

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.

The screenshot shows the Wireshark interface with a packet capture list at the top and a detailed view of the first packet below. The packet list shows a SYN packet from 192.168.0.12 to 93.114.64.118. The detailed view shows the Ethernet II frame with source MAC address 00:1b:21:ca:fe:d7 and destination MAC address 08:00:27:8c:29:85. Below the Ethernet II frame, the Internet Protocol Version 4 and Transmission Control Protocol details are visible.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.12	93.114.64.118	TCP	66	50450-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.212392	93.114.64.118	192.168.0.12	TCP	66	80-50450 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1367 SACK_PERM=1
3	0.212968	192.168.0.12	93.114.64.118	TCP	60	50450-80 [ACK] Seq=1 Ack=1 Win=65616 Len=0
4	0.213360	192.168.0.12	93.114.64.118	HTTP	372	GET /544b29bcd035b2dfd055f5deda91d648.swf HTTP/1.1
5	0.428593	93.114.64.118	192.168.0.12	TCP	60	80-50450 [ACK] Seq=1 Ack=319 Win=15744 Len=0
6	0.429368	93.114.64.118	192.168.0.12	HTTP	1306	HTTP/1.1 200 OK (application/x-shockwave-flash)
7	0.429868	93.114.64.118	192.168.0.12	TCP	60	80-50450 [FIN, ACK] Seq=1253 Ack=319 Win=15744 Len=0
8	0.430878	192.168.0.12	93.114.64.118	TCP	60	50450-80 [ACK] Seq=319 Ack=1254 Win=64364 Len=0

▼ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▼ Ethernet II, Src: 00:1b:21:ca:fe:d7 (00:1b:21:ca:fe:d7), Dst: 08:00:27:8c:29:85 (08:00:27:8c:29:85)
▼ Destination: 08:00:27:8c:29:85 (08:00:27:8c:29:85)
▼ Source: 00:1b:21:ca:fe:d7 (00:1b:21:ca:fe:d7)
▼ Address: 00:1b:21:ca:fe:d7 (00:1b:21:ca:fe:d7)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
Type: IP (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.0.12 (192.168.0.12), Dst: 93.114.64.118 (93.114.64.118)
▼ Transmission Control Protocol, Src Port: 50450 (50450), Dst Port: 80 (80), Seq: 0, Len: 0

```
0000 08 00 27 8c 29 85 00 1b 21 ca fe d7 08 00 45 00  .....)...!...E.
0010 00 34 6f cf 40 00 80 06 2c 58 c0 a8 00 0c 5d 72  .4o.@...;X...}r
0020 40 76 c5 12 00 50 27 7b db 73 00 00 00 80 02  @v...P'(.s.....
0030 20 00 28 28 00 00 02 04 05 b4 01 03 03 02 01 01  .((.....
0040 04 02  ..
```

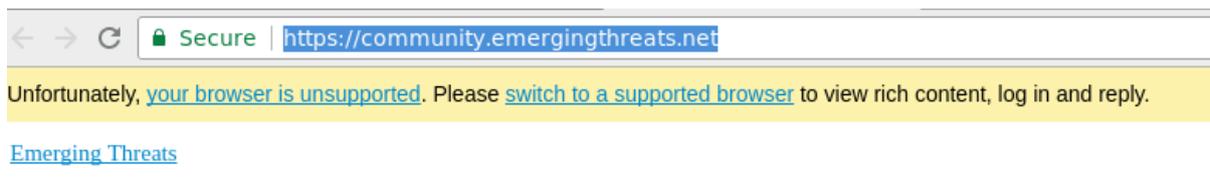
Source or Destination Hardware Address (eth.addr), 6 bytes ... Profile: Default

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

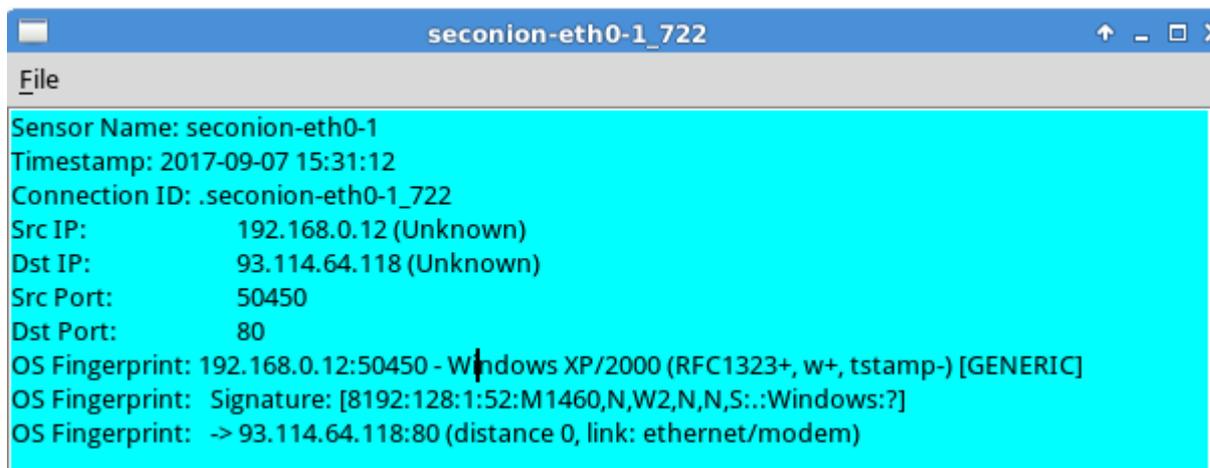
El origen de los SIDs es del sitio **emergingthreats.net** (<https://community.emergingthreats.net/>)

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**.

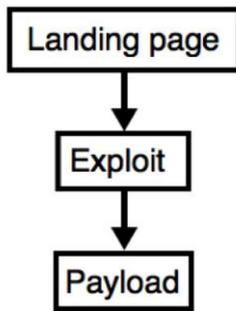
1j. El sistema operativo de la computadora es: Windows XP/2000



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 víctimas 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 comprensión:



- 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 encaja perfectamente en la definición porque realiza todos los pasos mencionados anteriormente, particularmente, explotando una vulnerabilidad sobre **Adobe Flash Player**.

Detalles

SI	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

Alert: alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"ET POLICY Outdated Flash Version M1"; flow:established,to_server; content:"x-flash-version|3a 20|"; http_header; content:"!26,0,0,137|0d 0a|"; distance:0; within:12; http_header; threshold: type limit, count 1, seconds 60, track by_src; reference:url,www.adobe.com/software/flash/about/; classtype:policy-violation; sid:2014726; rev:94); /nsm/server_data/securityonion/rules/seconion-eth0-1/downloaded.rules: Line 10768

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum						
IP	192.168.0.12	93.114.64.118	4	5	0	358	28660	2	0	128	11009						
TCP	Source Port	Dest Port	R	R	R	C	S	S	Y	I	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
TCP	50450	80	.	.	.	X	X	.	.	.	662428532	2120672956	5	0	16404	0	47551
DATA											47 45 54 20 2F 35 34 34 62 32 39 62 63 64 30 33	GET /544b29bcd03					
DATA											35 62 32 64 66 64 30 35 35 66 35 64 65 64 61 39	5b2dfd055f5deda9					
DATA											31 64 36 34 38 2E 73 77 66 20 48 54 54 50 2F 31	1d648.swf HTTP/1					
DATA											2E 31 0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D	.1..Accept: /*.*					

Update Interval (secs): 15 NOW

Search Packet Payload Hex Text NoCase

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 DRIVERBY 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	U
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

Alert top \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg: ET CURRENT_EVENTS DRIVERBY Angler EK Apr 01 2014; flow:established_to_client; content:"Expires [3a] Sat, 26 Jul 1997 05 [3a] [00] [3a] [00] GMT [0d 0a] Last-Modified [3a] Sat, 26 Jul 2040 05 [3a] [00] [3a] [00] GMT [0d 0a]"; fast_pattern:55,20; http_header; classtype:trojan-activity; sid:2019224; rev:4) /nsm/server_data/securityonion/rules/seconion-eth0-1/downloaded.rules: Line 3278

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum							
IP	192.99.198.158	192.168.0.12	4	5	0	1407	42915	2	0	51	21279							
TCP	Source Port	Dest Port	R	R	R	C	S	S	Y	I	Seq#	Ack#	Offset	Res	Window	Urp	ChkSum	
TCP	80	50467	.	.	.	X	2130161235	2333359248	5	0	980	0	30161	
DATA	48	54	54	50	2F	31	2E	31	20	32	30	20	4F	4B	0D	HTTP/1.1 200 OK. .Server: nginx/1 .2.1..Date: Thu, 04 Dec 2014 18:		
DATA	0A	53	65	72	76	65	72	3A	20	6E	67	69	6E	78	2F	31		
DATA	2E	32	2E	31	0D	0A	44	61	74	65	3A	20	54	68	75	2C		
DATA	20	30	34	20	44	65	63	20	32	30	31	34	20	31	38	3A		

Search Packet Payload Hex Text NoCase

- b. ET CURRENT_EVENTS Angler EK Oct 22 2014

a. Obtiene y ejecuta un archivo

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 DRIVERBY 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	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	U
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

Alert top \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg: ET CURRENT_EVENTS DRIVERBY Angler EK Oct 22 2014; flow:established_from_server; content:"Expires [3a] Sat, 26 Jul; http_header; content:"; http_header; fast_pattern:15,20; classtype:trojan-activity; sid:2019488; rev:2) /nsm/server_data/securityonion/rules/seconion-eth0-1/downloaded.rules: Line 3349

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum							
IP	192.99.198.158	192.168.0.12	4	5	0	1407	42915	2	0	51	21279							
TCP	Source Port	Dest Port	R	R	R	C	S	S	Y	I	Seq#	Ack#	Offset	Res	Window	Urp	ChkSum	
TCP	80	50467	.	.	.	X	2130161235	2333359248	5	0	980	0	30161	
DATA	48	54	54	50	2F	31	2E	31	20	32	30	20	4F	4B	0D	HTTP/1.1 200 OK. .Server: nginx/1 .2.1..Date: Thu, 04 Dec 2014 18:		
DATA	0A	53	65	72	76	65	72	3A	20	6E	67	69	6E	78	2F	31		
DATA	2E	32	2E	31	0D	0A	44	61	74	65	3A	20	54	68	75	2C		
DATA	20	30	34	20	44	65	63	20	32	30	31	34	20	31	38	3A		

Search Packet Payload Hex Text NoCase

- c. ET CURRENT_EVENTS DRIVERBY Angler EK Feb 04 2015

a. Obtiene y ejecuta un archivo

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	Update
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):

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:"25 Jul 2040"; http_header; fast_pattern:only; content:"Expires [3a] Sat, 26 Jul"; http_header; pcre:"/Last-Modifiedvx3av20[A-Z][a-z]+; 26 Jul 2040/"; classtype:trojan-activity; sid:20202556; 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	C	S	S	Y	I	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	80	50467	.	.	X	2130161235	2333359248	5	0	980	0	30161

DATA	Hex	Text
	48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 48 0D	HTTP/1.1 200 OK.
	0A 53 65 72 76 65 72 3A 20 6E 67 69 6E 78 2F 31	.Server: nginx/1
	2E 32 2E 31 0D 0A 44 61 74 65 3A 20 54 68 75 2C	2.1..Date: Thu,
	20 30 34 20 44 65 63 20 32 30 31 34 20 31 38 3A	04 Dec 2014 18:

Hex
 Text
 NoCase

i.

ET CURRENT_EVENTS Angler EK Encoded Shellcode IE

Descarga de archivo malicioso en qwe.mvdunalterableairreport.net

RealTime Events
Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Δ	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	La
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

Show Packet Data
Show Rule

alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET CURRENT_EVENTS Angler EK Encoded Shellcode IE"; flow:established,from_server; file_data; content: "[f1 f4 c2 a2 8b 34 6e 68]"; within:8; classtype:trojan-activity; sid:2018954; rev:1;) /nsm/server_data/securityonion/rules/seconion-eth0-1/downloaded.rules: Line 3164

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	21801	2	0	51	42393

TCP	Source Port	Dest Port	R	R	R	C	S	S	Y	I	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	80	50473	.	.	.	X	1770019335	2069494216	5	0	980	0	26303

DATA	Hex	ASCII
	48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D	HTTP/1.1 200 OK.
	0A 53 65 72 76 65 72 3A 20 6E 67 69 6E 78 2F 31	.Server: nginx/1
	2E 32 2E 31 0D 0A 44 61 74 65 3A 20 54 68 75 2C	.2.1..Date: Thu,
	20 30 34 20 44 65 63 20 32 30 31 34 20 31 38 3A	04 Dec 2014 18:

ET TROJAN Possible Bedep Connectivity Check

Realiza una solicitud para revisar la conexión.

RealTime Events
Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dest 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	Time
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 \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"ET TROJAN Possible Bedep Connectivity Check (2)";
 flow:established,to_server; content:"POST"; http_method:urllen:13; content:"/timezone/0/0"; http_uri; fast_pattern:only;
 content:"Host[3a 20]www.earthtools.org[0d 0a]"; http_header; content:"Content-Length[3a 20]0[0d 0a]"; http_header;
 content:"Referer[3a]"; http_header; reference:url,malware-traffic-analysis.net/2014/09/09/index.html; classtype:trojan-activity;
 sid:2020491; rev:5;)

/nsm/server_data/securityonion/rules/seconion-eth0-1/downloaded.rules: Line 17060

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	192.168.0.12	208.113.226.171	4	5	0	140	29112	2	0	128	5346

TCP	Source Port	Dest Port	R	R	U	A	P	R	S	F	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	50474	80	X	X	.	.	99867627	2671005687	5	0	256	0	48959

DATA	Hex	ASCII
50 4F 53 54 20 2F 74 69 6D 65 7A 6F 6E 65 2F 30 2F 30 20 48 54 54 50 2F 31 2E 31 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E		POST /timezone/0 /0 HTTP/1.1..Con nection: Keep-All ive..Content-Len

Search Packet Payload
 Hex Text NoCase

ET POLICY External Timezone Check

Realiza una solicitud de hora para verificar la conexión.

RealTime Events
Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Δ	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
RS	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	LA
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	2017-09-07
4	seconion-eth1	seconion-eth1	pcap	2024-04-2
5	seconion-eth1	seconion-eth1-1	snort	2017-07-31
6	seconion-eth2	seconion-eth2	pcap	2024-04-2
7	seconion-eth2	seconion-eth2-1	snort	2017-07-31

Update Interval (secs): 15
NOW

Show Packet Data
 Show Rule

```

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY External Timezone Check (earthtools.org)";
flow:established,to_server; content:"Host[3a 20]www.earthtools.org[0d 0a]"; http_header; fast_pattern:6,20; content:"/timezone";
depth:10; http_uri; content:"Referer[3a]"; http_header; classtype:policy-violation; sid:2021120; rev:1;)
/nsm/server_data/securityonion/rules/seconion-eth0-1/downloaded.rules: Line 10981
                    
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	192.168.0.12	208.113.226.171	4	5	0	140	29112	2	0	128	5346

TCP	Source Port	Dest Port	R	U	A	P	R	S	F	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
TCP	50474	80	.	.	.	X	X	.	.	99867627	2671005687	5	0	256	0	48959

DATA	Hex	ASCII
DATA	50 4F 53 54 20 2F 74 69 6D 65 7A 6F 6E 65 2F 30 2F 30 20 48 54 54 50 2F 31 2E 31 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E	POST /timezone/0 /0 HTTP/1.1..Con nection: Keep-Alive..Content-Len

Search Packet Payload
 Hex Text NoCase

ET TROJAN Zeus GameOver Possible DGA NXDOMAIN Response

Verifica la conexión a través de un DNS.

RealTime Events
Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Δ	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	Δ
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

Show Packet Data
 Show Rule

alert udp any 53 -> \$HOME_NET any (msg:"ET TROJAN Zeus GameOver Possible DGA NXDOMAIN Responses"; byte_test:1,&128,2; byte_test:1,&1,3; byte_test:1,&2,3; content:"[00 01 00 00 00 01]"; offset:4; depth:6; pcre:"/^\.[\x0d-\x20][a-z]{13,32}?:\x03(?:[com|net|org])\x04info[\x02ru]\x00\x00\x01\x00\x01/Rs"; threshold: type both, track by_dst, count 12, seconds 120; reference:url|vrt-blog.snort.org/2014/03/decoding-domain-generation-algorithms.html; classtype:trojan-activity; sid:2018316; rev:4)

/nsm/server_data/securityonion/rules/seconion-eth0-1/downloaded.rules: Line 16083

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	192.168.0.1	192.168.0.12	4	5	0	137	2750	0	0	128	44616

UDP	Source Port	Dest Port	Length	ChkSum
	53	59968	117	13355

AC 11 81 83 00 01 00 00 01 00 00 0E 7A 63 6A 69 70 69 74 69 6B 72 68 61 62 6B 03 63 6F 6D 00 00 01 00 01 C0 1B 00 06 00 01 00 00 03 83 00 3D 01 61 0C 67 74 6C 64 2D 73 65 72 76 65 72 73 03 6E 65 74 00 05 6E 73 74 6C 64 0C 76 65 72 69 73zCj ipitkrhbk.com.= .a.gtld-servers. net..nstld.veris
--	--

Update Interval (secs): 15
▼ NOW

Search Packet Payload
 Hex Text NoCase

ET TROJAN Bedep SSL Cert

Intenta cargar un certificado falso.

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	...
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

Show Packet Data | Show Rule

```

alert tcp $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ET TROJAN Bedep SSL Cert"; flow:established,from_server; content:"|16|";
content:"|0b|"; within:8; content:"|55 04 0a|"; content:"|0b|Company Ltd"; distance:1; within:12; fast_pattern; content:"|55 04 0b|";
content:"|06|office"; distance:1; within:7; reference:url,malware-traffic-analysis.net/2014/11/02/index.html;
reference:md5,11837229f834d296342b205433e9bc48; classtype:trojan-activity; sid:2019645; rev:1;)
/nsm/server_data/securityonion/rules/seconion-eth0-1/downloaded.rules: Line 16587
        
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	209.126.97.209	192.168.0.12	4	5	0	1063	46035	2	0	56	38649

TCP	Source Port	Dest Port	R	R	R	C	S	S	Y	I	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
TCP	443	50476	.	.	.	X	1450777151	4184817954	5	0	115	0	52045

DATA	Hex	ASCII
DATA	16 03 01 00 51 02 00 00 40 03 01 54 80 A7 A1 9A EC 89 62 AE E2 B7 CE 73 B7 7D D3 34 5D 4B F0 29 6D CD 1C 37 2F 3C 68 9E E2 72 A6 20 36 F8 87 67 70 8B 57 D4 29 69 4E 14 A7 D6 80 77 C0 98 98 48Q...M...T... ..b...s..4]K.) m../<h...f. 6..g p.W.)iN...w...H

Hex
 Text
 NoCase

ET CURRENT_EVENTS Angler EK Flash Exploit URI Struct

Redirección sobre **qwe.mvdunalterableairreport.net**

The screenshot shows a network security tool interface. The top part displays a list of events under 'RealTime Events' and 'Escalated Events'. The bottom part shows a detailed view of a specific event, including packet data and a rule definition.

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

Sid	Net	Hostname	Type	Last
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


```

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS Angler EK Flash Exploit URI Struct";
flow:established,to_server; urilen:65; content:"x-flash-version|3a|"; http_header; fast_pattern:only;
pcrc:"/^\[a-z0-9x2d\x5f\{62\}(\?:\{[a-z0-9x2d\x5f\}]=\)[a-z0-9x2d\x5f\{2\}\$|U"; classtype:trojan-activity; sid:2019513; rev:2);
/nsm/server_data/securityonion/rules/seconion-eth0-1/downloaded.rules: Line 3359
    
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	192.168.0.12	192.99.198.158	4	5	0	429	29204	2	0	128	16256

TCP	Source Port	Dest Port	R	R	R	R	C	S	S	Y	I	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
TCP	50468	80	X	X	.	.	.	2179758628	1581742675	5	0	16404	0	439

DATA	Hex	ASCII
DATA	47 45 54 20 2F 32 66 4E 45 43 59 78 76 61 52 68 4E 67 69 76 71 79 63 6D 37 6D 66 79 4F 37 30 74 44 43 63 59 6E 6E 6B 79 7A 4E 71 4A 2D 39 61 78 35 48 53 44 63 45 52 50 64 78 48 66 33 4F 77 31	GET /2fNECYxvaRh Ngivqycm7mfy070t DCcyNnkyzNqJ-9ax 5HSDCERPdxHf30w1

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.

```
Sensor Name: seconion-eth0-1
Timestamp: 2017-09-07 15:31:12
Connection ID: .seconion-eth0-1_722
Src IP:      192.168.0.12 (Unknown)
Dst IP:      93.114.64.118 (Unknown)
Src Port:    50450
Dst Port:    80
OS Fingerprint: 192.168.0.12:50450 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W2,N,N,S:::Windows:?]
OS Fingerprint: -> 93.114.64.118:80 (distance 0, link: ethernet/modem)

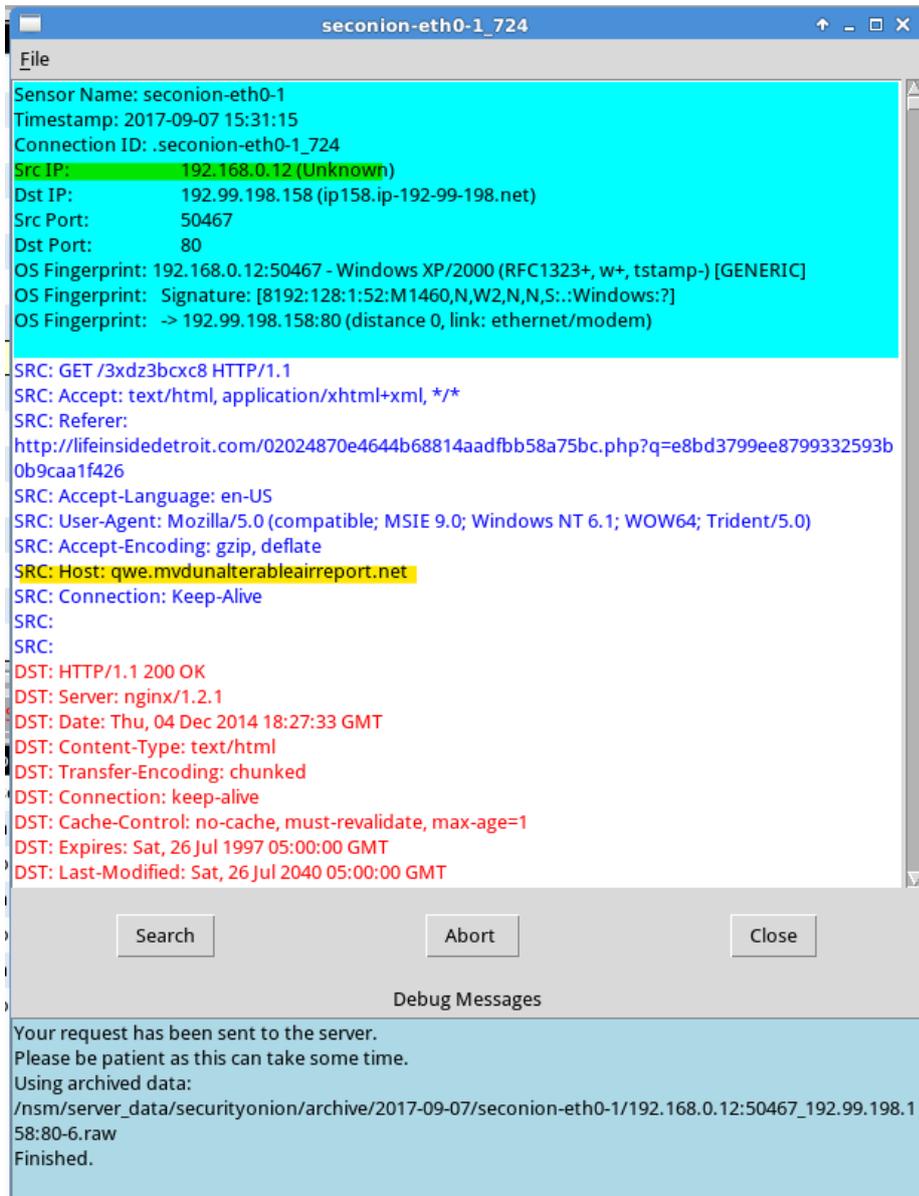
SRC: GET /544b29bcd035b2dfd055f5deda91d648.swf HTTP/1.1
SRC: Accept: */*
SRC: Accept-Language: en-US
SRC: Referer: http://www.earsurgery.org/
SRC: x-flash-version: 11,4,402,287
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
```

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

```
DST: HTTP/1.1 200 OK
DST: Date: Thu, 04 Dec 2014 18:27:29 GMT
DST: Server: Apache/2.2.21 (EL)
DST: Last-Modified: Tue, 02 Dec 2014 15:36:03 GMT
DST: ETag: "1682668-3bc-5093d7c159ec0"
DST: Accept-Ranges: bytes
DST: Content-Length: 956
DST: X-Powered-By: PleskLin
DST: Connection: close
DST: Content-Type: application/x-shockwave-flash
DST:
DST:
CWS.....x.}T.r.F...'.....e,#..4mj$$.....8.;.....0...J.c.@..}.~..N^.>.{.p'$.h.....(@.[.....5.B...._
...Z.QS.x...OP...q".YM{7.H.
DST: q..wj=..E.D.....<r'\..n\...Y%.. |..5..V.M[....j..4
DST:
..mu...wu.....n[. [. ....vG....ejM..6.<...I..iX.....~...y4.Y}.....ii.h5.=Ukt;....C...8$S...:f..j.~....KFUL.....u.&.. /
s.."..6UQ.....dD.S...3...i.=.....^'.....i.s....b.....~>.....U...pH...r=7.+..
DST: . ....Qii..@>....3,..Z.4..SujG.Y.....b_/..EwQL..#1s.K...<.....So{..'..vs.?gabz.
DST: .Ryv.3.....3...*.gw
.....)q.....}X.;;..>....fS....9Ac.H....}.v~.e=....On.k.....~.0{F...kv....b.vW.....%2.....Cw..?
```

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**.

The screenshot displays the SGUIL interface. At the top, a table lists various events. The event of interest is highlighted in yellow:

RT	Sid	Net	Hostname	Type	Time	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum	Alert
RT	1	seconion-eth0-1	seconion-eth0-1	pcap	2024-04-2 15:31:12	192.168.0.12	93.114.64.118	4	5	0	358	28660	2	0	128	11009	ET-POLICY Outdated Flash Version M1

Below the table, the 'System Msgs' tab is active, showing a detailed packet capture for the selected event. The packet is a TCP SYN packet from 192.168.0.12 to 93.114.64.118. The alert message is:

```

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET-POLICY Outdated Flash Version M1"; flow:established,to_server;
content:"x-flash-version|3a 20|"; http_header; content:"!26,0,0,137|0d 0a|"; distance:0; within:12; http_header; threshold: type limit,
count 1, seconds 60, track by_src; reference:url,www.adobe.com/software/flash/about/; classtype:policy-violation; sid:2014726; rev:94;)
/nsm/server_data/securityonion/rules/seconion-eth0-1/downloaded.rules: Line 10768
  
```

The packet details show:

- IP:** Source IP: 192.168.0.12, Dest IP: 93.114.64.118, Ver: 4, HL: 5, TOS: 0, len: 358, ID: 28660, Flags: 2, Offset: 0, TTL: 128, ChkSum: 11009
- TCP:** Source Port: 50450, Dest Port: 80, Seq #: 662428532, Ack #: 2120672956, Offset: 5, Res: 0, Window: 16404, Urp: 0, ChkSum: 47551
- DATA:** GET /544b29bc035b2dfd055f5deda91d648_swf HTTP/1.1 . . . Accept: */*

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.

The screenshot displays the SGUIL-0.9.0 interface. The top window shows a list of alerts with columns for ST, CNT, Sensor, Alert ID, Date/Time, Src IP, and SPort. The bottom window shows the details of a specific alert, including the sensor name, timestamp, connection ID, and various headers like SRC, DST, OS Fingerprint, and User-Agent. The User-Agent header is highlighted as 'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)' and the Host header is 'adstairs.ro'. The bottom right window shows a debug message: 'Your request has been sent to the server. Please be patient as this can take some time. Using archived data: /nsm/server_data/securityonion/archive/2017-09-07/seconion-eth0-1/192.168.0.12:50450_93.114.64.118-80-6.raw Finished.'

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	Dst Port
RT	27	seconion-eth1-1	5.5714	2017-07-31 19:22:00	209.165.200.235	192	192.168.0.12 (Unknown)	80
RT	67	seconion-eth1-1	5.5767	2017-07-31 19:23:09	209.165.201.17	20	192.168.0.12 (Unknown)	80
RT	67	seconion-eth2-1	7.5723	2017-07-31 19:23:09	209.165.201.17	20	192.168.0.12 (Unknown)	80
RT	67	seconion-eth2-1	7.5725	2017-07-31 19:25:01	192.168.0.11	20	192.168.0.12 (Unknown)	80
RT	67	seconion-eth2-1	7.5726	2017-07-31 19:25:01	192.168.0.11	20	192.168.0.12 (Unknown)	80
RT	7	seconion-ossec	1.4162	2017-07-31 19:33:07	0.0.0.0	0	192.168.0.12	50450
RT	1	seconion-eth0-1	3.722	2017-09-07 15:31:12	192.168.0.12	50450	93.114.64.118	80
RT	1	seconion-eth0-1	3.723	2017-09-07 15:31:13	192.168.0.12	50457	93.114.64.118	80
RT	28	seconion-eth0-1	3.724	2017-09-07 15:31:15	192.99.198.158	80	93.114.64.118	80
RT	28	seconion-eth0-1	3.728	2017-09-07 15:31:15	192.99.198.158	80	93.114.64.118	80
RT	28	seconion-eth0-1	3.732	2017-09-07 15:31:15	192.99.198.158	80	93.114.64.118	80
RT	12	seconion-eth0-1	3.772	2017-09-07 15:31:20	192.99.198.158	80	93.114.64.118	80
RT	1	seconion-eth0-1	3.785	2017-09-07 15:31:23	192.168.0.12	50474	93.114.64.118	80
RT	1	seconion-eth0-1	3.784	2017-09-07 15:31:23	192.168.0.12	50474	93.114.64.118	80
RT	1	seconion-eth0-1	3.786	2017-09-07 15:31:27	192.168.0.1	53	93.114.64.118	80
RT	2	seconion-eth0-1	3.787	2017-09-07 15:31:29	209.126.97.209	443	93.114.64.118	80
RT	1	seconion-eth0-1	3.788	2017-09-07 15:31:34	192.168.0.12	50468	93.114.64.118	80

```

SRC: x-flash-version: 11,4,402,287
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
SRC: Host: adstairs.ro
SRC: Connection: Keep-Alive
DST: HTTP/1.1 200 OK
DST: Date: Thu, 04 Dec 2014 18:27:29 GMT
DST: Server: Apache/2.2.21 (EL)
DST: Last-Modified: Tue, 02 Dec 2014 15:36:03 GMT
DST: ETag: "1682668-3bc-5093d7c159ec0"
DST: Accept-Ranges: bytes
DST: Content-Length: 956
DST: X-Powered-By: PleskLin
DST: Connection: close
DST: Content-Type: application/x-shockwave-flash
DST:
DST:
CWS.....x.)T.r.F.....e,#.4mj$$.8.;.....0..j.c.@.}.~.N^>
...Z.QS.x...OP...q"YM{7.H.
DST: q..wj=.E.D.....<r'.n\...Y%..|.5.V.M[....j..4
DST:
.mu...wu.....n[. [...vG....ejM..6.<...I..ix.....~...ly4.Y).....ii..h5.=
s..".6UQ.....dD.S...3...i=.....^'.....i.s...b.....>.....U...pH...F=7.
DST: . ....Qii...@>...3,...Z.4..SujG.Y.....b_/..EwQL..#1s.K...<.....
DST: .Ryv.3.....3...*.gw
....j)q....)X;...>....fs.....9Ac.H....).v~.e=....On.k.....~.0(F...kv....J
DST: X.l.m...H.j.IZ....L.....
DST: y...%I..T.v$Y....).@:..j.....#.....B.\~..b..YA.s.b.....oT6...Lu
DST: 8[...Q...k..c..c..QE@.....Px.1.
DST: :.....E
DST: s...30.B...!....g...a.....

```

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

```

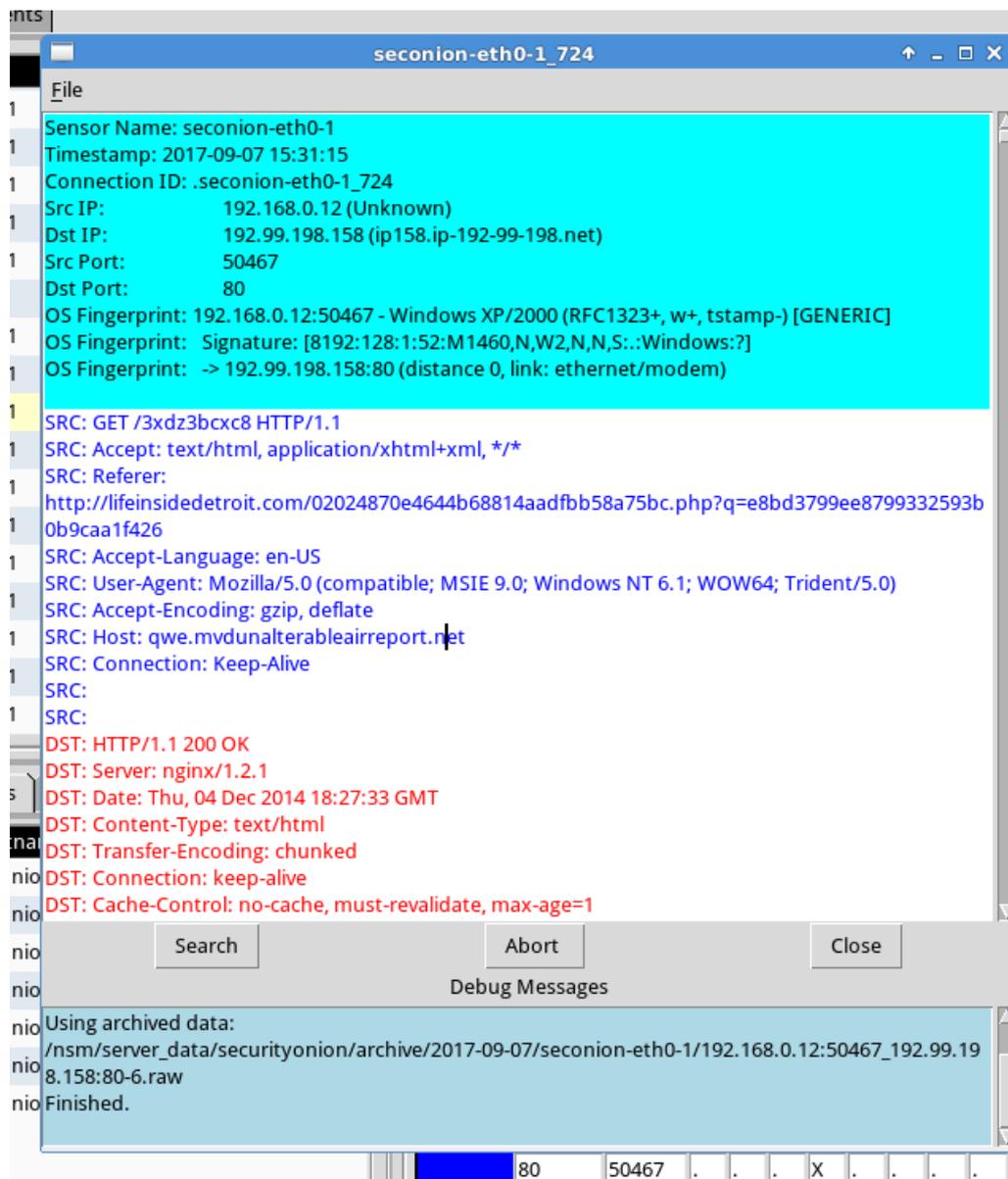
seconion-eth0-1_723
File
Sensor Name: seconion-eth0-1
Timestamp: 2017-09-07 15:31:13
Connection ID: seconion-eth0-1_723
Src IP: 192.168.0.12 (Unknown)
Dst IP: 173.201.198.128 (p3nlhg68c131.shr.prod.phx3.secureserver.net)
Src Port: 50457
Dst Port: 80
OS Fingerprint: 192.168.0.12:50457 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W2,N,N,S,::Windows:?]
OS Fingerprint: -> 173.201.198.128:80 (distance 0, link: ethernet/modem)

SRC: POST /02024870e4644b68814aadfb58a75bc.php?q=e8bd3799ee8799332593b0b9caa1f426
HTTP/1.1
SRC: Accept: text/html, application/xhtml+xml, */*
SRC: Accept-Language: en-US
SRC: Referer: http://adstairs.ro/544b29bcd035b2dfd055f5deda91d648.swf
SRC: Content-Type: application/x-www-form-urlencoded
SRC: User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
SRC: Accept-Encoding: gzip, deflate
SRC: Host: lifeinsidedetroit.com
SRC: Content-Length: 219
SRC: Connection: Keep-Alive
SRC: Cache-Control: no-cache
SRC:
SRC:
ip=6g55EYVkyXL3vjV5Qg%3D%3D&ua=tIP7Vt89hmr0vjdAW8YqmDT%2FsGfIyxROsPBX45R6HhinEeZC
%2BYGrgEA0mmA3NDIJUYzGWXcJQvX0Bz9j7EQjgwkNdqBPBg%3D%3D&furl=s0j1T4l%2ByDS29SkNB
cEwmyXysG1yxhMZ9fxN%2BIM%2FV1nIXuhb9Zvg3E8jwD0hd3xEWA%3D%3D
DST: HTTP/1.1 200 OK
DST: Date: Thu, 04 Dec 2014 18:27:30 GMT
DST: Server: Apache
DST: Cache-Control: no-store, no-cache, must-revalidate, max-age=0, post-check=0, pre-check=0

```

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_IIRelhrhqHAIWyTDbaOBMPWitjnX	1.4 kB	unknown