Falha de detecção e classificação de plug-in P2P para aplicativo com fluxos SSL no ASR5x00

Contents

Introduction

Este documento descreve um cenário específico em que o assinante usa aplicativos de taxa livre como Whatsapp, Snapchat etc. com fluxos SSL (Secure Sockets Layer) enquanto bloqueia o tráfego de outros usuários. Este aplicativo específico é executado nos Cisco Aggregated Service Routers (ASR) 5x00 Series. O SSL é um protocolo de rede de computador que gerencia a autenticação do servidor, a autenticação do cliente e a comunicação criptografada entre servidores e clientes.

Problema

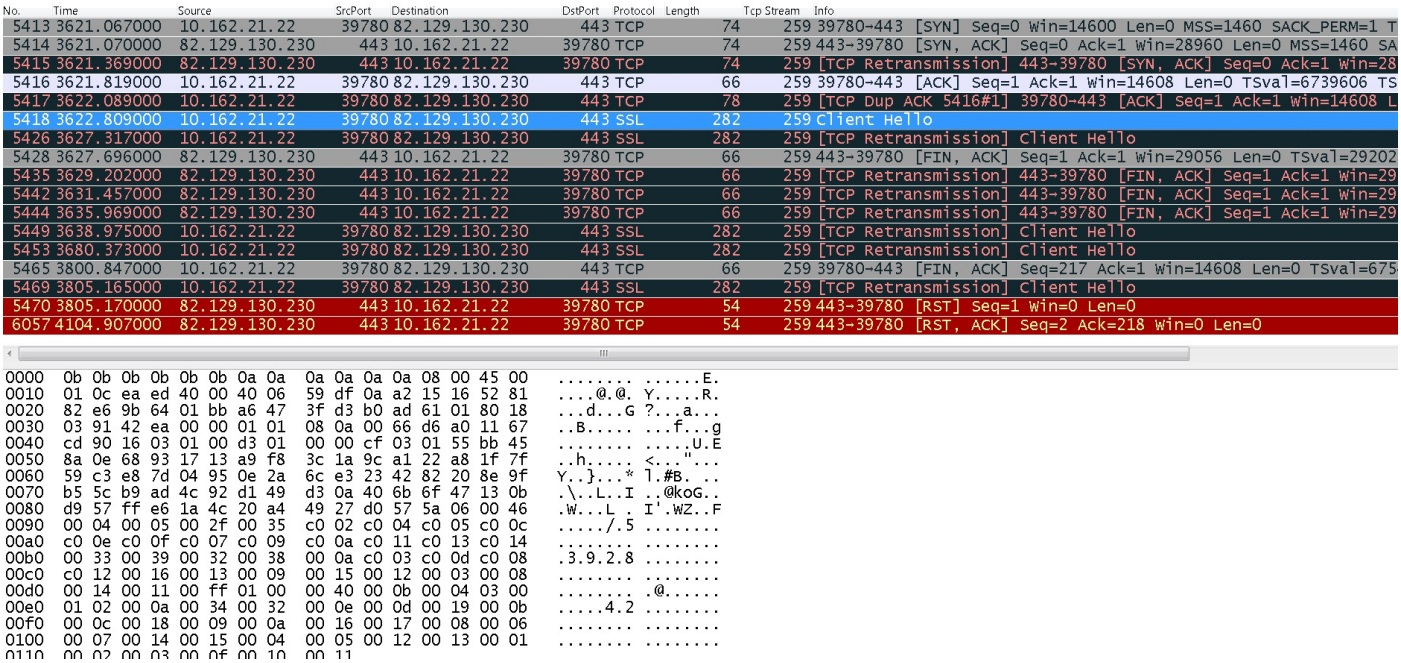
Para detectar qualquer aplicativo, você precisa de alguns pacotes iniciais para a análise. Estes dois requisitos contraditórios são cumpridos ao máximo.

a) A detecção deve ocorrer no próprio primeiro pacote

b) A precisão da detecção deve ser de 100%

Se você tentar cumprir os requisitos (a) e marcar todos os aplicativos no primeiro pacote (o que não é praticamente possível), o requisito (b) sobre a precisão da detecção sofre.Para tornar a precisão da detecção boa, você precisa de mais pacotes para analisar vários aplicativos (há aplicativos e fluxos onde o aplicativo é detectado no primeiro pacote propriamente dito). No caso do mesmo aplicativo, pode acontecer que você seja capaz de marcar alguns fluxos no próprio pacote enquanto outros fluxos do mesmo aplicativo precisam de mais pacotes para análise.

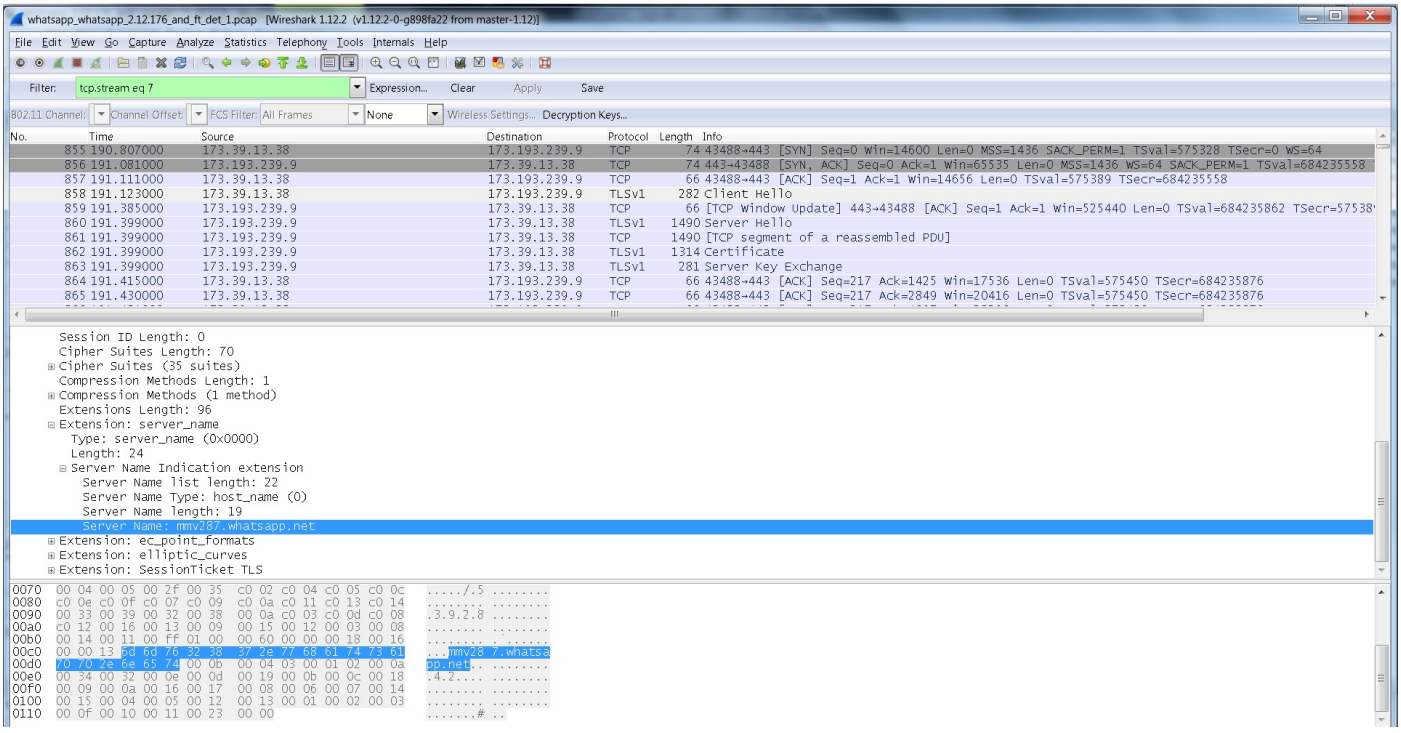
Assim, se algum aplicativo for gratuito enquanto bloqueia qualquer outro tráfego, pode acontecer que o pacote inicial do aplicativo não seja detectado, pois ele não transporta informações suficientes. Em particular, no caso de aplicativos baseados em fluxos SSL, o protocolo é marcado usando o campo server-name-reference presente no pacote client-hello ou o nome comum presente no certificado SSL. Como o nome do servidor é opcional, ele nem sempre está presente. Como mostrado nesta imagem, em um fluxo SSL do Whatsapp, após o handshake triplo (TWH), o pacote hello do cliente é enviado pelo aplicativo. **Um rastreamento PCAP mostrando nenhum campo SNI (Server Name Indication, indicação de nome do servidor). Também são vistas várias retransmissões de pacotes hello do cliente que eventualmente são descartados.**



No.	Time	Source	SrcPort	Destination	DstPort	Protocol	Length	Tcp Stream	Info
5413	3621.067000	10.162.21.22	39780	82.129.130.230	443	TCP	74	259	39780→443 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 T
5414	3621.070000	82.129.130.230	443	10.162.21.22	39780	TCP	74	259	443→39780 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SA
5415	3621.369000	82.129.130.230	443	10.162.21.22	39780	TCP	74	259	[TCP Retransmission] 443→39780 [SYN, ACK] Seq=0 Ack=1 Win=28
5416	3621.819000	10.162.21.22	39780	82.129.130.230	443	TCP	66	259	39780→443 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=6739606 TS
5417	3622.089000	10.162.21.22	39780	82.129.130.230	443	TCP	78	259	[TCP Dup ACK 5416#1] 39780→443 [ACK] Seq=1 Ack=1 Win=14608 L
5418	3622.809000	10.162.21.22	39780	82.129.130.230	443	SSL	282	259	Client Hello
5426	3627.317000	10.162.21.22	39780	82.129.130.230	443	SSL	282	259	[TCP Retransmission] Client Hello
5428	3627.696000	82.129.130.230	443	10.162.21.22	39780	TCP	66	259	443→39780 [FIN, ACK] Seq=1 Ack=1 Win=29056 Len=0 TSval=29202
5435	3629.202000	82.129.130.230	443	10.162.21.22	39780	TCP	66	259	[TCP Retransmission] 443→39780 [FIN, ACK] Seq=1 Ack=1 Win=29
5442	3631.457000	82.129.130.230	443	10.162.21.22	39780	TCP	66	259	[TCP Retransmission] 443→39780 [FIN, ACK] Seq=1 Ack=1 Win=29
5444	3635.969000	82.129.130.230	443	10.162.21.22	39780	TCP	66	259	[TCP Retransmission] 443→39780 [FIN, ACK] Seq=1 Ack=1 Win=29
5449	3638.975000	10.162.21.22	39780	82.129.130.230	443	SSL	282	259	[TCP Retransmission] Client Hello
5453	3680.373000	10.162.21.22	39780	82.129.130.230	443	SSL	282	259	[TCP Retransmission] Client Hello
5465	3800.847000	10.162.21.22	39780	82.129.130.230	443	TCP	66	259	39780→443 [FIN, ACK] Seq=217 Ack=1 Win=14608 Len=0 TSval=675
5469	3805.165000	10.162.21.22	39780	82.129.130.230	443	SSL	282	259	[TCP Retransmission] Client Hello
5470	3805.170000	82.129.130.230	443	10.162.21.22	39780	TCP	54	259	443→39780 [RST] Seq=1 Win=0 Len=0
6057	4104.907000	82.129.130.230	443	10.162.21.22	39780	TCP	54	259	443→39780 [RST, ACK] Seq=2 Ack=218 Win=0 Len=0

```
0000  0b 0b 0b 0b 0b 0b 0a 0a  0a 0a 0a 0a 08 00 45 00   ........ ......E.
0010  01 0c ea ed 40 00 40 06  59 df 0a a2 15 16 52 81   ....@.@. Y.....R.
0020  82 e6 9b 64 01 bb a6 47  3f d3 b0 ad 61 01 80 18   ...d...G ?...a...
0030  03 91 42 ea 00 00 01 01  08 0a 00 66 d6 a0 11 67   ..B..... ...f...g
0040  cd 90 16 03 01 00 d3 01  00 00 cf 03 01 55 bb 45   ........ .....U.E
0050  8a 0e 68 93 17 13 a9 f8  3c 1a 9c a1 22 a8 1f 7f   ..h..... <..."...
0060  59 c3 e8 7d 04 95 0e 2a  6c e3 23 42 82 20 8e 9f   Y..}...* l.#B. ..
0070  b5 5c b9 ad 4c 92 d1 49  d3 0a 40 6b 6f 47 13 0b   .\..L..I ..@koG..
0080  d9 57 ff e6 1a 4c 20 a4  49 27 d0 57 5a 06 00 46   .W...L . I'.WZ..F
0090  00 04 00 05 00 2f 00 35  c0 02 c0 04 c0 05 c0 0c   ...../.5 ........
00a0  c0 0e c0 0f c0 07 c0 09  c0 0a c0 11 c0 13 c0 14   ........ ........
00b0  00 33 00 39 00 32 00 38  00 0a c0 03 c0 0d c0 08   .3.9.2.8 ........
00c0  c0 12 00 16 00 13 00 09  00 15 00 12 00 03 00 08   ........ ........
00d0  00 14 00 11 00 ff 01 00  00 40 00 0b 00 04 03 00   ........ .@......
00e0  01 02 00 0a 00 34 00 32  00 0e 00 0d 00 19 00 0b   .....4.2 ........
00f0  00 0c 00 18 00 09 00 0a  00 16 00 17 00 08 00 06   ........ ........
0100  00 07 00 14 00 15 00 04  00 05 00 12 00 13 00 01   ........ ........
0110  00 02 00 03 00 0f 00 10  00 11
```

Além disso, como mostrado nesta imagem, eles são os hex-bytes do pacote client-hello no qual o campo SNI, usado para marcar o Whatsapp, não está presente. Portanto, o pacote client-hello não pode ser marcado como Whatsapp e não é detectado. À medida que esse pacote cai em um grupo de classificação diferente, ele é descartado e, portanto, várias retransmissões do pacote client-hello são vistas (consulte quadro n.o 5449, 5453, 5469). Finalmente, a conexão é encerrada. Vários desses fluxos são vistos na tabela de preços. Essa é a razão pela qual nenhuma atividade útil, por exemplo o carregamento de imagem para o Whatsapp, pode ser feita.



Troubleshoot

1. capture monitor subscriber imsi XXXX with following options
19 - User L3

```
X - PDU Hexdump
Verbosity level 5
```

Esses comandos fornecem as estatísticas do analisador para os aplicativos.

```
# show act analyzer statistics name p2p application snapchat
# show act analyzer statistics name p2p application whatsapp
```

Para verificar a versão do plug-in:

```
#show plugin p2p
Wednesday July 29 22:12:07 SAST 2015
plugin p2p
  patch-directory /var/opt/lib
  base-directory /lib
  base-version 1.50.52055
  module priority 1 version 1.139.505
```

Solução

Para evitar, você precisa garantir que os pacotes antes de um aplicativo (diga o que sapp) sejam marcados e passem por ele.

Use esta regra def:

```
ruledef ssl_clienthello
      tcp either-port = 443
      tcp payload-length >= 44
      tcp payload  starts-with hex-signature 16-03
#exit
```

Nenhum pacote correspondente à régua acima deve ser descartado. A prioridade desta régua deve estar logo acima da régua padrão (ip-any ruledef) que estava correspondendo a este pacote e fazendo com que ele fosse descartado.

Usando essa configuração, somente os pacotes que correspondem às três linhas de regra acima são gratuitos. Eles incluem apenas os pacotes iniciais de handshake no fluxo SSL (como client-hello, server-hello) que são permitidos usando essa régua def, enquanto todos os outros pacotes no fluxo SSL não correspondem a essa régua def. Assim, se houver um fluxo SSL que pertença a algum outro aplicativo (que não o que você deseja liberar), não poderá haver nenhuma transação útil, pois somente os dois ou três pacotes iniciais de um fluxo SSL podem usar esse tipo de regra.

Configuração de exemplo

A régua sugerida precisa ter uma prioridade mais alta que all-ip_004_012_00016 ruledef (ip any-match = TRUE) e

ação de cobrança que permite o tráfego similar ao que sapp ruledef.(sid_040_rg_400_rate_9999/sid_040_rg_400_rate_00032/ sid_040_rg_400_rate_00 0064 com o grupo de classificação 400 e qualquer taxa).

Com essa configuração, o pacote hello do cliente atinge a régua proposta e é permitido em vez de ser redirecionado. Estas são as duas bases de regras em que as regras do What sapp são vistas:

```
rulebase mbc-internet-rs action priority 1087 dynamic-only ruledef WhatsApp_P2P_040_400_99999_All_internet charging-action sid_040_rg_400_rate_99999 action priority 1088 dynamic-only ruledef WhatsApp_P2P_040_400_00064_All_internet charging-action sid_040_rg_400_rate_00064 action priority 1089 dynamic-only ruledef WhatsApp_P2P_040_400_00032_All_internet charging-action sid_040_rg_400_rate_00032 action priority [1090-9909] dynamic-only ruledef ssl_clienthello charging-action sid_040_rg_400_rate99999/00064/00032 --> Higher priority than all-ip ruledef and charging action with rating group 400
action priority 9910 dynamic-only ruledef all-ip_004_012_00016_MI_internet charging-action sid_004_rg_012_rate_00016
action priority 9920 dynamic-only ruledef all-ip_004_012_00032_MI_internet charging-action sid_004_rg_012_rate_00032
action priority 9930 dynamic-only ruledef all-ip_004_012_00064_MI_internet charging-action sid_004_rg_012_rate_00064


rulebase mbc-iphone-rs
action priority 1206 dynamic-only ruledef WhatsApp_P2P_040_400_99999_All_iphone charging-action sid_040_rg_400_rate_99999
action priority 1207 dynamic-only ruledef WhatsApp_P2P_040_400_00064_All_iphone charging-action sid_040_rg_400_rate_00064
action priority 1208 dynamic-only ruledef WhatsApp_P2P_040_400_00032_All_iphone charging-action sid_040_rg_400_rate_00032
action priority [1209-8999] dynamic-only ruledef ssl_clienthello charging-action sid_040_rg_400_rate99999/00064/00032 --> Higher priority than all-ip ruledef and charging action with rating group 400
action priority 9000 dynamic-only ruledef all-ip_015_150_00016_ALL_iphone charging-action sid_015_rg_150_rate_00016
action priority 9010 dynamic-only ruledef all-ip_015_150_00032_ALL_iphone charging-action sid_015_rg_150_rate_00032
action priority 9020 dynamic-only ruledef all-ip_015_150_00064_ALL_iphone charging-action sid_015_rg_150_rate_00064
action priority 9030 dynamic-only ruledef all-ip_015_150_99999_ALL_iphone charging-action sid_015_rg_150_rate_99999

charging-action sid_040_rg_400_rate_99999
content-id 400
service-identifier 40
billing-action egcdr
cca charging credit
exit

ruledef ssl_clienthello
tcp either-port = 443
tcp payload-length >= 44
tcp payload  starts-with hex-signature 16-03
exit
```