

**PAY NO ATTENTION TO
THAT HACKER BEHIND
THE CURTAIN:
*A LOOK INSIDE THE BLACK HAT
NETWORK***

Neil R. Wyler

Bart Stump

@grifter801

@theStump3r

Introductions

• Neil Wyler

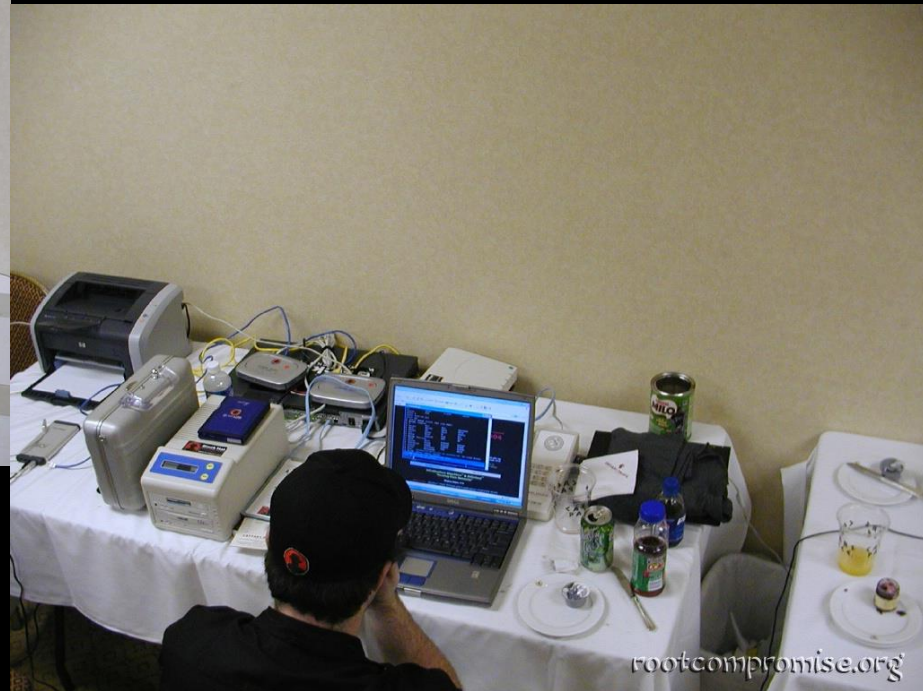
- 14 years at Black Hat
- By day – Threat Hunting and IR Specialist @ RSA
- Black Hat Review Board and Training Review Board
- DEF CON Review Board
- DEF CON Department Lead
- 801 Labs Board Member

• Bart Stump

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

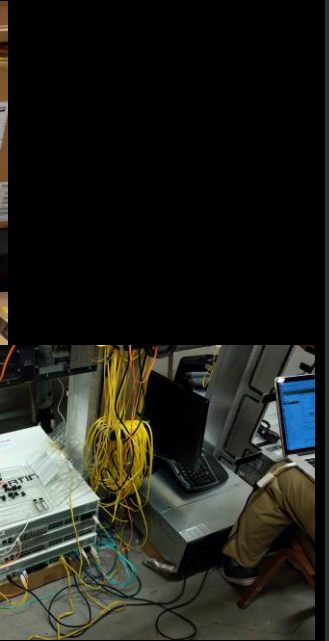
@grifter801
@theStump3r

Then



@grifter801
@theStump3r

Now



@grifter801
@theStump3r

Now



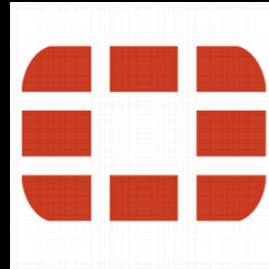
@grifter801
@theStump3r

The NOC Team

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

The Extended Team

- Fortinet
- RSA
- Ruckus
- Century Link



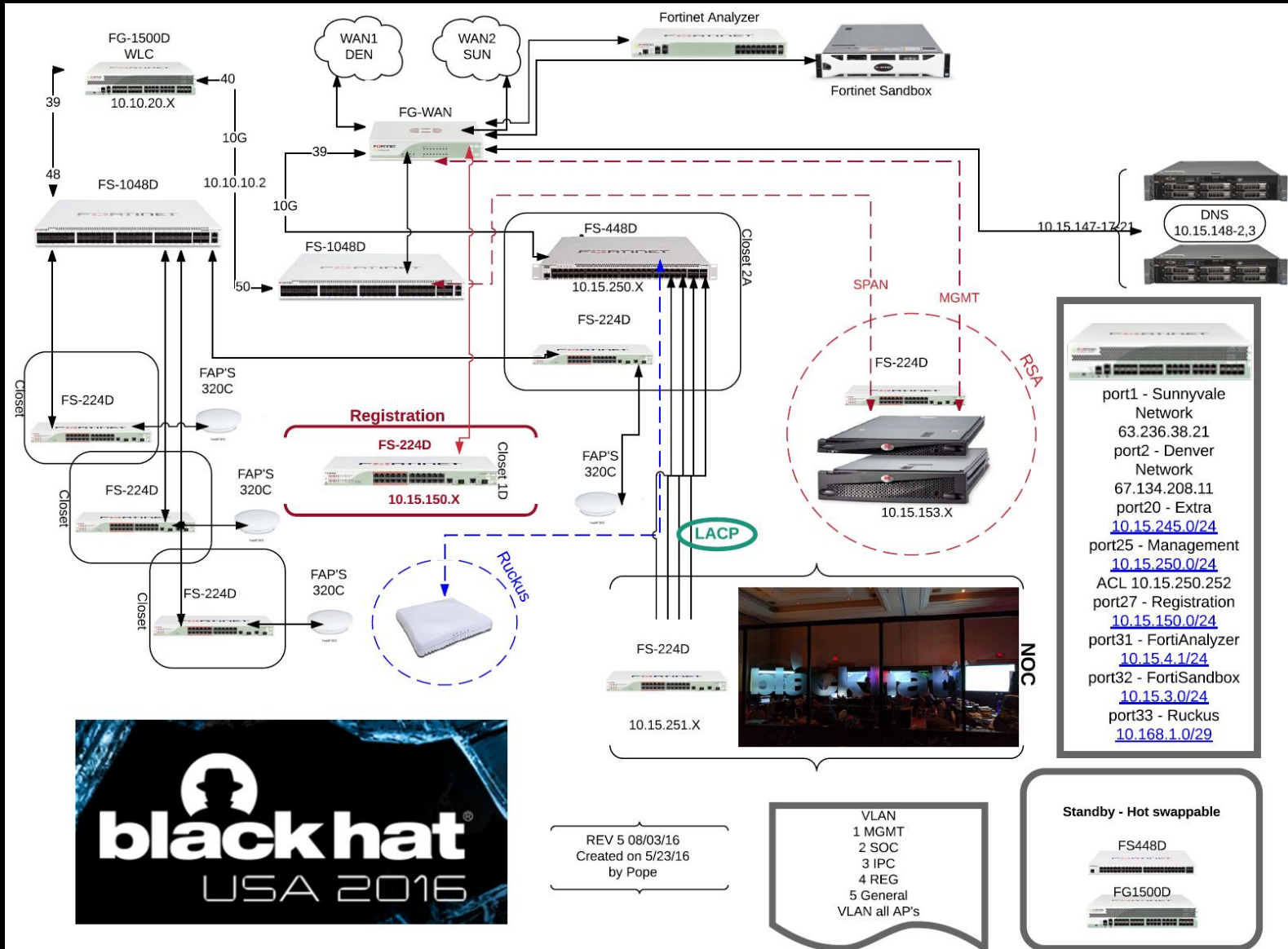
RSA



Equipment

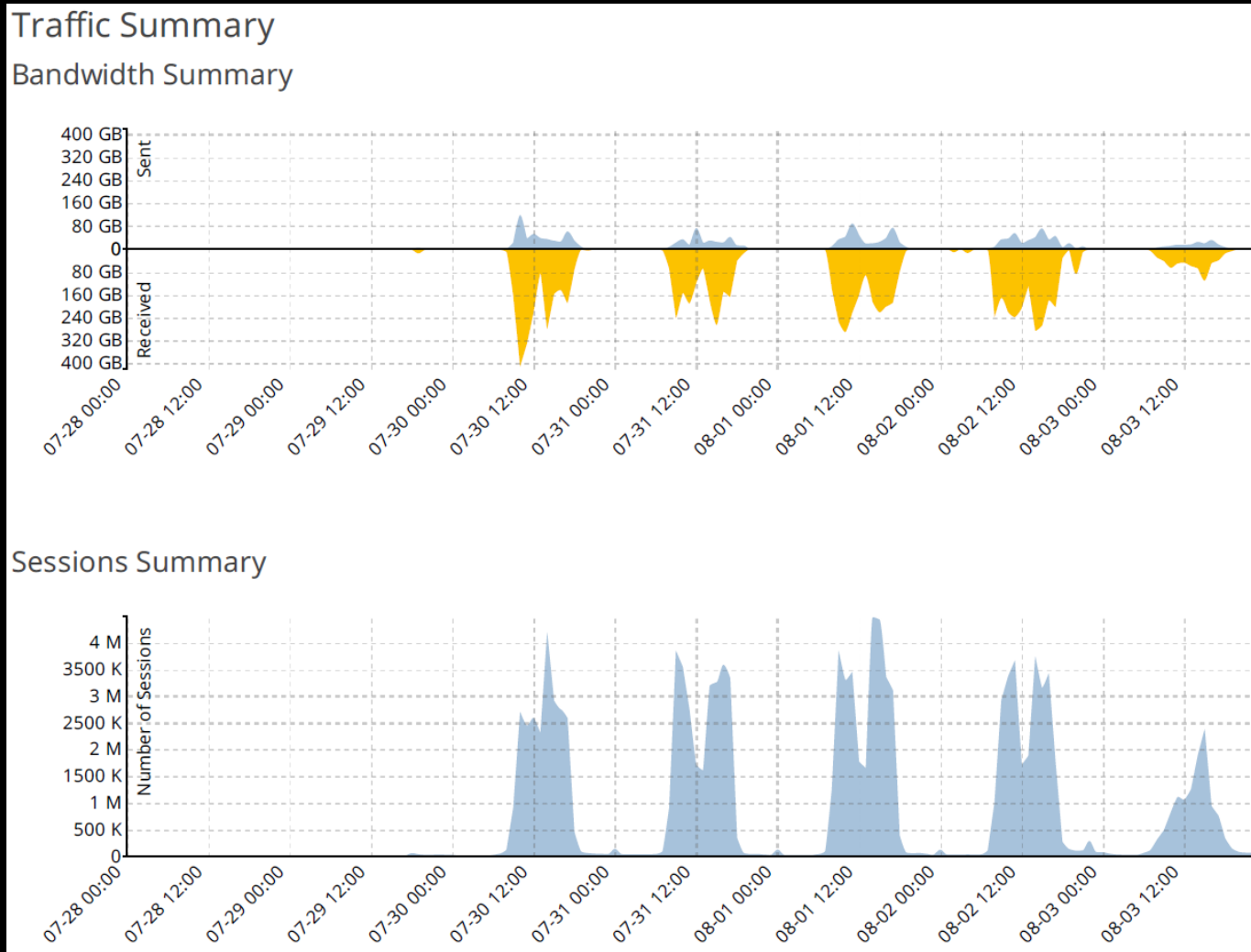
- RSA
 - 2 Analytics Servers
 - 1 Packet Decoder
 - 1 Hybrid for Packets
 - 1 Hybrid for Logs
 - 1 Packets Concentrator
 - 1 Event Stream Analysis
 - 1 Head Unit for Malware
 - ~80 TB of Storage
- Ruckus
 - 125 AP's
 - 20 Brocade Switches
 - 2 RG Nets Servers
 - 2 AP Controllers
- Fortinet
 - 3 1500D's
 - 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

Top Applications

Application Traffic

Top 30 Applications by Bandwidth and Sessions

#	Application	Bandwidth	Sessions
		Sent Received	
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 <i>Trainings</i> <i>Conference Wifi</i>	~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

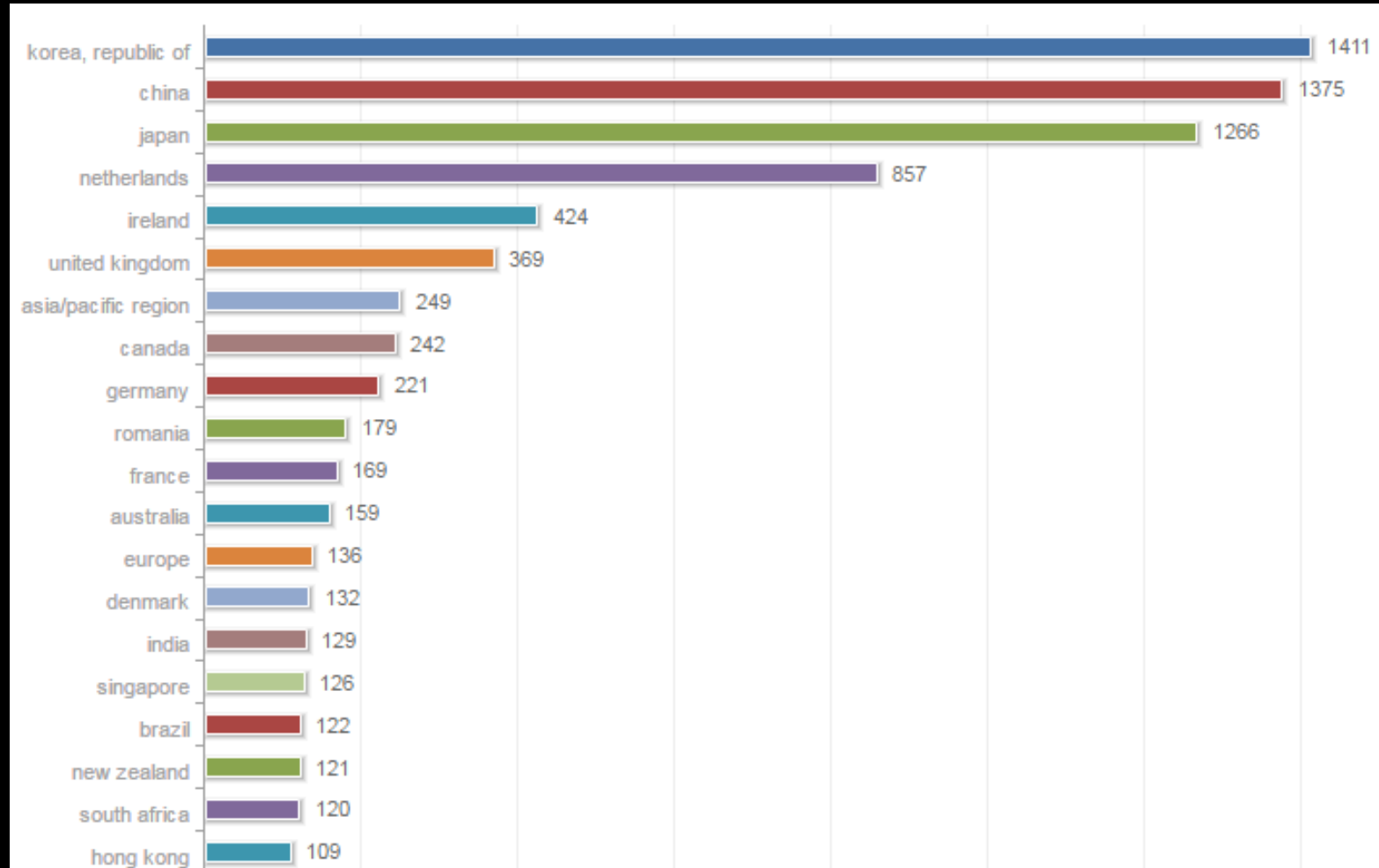
More Stats

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 <i>Executables run through automated malware analysis</i> <i>Confirmed malicious via automated malware analysis</i>	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)



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; loaded from cache

Event Reconstruction

service	id	type	source	destination	service	first packet time
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

```
:nickserv!nickserv@services. NOTICE psyflame :help you can join #freenode to find network staff.
:octave!~octave@unaffiliated/octave QUIT :Quit: Leaving
```

Request

```
PRIVMSG nickserv :verify register qayopajfyng
```

Response

```
:NickServ!NickServ@services. NOTICE psyflame :Insufficient parameters for .VERIFY..
:NickServ!NickServ@services. NOTICE psyflame :Syntax: VERIFY <operation> <account> <key>
:magool!~magool@pool-173-72-129-104.clppva.fios.verizon.net QUIT :Quit: Leaving
:wilsonfisk!uid167036@gateway/web/irccloud.com/x-ovzuckedbuncbevq 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 qayopajfyng
```

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" ▾

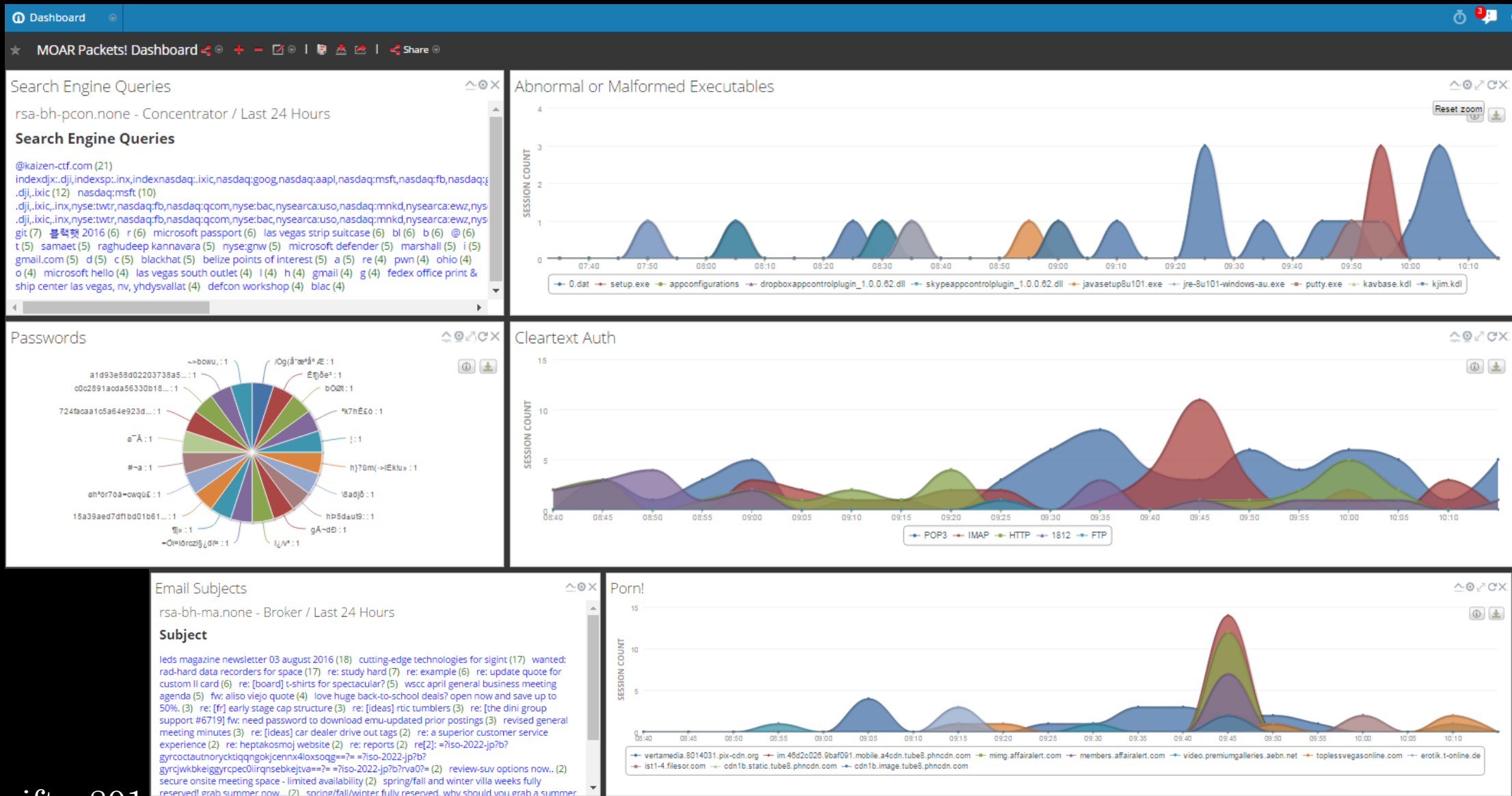
action = "user" ▾

username = "psyflame" ▾

action = "join" ▾

group = "#defcon" ▾

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)

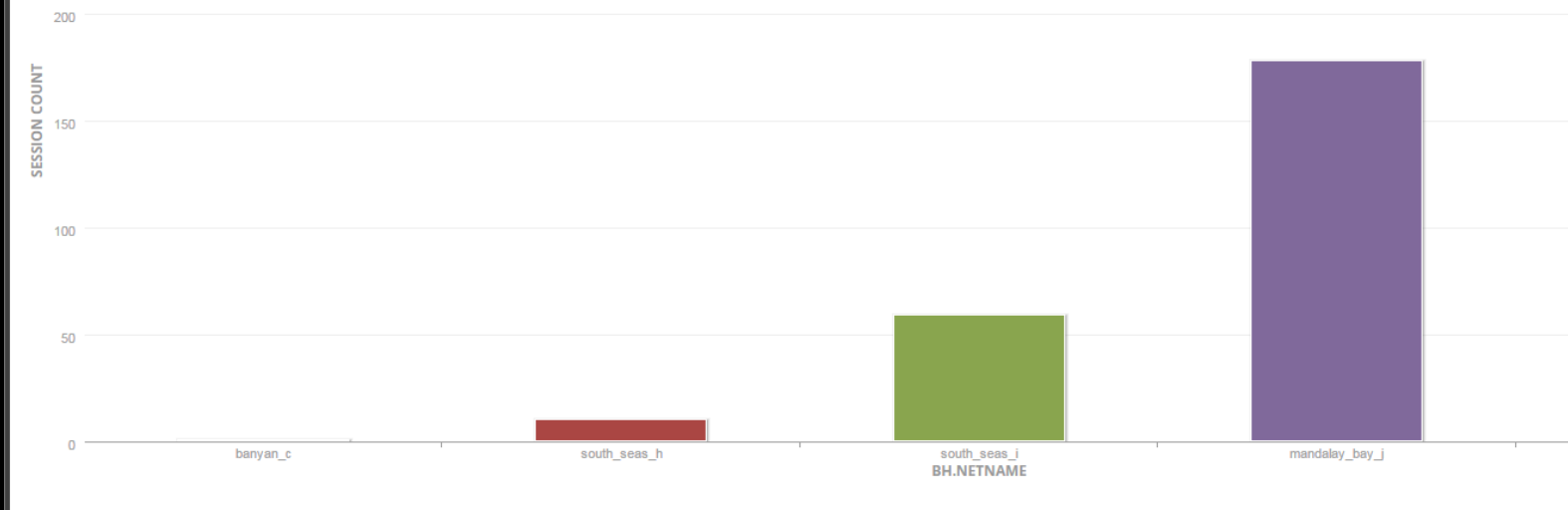
-(178)

Forensic Fingerprint (2 values)

apple iwork (178) - zip (178)

Source IP Address (9 values)

172.16.43.54 (170) - 24.16.214.96 (1) - 37.40.126.105 (1) - 71.69.173.183 (1) - 73.41.70.162 (1) - 76.14.3.147 (1) - 111.13.176.107 (1) - 112.00.108.144 (1) - 100.77.207.04 (1)



@grifter801
@theStump3r

I <3 Grifter

Event Reconstruction

service	id	type	source	destination	service	first packet time
rsa-bh-pcon.none - Concentrator	26043483	Network Session	172.16.43.57	10.10.10.1	0	2016-08-01T13:45:32.529

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

..🔍🔍🔍🔍II<3Grifter

Response

..🔍🔍🔍🔍II<3Grifter

Request

..🔍🔍🔍🔍II<3Grifter

Response

..🔍🔍🔍🔍II<3Grifter

Request

..🔍🔍🔍🔍II<3Grifter

Response

..🔍🔍🔍🔍II<3Grifter

Request

..🔍🔍🔍🔍II<3Grifter

Response

..🔍🔍🔍🔍II<3Grifter

processed 5,000 of 110,377 packets; 1 new event(s) | Show Reconstruction Log

Event Reconstruction

service	id	type	source	destination
rsa-bh-pcon.none - Concentrator	26043483	Network Session	172.16.43.57	10.10.10.1

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

ip.dst = 10.10.10.1

netname = "private dst"

direction = "lateral"

ip.proto = 1

service = 0

streams = 2

packets = 74575

lifetime = 61

session.split = 1

action = "Echo"

action = "Echo Reply"

requestpayload = 708453

responsepayload = 708472

session = "ratio medium transmitted"

session = "icmp large session"

session = "long connection"

ir.general = "icmp tunnel"

bh.classroom = "Mandalay_Bay_J"

netname = "classrooms"

netname = "wireless network"

@grifter801
@theStump3r

BigFix – Why You Exfil So hard?

```
Event Reconstruction
service      id      type      source      destination  service
rsa-bh-pcon.none - Concentrator 42971070 Network Session 172.16.40.87 : 58777 205.144.64.248 : 443 80

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

Request

POST /cgi-bin/bfenterprise/PostResults.exe HTTP/1.0
Connection: Keep-Alive
Content-Length: 7683
Host: 205.144.64.248:443
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32; BigFix BESClient 9.2.6.94)
x-bigfix-itclient: 1
Pragma: no-cache
Cache-Control: no-cache
content-type: application/x-bigfix-itclient-report

MIME-Version: 1.0
Content-Type: multipart/signed; protocol="application/x-pkcs7-signature"; micalg=sha256; boundary="--9FfIg++4GZsn18qW_DQeBi?pd/19ui56"

This is an S/MIME signed message
```

```
--9FfIg++4GZsn18qW_DQeBi?pd/19ui56
ResultsMessageVersion: 1.4
ComputerID: 4769620
ComputerName: WAMJLL7N26L12
ActionSiteEpoch: 09 Feb 2011 21:02:50
LicenseID: 1
Licensed: 1
InGracePeriod: 0
Date: Tue, 02 Aug 2016 16:07:54 -0500
ReportSequenceRangeStart: 237
ReportSequenceRangeEnd: 237
ReportEncoding: windows-1252
```

```
====
SiteName: actionsite
SiteVersion: 23263
ManySiteVersion: 439551
SiteURL: http://USILIBIGFIX01.AM.JLLNET.com:52311/cgi-bin/bfgather.exe
SiteType: Questions
```

```
Event Reconstruction
service      id      type      source      destination  service
rsa-bh-pcon.none - Concentrator 19931782 Network Session 172.16.41.47 : 7095 199.253.202.102 : 52311 80

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

Thu, 02 Aug 2016 16:07:54 -0500
====
SiteName: BigFix DSS Software Asset Management
SiteVersion: 50
SiteURL: http://sync.bigfix.com/cgi-bin/bfgather/dssassetmanagement
SiteType: Questions
FixletContext: 3

1m:
1i: string
1m: $$DeleteMe.spoolsv.exe.01d17ed8d8d784c3.002e;Tue, 15 Mar 2016 09:36:58 -0700;Tue, 15 Mar 2016 09:36:58 -0700;Tue, 15 Mar 2016 09:37:39 -0700;False;00:00:40.984;1
1m: 1451594384-bomgar-rep-installer.exe.exe;Thu, 31 Dec 2015 12:54:45 -0700;Thu, 31 Dec 2015 12:54:45 -0700;Thu, 31 Dec 2015 12:54:45 -0700;False;00:00:00;1
1m: 1463a0.rbf;Sun, 15 May 2016 20:48:09 -0700;Sun, 15 May 2016 20:48:09 -0700;Sun, 15 May 2016 20:51:16 -0700;False;00:03:07.016;1
1m: 50.0.2661.102_chrome_installer.exe;Wed, 18 May 2016 13:16:32 -0700;Wed, 18 May 2016 13:16:32 -0700;False;00:00:00;1
1m: 51.0.2704.103_51.0.2704.84_chrome_updater.exe;Mon, 20 Jun 2016 10:01:43 -0700;Mon, 20 Jun 2016 10:01:43 -0700;Mon, 20 Jun 2016 10:02:13 -0700;False;00:00:30.188;1
1m: 51.0.2704.103_chrome_installer.exe;Mon, 20 Jun 2016 15:02:36 -0700;Mon, 20 Jun 2016 15:02:36 -0700;Mon, 20 Jun 2016 15:02:36 -0700;False;00:00:00;1
1m: 51.0.2704.84_50.0.2661.102_chrome_updater.exe;Mon, 06 Jun 2016 11:02:07 -0700;Mon, 06 Jun 2016 11:02:07 -0700;Mon, 06 Jun 2016 11:02:31 -0700;False;00:00:23.781;1
1m: 52.0.2743.82_51.0.2704.103_chrome_updater.exe;Thu, 21 Jul 2016 11:11:18 -0700;Thu, 21 Jul 2016 11:11:18 -0700;Thu, 21 Jul 2016 11:11:56 -0700;False;00:00:37.516;1
1m: 7za.exe;Tue, 01 Mar 2016 08:23:06 -0700;Tue, 01 Mar 2016 08:23:06 -0700;Tue, 01 Mar 2016 08:23:27 -0700;False;00:00:20.547;1
1m: 7zFM.exe;Thu, 17 Dec 2015 13:33:49 -0700;Tue, 07 Jun 2016 22:54:28 -0700;Tue, 07 Jun 2016 22:56:33 -0700;False;07:06:24.280;5
1m: 7zG.exe;Thu, 17 Dec 2015 13:34:10 -0700;Tue, 05 Jul 2016 11:51:17 -0700;Tue, 05 Jul 2016 11:52:29 -0700;False;00:02:16.186;5
1m: a04bfd6.rbf;Fri, 20 May 2016 11:44:48 -0700;Fri, 20 May 2016 11:44:48 -0700;Fri, 20 May 2016 17:26:09 -0700;False;05:41:21.266;1
1m: A7E7.tmp.SmartConsole.exe;Mon, 01 Feb 2016 12:54:51 -0700;Mon, 01 Feb 2016 12:54:51 -0700;Mon, 01 Feb 2016 13:00:48 -0700;False;00:05:56.922;1
```

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

WebShell on 54.166.72.50

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

Event Reconstruction

service	id	type	source	destination	service	first packet time
rsa-bh-pcon.none - Concentrator	47495156	Network Session	172.16.47.2 : 64540	104.236.137.130 : 80	80	2016-08-02T16:35:07.103

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

Request

```
GET /57025d55c7f3cb2e83bc4761b37da042f245bbfcb7c6067e3bbb2804931dcb16/Rakhni HTTP/1.1
Host: repository.attackiq.com
Accept-Encoding: gzip, deflate, compress
Accept: */*
User-Agent: python-requests/2.2.1 CPython/2.7.10 Darwin/15.6.0
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Tue, 02 Aug 2016 23:35:07 GMT
Content-Type: application/octet-stream
Content-Length: 5632
Last-Modified: Fri, 24 Jun 2016 17:30:34 GMT
Connection: keep-alive
ETag: "576d6e3a-1600"
Accept-Ranges: bytes
```

processed ; 1 new event(s) | Show

virustotal

SHA256: 57025d55c7f3cb2e83bc4761b37da042f245bbfcb7c6067e3bbb2804931dcb16

File name: dorooop.scr

Detection ratio: 48 / 55

Analysis date: 2016-07-27 06:30:51 UTC (6 days, 18 hours ago)

14 (Bad) 1 (Good)

Analysis | File detail | Relationships | Additional information | Comments (2) | Votes | Behavioural information

Antivirus	Result	Update
ALYac	Trojan.AgentWDCR.EAZ	20160727
AVG	Generic12_c.CBXL	20160727
AVware	Trojan.Win32.GenericIBT	20160727
Ad-Aware	Trojan.AgentWDCR.EAZ	20160727
AegisLab	Troj.Ransom.W32.Rakhni.silc	20160727
AhnLab-V3	Trojan/Win32.Downloader.N1525422332	20160727
Antiy-AVL	Trojan[Ransom]/Win32.Rakhni	20160727

@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	Digital 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-khejggxapfkthf.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) - bucbl (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)