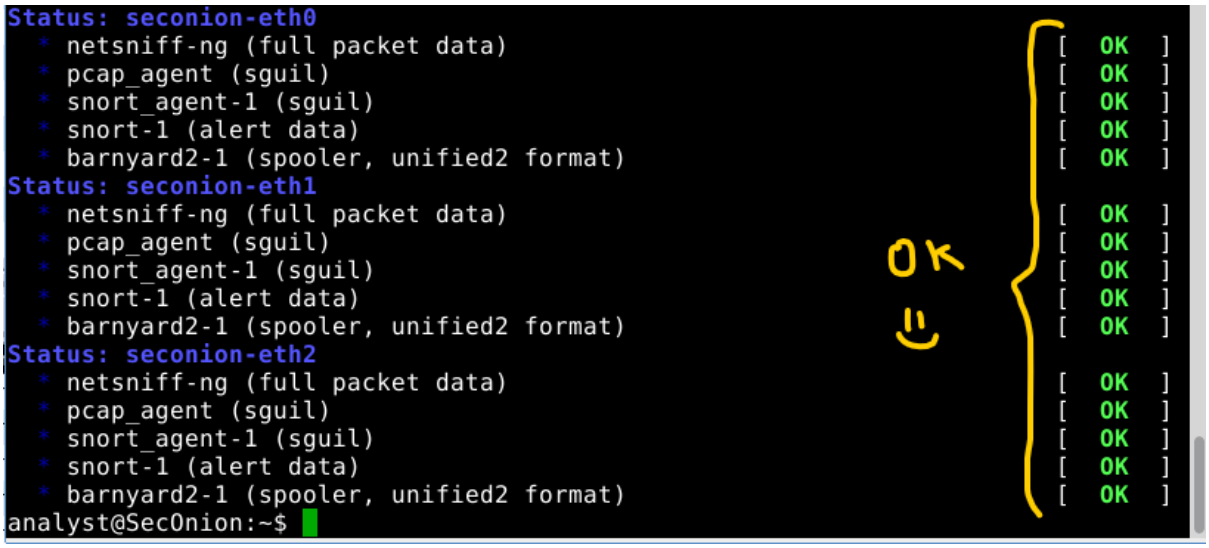
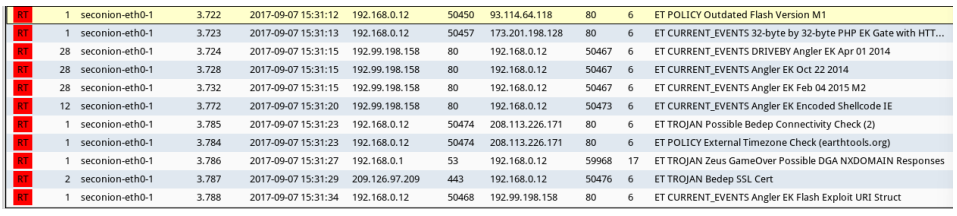
Alumna: Valentina Solange, Vispo.

1c. Todos los sensores están listos.



1d. El ataque genero **103** eventos de 11 alertas, identificando el exploit como ANGLER EK.

Tipo	Alert ID	Contador de alertas	Eventos por alerta
Roja	3772	1	1
Roja	3723	2	1
Roja	3724	3	28
Roja	3728	4	28
Roja	3732	5	28
Roja	3772	6	12
Roja	3785	7	1
Roja	3784	8	1
Roja	3786	9	1
Roja	3787	10	2
Roja	3788	11	1
TOTAL	N/A	11 alertas	(7+28*3+12) = 103 eventos



RT	1	seconion-eth0-1	3.722	2017-09-07 15:31:12	192.168.0.12	50450	93.114.64.118	80	6	ET POLICY Outdated Flash Version M1
RT	1	seconion-eth0-1	3.723	2017-09-07 15:31:13	192.168.0.12	50457	173.201.198.128	80	6	ET CURRENT_EVENTS 32-byte by 32-byte PHP EK Gate with HTT...
RT	28	seconion-eth0-1	3.724	2017-09-07 15:31:15	192.99.198.158	80	192.168.0.12	50467	6	ET CURRENT_EVENTS DRIVEBY Angler EK Apr 01 2014
RT	28	seconion-eth0-1	3.728	2017-09-07 15:31:15	192.99.198.158	80	192.168.0.12	50467	6	ET CURRENT_EVENTS Angler EK Oct 22 2014
RT	28	seconion-eth0-1	3.732	2017-09-07 15:31:15	192.99.198.158	80	192.168.0.12	50467	6	ET CURRENT_EVENTS Angler EK Feb 04 2015 M2
RT	12	seconion-eth0-1	3.772	2017-09-07 15:31:20	192.99.198.158	80	192.168.0.12	50473	6	ET CURRENT_EVENTS Angler EK Encoded Shellcode IE
RT	1	seconion-eth0-1	3.785	2017-09-07 15:31:23	192.168.0.12	50474	208.113.226.171	80	6	ET TROJAN Possible Bedep Connectivity Check (2)
RT	1	seconion-eth0-1	3.784	2017-09-07 15:31:23	192.168.0.12	50474	208.113.226.171	80	6	ET POLICY External Timezone Check (earthtools.org)
RT	1	seconion-eth0-1	3.786	2017-09-07 15:31:27	192.168.0.1	53	192.168.0.12	59968	17	ET TROJAN Zeus GameOver Possible DGA NXDOMAIN Responses
RT	2	seconion-eth0-1	3.787	2017-09-07 15:31:29	209.126.97.209	443	192.168.0.12	50476	6	ET TROJAN Bedep SSL Cert
RT	1	seconion-eth0-1	3.788	2017-09-07 15:31:34	192.168.0.12	50468	192.99.198.158	80	6	ET CURRENT_EVENTS Angler EK Flash Exploit URI Struct

1e. El ataque empezó el **2017-09-05 15:31:12**

El ataque finalizó el **2017-09-07 15:31:34**

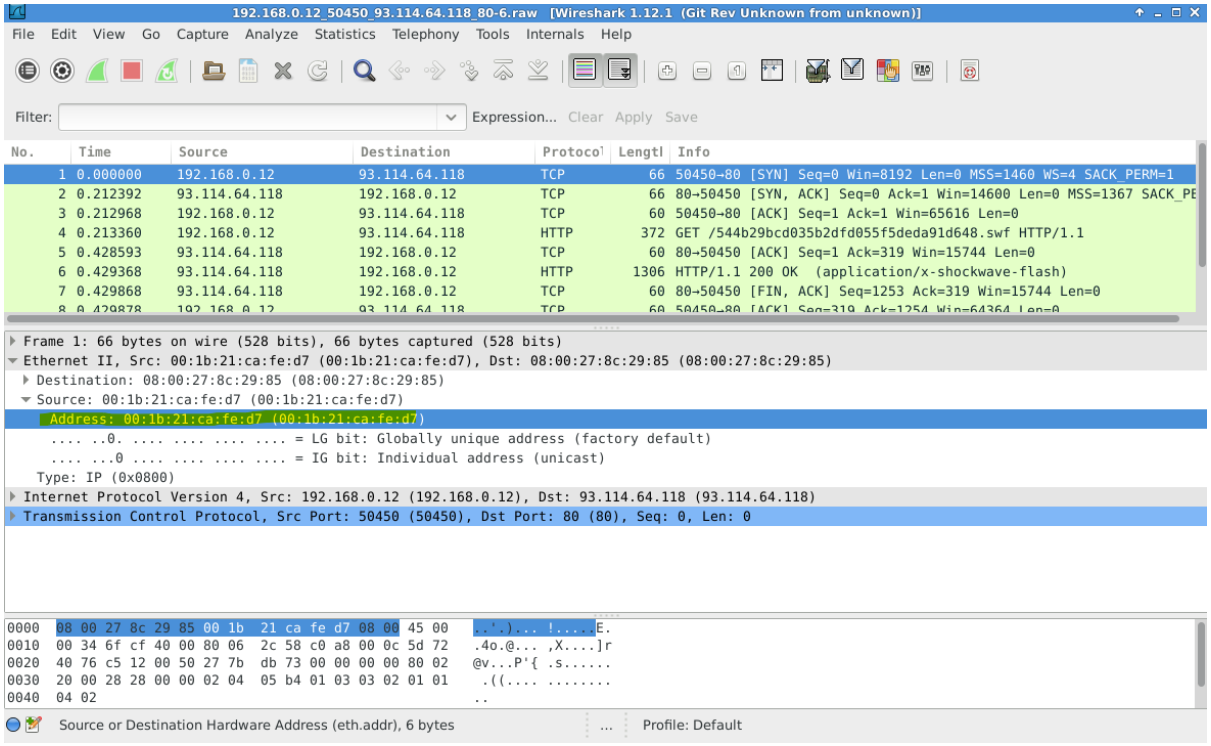
El ataque duró aproximadamente **22 segundos**.

1f. La dirección IP de la computadora interna involucrada en los eventos es: **192.168.0.12** con puerto **50457**

La averigüé con Wireshark, en la IP de origen (Source).

1g. La dirección MAC de la computadora interna involucrada en los eventos es: **00:1b:21:ca:fe:d7**

La averigüé con Wireshark, entrando en el primero, dentro de Ethernet II>Source.

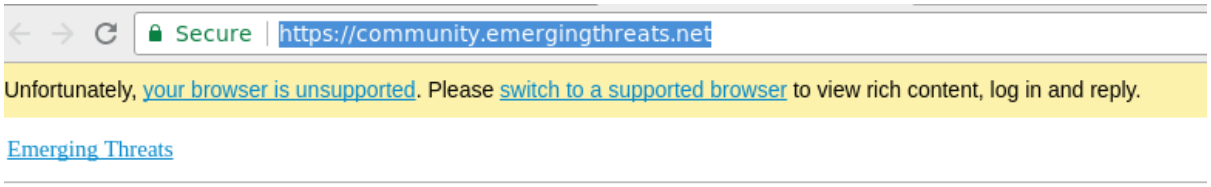


1h. Los IDs de origen de las reglas que se activan cuando ocurre el ataque son:

Alert ID	SID Rule
3772	2014726
3723	2018442
3724	2019224
3728	2019488
3732	2020356
3772	2018954
3785	2020491
3784	2021120
3786	2018316
3787	2019645
3788	2019513

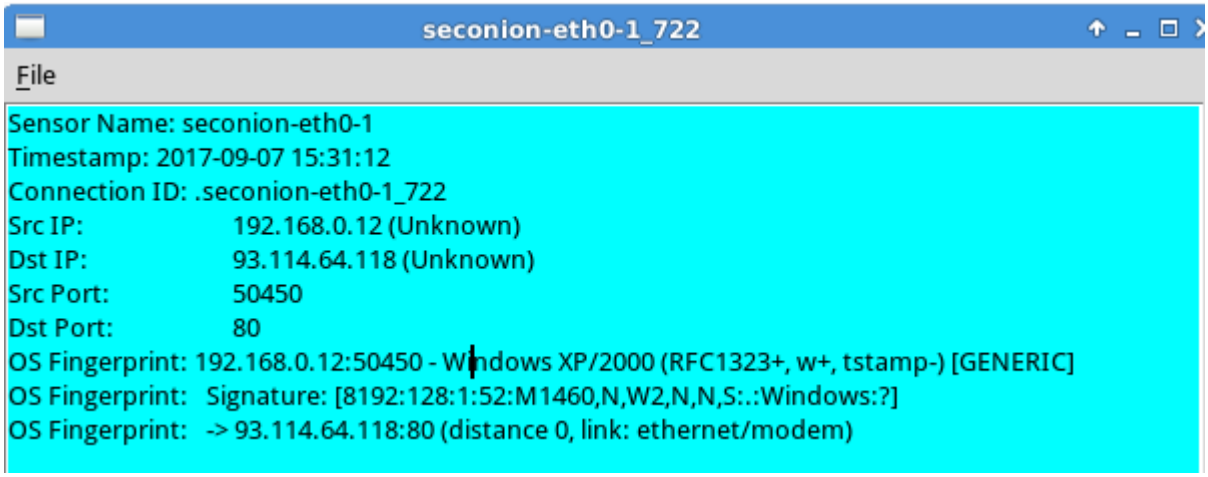
El origen de los SIDs es del sitio **emergingthreats.net** (https://community.emergingthreats.net/)

Aunque desde la máquina virtual no es posible visualizarlo, terminar redireccionando.



1i. Si, los eventos me parecen sospechosos. La computadora interna parece estar infectada dado que tiene una vulnerabilidad por tener ***Flash Player desactualizado***.

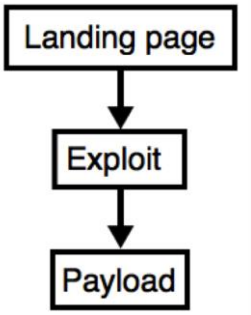
1j. El sistema operativo de la computadora es: Windows XP/2000



2a. Según Snort el kit de ataque es: **Angler EK Flash Exploit URI Struct**.

2b. Un kit de ataque o kit de exploit es un software diseñado para ejecutarse de forma encubierta en servidores web con el fin de identificar vulnerabilidades de software en dispositivos de las victimas que visitan el sitio web, para que las vulnerabilidades detectadas sean aprovechadas para descargar y ejecutar código malicioso en la máquina de la víctima, frecuentemente se usan para distribuir malware como ransomware.

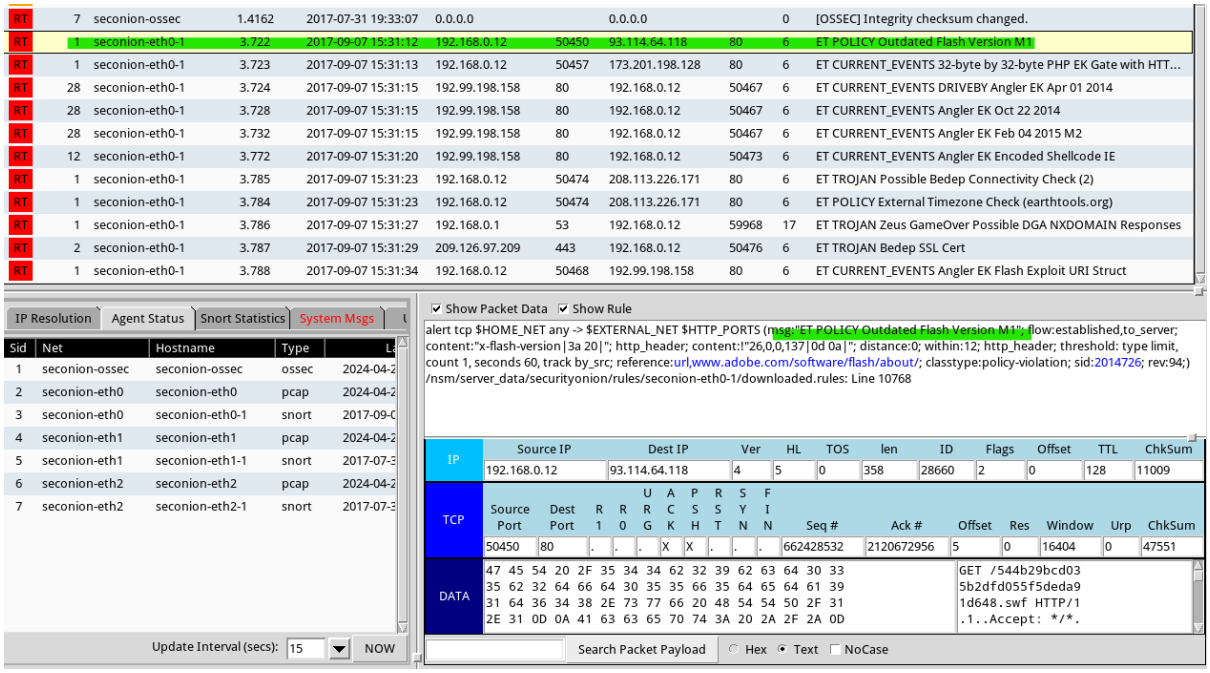
2c. **Angler EK** es una herramienta sofisticada usada por los cibercriminales para distribuir malware, tiene 3 etapas marcadas, pero lo separaré en 4 para mejor compresión:



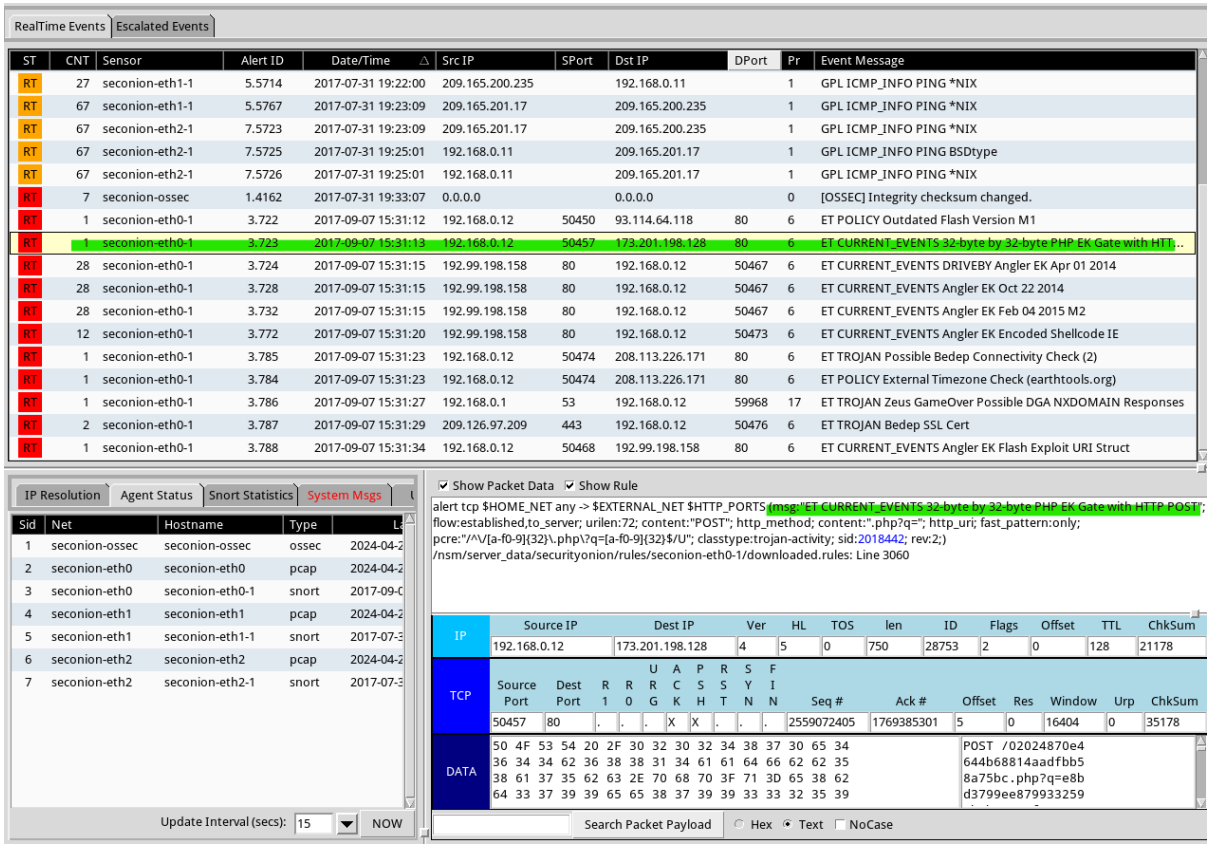
1. HTTP Redirection: un usuario res redirigido a un “servidor EK” o “servidor comprometido”.
2. Angler EK Landing Page: esta página es recibida de forma oculta, el código malicioso no está a simple vista. Sirve para recolectar información de la potencial víctima. El atacante busca vulnerabilidades, como, por ejemplo: Adobe Flash Player, JRE, Microsoft Silverlight.
3. Exploit: Si existe una vulnerabilidad conocida, el EK envía un exploit correspondiente a la vulnerabilidad detectada en el host víctima.
4. Payload: el payload del EK es un malware que puede tener un archivo que realiza o facilita la descarga de archivos.

2d. Este exploit encanja perfectamente en la definición porque realiza todos los pasos mencionados anteriormente, particularmente, explotando una vulnerabilidad sobre **Adobe Flash Player**.

Detalles

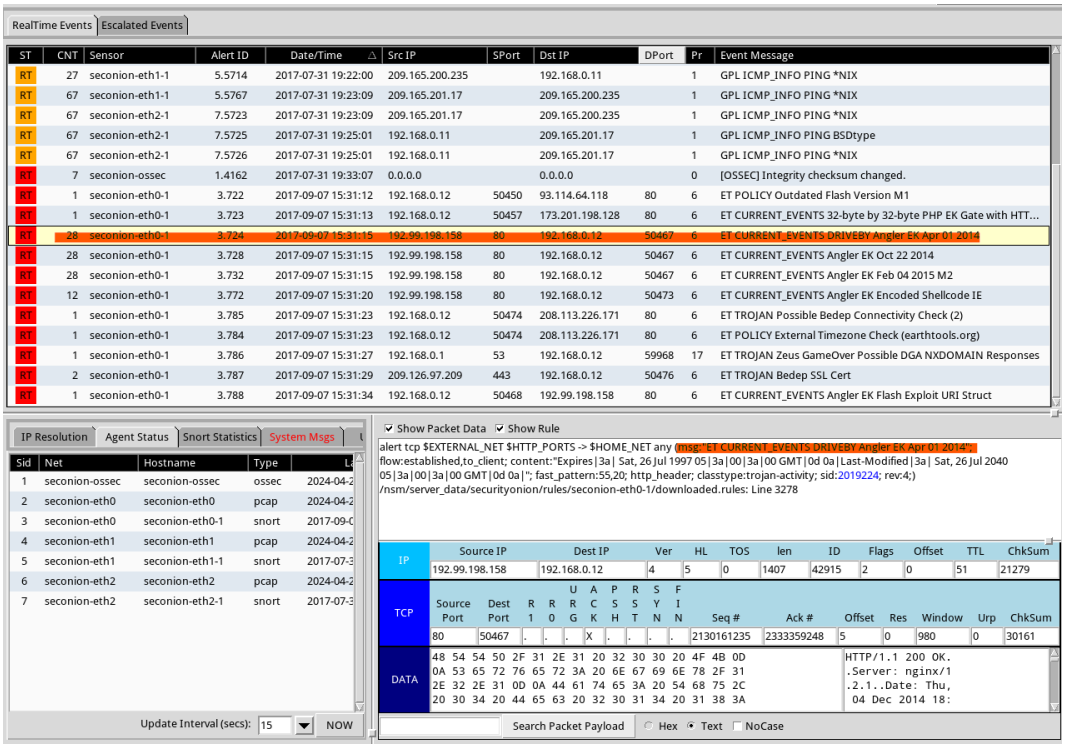


Redirección a lifeinsidedetroit.com, que contiene un archivo en PHP, que es ejecutado y procede a la explotación de las siguientes vulnerabilidades



- **a. ET CURRENT_EVENTS DRIVERBY Angler EK Apr 01 2014**
  - a. Obtiene y ejecuta un archivo.

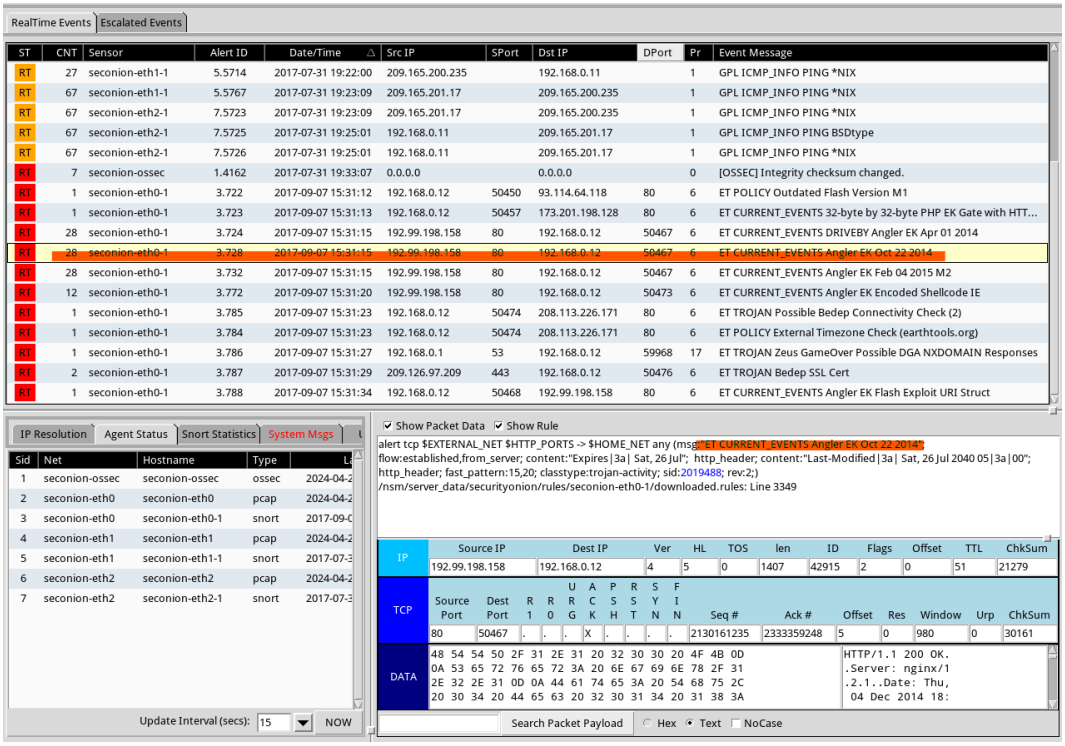
b.



b. ET CURRENT_EVENTS Angler EK Oct 22 2014

a. Obtiene y ejecuta un archivo

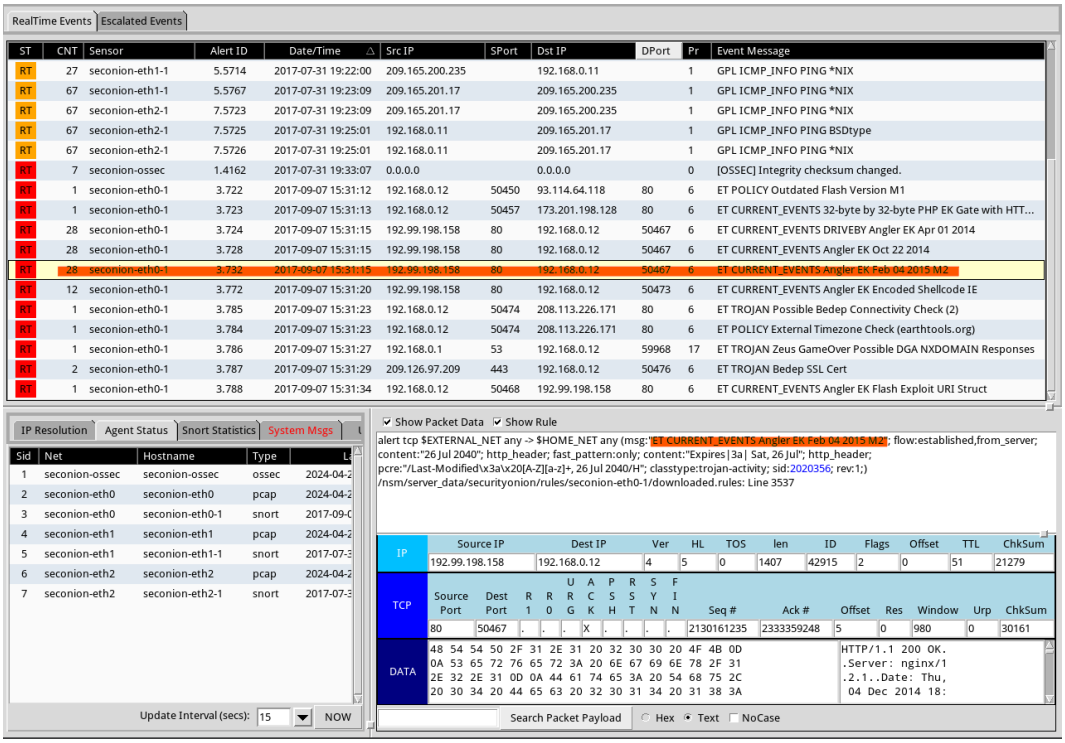
i.



c. ET CURRENT_EVENTS DRIVER Angler EK Feb 04 2015

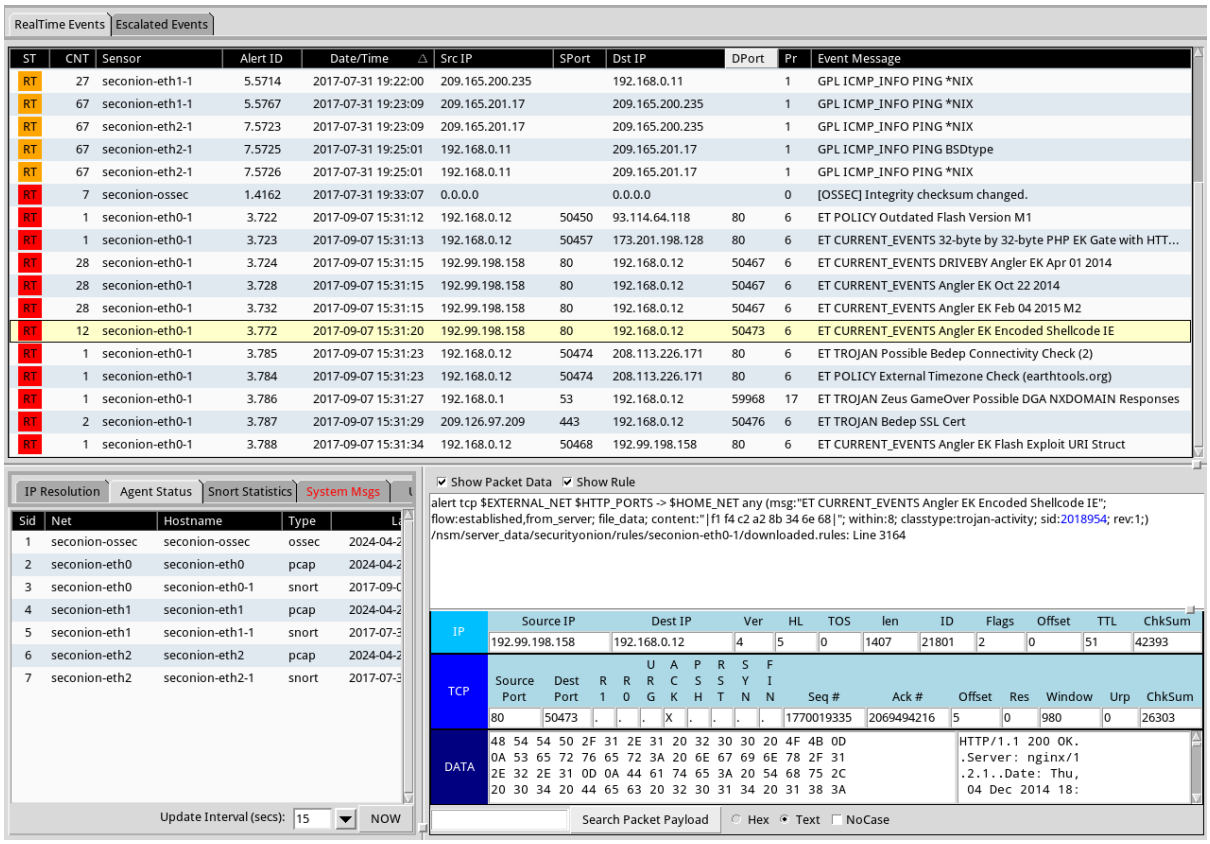
a. Obtiene y ejecuta un archivo

i.


RealTime Events
Escalated Events
ST CNT Sensor Alert ID Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 27 seconion-eth1-1 5.5714 2017-07-31 19:22:00 209.165.200.235 192.168.0.11 1 GPL ICMP_INFO PING *NIX
RT 67 seconion-eth1-1 5.5767 2017-07-31 19:23:09 209.165.201.17 209.165.200.235 1 GPL ICMP_INFO PING *NIX
RT 67 seconion-eth2-1 7.5723 2017-07-31 19:23:09 209.165.201.17 209.165.200.235 1 GPL ICMP_INFO PING *NIX
RT 67 seconion-eth2-1 7.5725 2017-07-31 19:25:01 192.168.0.11 209.165.201.17 1 GPL ICMP_INFO PING BSDtype
RT 67 seconion-eth2-1 7.5726 2017-07-31 19:25:01 192.168.0.11 209.165.201.17 1 GPL ICMP_INFO PING *NIX
RT 7 seconion-ossec 1.4162 2017-07-31 19:33:07 0.0.0.0 0.0.0.0 0 [OSSEC] Integrity checksum changed.
RT 1 seconion-eth0-1 3.722 2017-09-07 15:31:12 192.168.0.12 50450 93.114.64.118 80 6 ET POLICY Outdated Flash Version M1
RT 1 seconion-eth0-1 3.723 2017-09-07 15:31:13 192.168.0.12 50457 173.201.198.128 80 6 ET CURRENT_EVENTS 32-byte by 32-byte PHP EK Gate with HTT...
RT 28 seconion-eth0-1 3.724 2017-09-07 15:31:15 192.99.198.158 80 192.168.0.12 50467 6 ET CURRENT_EVENTS DRIVEBY Angler EK Apr 01 2014
RT 28 seconion-eth0-1 3.728 2017-09-07 15:31:15 192.99.198.158 80 192.168.0.12 50467 6 ET CURRENT_EVENTS Angler EK Oct 22 2014
RT 28 seconion-eth0-1 3.732 2017-09-07 15:31:15 192.99.198.158 80 192.168.0.12 50467 6 ET CURRENT_EVENTS Angler EK Feb 04 2015 M2
RT 12 seconion-eth0-1 3.772 2017-09-07 15:31:20 192.99.198.158 80 192.168.0.12 50473 6 ET CURRENT_EVENTS Angler EK Encoded Shellcode IE
RT 1 seconion-eth0-1 3.785 2017-09-07 15:31:23 192.168.0.12 50474 208.113.226.171 80 6 ET TROJAN Possible Bedep Connectivity Check (2)
RT 1 seconion-eth0-1 3.784 2017-09-07 15:31:23 192.168.0.12 50474 208.113.226.171 80 6 ET POLICY External Timezone Check (earthtools.org)
RT 1 seconion-eth0-1 3.786 2017-09-07 15:31:27 192.168.0.1 53 192.168.0.12 59968 17 ET TROJAN Zeus GameOver Possible DGA NXDOMAIN Responses
RT 2 seconion-eth0-1 3.787 2017-09-07 15:31:29 209.126.97.209 443 192.168.0.12 50476 6 ET TROJAN Bedep SSL Cert
RT 1 seconion-eth0-1 3.788 2017-09-07 15:31:34 192.168.0.12 50468 192.99.198.158 80 6 ET CURRENT_EVENTS Angler EK Flash Exploit URI Struct
IP Resolution
Agent Status
Snort Statistics
System Msgs
Sid Net Hostname Type L
1 seconion-ossec seconion-ossec ossec 2024-04-2
2 seconion-eth0 seconion-eth0 pcap 2024-04-2
3 seconion-eth0 seconion-eth0-1 snort 2017-09-0
4 seconion-eth1 seconion-eth1 pcap 2024-04-2
5 seconion-eth1 seconion-eth1-1 snort 2017-07-3
6 seconion-eth2 seconion-eth2 pcap 2024-04-2
7 seconion-eth2 seconion-eth2-1 snort 2017-07-3
Update Interval (secs): 15 NOW
Show Packet Data
Show Rule
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET CURRENT_EVENTS Angler EK Feb 04 2015 M2"; flow:established,from_server; content:"26 Jul 2040"; http_header; fast_pattern:only; content:"Expires|3a| Sat, 26 Jul"; http_header; pcre:"/Last-Modified\x3a\x20[A-Z][a-z]+, 26 Jul 2040/H"; classtype:trojan-activity; sid:2020356; rev:1;)
/nsm/server_data/securityonion/rules/seconion-eth0-1/downloaded.rules: Line 3537
IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
192.99.198.158 192.168.0.12 4 5 0 1407 42915 2 0 51 21279
TCP Source Port Dest Port R R U A P R S F Seq # Ack # Offset Res Window Urp ChkSum
80 50467 . . . X . . . 2130161235 2333359248 5 0 980 0 30161
DATA
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D
0A 53 65 72 76 65 72 3A 20 6E 67 69 6E 78 2F 31
2E 32 2E 31 0D 0A 44 61 74 65 3A 20 54 68 75 2C
20 30 34 20 44 65 63 20 32 30 31 34 20 31 38 3A
HTTP/1.1 200 OK.
.Server: nginx/1
.2.1..Date: Thu,
04 Dec 2014 18:
Search Packet Payload
Hex
Text
NoCase

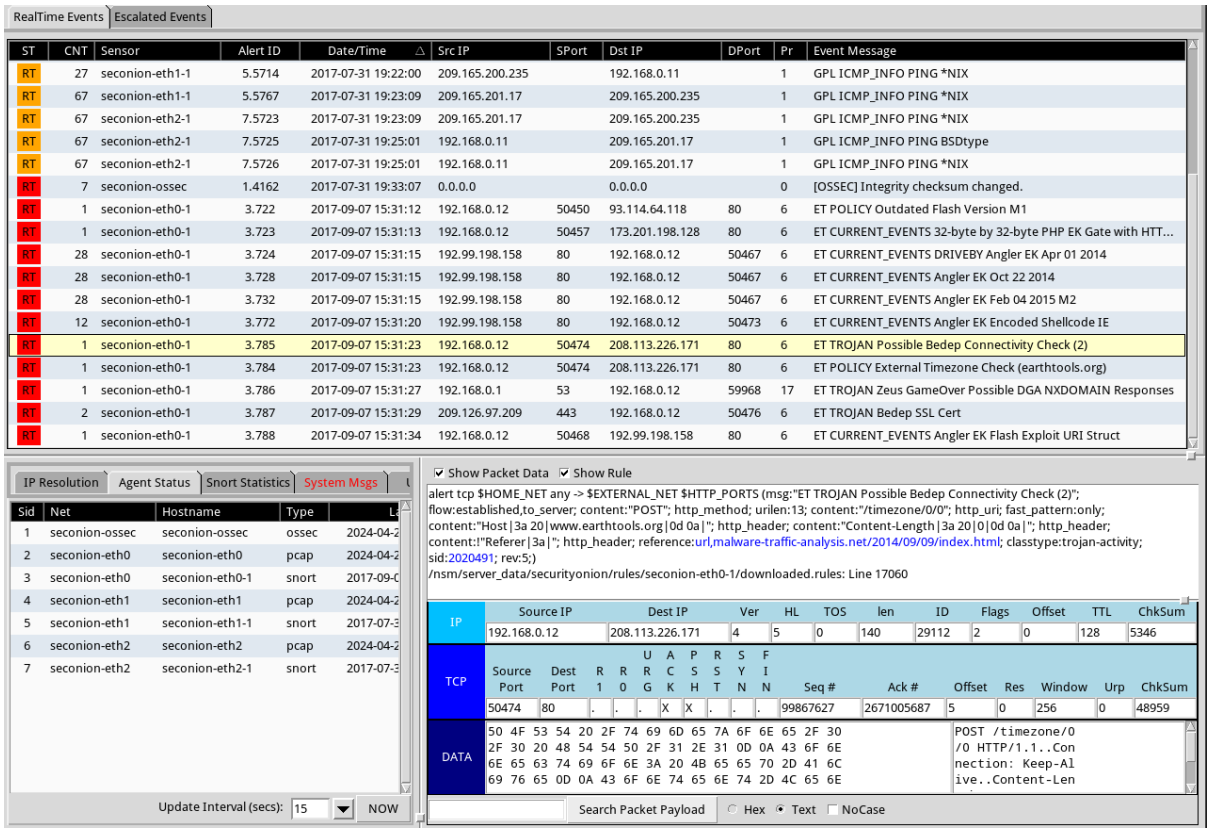
ET CURRENT_EVENTS Angler EK Encoded Shellcode IE

Descarga de archivo malicioso en **qwe.mvdunalterableairreport.net**



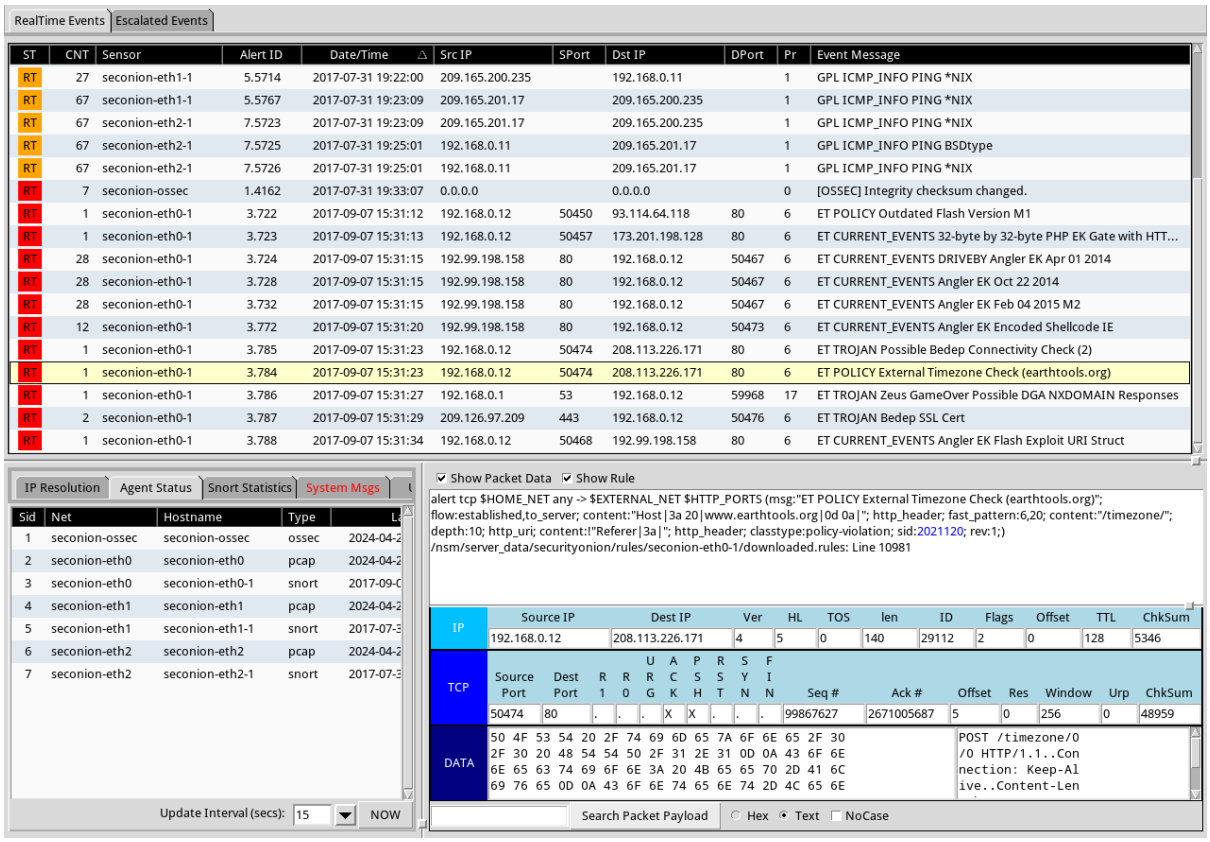
ET TROJAN Possible Bedep Connectivity Check

Realiza una solicitud para revisar la conexión.



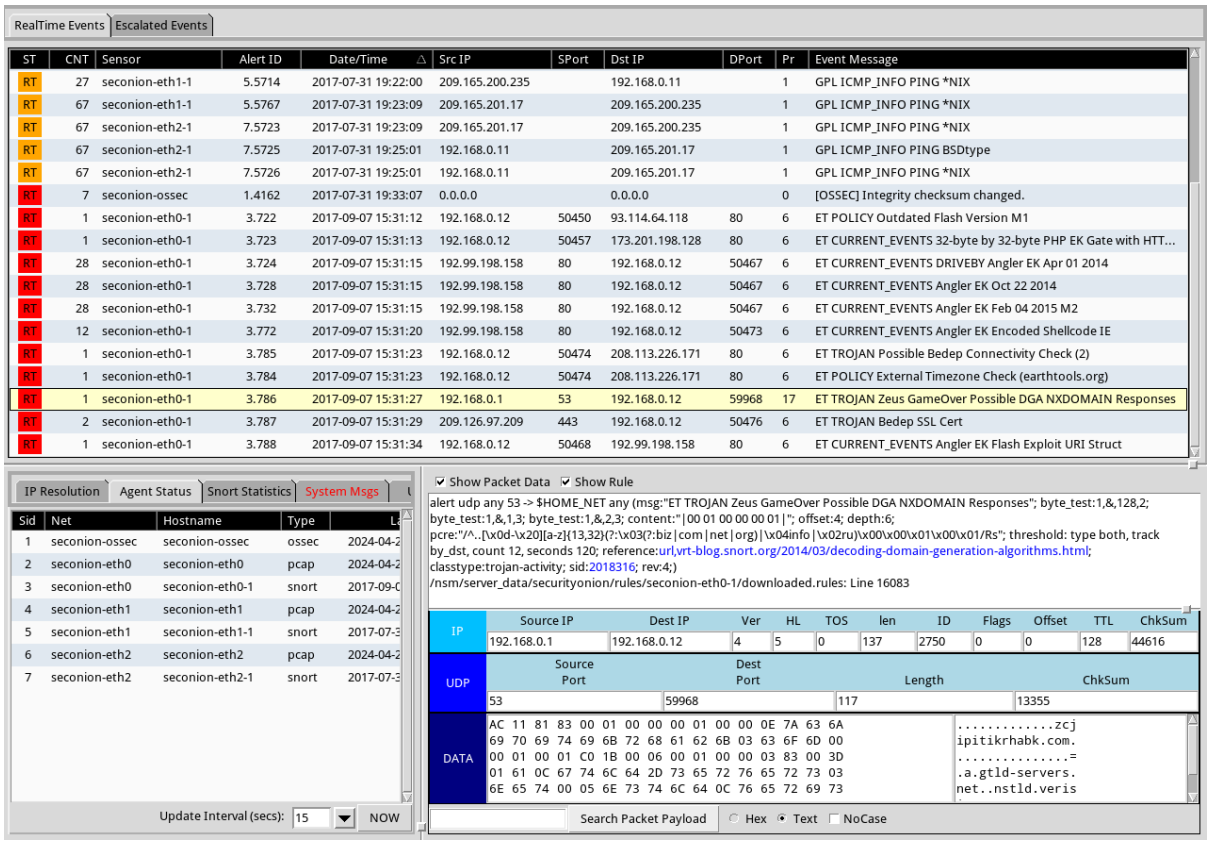
ET POLICY External Timezone Check

Realiza una solicitud de hora para verificar la conexión.



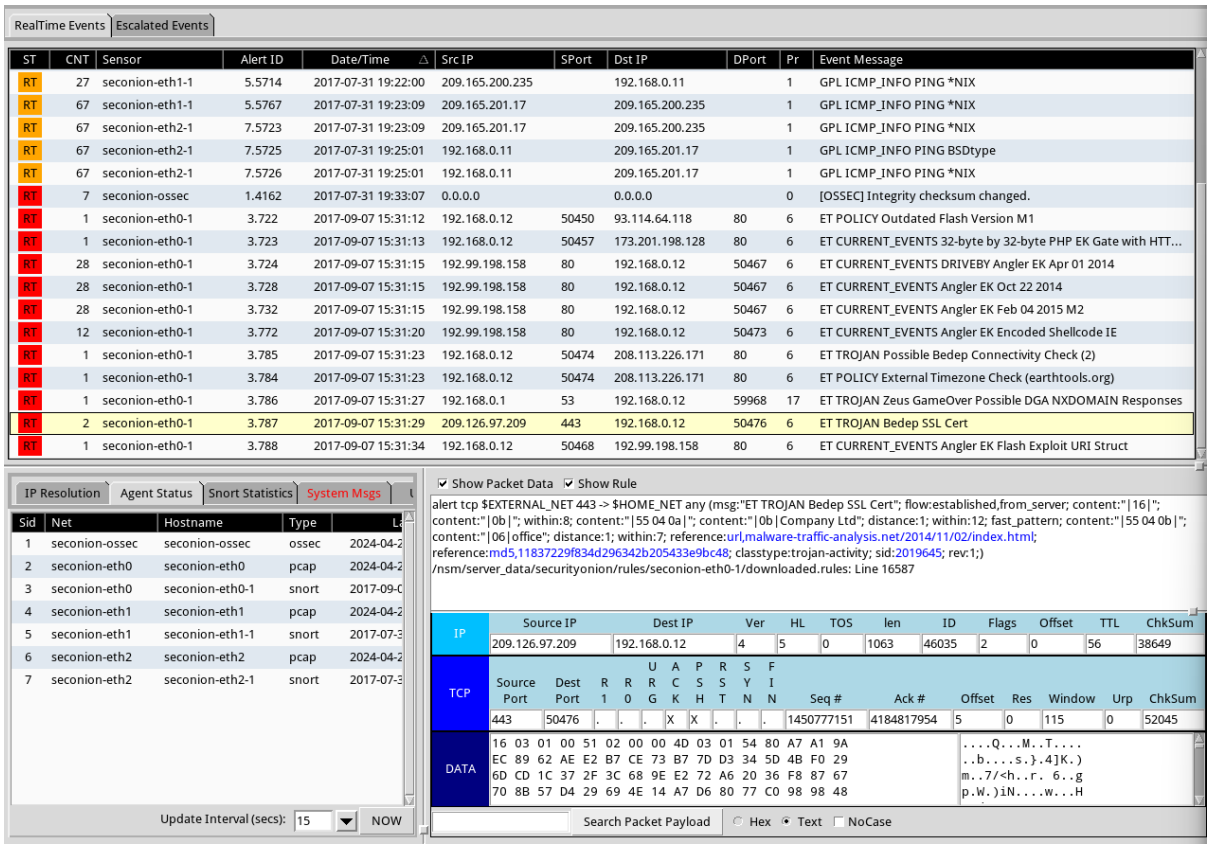
ET TROJAN Zeus GameOver Possible DGA NXDOMAIN Response

Verifica la conexión a través de un DNS.



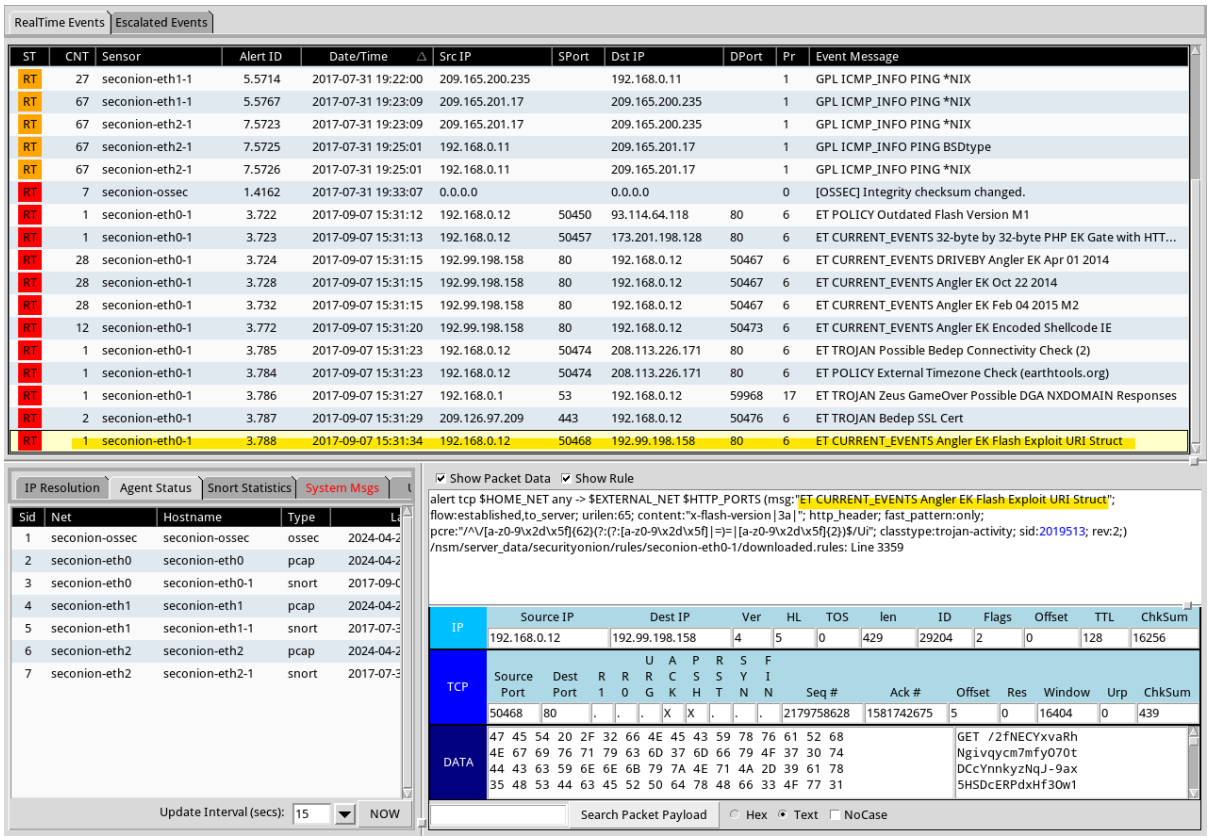
ET TROJAN Bedep SSL Cert

Intenta cargar un certificado falso.



ET CURRENT_EVENTS Angler EK Flash Exploit URI Struct

Redirección sobre **qwe.mvdunalterableairreport.net**



2e. Las principales etapas de los kits de ataque son:

1. **Redirección** a un servidor con código malicioso. Esta redirección suele hacerse comprometiendo un sitio con alto tráfico, generalmente con publicidad o phishing.
2. Las potenciales víctimas acceder al sitio comprometido, cargando el código malicioso.
3. El software maligno **obtiene información** sobre el host.
4. Escanea sobre la información obtenida si se **encuentra** alguna **vulnerabilidad**. Si las encuentra, las envía vía POST a otro servidor.
5. El segundo servidor, recibe los datos del primer servidor. El servidor que recibe la información devuelve un exploit adaptado a la vulnerabilidad detectada.
6. El host recibe el exploit enviado del servidor 2 al servidor 1, entonces, el host termina siendo vulnerado.

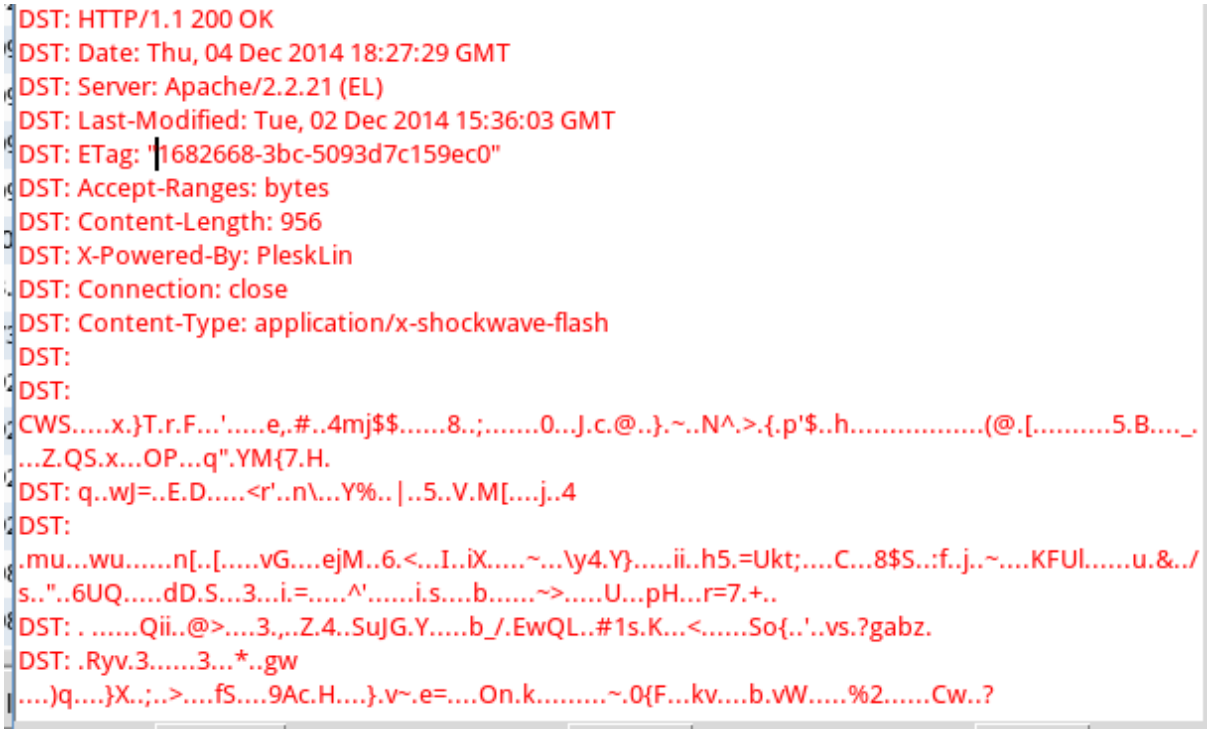
3a. Direcciones IP involucradas, listado: **192.168.0.12**, **93.114.64.118**, **173.201.198.128**, **192.99.198.158**, **208.113.226.171**, **209.126.97.209**

Tabla

Alert ID	IP Origen	IP Destino
3772	**192.168.0.12**	**93.114.64.118**
3723	192.168.0.12	**173.201.198.128**
3724	**192.99.198.158**	192.168.0.12
3728	192.99.198.158	192.168.0.12
3732	192.99.198.158	192.168.0.12
3772	192.99.198.158	192.168.0.12
3785	192.168.0.12	**208.113.226.171**
3784	192.168.0.12	208.113.226.171
3786	192.168.0.1	192.168.0.12
3787	**209.126.97.209**	192.168.0.12
3788	192.168.0.12	192.99.198.158

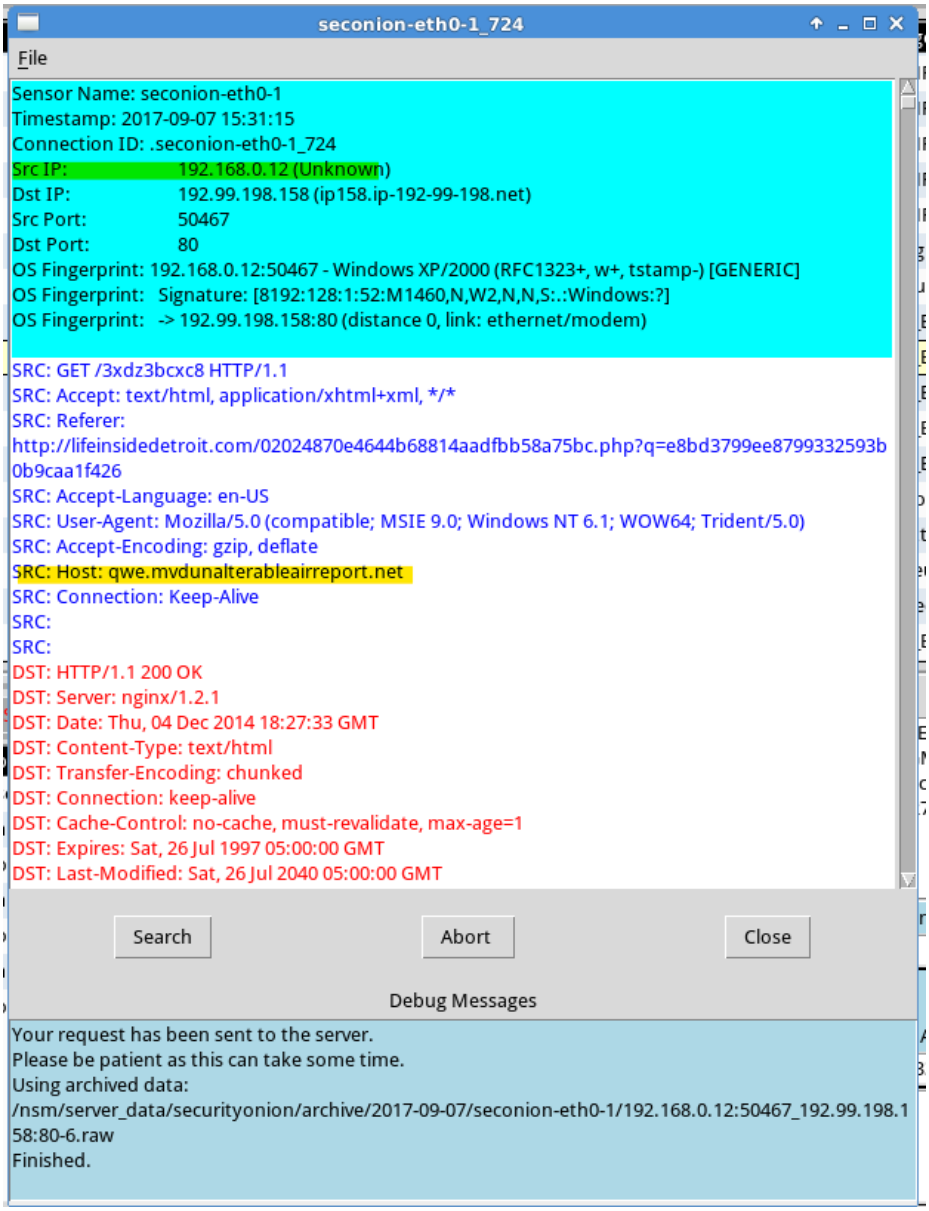
3b. El evento con el mensaje “ET Policy Outdated Flash Version M1” se refiere al host con IP **192.168.0.12** y este evento implica que este host tenía desactualizado un plugin de Flash Player, originando así la vulnerabilidad. Esta vulnerabilidad luego es explotada por **93.114.64.118** cuando el host se conecta al sitio por el puerto 80.

Luego el navegador se conecta a **http://www.earsugery.org/** tiene un objeto Flash, que ejecuta un script malicioso.



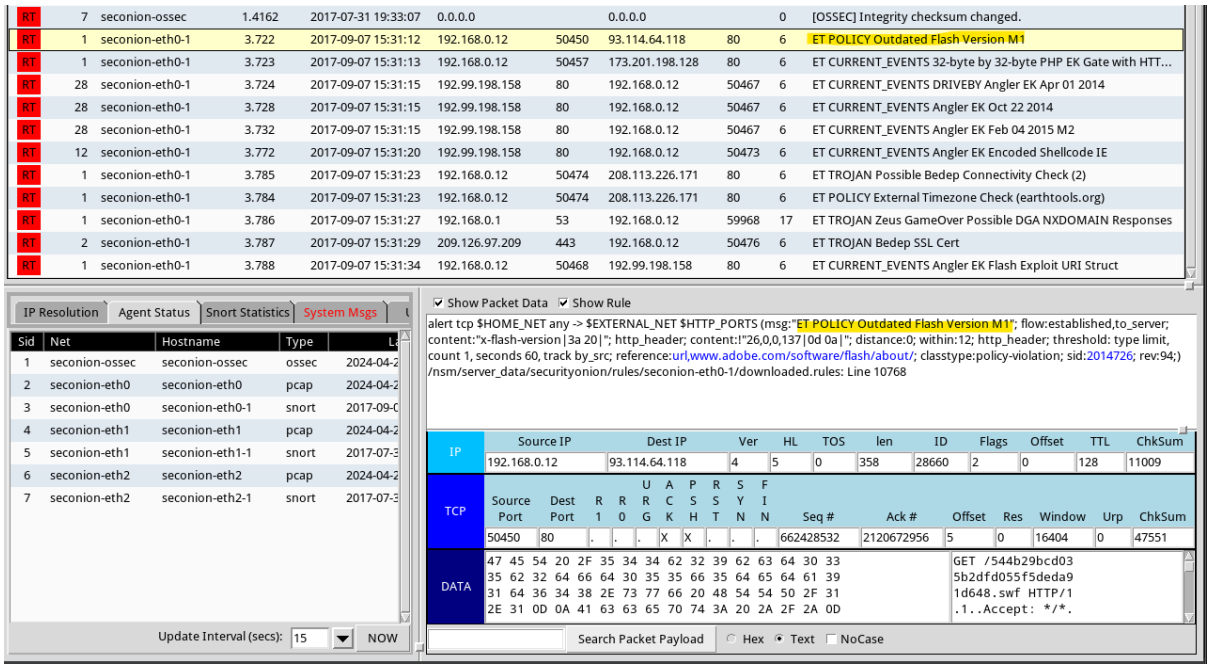
3c. SGUIL indica que el responsable (atacante) de aplicar este ataque corresponde a la dirección IP **93.114.64.118** con puerto 80.

3d. El nombre del dominio asociado a la dirección IP del host que parece haber aplicado el ataque es **qwe.mvdunalterableairreport.net**



3e. Angler EK habitualmente tiene como objetivo vulnerabilidades de 3 aplicaciones de software: **Adobe Flash Player, JRE** y **Microsoft Silverlight.** Al encontrar vulnerabilidades sobre alguna de estas, procede a explotarlas.

3f. Según los eventos de SGUIL la vulnerabilidad que este kit de ataque, Angler EK ha utilizado es el plugin de **Flash Player desactualizado**.



3g. El tipo de archivo más común relacionado con **Flash Player vulnerable** es: **SWF (Shockwave Flash Movie) y FLA (Adobe Flash Animation).**

3h. ELSA afirma que el host víctima recibió malware explotando la vulnerabilidad del plugin de Flash Player.

3i. El host victima **192.168.0.12** con Windows XP/2000 sufrió un ataque de malware desde **IP 192.99.198.158**, provocada por una vulnerabilidad en Adobe Flash Player, dado que estaba desactualizado. Angler EK detectó esa vulnerabilidad. El exploit hizo que el host victima descargase un archivo malicioso desde **qwe.mvdunalterableairreport.net**, concretando así la vulneración.

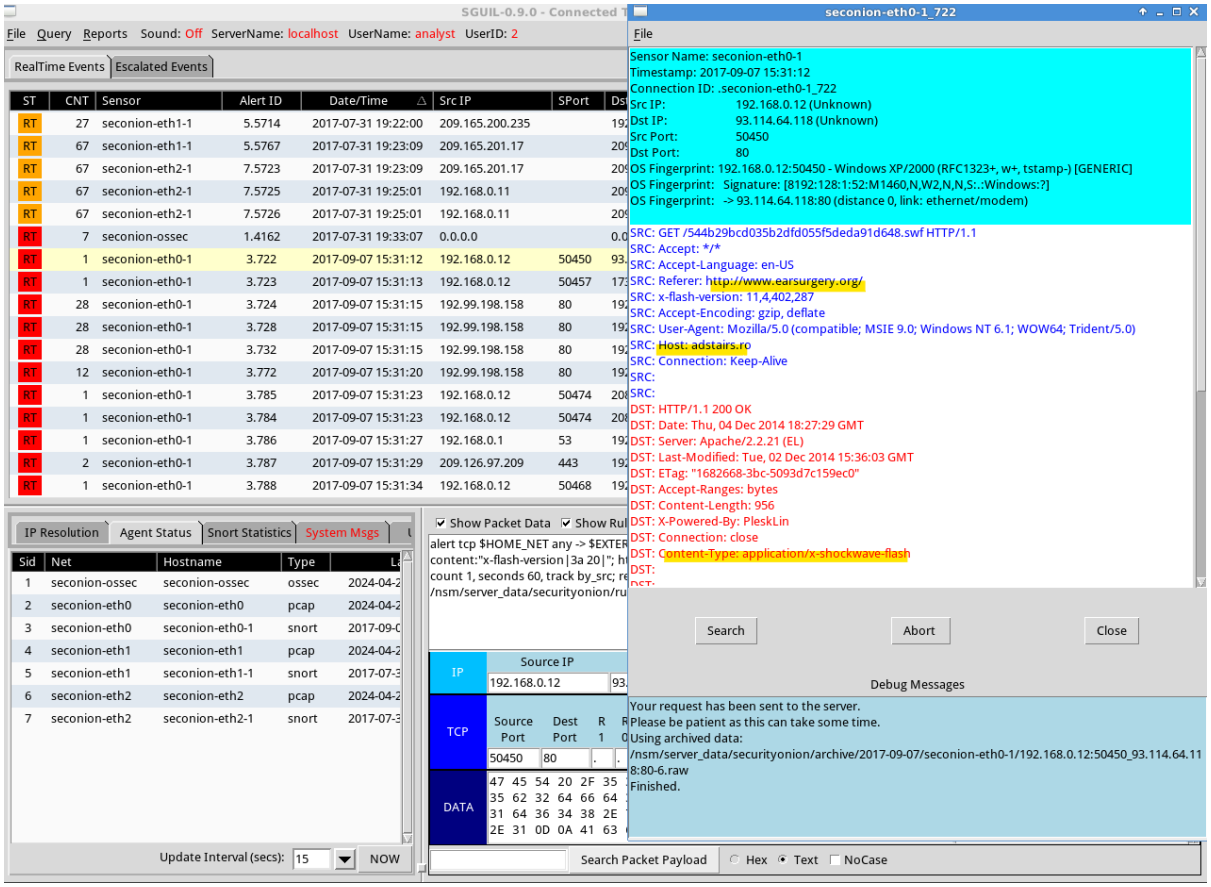
4a. Detalles del exploit son:

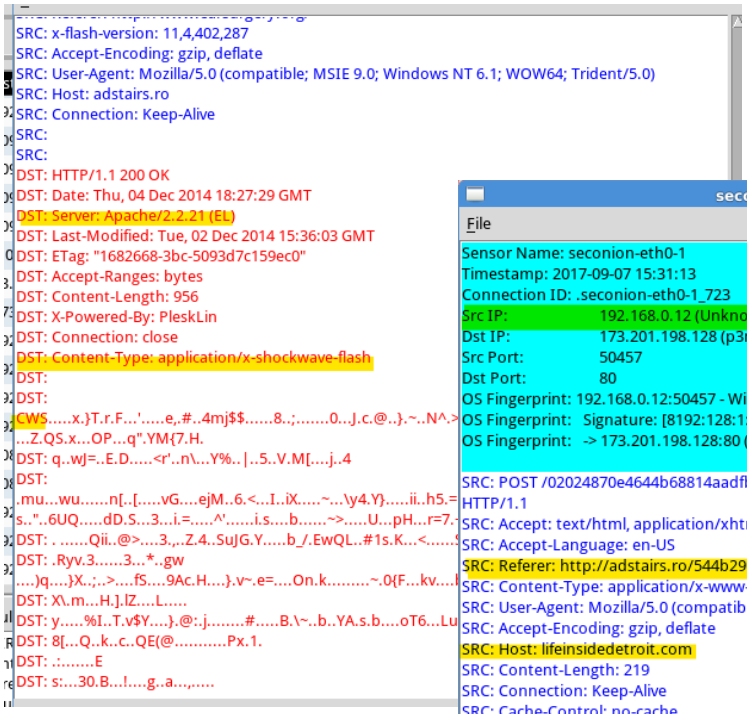
()

Landing page

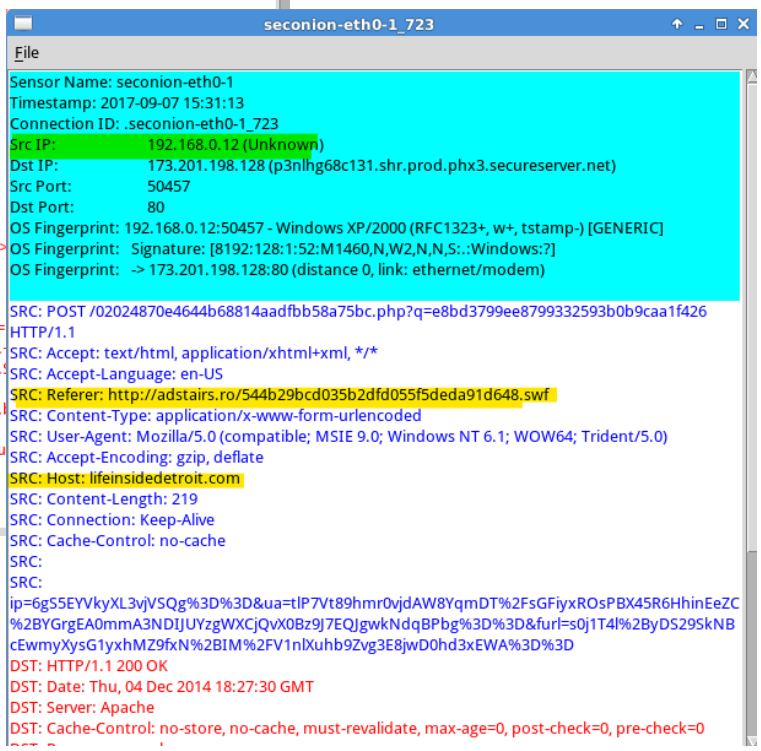
Recolectar información y elegir el exploit del host de acuerdo con los softwares vulnerables del mismo. En este caso, las potenciales víctimas visitan el servidor comprometido http://www.earsurgery.org/ (IP 93.114.64.118) en donde son redireccionados a otro servidor.

Este servidor es **adstairs.ro** tiene un malware en **Flash Player** con el cual se escanea a la potencial victima en busca de vulnerabilidades para posteriormente filtrarlas a la Landing Page del Angler EK.



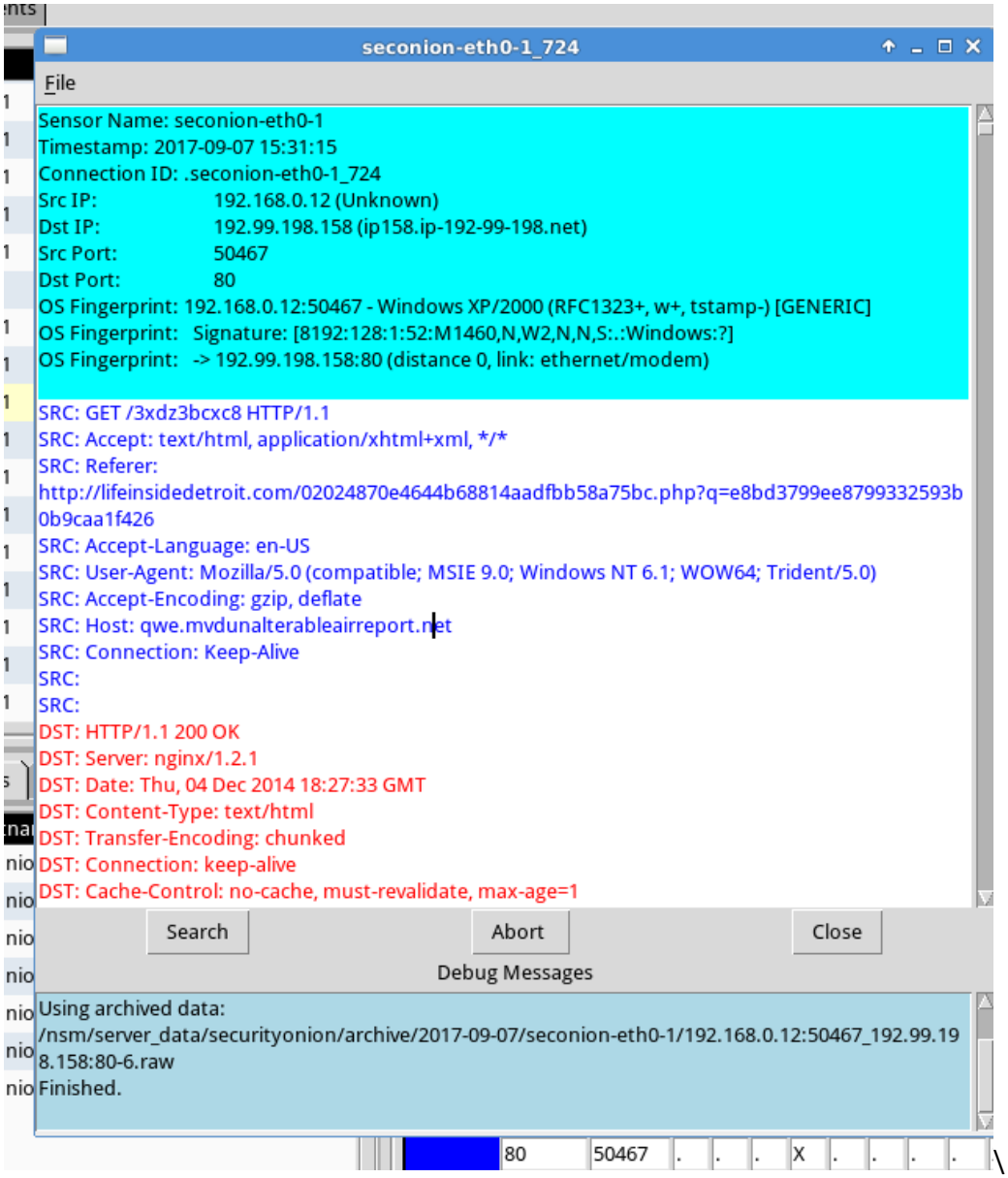


Podemos observar que el servidor es un **Apache/2.2.21 (EL)** que mediante el script de **Flash Player** realiza un POST a un script en PHP



Finalmente tenemos el **servidor de destino** con IP **173.201.198.128,** con URL **lifeinsidedetroit.com**

4b. El nombre del dominio que aplicó el kit de ataque y la carga útil del malware es **qwe.mvdunalterableairreport.net**



4c. La dirección IP que aplicó el kit de ataque y la carga útil del malware es **192.99.198.158**

4d. Los archivos o programas que pude exportar con éxito son:

Name	Size	Type
0	495 bytes	XML document
3xdz3bcxc8	1.4 kB	unknown
3xdz3bcxc8(1)	1.4 kB	unknown
3xdz3bcxc8(2)	1.4 kB	unknown
3xdz3bcxc8(3)	1.4 kB	unknown
3xdz3bcxc8(4)	1.4 kB	unknown
3xdz3bcxc8(5)	1.4 kB	unknown
3xdz3bcxc8(6)	1.4 kB	unknown
3xdz3bcxc8(7)	1.4 kB	unknown
3xdz3bcxc8(8)	1.4 kB	unknown
3xdz3bcxc8(9)	1.4 kB	unknown
544b29bcd035b2dfd055f5deda91d648.swf	956 bytes	Shockwave Flash file
680VBFhpBNBJOYXebSxgwLrtbh3g6JFUllqksWFSsGshhwsguyNL26MGul2oZ3b8	1.9 kB	unknown
02024870e4644b68814aadfbb58a75bc.php%3fq=e8bd3799ee8799332593b0b9caa1	219 bytes	plain text document
02024870e4644b68814aadfbb58a75bc(1).php%3fq=e8bd3799ee8799332593b0b9ca	140 bytes	HTML document
xPF_HAXN7TK9bMAgBjZDwQzO1-Wf5GvrN5_IIRelhbrhqHAlWyTDbaOBMPWitjnX	1.4 kB	unknown