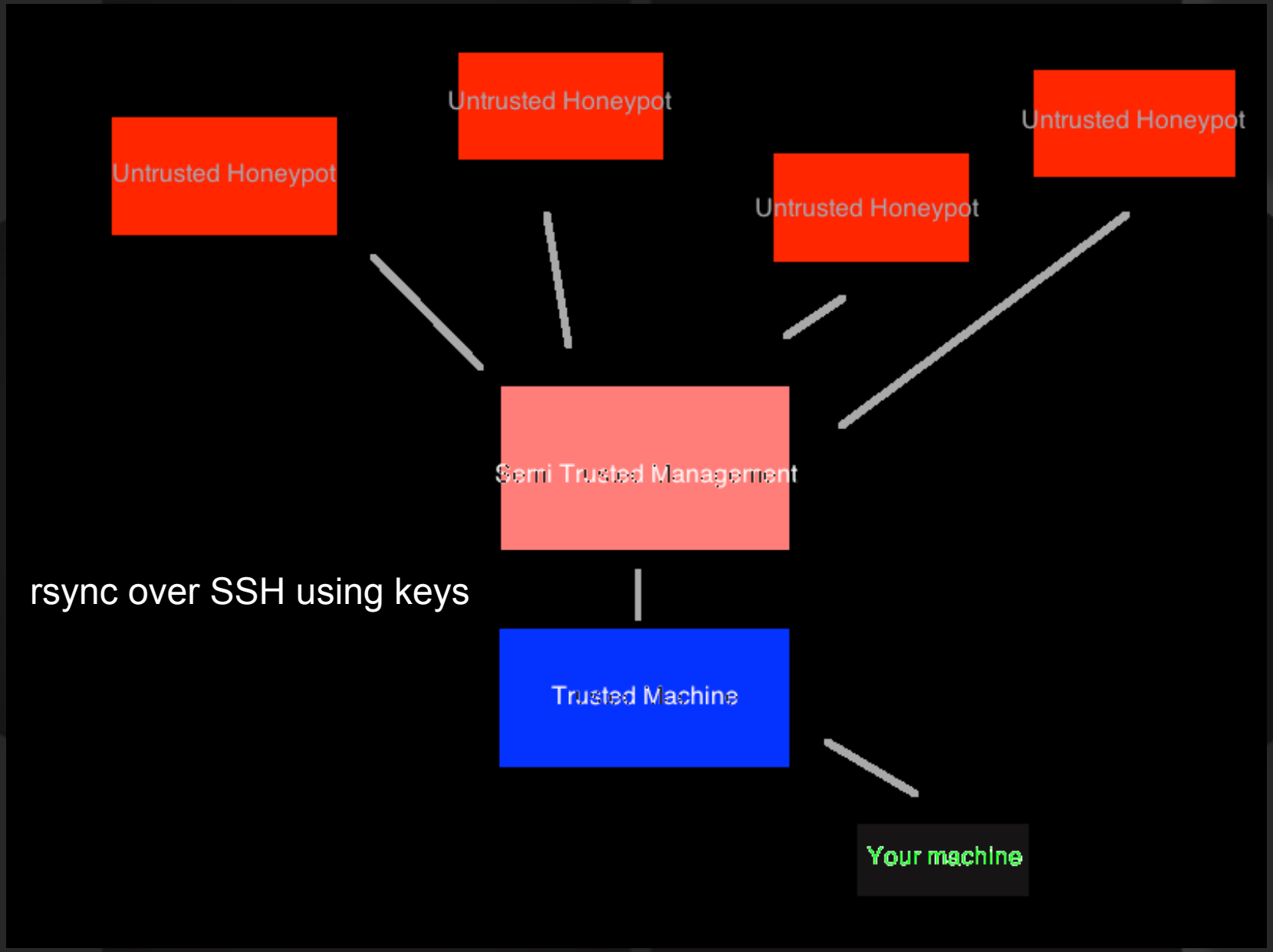
TOP 5 Attacker IPs:

1. ? **103.41.124.46 (27,433 attacks)**
2. ? **103.41.124.12 (19,255 attacks)**
3. ? **103.41.124.27 (12,026 attacks)**
4. ? **103.41.124.35 (5,543 attacks)**
5. ? **103.41.124.38 (5,387 attacks)**

TOP 5 Attacked ports:

MHN (cont'd)

- Quick gotcha:
  - MHN has deploy scripts
    - Update them to have more stuff, add SSH public keys, update system, install packages, change password, set hostname
  - MHN pulls from threatstream forks of popular Github repos by default
    - Consider forking your own repos
  - Maintain "safe lists" to # grep -v later



No budget architectural diagrams

See other talk for more info

"Ballin on a Budget" at BSides Charleston for more info on infrastructure

- Background
- Infrastructure (TL;DR)
- **Discovery & Investigation**
- Automation
- Defensive Strategies
- Roadmap

Shellshock

- Grep Apache logs for the standard shellshock characters

  () { :;};

- Discovered several groups that are still using shellshock to propagate

SSH

- Bad guys attempt *lots* of passwords
- There's a group in Hong Kong that I've seen over 100,000 authentication attempts per day from

  103.41.124.0/24
- Usually automated scripts
- On successful login, the script will run "uname -a" and wget a malware sample based on system version

SSH data

```
24836 root
22520 admin
 6755 123456
 5808
 5637 password
 5334 1234
 5273 12345
 5057 12345678
 4998 toor
 4987 1234567890
 4965 123qwe!@#
 4856 admin123
 4820 root123
 4797 123123
 4747 1qaz2wsx
 4727 qwe123
 4702 qweasd
 4678 P@ssw0rd
 4669 -
 4636 142536
 4632 passw0rd
 4629 root@123
 4605 666666
 4580 123456789
 4547 cisco
 4544 2wsx3edc
 4500 manager
 4492 rootme
 4485 data
 4469 zaq12wsx
```

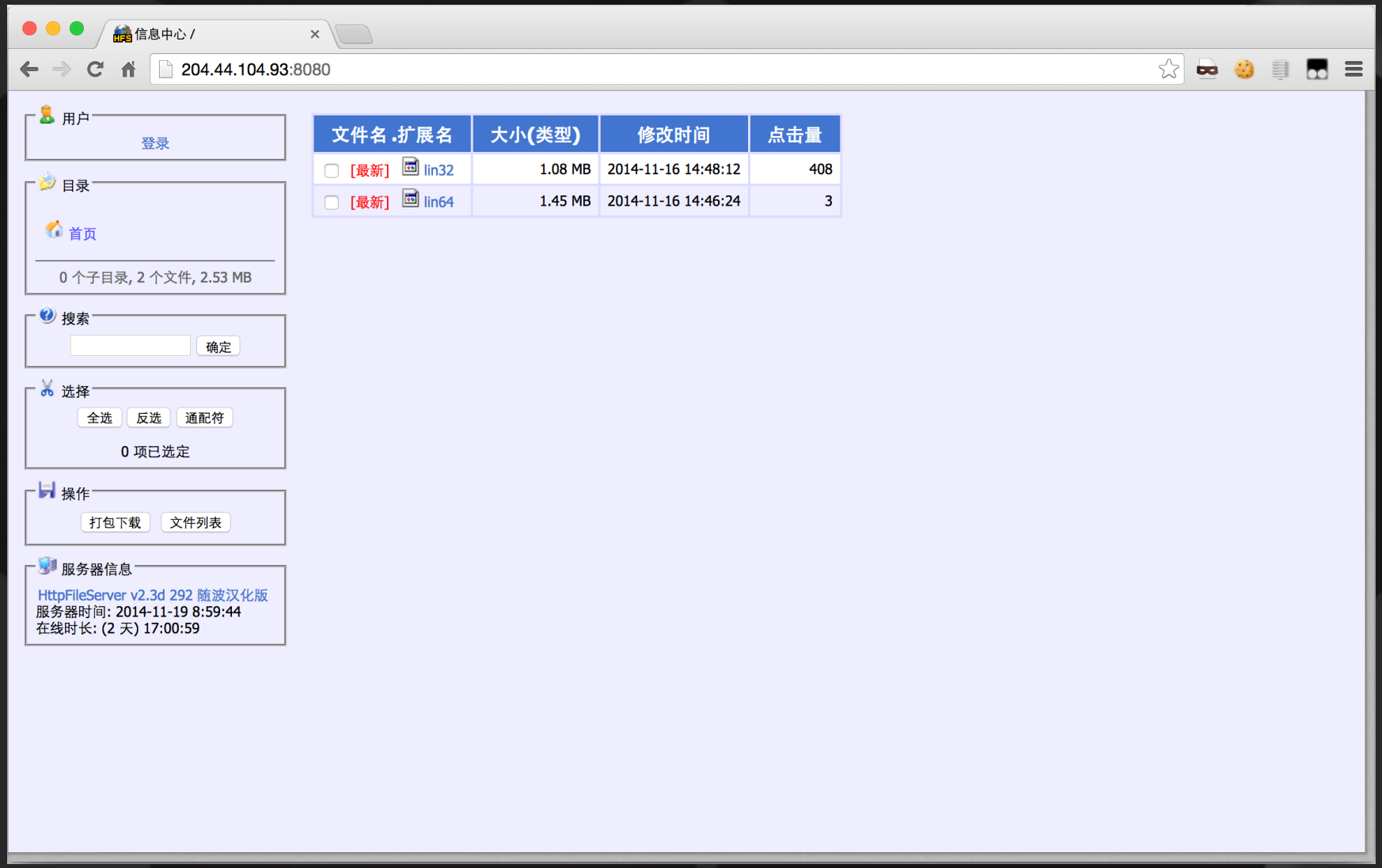
56 lines (55 sloc) | 1.716 kb

```
1593773 SSH-2.0-PUTTY
  76524 SSH-2.0-libssh2_1.4.2
  32160 SSH-2.0-libssh2_1.4.3
  17606 SSH-2.0-PuTTY_Release_0.63
  10789 SSH-2.0-libssh2_1.4.1
   4040 SSH-2.0-PuTTY_Release_0.63cn
   3596 SSH-2.0-JSCH-0.1.51
   1634 SSH-2.0-PuTTY_Release_0.63cn3
    459 SSH-2.0-Granados-1.0
    407 SSH-2.0-paramiko_1.8.1
    223 SSH-2.0-paramiko_1.7.5
    214 SSH-2.0-libssh2_1.0
    165 SSH-2.0-PuTTY_Release_0.62
    164 SSH-2.0-OpenSSH_5.2
    157 SSH-2.0-OpenSSH_6.2
    125 SSH-2.0-dropbear_0.47
     91 SSH-2.0-1.91
     55 SSH-2.0-paramiko_1.15.1
     49 SSH-2.0-libssh2_1.4.0
     36 SSH-1.99-3.2.9
     32 SSH-2.0-libssh2_1.2.8
     30 SSH-2.0-paramiko_1.14.0
     24 SSH-2.0-Pipls-1.0
     24 SSH-2.0-Erlang
     22 SSH-2.0-JSCH-0.1.44
     21 SSH-2.0-Go
     18 SSH-2.0-WinSCP_release_5.5.4
     18 SSH-2.0-OpenSSH_6.6.1p1
     17 SSH-2.0-PuTTY_Local:_May_14_2009_21:12:18
```

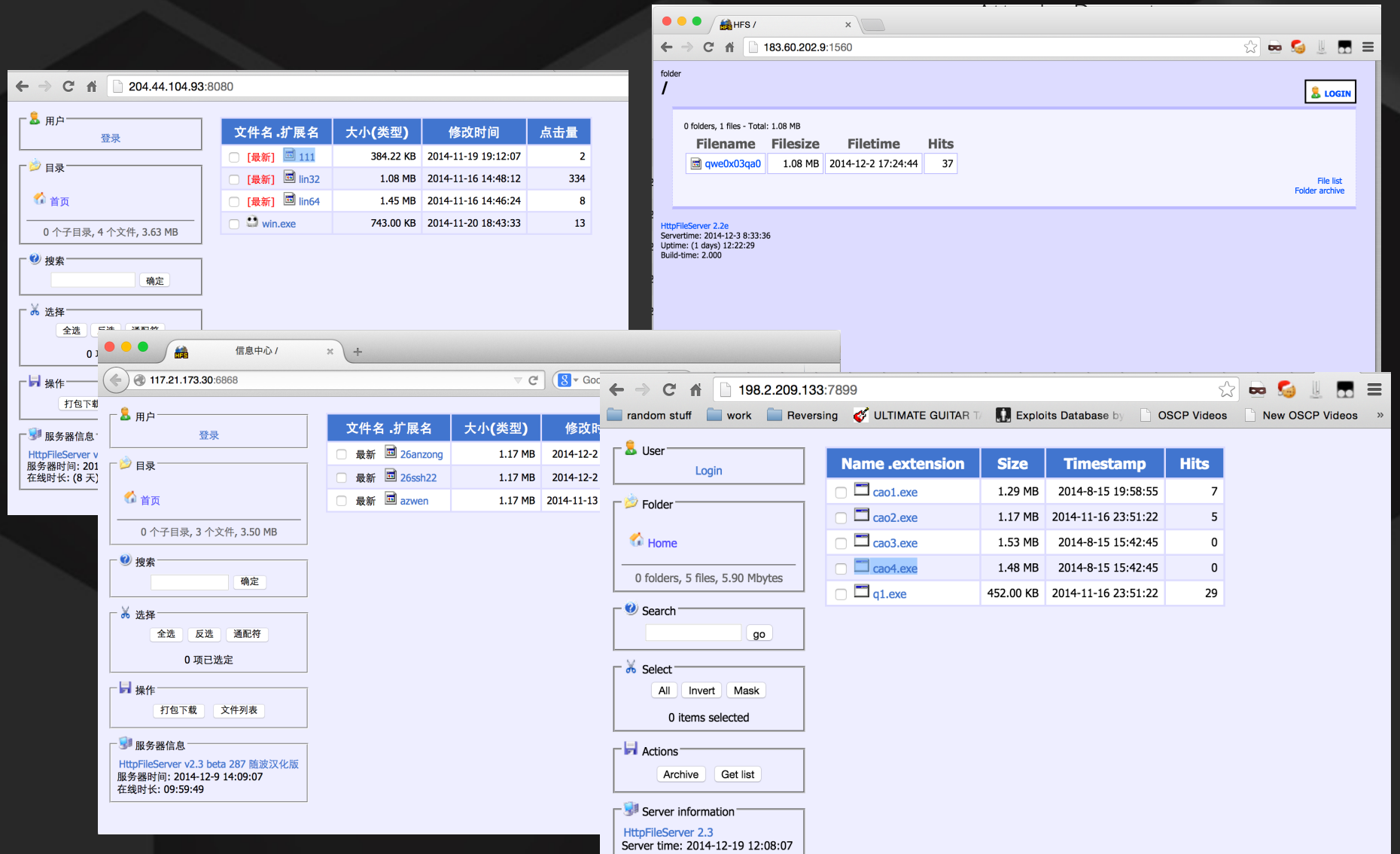
SSH gotchas

- Bad guys love using SFTP
- Kippo doesn't include SFTP by default
- Someone wrote a patch for it
- Couple gotchas, but I implemented it in a fork on my Github
  - https://github.com/andrew-morris/kippo
- Added SFTP patch, added option to disable fake jail, added some more default creds, disabled wget port 80 restriction

Couple groups love HFS



Couple groups love HFS



No budget tactics

- Google dork for these web servers
- intext:”httpfileserver”
- If you feel like grotesquely violating the law, most versions of HFS are vulnerable to an RCE bug
  - http://www.exploit-db.com/exploits/34668/

Reversing samples

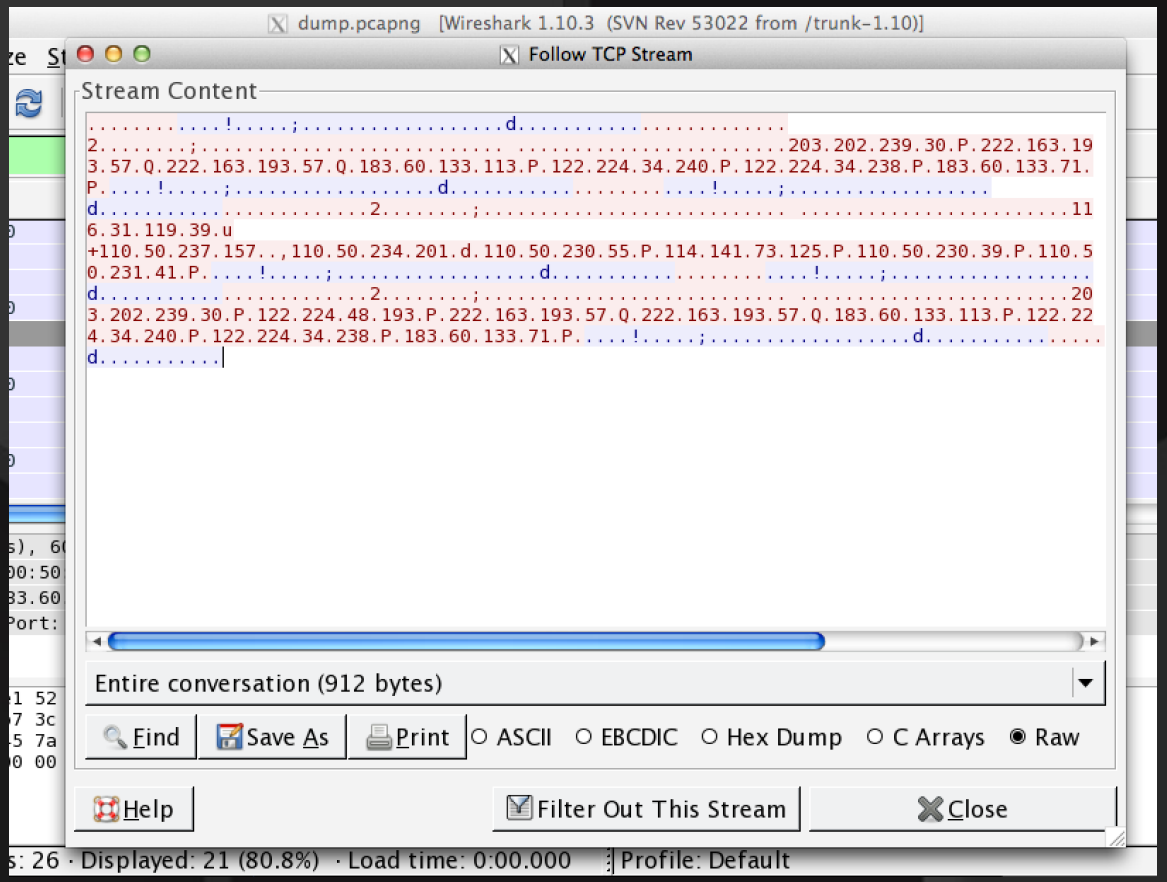
- Talk in itself
- I'm not the best reverser so don't listen to anything I say
- If you're also bad at reversing:
  - Malwr - malwr.com
  - VirusTotal - virustotal.com

Reversing samples (cont'd)

- I was getting hit a lot by one particular IP address
- Once they guessed a good password, logged in a wgot a malware sample
- Same web server they were grabbing from had directory traversal enabled (which happens all the time)
- Found a bunch of Windows samples as well

Reversing samples (cont'd)

- Passing tons of IP addresses over some custom binary protocol over port 36000



Reversing samples (cont'd)

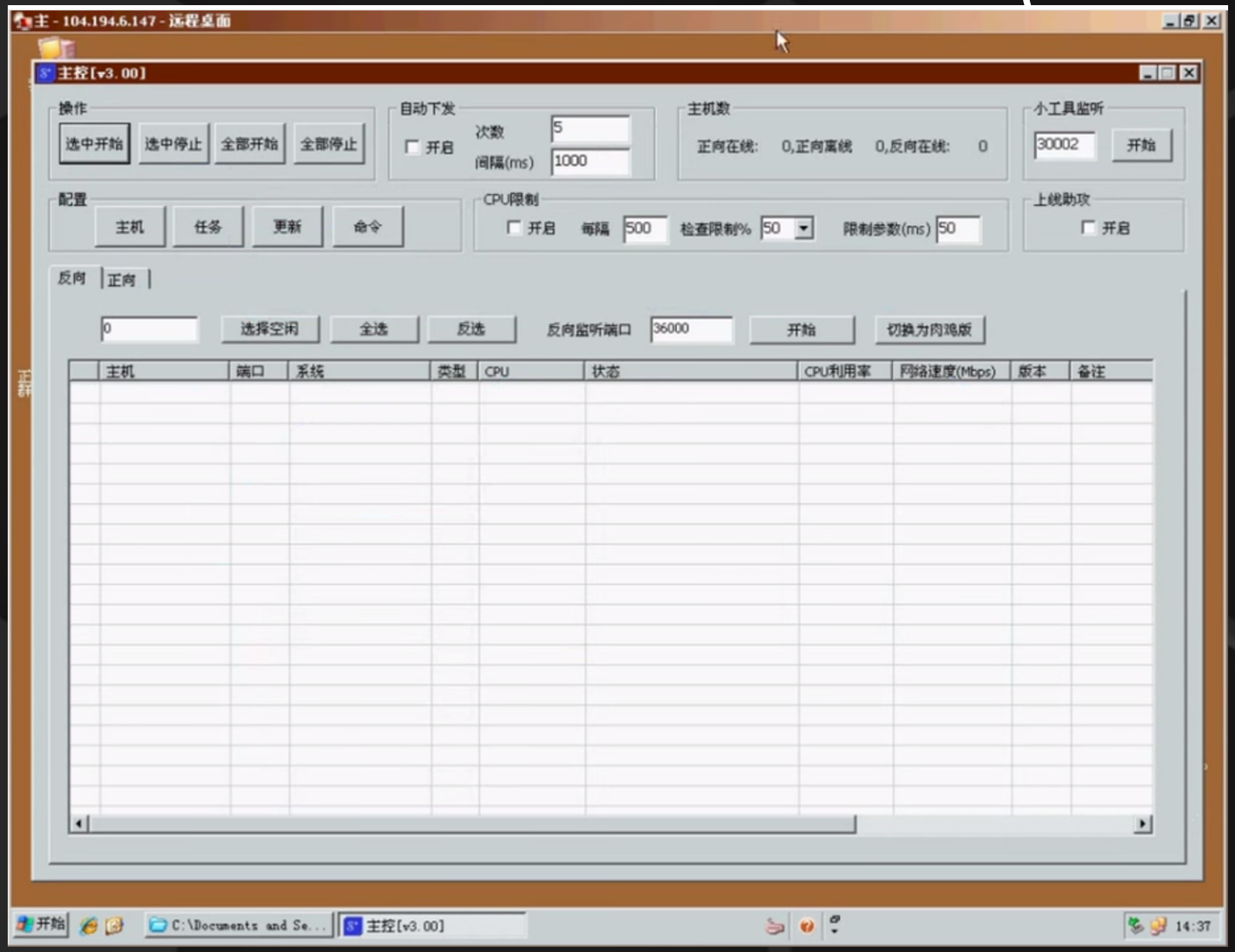
- These IP addresses were DDOS targets
- The C2 was architected to pass IP addresses to all bots
- Bots receive IP addresses and start spraying traffic at them

Shoutout

#MalwareMustDie

Reversing samples (cont'd)

- I stumbled across this…




主 - 104.194.6.147 - 远程桌面
主控[v3.00]
操作
选中开始
选中停止
全部开始
全部停止
自动下发
开启
次数
5
间隔(ms)
1000
主机数
正向在线:
0,正向离线
0,反向在
配置
主机
任务
更新
命令
CPU限制
开启
每隔
500
检查限制%
50
限制参数(ms)
反向
正向
0
选择空闲
全选
反选
反向监听端口
36000
开始
主机
端口
系统
类型
CPU
状态
CPU利用率

Chuilang C2 Scanner

- I realized the C2 was one of many C2s
- I fingerprinted the C2 network service and wrote a scanner
  - Including an Nmap NSE script
- I also stared at Wireshark for what felt like an eternity and wrote a script that connects to the C2, speaks the same custom binary language as the C2, and logs all of the DDOS targets

Chuilang C2 Scanner Gotchas

- Turns out it's really hard to write a client for a server that you can't control, with no source code
- Had to cycle through a few different C2s since they'd go up and down
- Like trying to learn Spanish by being in the same room as two Spanish people as they speak to each other in Spanish
- Then they keep leaving the room and you have to find more Spanish people

Chuilang C2 Scanner

```
[+] Connecting to host...
[+]                     Initial Response
================================================================================
00000000: 08 00 00 00 0C 00 00 00  00 00 00 00 00 00 00 00  ................
00000010: E8 FD 00 00                                      ....
None
================================================================================
[+] Sending initial heartbeat...
[+] Response received
[+] 010000001c010000
[+] Sending response...
[+] Waiting for response...
[+]                     Response
================================================================================
00000000: 00 F4 01 00 00 32 00 00  00 E8 03 00 00 73 DF 03  .....2.......s..
00000010: 00 00 00 00 00 01 00 00  00 01 00 00 00 10 02 00  ................
00000020: D0 07 00 00 00 00 01 00  00 00 20 00 00 00 04 00  .......... .....
00000030: 00 00 04 00 00 01 00 00  00 1E 00 00 00 00 00 0E  ................
00000040: 00 00 00 31 30 33 2E 32  35 32 2E 32 34 34 2E 32  ...103.252.244.2
00000050: 34 32 00 50 00 31 39 30  2E 31 31 35 2E 32 36 2E  42.P.190.115.26.
00000060: 32 33 30 00 50 00 31 39  32 2E 39 39 2E 39 36 2E  230.P.192.99.96.
00000070: 32 30 36 00 50 00 31 39  32 2E 39 39 2E 39 36 2E  206.P.192.99.96.
00000080: 32 30 36 00 50 00 31 39  32 2E 39 39 2E 39 36 2E  206.P.192.99.96.
00000090: 32 30 36 00 50 00 31 39  32 2E 39 39 2E 39 36 2E  206.P.192.99.96.
000000A0: 32 30 36 00 50 00 31 39  32 2E 39 39 2E 39 36 2E  206.P.192.99.96.
000000B0: 32 30 36 00 50 00 31 36  32 2E 32 31 38 2E 33 31  206.P.162.218.31
000000C0: 2E 31 33 34 00 50 00 31  39 39 2E 38 33 2E 31 32  .134.P.199.83.12
000000D0: 39 2E 32 00 50 00 32 37  2E 35 30 2E 32 2E 31 34  9.2.P.27.50.2.14
000000E0: 30 00 50 00 32 37 2E 35  30 2E 32 2E 31 34 30 00  0.P.27.50.2.140.
000000F0: 50 00 32 37 2E 35 30 2E  32 2E 31 33 31 00 50 00  P.27.50.2.131.P.
00000100: 32 37 2E 35 30 2E 32 2E  31 33 31 00 50 00 32 37  27.50.2.131.P.27
00000110: 2E 35 30 2E 32 2E 31 33  31 00 50 00              .50.2.131.P.
None
================================================================================
```

- Background
- Infrastructure (TL;DR)
- Discovery & Investigation
- **Automation**
- Defensive Strategies
- Roadmap

Animus

Automated Threat Reporting System

Animus Threat Reports

- Github page that publishes sensor data daily
  - https://github.com/animus-project
- Currently only publishes SSH threat reports
- Currently includes the following:
  - Attacker IP addresses
  - Credentials being attempted
  - SSH library versions

Animus SSH Threat Report

This is the daily threat report generated by the Animus system on January 17, 2015. This data was collected by various SSH honeypot sensors around the Internet and published by a bot.

Text files containing a full list of today's usernames, passwords, attacker IP addresses, and SSH library versions are available above for download.

As always, don't hesitate to reach out via Twitter or Email if you have any questions or feedback.

blog | twitter | email
FFB1 47C1 326E A063

Summary

Date: January 17, 2015
Total attacks today: 252983

IP addresses

The following are the top 10 attacker IP addresses today, including the frequency of usage:

```
81688 103.41.124.46
57294 103.41.124.12
29149 103.41.124.66
24736 103.41.124.17
16379 103.41.124.35
15864 103.41.124.38
 7082 103.41.124.26
 3420 103.41.124.36
```

INTREPIDUS GROUP
MOBILE SECURITY

5561	95.110.255.254
5562	95.140.125.65
5563	95.142.165.200
5564	95.163.121.234
5565	95.173.185.166
5566	95.173.186.136
5567	95.173.186.166
5568	98.126.135.138
5569	98.126.44.210
5570	98.126.52.114
5571	98.126.68.194
5572	98.25.53.159
5573	98.25.53.46

Pushing threat report for 2015-01-17

threatbot authored 4 hours ago

..

2014-10-09	adding initial data
2014-10-10	adding initial data
2014-10-11	adding initial data
2014-10-12	adding initial data
2014-10-13	adding initial data
2014-10-14	adding initial data
2014-10-15	adding initial data
2014-10-16	adding initial data
2014-10-17	adding initial data
2014-10-18	adding initial data
2014-10-19	adding initial data
2014-10-20	adding initial data
2014-10-21	adding initial data
2014-10-22	adding initial data
2014-10-23	adding initial data
2014-10-24	adding initial data

unrelated fun fact about Github

- Github actually trusts the client's clock
- You can commit changes that happened "in the past" by changing your system time
- ~*~*~*~ the more you know ~*~*~*~

Animus Threat Reports (con'd)

- Animus is constantly mass-scanning the Internet to locate Chuilang C2s
- Once a C2 is located, it will connect to it and start logging DDOS targets, maintained in real time
- Published an alpha NSE script for Chuilang C2s
  - https://github.com/andrew-morris/chuilang-c2-detect

Threatbot

- Tweet to @threatbot on Twitter with one or more IP addresses
- He'll tweet back if that IP address has ever conducted any attacks that I've seen
- Tweet includes number of attacks we've seen from the host, the date of the first attack, and the date of the most recent attack
- Threatbot also tweets daily statistics of how many attacks we've seen and the IP address of today's top attacker IP address

INTREPIDUS GROUP
MOBILE SECURITY

Animus Threat Bot
@threatbot

Following

Total SSH attacks today: 252983
Top attacker IP today: 103.41.124.46
Today's report at github.com/animus-project
...

Andrew Morris @Andrew___Morris · Jan 14
@threatbot 103.41.124.111

Animus Threat Bot
@threatbot

Following

@Andrew___Morris
Number of attacks from 103.41.124.111: 19399
First attack: Jan 2, 2015
Most recent attack: Jan 14, 2015

1:13 PM - 14 Jan 2015

- Background
- Infrastructure (TL;DR)
- Discovery & Investigation
- Automation
- **Defensive Strategies**
- Roadmap

Defensive Strategies

- Check for connections to (or block) known C2s
- Flag connections to known-malicious subnets
- Look for connections to malware distribution web servers
- Presence of files with md5s or yara signatures that match known bad

Defending against attacks on SSH

- This is really easy
- Use SSH keys, disable password authentication
- If this is not possible for whatever reason, use strong passwords, audit against the wordlists I provide with JTR
- Even load up the wordlists bad guys are using and blast your network with Medusa/Hydra

- Background
- Infrastructure (TL;DR)
- Discovery & Investigation
- Automation
- Defensive Strategies
- **Roadmap**

Recap

sensors > attacks > malware samples > ddos target leak > mass scan

Stats (SSH)

- Total auth attempts:
  - 6,279,676
- Total unique attacker IPs:
  - 5,573
- Total unique passwords:
  - 538,512
- Total unique C2s identified:
  - 30
- Total unique malware samples:
  - 27
- Total DDOS targets:
  - 750 IPs belonging to over 40 organizations (in one month)

INTREPIDUS GROUP
MOBILE SECURITY

Future plans

- Build more signatures to identify different C2s
- Expand Threatbot's capability
- Deploy more sensors
- Build automation for warning that a DDOS attack is coming
- Expand shellshock, heartbleed, other attack capabilities
- Build HFS web server watch script
- Improve mass scanning / dorking for HFS
- Automate signature generation
- Build more useful information into Animus threat reports
- SO MUCH MORE DATA TO COLLECT

Credit

- Threatstream / Jason Trost
- Kippo developers
- HD Moore
- Brian Baskin
- Johnny Vestergaard
- @MalwareMustDie
- Rob Blody
- Shmoocon
- Linode abuse team
- Michel Oosterhof - Authored SFTP patches (and more)

Questions?

Thank you!

Andrew Morris

Twitter - @andrew___morris

Email - andrew@morris.guru

PGP Fingerprint - FFB1 47C1 326E A063

Github - https://github.com/andrew-morris

Gtalk - morr.drew