PAY NO ATTENTION TO THAT HACKER BEHIND THE CURTAIN:

A LOOK INSIDE THE BLACK HAT NETWORK

Neil R. Wyler

Bart Stump

@grifter801
@theStump3r

Black Hat USA 2016

Introductions

- **Neil Wyler**
  - 14 years at Black Hat
  - By day – Threat Hunting and IR Specialist @ RSA
  - Black Hat Review Board and Training Review Board
  - DEF CON Review Board
  - DEF CON Department Lead
  - 801 Labs Board Member

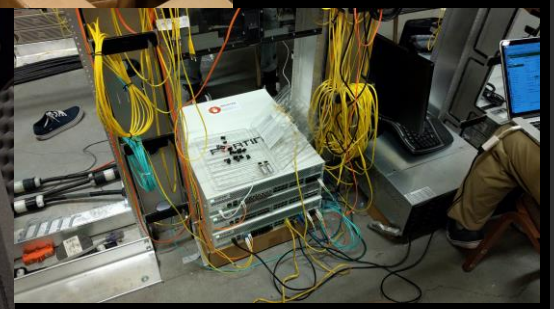
- **Bart Stump**
  - 9 years at Black Hat
  - By day – SE @ Optiv
  - Black Hat Training Review Board
  - DEF CON Goon
  - 801 Labs Board Member

@grifter801
@theStump3r

Then

@grifter801
@theStump3r

Now



@grifter801
@theStump3r

Now

@grifter801
@theStump3r

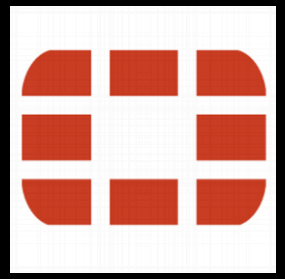
The NOC Team

- 2 Idiots
- 21 Industry Professionals
- Covering multiple states/countries
- All on vacation!

@grifter801
@theStump3r

The Extended Team

- Fortinet
- RSA
- Ruckus
- Century Link



RSA

Ruckus™ WIRELESS

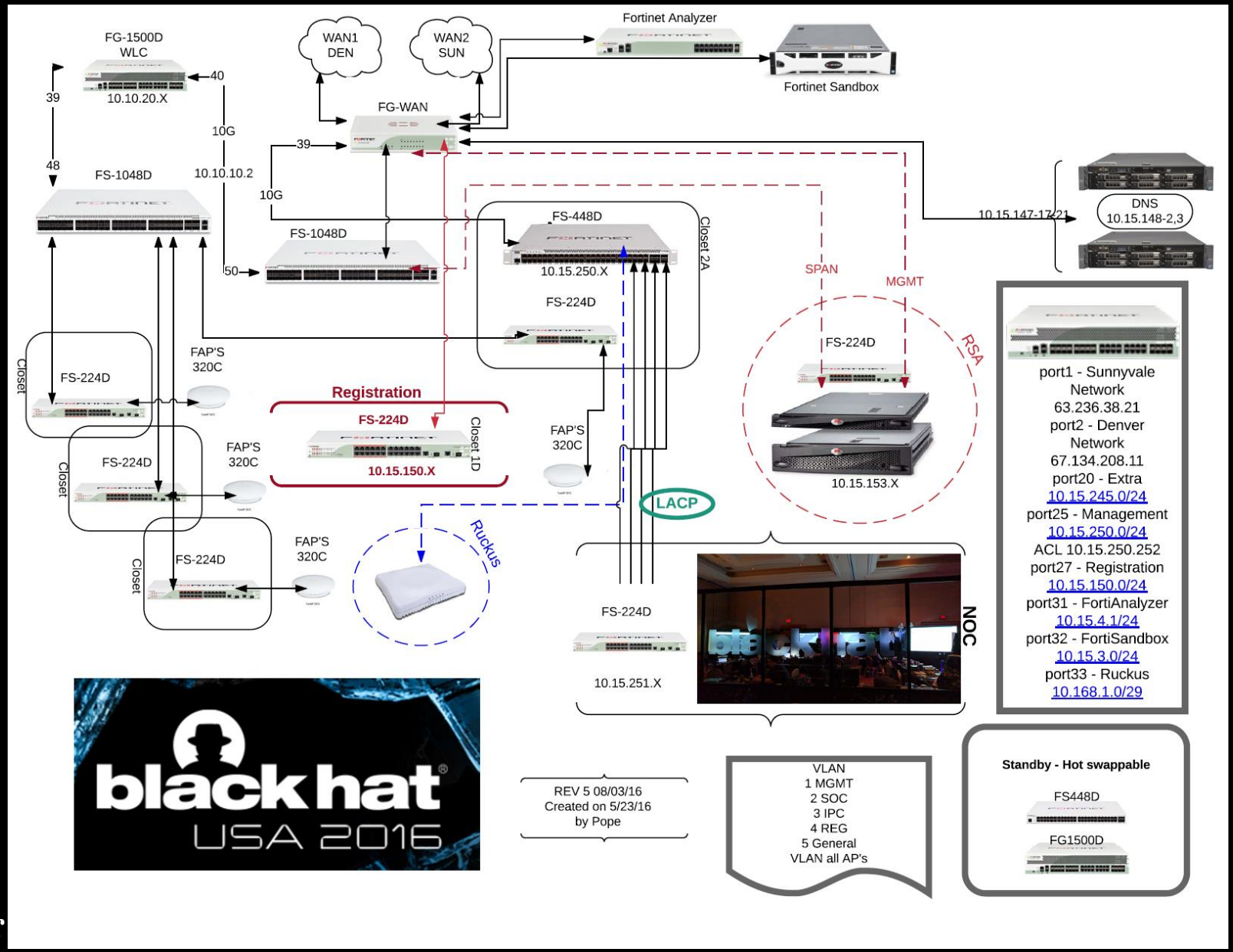
CenturyLink™

@grifter801
@theStump3r

Equipment

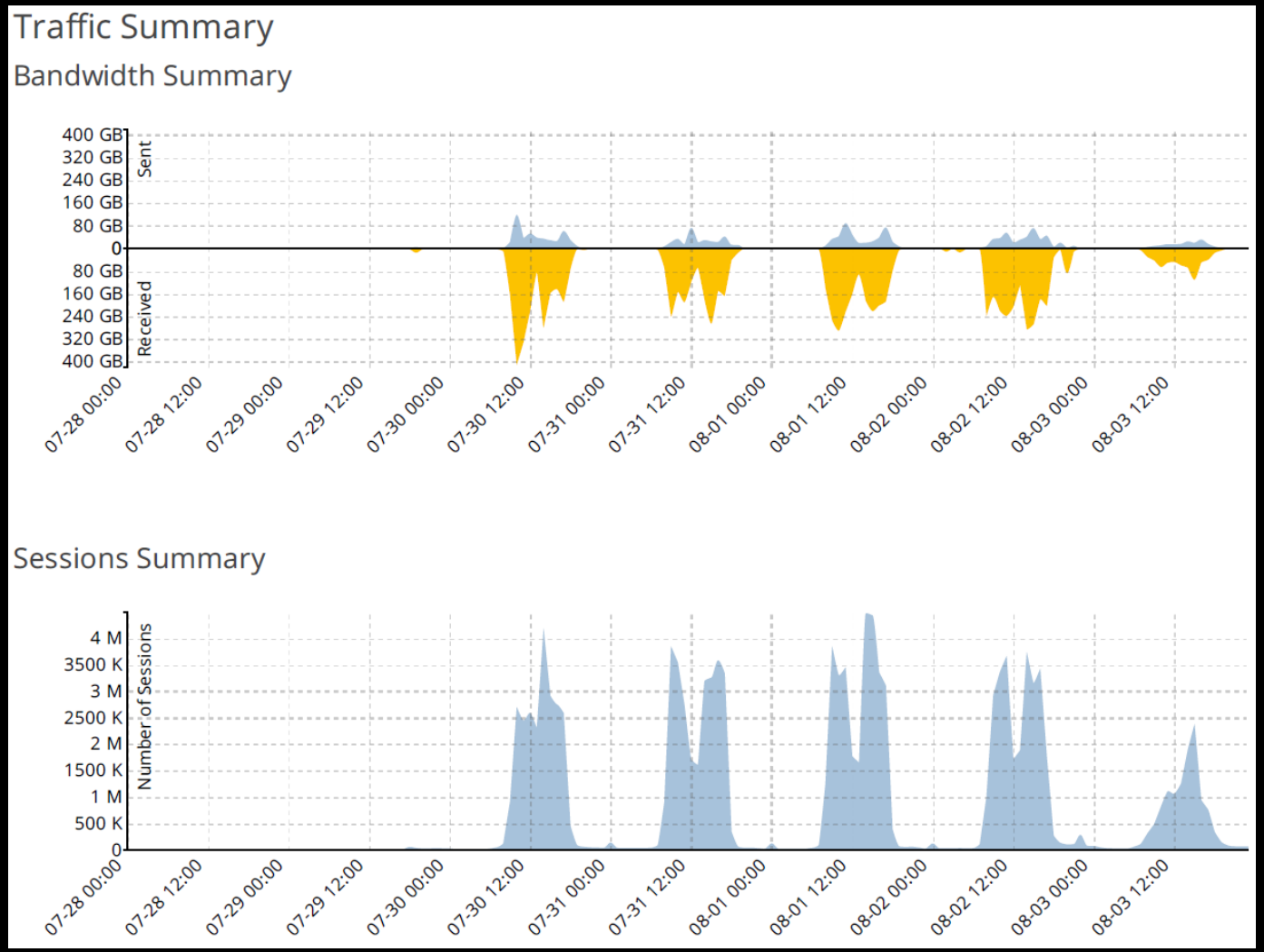
- RSA
  - 2 Analytics Servers
  - 1 Packet Decoder
  - 1 Hybrid for Packets
  - 1 Hybrid for Logs
  - 1 Packets Concentrator
  - 1 Event Stream Analysis
  - 1 Head Unit for Malware
  - ~80 TB of Storage
- Ruckus
  - 125 AP's
  - 20 Brocade Switches
  - 2 RG Nets Servers
  - 2 AP Controllers
- Fortinet
  - 3 1500D's
  - 27 224D Switches
  - 2 448D Switches
  - 2 1048D Switches
  - ~100 320B FortiAP's
  - 1 FortiSandbox
  - 1 FortiSiem
  - 1FortiManager
- Black Hat
  - Thousands of CAT5 cables
  - Hundreds of power strips
  - 4 Intel NUC's
  - 8 raspberry pi's

Network



@grifter801
@theStump3r

Traffic Summary



@grifter801
@theStump3r

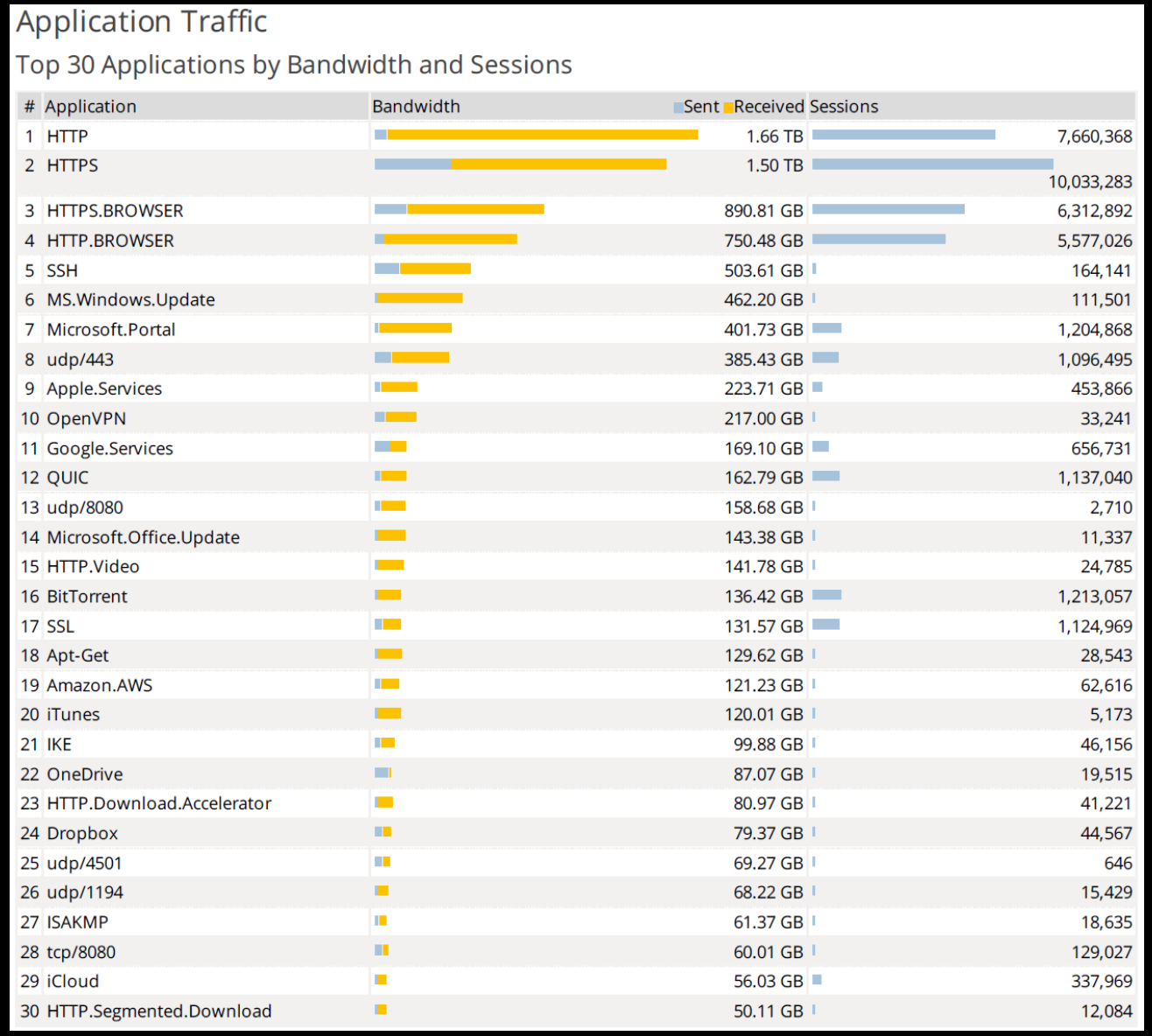
General Network Stats

Traffic Statistics

#	Summary	Statistics
1	Total Sessions	125,840,893
2	Total Bytes Transferred	10,505.74GB
3	Most Active Date By Sessions	2016-08-01
4	Total Users	16,118
5	Total Applications	193,481
6	Total Destinations	716,508
7	Average Sessions Per Day	17,977,270
8	Average Bytes Per Day	1,500.82GB

@grifter801
@theStump3r

Top Applications



Application Traffic

Top 30 Applications by Bandwidth and Sessions

#	Application	Bandwidth	Sent	Received	Sessions
1	HTTP			1.66 TB	7,660,368
2	HTTPS			1.50 TB	10,033,283
3	HTTPS.BROWSER			890.81 GB	6,312,892
4	HTTP.BROWSER			750.48 GB	5,577,026
5	SSH			503.61 GB	164,141
6	MS.Windows.Update			462.20 GB	111,501
7	Microsoft.Portal			401.73 GB	1,204,868
8	udp/443			385.43 GB	1,096,495
9	Apple.Services			223.71 GB	453,866
10	OpenVPN			217.00 GB	33,241
11	Google.Services			169.10 GB	656,731
12	QUIC			162.79 GB	1,137,040
13	udp/8080			158.68 GB	2,710
14	Microsoft.Office.Update			143.38 GB	11,337
15	HTTP.Video			141.78 GB	24,785
16	BitTorrent			136.42 GB	1,213,057
17	SSL			131.57 GB	1,124,969
18	Apt-Get			129.62 GB	28,543
19	Amazon.AWS			121.23 GB	62,616
20	iTunes			120.01 GB	5,173
21	IKE			99.88 GB	46,156
22	OneDrive			87.07 GB	19,515
23	HTTP.Download.Accelerator			80.97 GB	41,221
24	Dropbox			79.37 GB	44,567
25	udp/4501			69.27 GB	646
26	udp/1194			68.22 GB	15,429
27	ISAKMP			61.37 GB	18,635
28	tcp/8080			60.01 GB	129,027
29	iCloud			56.03 GB	337,969
30	HTTP.Segmented.Download			50.11 GB	12,084

@grifter801
@theStump3r

Net Statistics

Max Packet Capture Rate	**~1Gbps**
Total Packets Captured *Trainings* *Conference Wifi*	**~10 Terabytes** *~9TB* *~1TB*
Network Sessions	**~125,000,000**
Total Logs Captured	**160,000,000**
Number of unique network protocols/service	**43**
Non-standard traffic (non HTTP via 80, non DNS via 53, etc.)	**1.5M sessions (~60GB)**

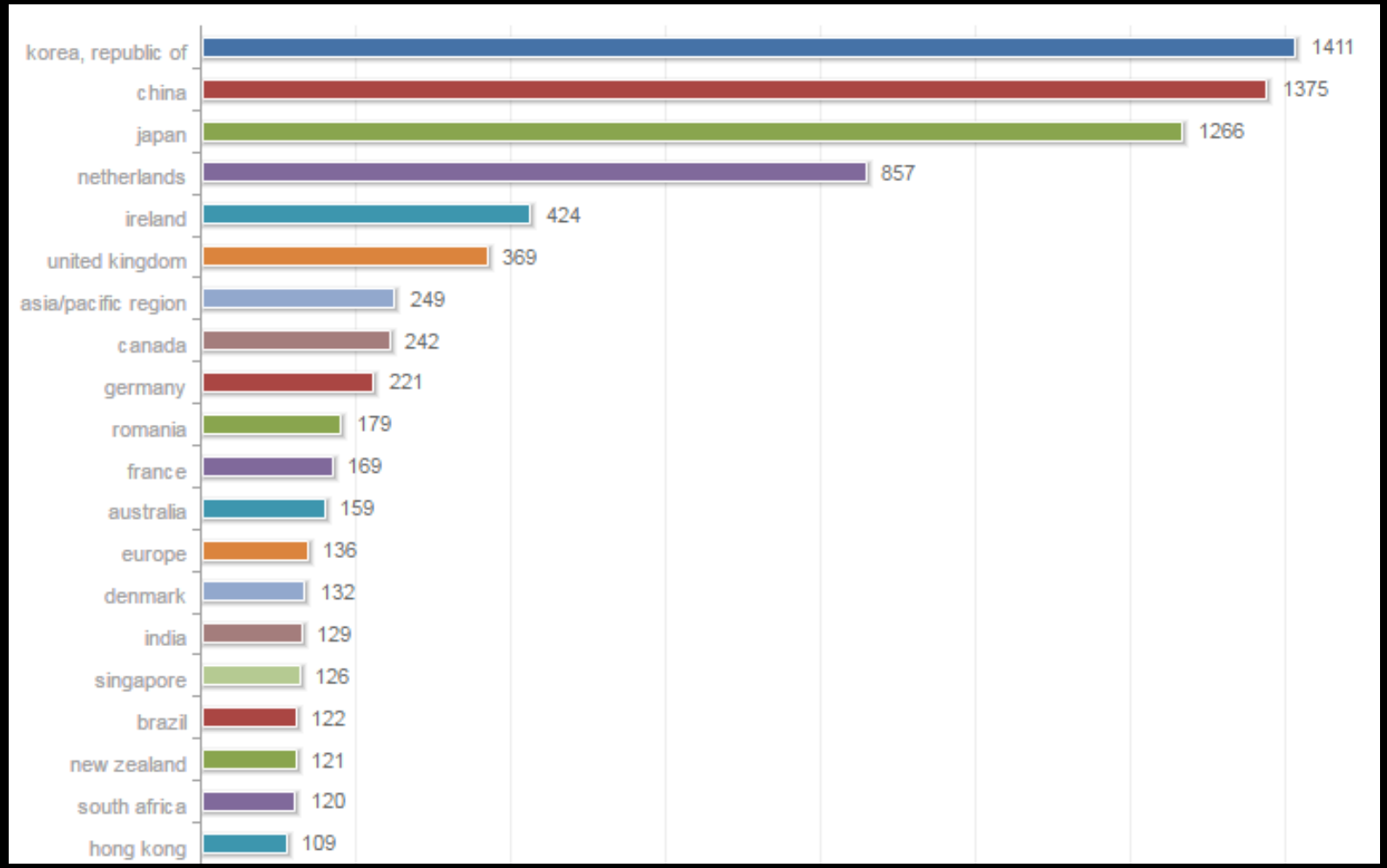
@grifter801
@theStump3r

More Stats

Network Sessions with Cleartext Auth	**~315,000 (~200K non-SNMP)**
Unique Usernames Found	**568**
Unique Passwords Found	**800**
Found Porn!	**2,596**
Executables DL via HTTP *Executables run through automated malware analysis* *Confirmed malicious via automated malware analysis*	**8,500** *1,323* *107*
Port Scans (various)	**Lost count. ~150,000**
Cleartext Search Engine Queries	**5,355**
Cleartext Emails	**687**
ICMP Data Tunneled	**~500MB (HTTP, text, file transfer)**
Confirmed WebShell Interaction (sessions)	**25** (from Training classes)

@grifter801
@theStump3r

Top non-US Countries with Threat Indicators (malware DL, beaconing, tunneling)



@grifter801
@theStump3r

IRC

Event Reconstruction

service	id	type	source	destination	service	first packet time
rsa-bh-pcon.none - Concentrator	3742619	Network Session	172.16.31.3 : 49815	192.186.157.43 : 6667	6667	2016-07-30T14:58:56.696

Request & Response | Top To Bottom | View Text | Actions | Open Event in New Tab | Cancel

Request

```
WHO ##stuffedninja
```

Response

```
:tepper.freenode.net 352 m1m ##stuffedninja ~math_aeta unaffiliated/mimatas tepper.freenode.net m1m H@ :0 New Now Know How
:tepper.freenode.net 352 m1m ##stuffedninja ~s7oneghos pdpc/supporter/active/s7oneghos7 sendak.freenode.net s7oneghos7 H@ :0 s7oneghos7
:tepper.freenode.net 352 m1m ##stuffedninja 424b2611 gateway/web/freenode/ip.66.75.38.17 herbert.freenode.net peacefrogturtle H@ :0
cpe-66-75-38-17.san.res.rr.com/66.75.38.17
:tepper.freenode.net 352 m1m ##stuffedninja ChanServ services. services. ChanServ H@ :0 Channel Services
:tepper.freenode.net 315 m1m ##stuffedninja :End of /WHO list.
```

Request

```
PING :ALIVECHECK
```

Response

```
:tepper.freenode.net PONG tepper.freenode.net :ALIVECHECK
```

Request

```
PRIVMSG ##stuffedninja :s7oneghos7: do you still have that RF pager script?
PRIVMSG ##stuffedninja :rotoruter has a HackRF now as well
PRIVMSG ##stuffedninja :I'm thinking it might be worth trying it out at the luxor
```

14 packets; lo

Event Reconstruction

service	id	type	source	destination	service
rsa-bh-pcon.none - Concentrator	19414370	Network Session	172.16.42.26 : 57500	192.186.157.43 : 6667	6667

Request & Response | Top To Bottom | View Text | Actions | Open Event in New Tab | Cancel

```
:octave!~octave@unaffiliated/octave QUIT :Quit: Leaving
```

Request

```
PRIVMSG nickserv :verify register qayopajyfnyg
```

Response

```
:NickServ!NickServ@services. NOTICE psyflame :Insufficient parameters for .VERIFY..
:NickServ!NickServ@services. NOTICE psyflame :Syntax: VERIFY <operation> <account> <key>
:magoo!~magoo@pool-173-72-129-104.clppva.fios.verizon.net QUIT :Quit: Leaving
:wilsonfisk!uid167036@gateway/web/irccloud.com/x-ovzuckedbuncbevg PRIVMSG ##security :.ACTION wants USB FLIR :P so he can play with
FLIR && OpenCV.
:LambdaSource!~LambdaSou@216-71-197-35.dyn.novuscom.net QUIT :Ping timeout: 252 seconds
```

Request

```
PONG tepper.freenode.net
PRIVMSG nickserv :verify register psyflame qayopajyfnyg
```

Response

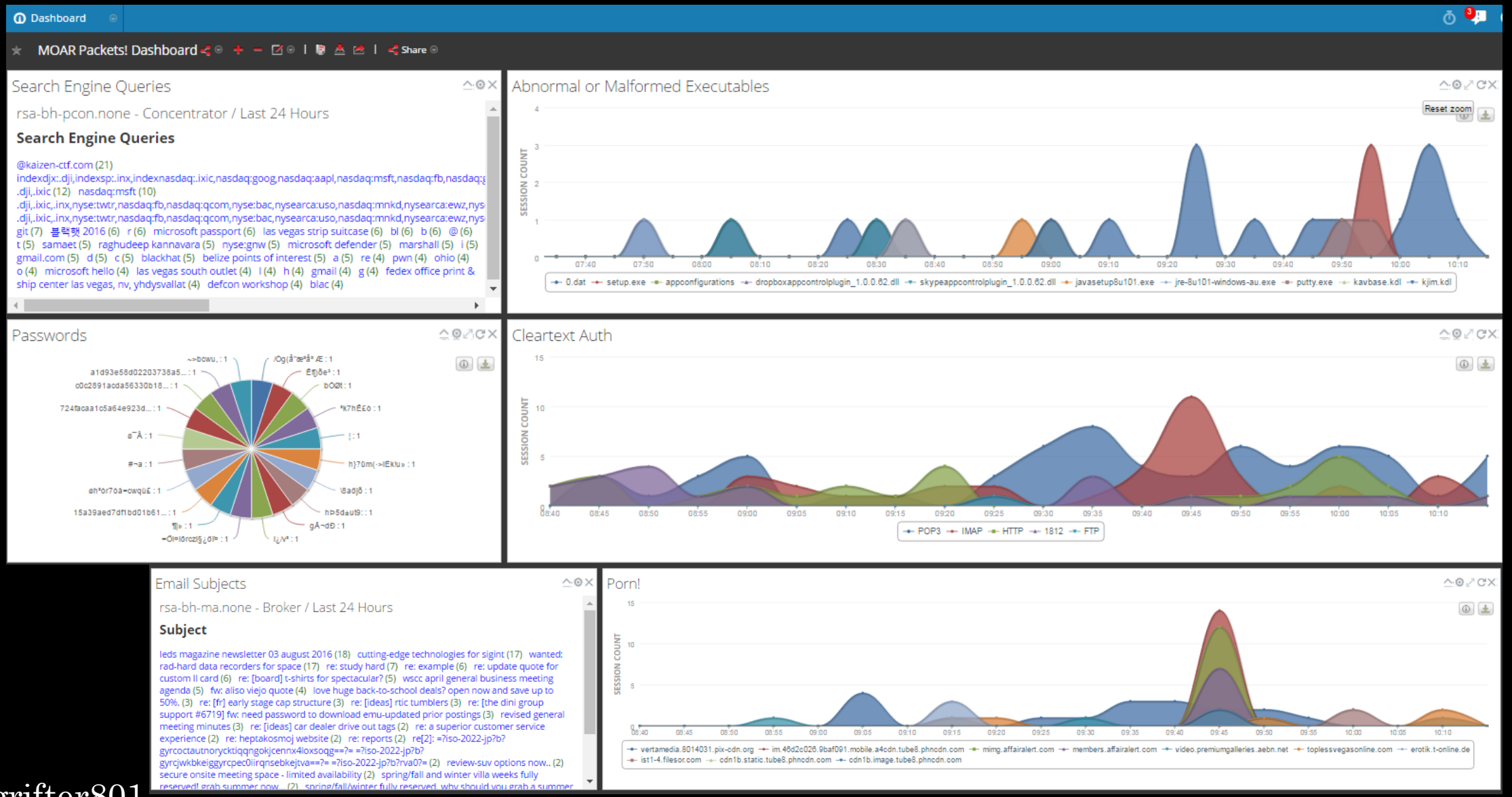
```
:NickServ!NickServ@services. NOTICE psyflame :.psyflame. has now been verified.
:NickServ!NickServ@services. NOTICE psyflame :Thank you for verifying your e-mail address! You have taken steps in ensuring that
your registrations are not exploited.
:botmaster!~administr@unaffiliated/botmaster QUIT :Ping timeout: 250 seconds
:_FBi!~B@Aircrack-NG/User PRIVMSG ##security :I think of FLIR as thermal
```

100 of 327 packets; loaded from cache | Show Reconstruction Log

action	=	"nick"
username	=	"psyflame"
action	=	"user"
username	=	"psyflame"
action	=	"join"
group	=	"#defcon"

@grifter801
@theStump3r

MOAR Packets



@grifter801
@theStump3r

Suspicious Binaries by Classroom

Service Type (1 value)
OTHER (178)

Service Inspection (1 value)
zip file encrypted (178)

Behaviors of Compromise (2 values)
file transport over unknown protocol (178) - file transport over icmp (1)

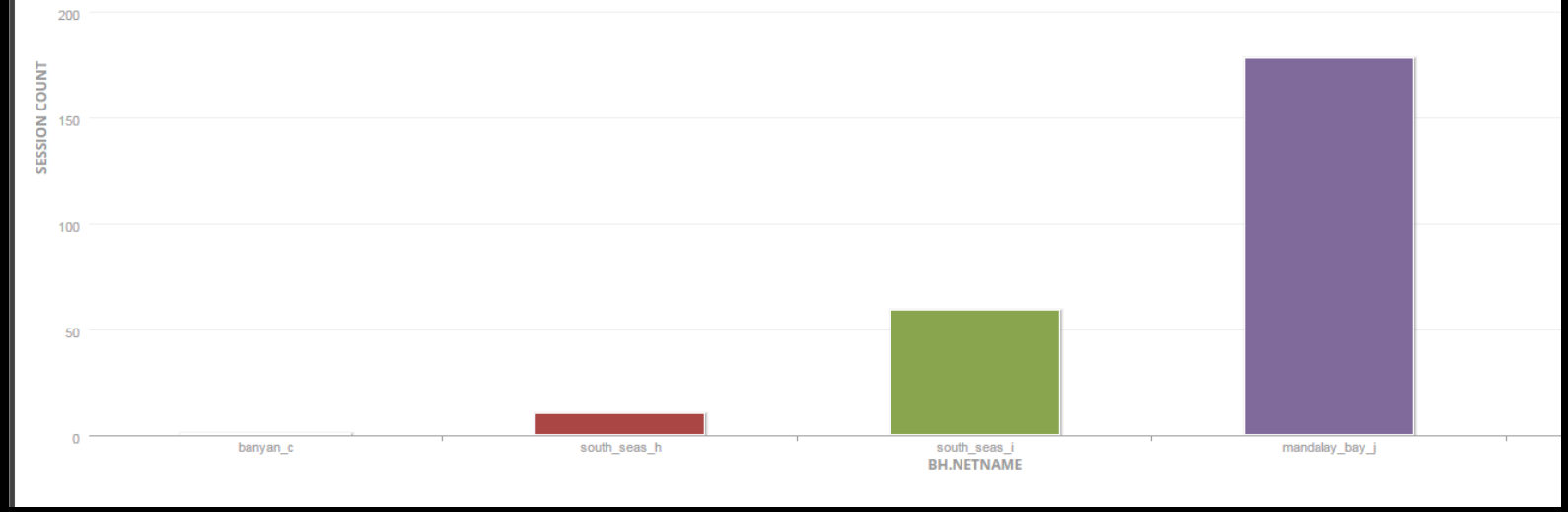
Action Event (1 value)
destination unreachable (1)

Destination Country (14 values)
united states (136) - china (8) - chile (5) - brazil (4) - jamaica (3) - venezuela (3) - argentina (2) - haiti (2) - hong kong (2) - aruba (1) - canada (1) - costa rica (1) - mexico (1) - peru (1)

Filename (1 value)
- (178)

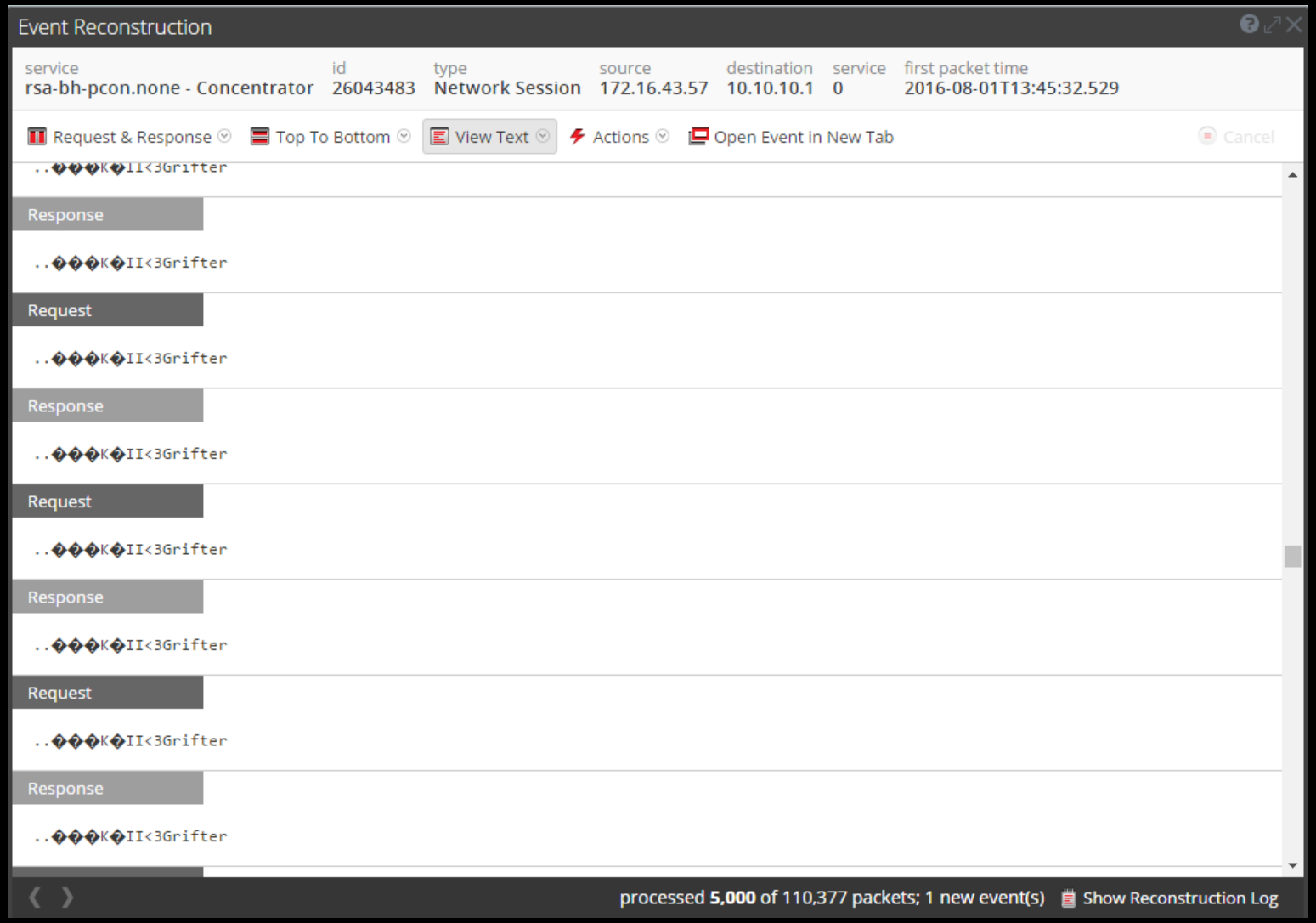
Forensic Fingerprint (2 values)
apple iwork (178) - zip (178)

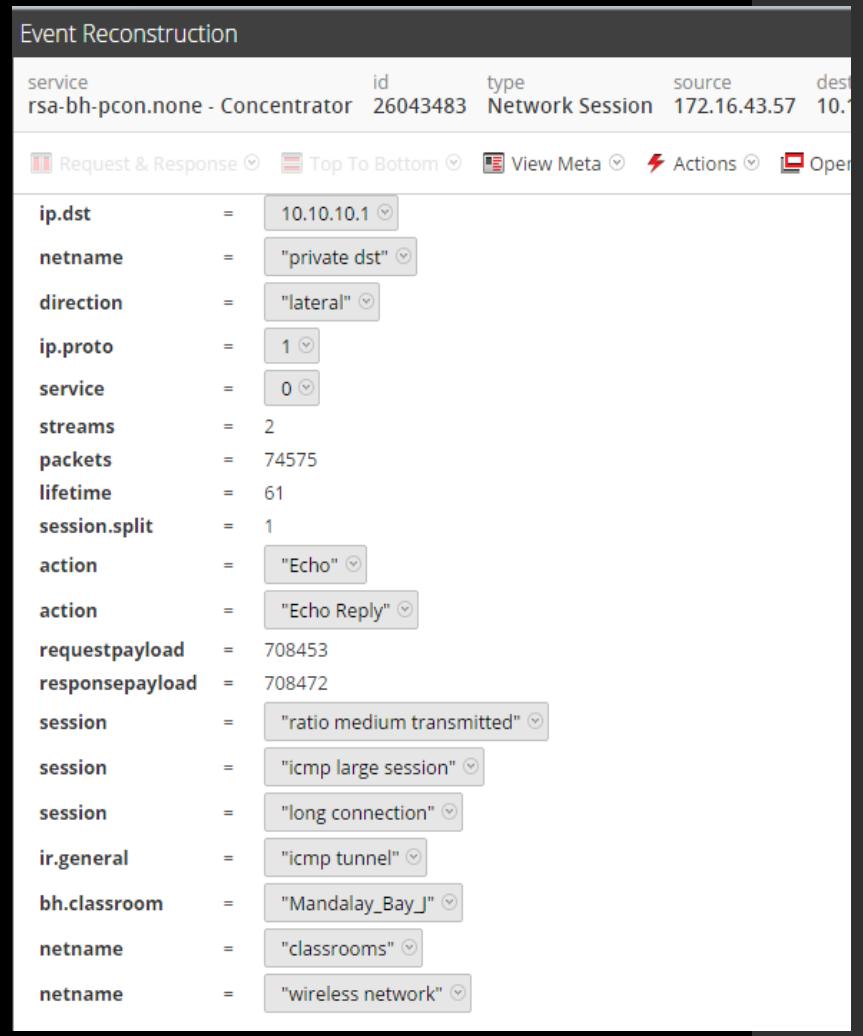
Source IP Address (9 values)



@grifter801
@theStump3r

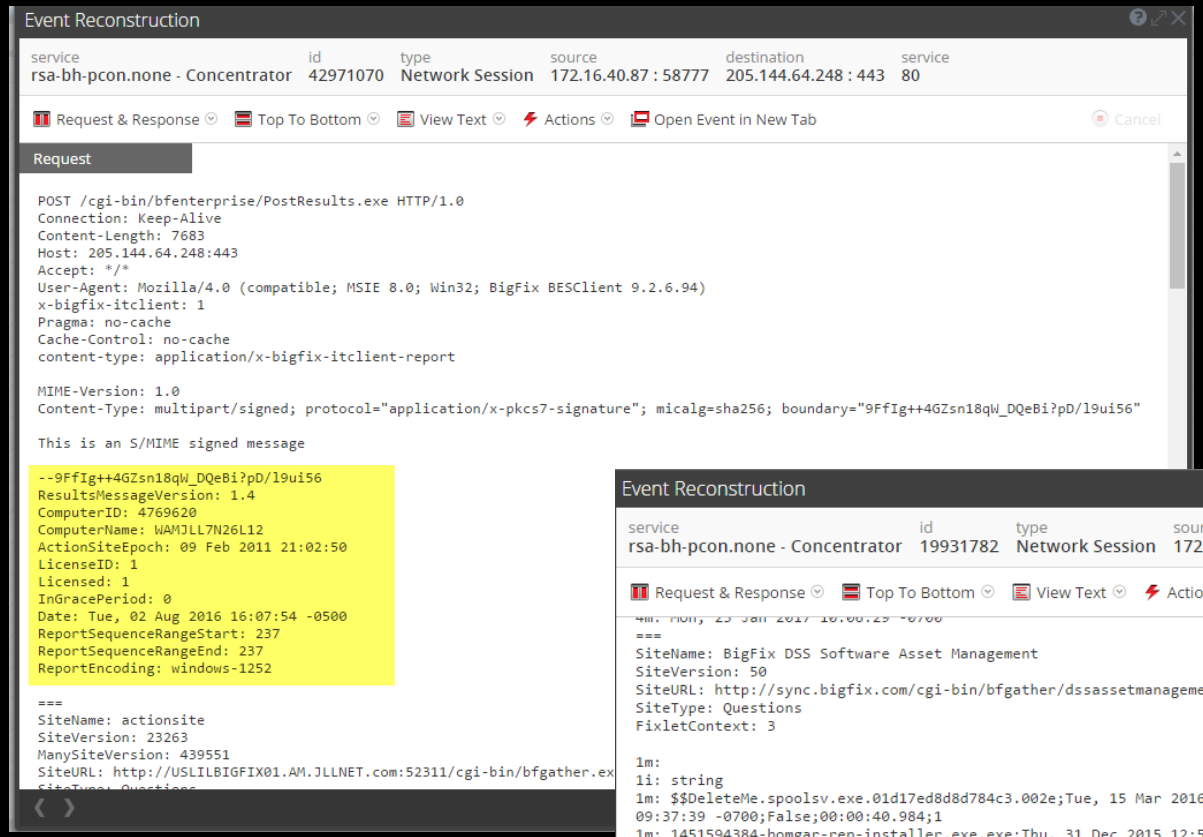
I <3 Grifter





@grifter801
@theStump3r

BigFix – Why You Exfil So hard?



- 12 hours
- 10 MB of Hostname, License Status, File Inventory
- 7 Enterprise BigFix Servers
- ~50 Black Hat hosts
- Cleartext HTTP, all non-standard ports

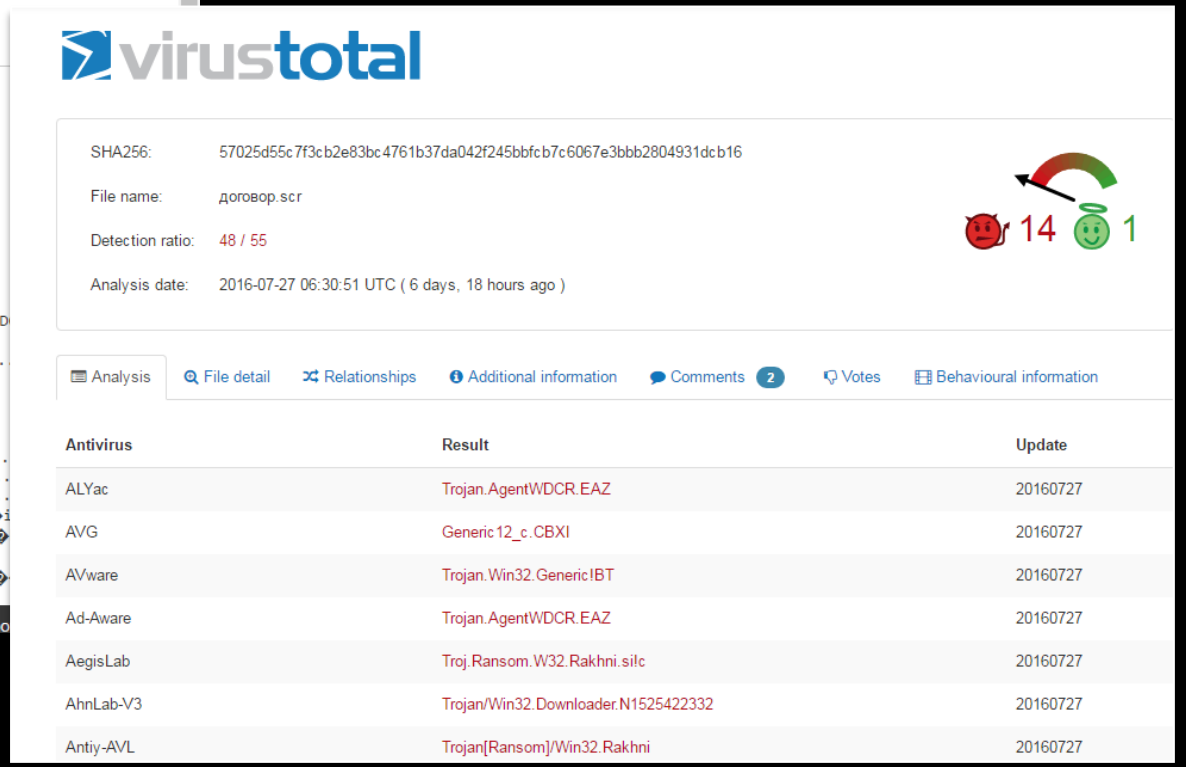
@grifter801
@theStump3r

WebShell on 54.166.72.50

Event Time	Event Type	Source IP Addres	Destination IP Ad	Destination Port	Service Name	Full Name	Payload Size	Filename	Domain	Host ID
2016-08-02T15:46:55	Network	10.168.1.4	54.166.72.50	80	HTTP		3594	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T15:47:51	Network	10.168.1.4	54.166.72.50	80	HTTP		4256	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T15:48:23	Network	10.168.1.4	54.166.72.50	80	HTTP		3145	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T15:49:11	Network	10.168.1.4	54.166.72.50	80	HTTP		15574	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T16:48:39	Network	172.16.3.32	54.166.72.50	80	HTTP		4230	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T16:48:42	Network	172.16.3.32	54.166.72.50	80	HTTP		4228	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T16:48:46	Network	172.16.3.32	54.166.72.50	80	HTTP		4228	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T16:48:49	Network	172.16.3.32	54.166.72.50	80	HTTP		4228	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T16:48:51	Network	172.16.3.32	54.166.72.50	80	HTTP		4228	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T16:48:52	Network	172.16.3.32	54.166.72.50	80	HTTP		4226	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T16:48:58	Network	172.16.3.32	54.166.72.50	80	HTTP		4226	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T16:48:59	Network	172.16.3.32	54.166.72.50	80	HTTP		4230	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T16:49:00	Network	172.16.3.32	54.166.72.50	80	HTTP		4230	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T16:49:02	Network	172.16.3.32	54.166.72.50	80	HTTP		4230	Default.aspx		f1ad9edda2c9.mdseclabs.net
2016-08-02T16:49:06	Network	172.16.3.32	54.166.72.50	80	HTTP		4230	Default.aspx		f1ad9edda2c9.mdseclabs.net

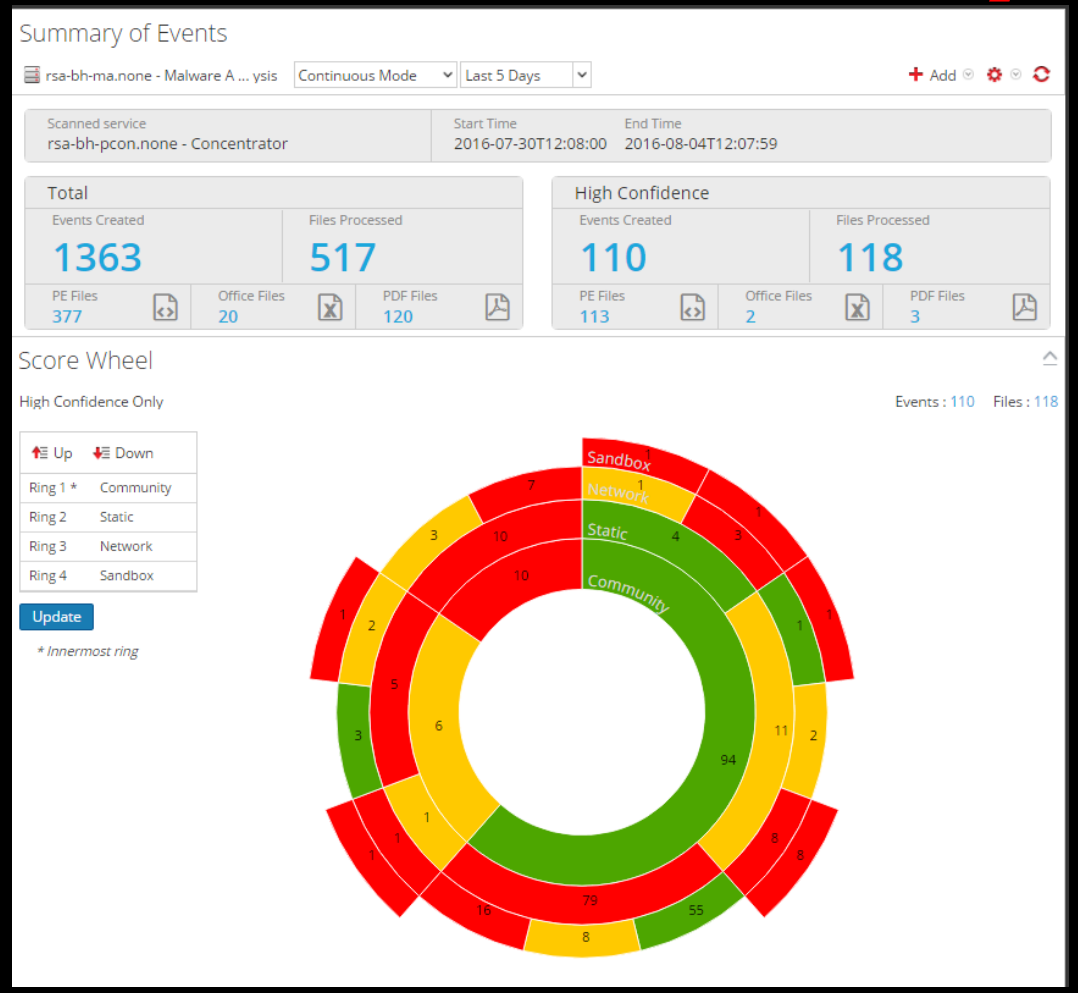
@grifter801
@theStump3r

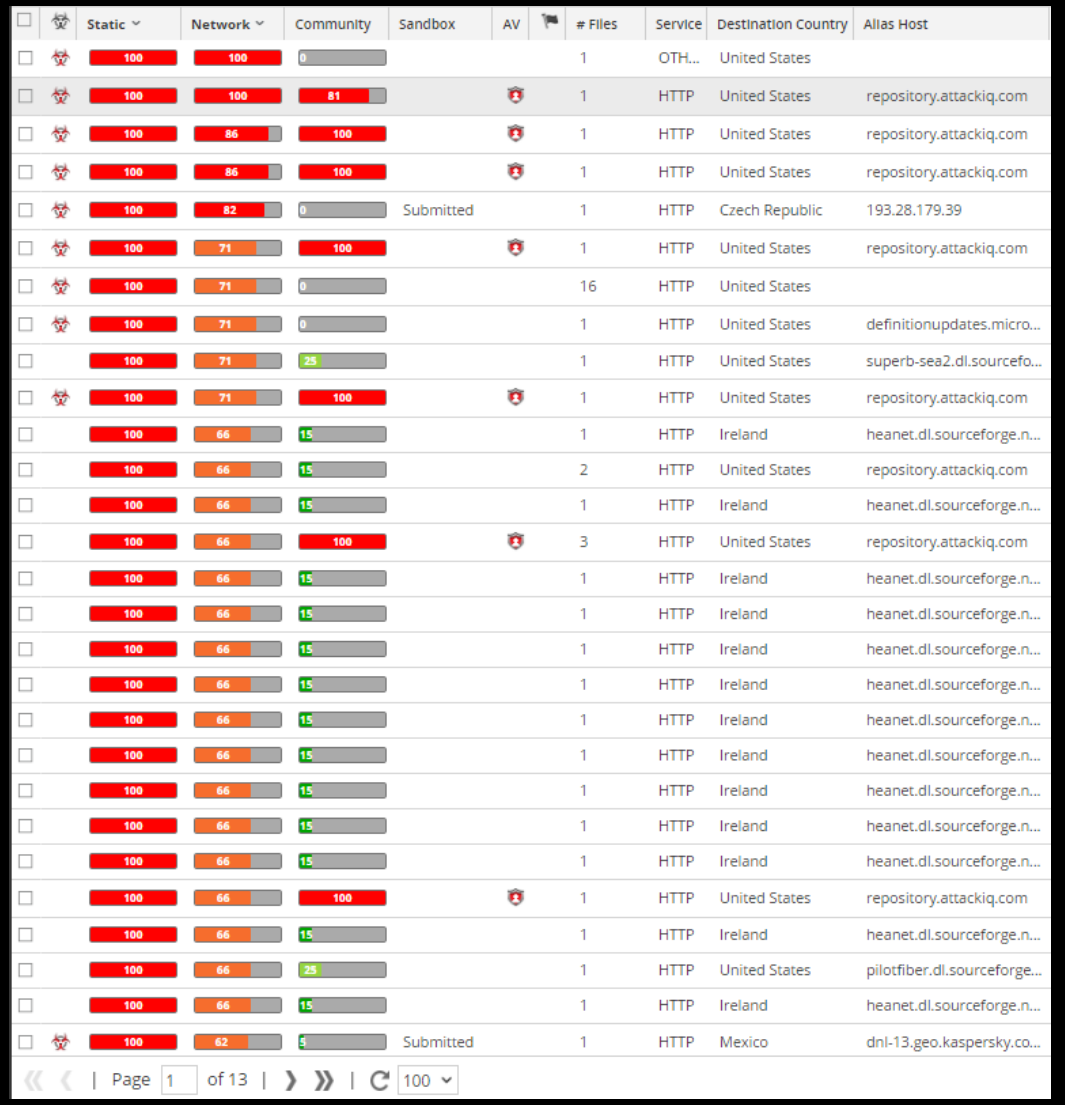
Rakhini Ransomware Download



@grifter801
@theStump3r

Executable Analysis





@grifter801
@theStump3r

Playing or Pwned?

Static	Network	Community	Sandbox	AV	# Files	Service	Destination Country	Destination Organization
76	100	100	100		1	HTTP	United States	Digital Ocean
100	100	66	100		1	HTTP	United States	Digital Ocean
100	100	81	100		1	HTTP	United States	Digital Ocean
76	100	100	100		1	HTTP	United States	Digital Ocean
100	100	81	100		1	HTTP	United States	Digital Ocean
76	100	100	100		1	HTTP	United States	al Ocean

AttackIQ.com Research

LoJack for Laptops

Request

GET /
(host: lojackforlaptops.absolute.com)

Filename (60 values)

eicar.com (3) - eicar_com.zip (2) - 2014-11-14-internal_04531572.scr (1) - 2015-01-27-khejkggxapfkthf.exe (1) - 2015-01-27-voice.exe (1) - 2015-01-30-angler-ek-malware-payload.exe (1) - 2015-03-30-fiesta-ek-flash-exploit.swf (1) - 2015-03-30-fiesta-ek-malware-payload.exe (1) - 7ev3n (1) - alpha_ransomware (1) - autolocky (1) - badblock (1) - bandarchor (1) - blackshades_crypter (1) - bucbi (1) - cerber (1) - chimera (1) - coinvault (1) - coverton (1) - crypren (1) - cryptear (1) - cryptodefense (1) - cryptolocker (1) - cryptowall (1) - cryptxxx (1) - ctblocker (1) - dmalocker (1) - eicar.com.txt (1) - eicarcom2.zip (1) - fakben (1) - ghostcrypt (1) - harasom (1) - hydracrypt (1) - jigsaw (1) - keranger (1) - kimcilware (1) - lechiffre (1) - linux-encoder (1) - locky (1) - maktub (1) - mischa (1) - mobef (1) - nemucod (1) - ocdocd (1) - petya (1) - powerware (1) - radamant (1) - rakhni (1) - ransom32 (1) - rector (1) - rokku (1) - sanction (1) - snslock (1) - synolocker (1) - teslacrypt (1) - truecrypter (1) - vaultcrypt (1) - xorist (1) - zcrypt (1) - zyklon (1)

@grifter801
@theStump3r

THANKS!

Neil Wyler (@grifter801)

Bart Stump (@theStump3r)