2014-11-16 pcap Analysis

1) Analysis performed in Ubuntu VM since malware is Windows based.

2) Exercise and pcap file located at:

   - https://www.malware-traffic-analysis.net/2014/11/23/index.html

1) What is the IP address of the Windows VM that gets infected?

Statistics > Conversations

Wireshark · Conversations · 2014-11-23-traffic-analysis-exercise.pcap

Conversation Settings

- [ ] Name resolution
- [ ] Absolute start ti
- [ ] Limit to display f

Copy

Follow Stream...

Graph...

Protocol	
[ ]	Bluetooth
[ ]	DCCP
[x]	Ethernet
[ ]	FC
[ ]	FDDI
[ ]	IEEE 802.11
[ ]	IEEE 802.15.
[x]	IPv4
[x]	IPv6
[ ]	IPX
[ ]	JXTA

Filter list for specifi...

Ethernet · 1 | IPv4 · 95 | IPv6 | TCP · 172 | UDP · 99

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Pac
172.16.165.132	2.18.118.74	15	3.602 KiB	7	1.281 KiB	
172.16.165.132	2.18.187.141	17	8.027 KiB	7	722 bytes	
172.16.165.132	2.18.189.224	21	6.509 KiB	9	1.333 KiB	
172.16.165.132	5.10.75.178	12	2.268 KiB	6	770 bytes	
172.16.165.132	5.175.83.84	9	2.311 KiB	4	634 bytes	
172.16.165.132	23.51.193.8	18	3.022 KiB	10	1.292 KiB	
172.16.165.132	23.215.60.227	12	2.916 KiB	6	794 bytes	
172.16.165.132	23.235.43.166	92	24.288 KiB	42	6.477 KiB	
172.16.165.132	23.251.128.113	15	3.300 KiB	7	1.137 KiB	
172.16.165.132	31.186.225.23	30	12.577 KiB	14	1.743 KiB	
172.16.165.132	31.186.225.24	99	35.747 KiB	45	17.184 KiB	
172.16.165.132	37.143.15.180	447	424.435 KiB	125	7.517 KiB	
172.16.165.132	37.157.6.226	15	3.867 KiB	7	1.199 KiB	
172.16.165.132	37.252.163.96	35	9.691 KiB	16	3.253 KiB	
172.16.165.132	38.65.9.35	10	1.452 KiB	5	680 bytes	
172.16.165.132	46.51.183.190	12	2.186 KiB	6	762 bytes	
172.16.165.132	46.137.160.237	15	4.125 KiB	7	1.170 KiB	
172.16.165.132	46.228.164.11	51	10.361 KiB	25	3.536 KiB	
172.16.165.132	46.228.164.13	12	2.063 KiB	6	830 bytes	
172.16.165.132	50.87.149.90	12	2.455 KiB	6	664 bytes	
172.16.165.132	54.72.16.243	15	3.340 KiB	7	1.189 KiB	
172.16.165.132	54.72.19.177	15	3.211 KiB	7	1.168 KiB	
172.16.165.132	54.72.27.14	15	3.150 KiB	7	1.186 KiB	
172.16.165.132	54.76.34.243	15	3.558 KiB	7	1.340 KiB	
172.16.165.132	54.88.228.143	15	3.347 KiB	7	1.270 KiB	
172.16.165.132	54.91.219.84	15	3.064 KiB	7	1.175 KiB	

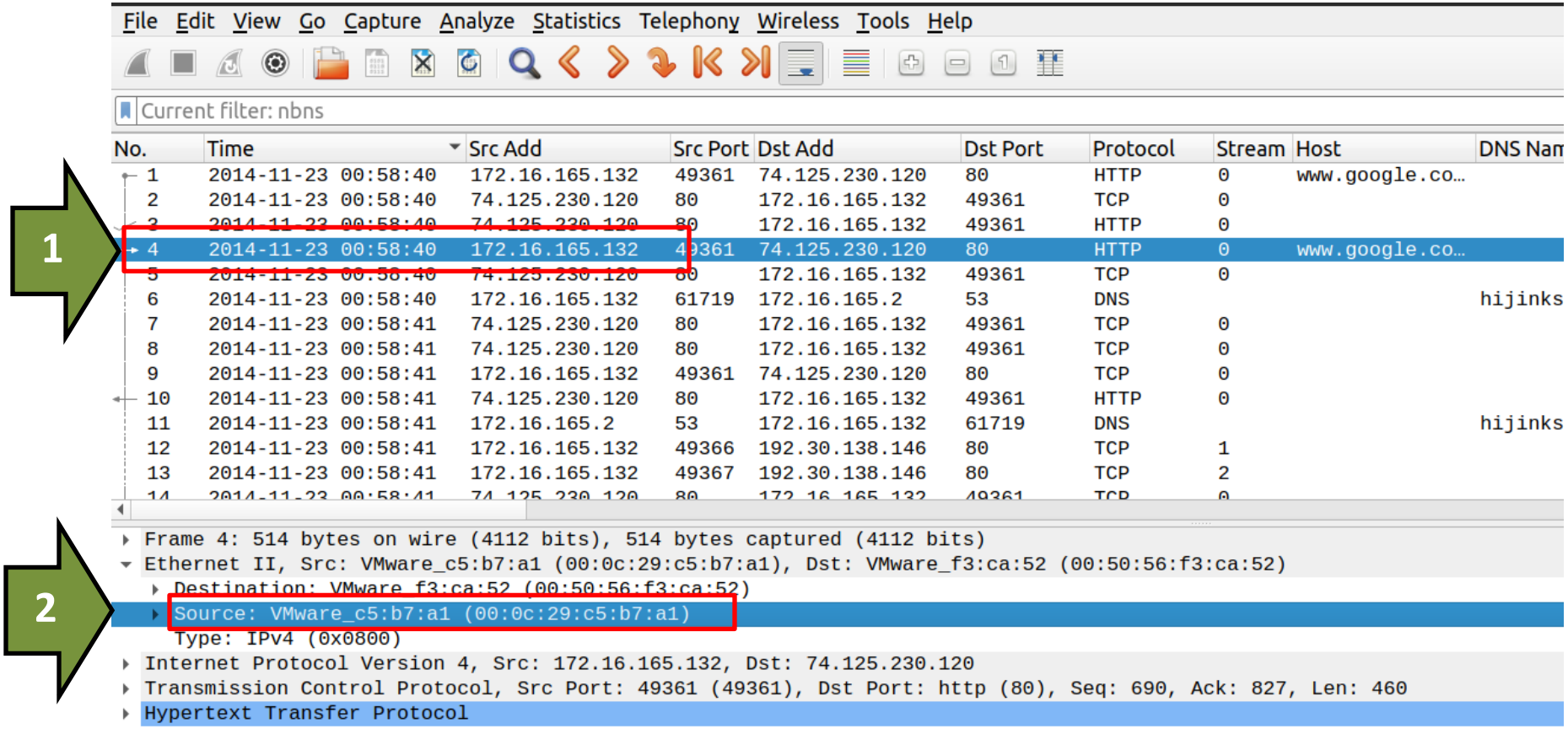
Answer: - 172.16.165.132

- This is the only private IP address communicating with other hosts in Conversations
- This is also the top talker having the most bytes and packets
- View all other tabs to verify this is the only IP address

2) What is the MAC address of the infected VM?

1) **Select any packet with source IP 172.16.165.132**

2) **Packet Details Pane > Expand Ethernet II > Source**



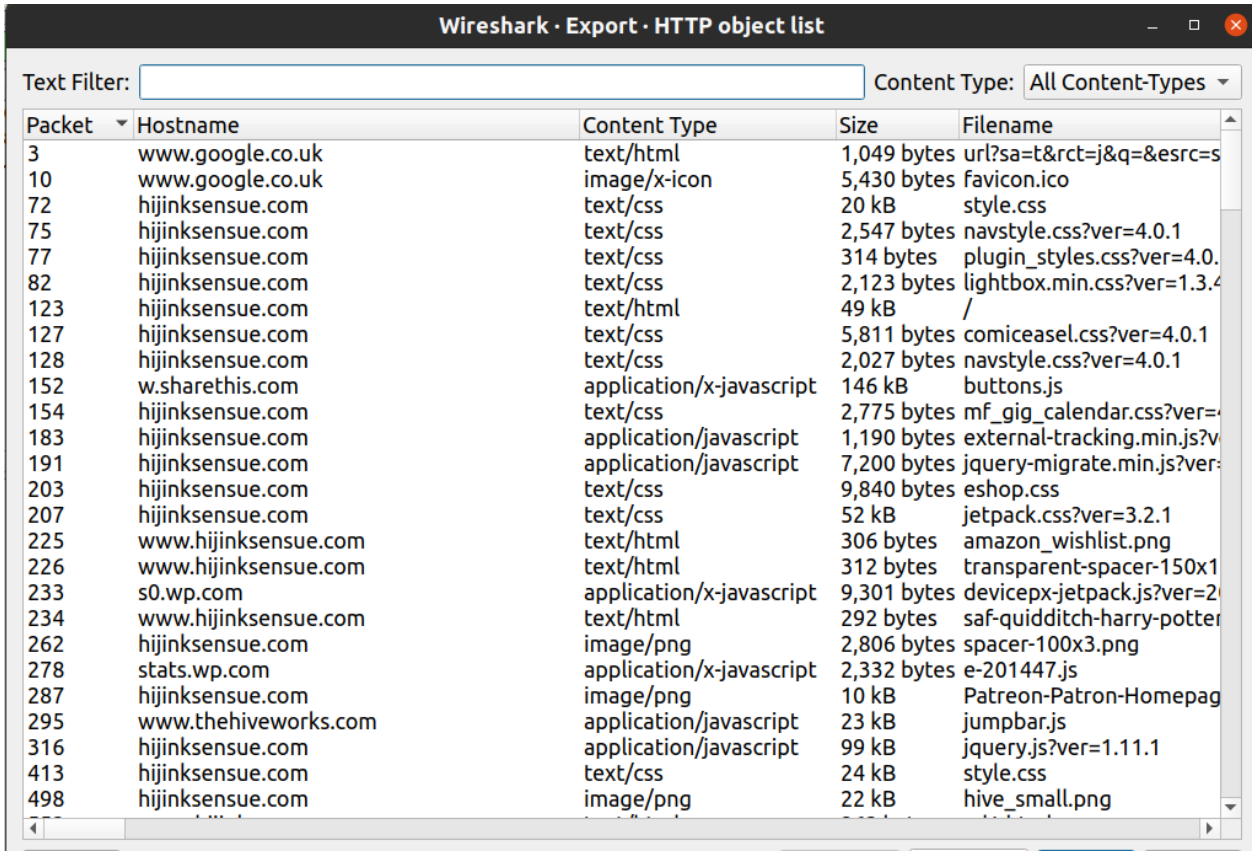
Answer: - 00:0c:29:c5:b7:a1 (VMWare)

- Any packet with the source or destination IP address of the infected device will have this information

- This is OSI Layer II data

3) What is the IP address and domain name that delivered the exploit kit and malware?

- We can find all files downloaded in this pcap by going to
  - **File > Export Objects > HTTP**



Packet	Hostname	Content Type	Size	Filename
3	www.google.co.uk	text/html	1,049 bytes	url?sa=t&rct=j&q=&esrc=s
10	www.google.co.uk	image/x-icon	5,430 bytes	favicon.ico
72	hijinksensue.com	text/css	20 kB	style.css
75	hijinksensue.com	text/css	2,547 bytes	navstyle.css?ver=4.0.1
77	hijinksensue.com	text/css	314 bytes	plugin_styles.css?ver=4.0.
82	hijinksensue.com	text/css	2,123 bytes	lightbox.min.css?ver=1.3.4
123	hijinksensue.com	text/html	49 kB	/
127	hijinksensue.com	text/css	5,811 bytes	comiceasel.css?ver=4.0.1
128	hijinksensue.com	text/css	2,027 bytes	navstyle.css?ver=4.0.1
152	w.sharethis.com	application/x-javascript	146 kB	buttons.js
154	hijinksensue.com	text/css	2,775 bytes	mf_gig_calendar.css?ver=
183	hijinksensue.com	application/javascript	1,190 bytes	external-tracking.min.js?v
191	hijinksensue.com	application/javascript	7,200 bytes	jquery-migrate.min.js?ver
203	hijinksensue.com	text/css	9,840 bytes	eshop.css
207	hijinksensue.com	text/css	52 kB	jetpack.css?ver=3.2.1
225	www.hijinksensue.com	text/html	306 bytes	amazon_wishlist.png
226	www.hijinksensue.com	text/html	312 bytes	transparent-spacer-150x1
233	s0.wp.com	application/x-javascript	9,301 bytes	devicepx-jetpack.js?ver=2
234	www.hijinksensue.com	text/html	292 bytes	saf-quidditch-harry-potter
262	hijinksensue.com	image/png	2,806 bytes	spacer-100x3.png
278	stats.wp.com	application/x-javascript	2,332 bytes	e-201447.js
287	hijinksensue.com	image/png	10 kB	Patreon-Patron-Homepag
295	www.thehiveworks.com	application/javascript	23 kB	jumpbar.js
316	hijinksensue.com	application/javascript	99 kB	jquery.js?ver=1.11.1
413	hijinksensue.com	text/css	24 kB	style.css
498	hijinksensue.com	image/png	22 kB	hive_small.png

- If there were hundreds of files, it would not be efficient to submit all to Virustotal.
- Let's narrow down this list by looking for http requests out of the ordinary
  - Look for suspicious User-Agents

    1) Grab an http GET request packet and set User-Agent as a column

    2) **Display filter > http.request > sort User-Agent column**

    3) By scrolling all requests have the same User-Agent except the top one. Take note of this.

http.request

Time	Source	Src Port	Destination	Dst Port	Length	Host	User-Agent
2014-11-23 00:58:48	172.16.165.132	49398	37.143.15.180	51439	289	h.trinketking.com:51439	Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpReques
2014-11-23 00:58:40	172.16.165.132	49361	74.125.230.120	80	743	www.google.co.uk	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; W
2014-11-23 00:58:40	172.16.165.132	49361	74.125.230.120	80	514	www.google.co.uk	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; W
2014-11-23 00:58:41	172.16.165.132	49367	192.30.138.146	80	525	hijinksensue.com	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; W
2014-11-23 00:58:42	172.16.165.132	49366	192.30.138.146	80	365	hijinksensue.com	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; W
2014-11-23 00:58:42	172.16.165.132	49368	192.30.138.146	80	384	hijinksensue.com	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; W
2014-11-23 00:58:42	172.16.165.132	49369	192.30.138.146	80	397	hijinksensue.com	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; W
2014-11-23 00:58:42	172.16.165.132	49370	192.30.138.146	80	380	hijinksensue.com	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; W
2014-11-23 00:58:42	172.16.165.132	49371	192.30.138.146	80	366	hijinksensue.com	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; W
2014-11-23 00:58:42	172.16.165.132	49372	88.221.134.170	80	355	w.sharethis.com	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; W
2014-11-23 00:58:42	172.16.165.132	49366	192.30.138.146	80	373	hijinksensue.com	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; W
2014-11-23 00:58:42	172.16.165.132	49369	192.30.138.146	80	386	hijinksensue.com	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; W
2014-11-23 00:58:42	172.16.165.132	49368	192.30.138.146	80	354	hijinksensue.com	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; W
2014-11-23 00:58:42	172.16.165.132	49370	192.30.138.146	80	382	hijinksensue.com	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; W

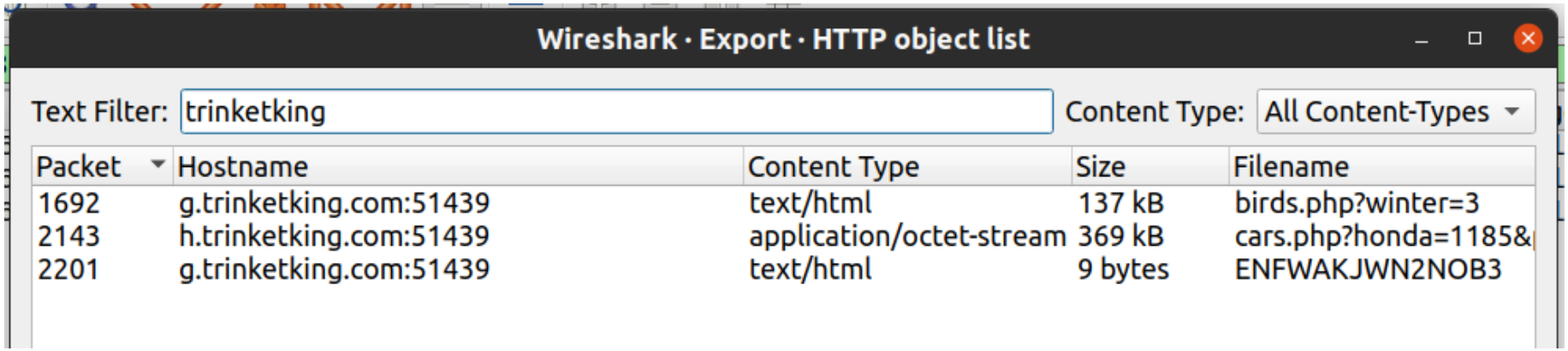
- Look for suspicious port numbers
  1) Sort by destination port or filter out port 80
  2) Sorting out port 80 makes other ports stand out
  3) **http.request && !(tcp.dstport == 80)**
  4) These ports are not communicating on port 80 (suspicious)

http.request && !(tcp.dstport == 80)

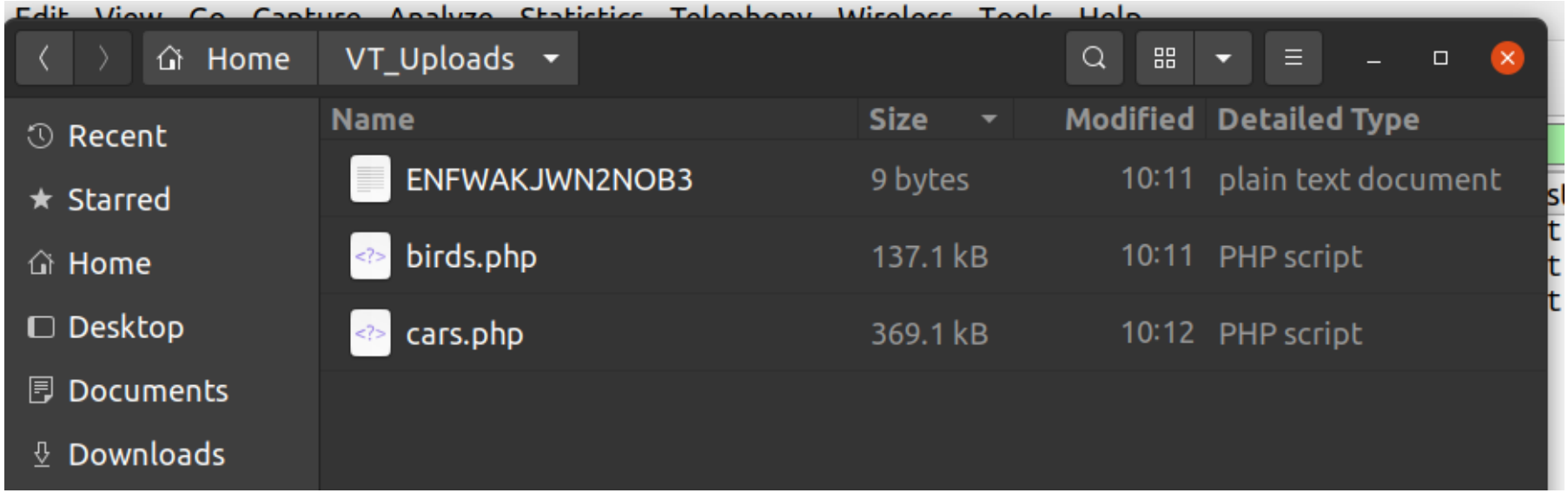
Time	Source	Src Port	Destination	Dst Port	Length	Host	User-Agent
2014-11-23 00:58:48	172.16.165.132	49398	37.143.15.180	51439	289	h.trinketking.com:51439	Mozilla/4.0 (compatible
2014-11-23 00:58:46	172.16.165.132	49393	37.143.15.180	51439	383	g.trinketking.com:51439	Mozilla/5.0 (compatible
2014-11-23 00:58:54	172.16.165.132	49393	37.143.15.180	51439	413	g.trinketking.com:51439	Mozilla/5.0 (compatible

- Take note of the host name
- Back to **File > Export Objects > HTTP**

- Filter for “trinketking” and save these 3 files



- Saved files



- Perform a quick analysis to check the file type
- **Open a terminal > cd <malware folder> > use command: file ***
- Are these files what they claim to be?

```
user1@ubuntu-vm:~/VT_Uploads$ file *
birds.php:      HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
cars.php:       PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
ENFWAKJWN2NOB3: ASCII text, with no line terminators
user1@ubuntu-vm:~/VT_Uploads$
```

- Cars.php is definitely suspicious since this is not a php file, but a PE32 executable for MS Windows

- Use the **cat <filename>** command to view the other non-PE32 files
  - If you scroll through birds.php, you will see this does not look like normal html code; this is in fact, obfuscated JavaScript code

- Next submit these files or their hashes to Virustotal:

- Birds.php came back as malicious

318f07c5fcaa167893f1505e4dc66c23c267a48773eded0a4b2d6eacb7d3e00a

3 / 59

Community Score

3 security vendors and no sandboxes flagged this file as malicious

318f07c5fcaa167893f1505e4dc66c23c267a48773eded0a4b2d6eacb7d3e00a

birds.php

html contains-embedded-js

133.84 KB
Size

2021-08-19 14:52:00 U
1 year ago

DETECTION DETAILS COMMUNITY

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

Security vendors' analysis

Baidu	JS.Trojan.Kryptik.nd	Fortinet	JS/Moat.F93F1FA5!tr
Sophos	Mal/ExpJS-FE	Acronis (Static ML)	Undetected

- cars.php came back as malicious

cc185105946c202d9fd0ef18423b078cd8e064b1e2a87e93ed1b3d4f2cbdb65d

54 / 70

Community Score

54 security vendors and 2 sandboxes flagged this file as malicious

cc185105946c202d9fd0ef18423b078cd8e064b1e2a87e93ed1b3d4f2cbdb65d

Stencyl.exe

360.41 KB
Size

2023-03-01 19:17:48 UTC
8 days ago

peexe | ftp | overlay | revoked-cert | runtime-modules | signed | detect-debug-environment | idle | long-sleeps | direct-cpu-clock-access | checks-user-input | persistence

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 9

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

Popular threat label trojan.spyeyes/mint

Threat categories trojan | dropper | worm

Family labels spyeyes | mint | zard

Security vendors' analysis

Do you want to

AhnLab-V3	Trojan/Win32.SpyEyes.R127534	Alibaba	TrojanSpy:Win32/SpyEyes.0d278040
ALYac	Gen:Heur.Mint.Zard.24	Antiy-AVL	Trojan[Spy]/Win32.SpyEyes

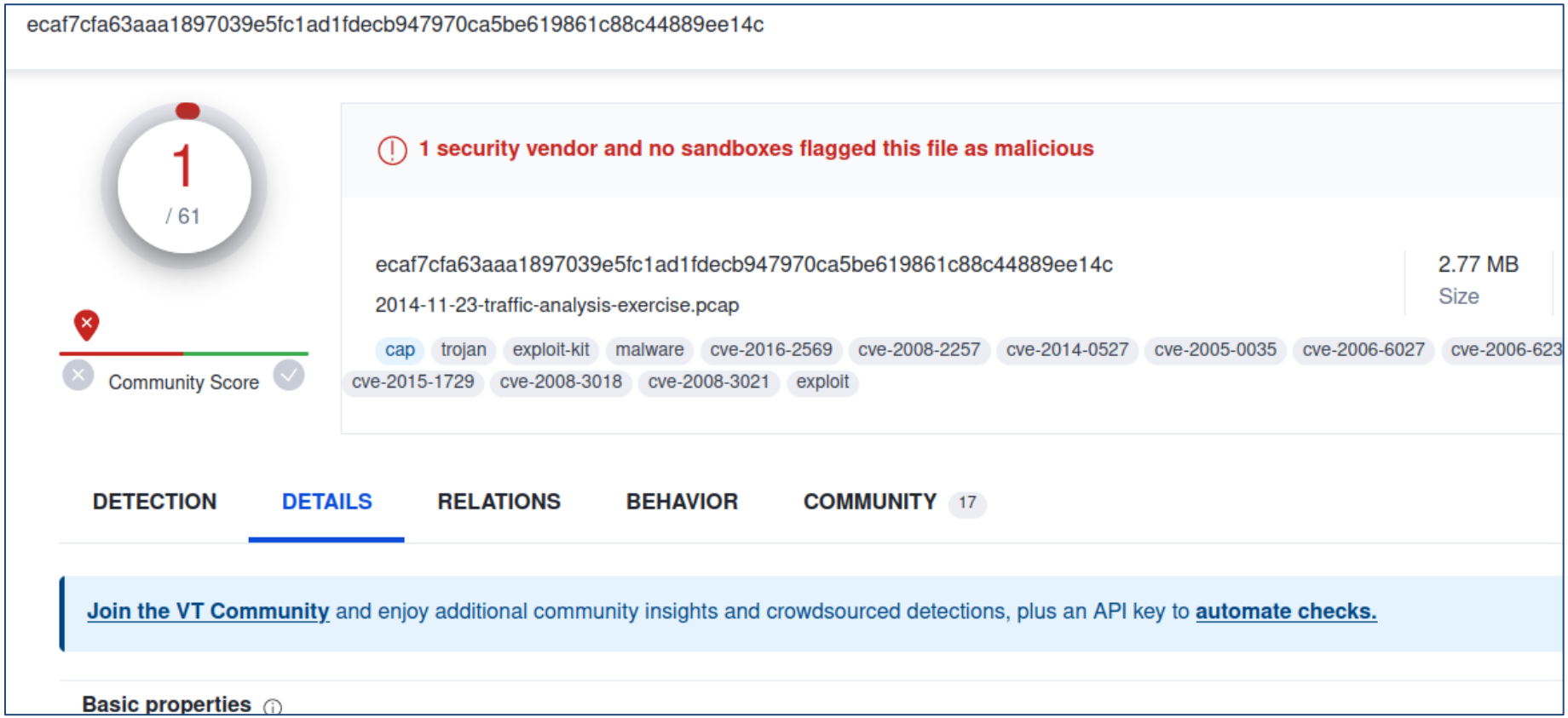
- We can conclude that two hosts are malicious:
  - **g.trinketking.com** delivered the exploit kit (birds.php)
  - **h.tinketking.com** delivered the malware (cars.php)
  - These hosts use one IP address of **37.143.15.180** over port **51439**

http.request && !(tcp.dstport == 80)

Time	Source	Src Port	Destination	Dst Port	Length	Host	User-Agent
2014-11-23 00:58:48	172.16.165.132	49398	37.143.15.180	51439	289	h.trinketking.com:51439	Mozilla/4
2014-11-23 00:58:46	172.16.165.132	49393	37.143.15.180	51439	383	g.trinketking.com:51439	Mozilla/5
2014-11-23 00:58:54	172.16.165.132	49393	37.143.15.180	51439	413	g.trinketking.com:51439	Mozilla/5

4) What is the exploit kit (EK) that delivers the malware?

- Upload the pcap file to Virustotal > Select **Details**



- Scroll down to Suricata or Snort Alerts
- Expand “A Network Trojan was Detected”:

Suricata Alerts

+ Potentially Bad Traffic
+ Potential Corporate Privacy Violation
+ Web Application Attack
— A Network Trojan was Detected

ET CURRENT_EVENTS Sweet Orange CDN Gate Sept 09 2014 Method 2 [2019146]
ET CURRENT_EVENTS Sweet Orange Landing Nov 3 2014 [2019634]
ET CURRENT_EVENTS Possible Sweet Orange redirection Nov 4 2014 [2019642]
ET CURRENT_EVENTS Sweet Orange Landing Nov 04 2013 [2019647]
ET CURRENT_EVENTS SweetOrange EK Landing Nov 19 2014 [2019751]
ET CURRENT_EVENTS Possible Sweet Orange CVE-2014-6332 Payload Request [2019752]
ET CURRENT_EVENTS WinHttpRequest Downloading EXE [2019822]
ET CURRENT_EVENTS WinHttpRequest Downloading EXE Non-Port 80 (Likely Exploit Kit) [2019823]
ET CURRENT_EVENTS Likely Evil EXE download from WinHttpRequest non-exe extension [2022653]

+ Misc activity

5) What is the redirect URL and IP address that points to the exploit kit (EK) landing page?

- From Question 2 above, use the malicious URL as a pivot
- **Display filter > dns.qry.name == g.trinketking.com**

dns.qry.name == g.trinketking.com

Domains

No.	Time	Src Add	Src Port	Dst Add	Dst Port	Protocol	Info
1212	2014-11-23 00:58:46	172.16.165.132	56794	172.16.165.2	53	DNS	Standard query 0x1abf A g.trinketking.com
1273	2014-11-23 00:58:46	172.16.165.2	53	172.16.165.132	56794	DNS	Standard query response 0x1abf A g.trinketking.com

- Let's select packet 1212, then clear the Display Filter

- What happened just before this DNS query?
- There must have been some sort of instruction over http that requested the malicious URL
- Let's have a look at the http packet just before packet 1212

).	Time	Src Add	Src Port	Dst Add	Dst Port	Protocol	Stream	Info
1203	2014-11-23 00:58:46	172.16.165.132	49369	192.30.138.146	80	TCP	4	49369 → http(80) [ACK] Seq=1413 Ack=85975 Wi
1204	2014-11-23 00:58:46	172.16.165.132	49369	192.30.138.146	80	TCP	4	[TCP Window Update] 49369 → http(80) [ACK] S
1205	2014-11-23 00:58:46	192.30.138.146	80	172.16.165.132	49368	HTTP	3	HTTP/1.1 200 OK (text/html)
1206	2014-11-23 00:58:46	192.30.138.146	80	172.16.165.132	49389	HTTP	24	HTTP/1.1 200 OK (text/html)
1208	2014-11-23 00:58:46	192.30.138.146	80	172.16.165.132	49368	TCP	3	http(80) → 49368 [ACK] Seq=45170 Ack=1957 Wi
1210	2014-11-23 00:58:46	192.30.138.146	80	172.16.165.132	49389	TCP	24	http(80) → 49389 [ACK] Seq=1039 Ack=645 Win=
1211	2014-11-23 00:58:46	50.87.149.90	80	172.16.165.132	49388	HTTP	23	HTTP/1.1 200 OK (text/javascript)
1212	2014-11-23 00:58:46	172.16.165.132	56794	172.16.165.2	53	DNS		Standard query 0x1abf A g.trinketking.com
1213	2014-11-23 00:58:46	192.30.138.146	80	172.16.165.132	49369	TCP	4	http(80) → 49369 [PSH, ACK] Seq=85975 Ack=14

- Follow the HTTP stream
- First thing to notice is the strange GET request file
- Take note of the Host

```
GET /k?tstmp=3701802802 HTTP/1.1
Accept: application/javascript, */*;q=0.8
Referer: http://hijinksensue.com/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Accept-Encoding: gzip, deflate
Host: static.charlotteretirementcommunities.com
Connection: Keep-Alive
```

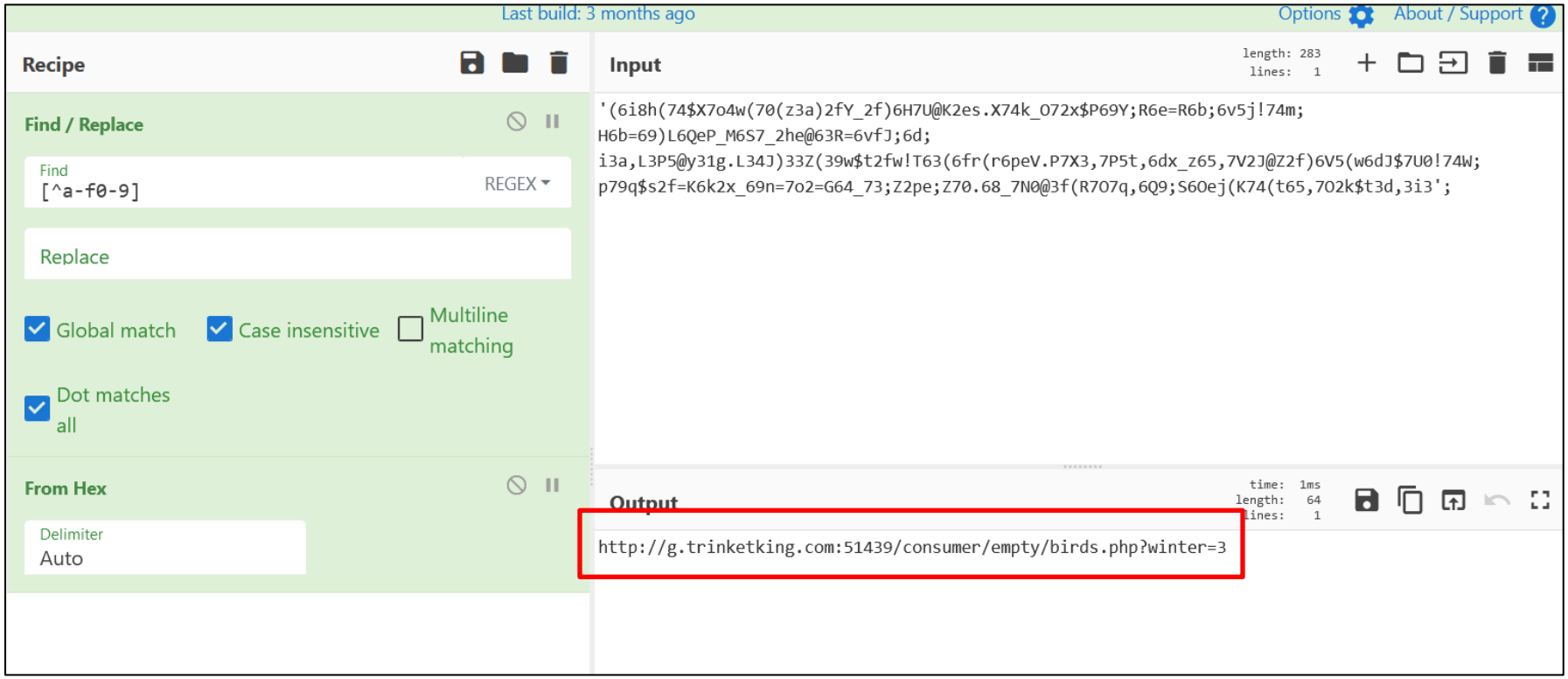
- Scroll down to see the response
- Notice the obfuscated code

```
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Sun, 23 Nov 2014 00:58:33 GMT
Content-Type: text/javascript; charset=ISO-8859-1
Transfer-Encoding: chunked
Connection: keep-alive
P3P: policyref="/w3c/p3p.xml", CP="policyref="/html/p3p.xml", CP="NON DSP COR NID DEVa PSAa PSDa
OUR BUS""
Set-cookie: fshsp=Ty0bADIAAgAPAKg.cVT__6g.cVRAAAEAAACoPnFUAA--; expires=Mon, 23-Nov-2015 01:55:52
GMT; path=/; domain=altaipower.net
Content-Encoding: gzip

var main_request_data_content='(6i8h(74$X7o4w(70(z3a)2fY_2f)6H7U@K2es.X74k_O72x$P69Y;R6e=R6b;6v5j!
74m;H6b=69)L6QeP_M6S7_2he@63R=6vfJ;6d;i3a,L3P5@y31g.L34J)33Z(39w$t2fw!T63(6fr(r6peV.P7X3,7P5t,
6dx_z65,7V2J@Z2f)6V5(w6dJ$7U0!74W;p79q$s2f=K6k2x_69n=7o2=G64_73;Z2pe;Z70.68_7N0@3f(R7O7q,
6Q9;S6Oej(K74(t65,7O2k$t3d,3i3';
```

- A common encoding method is to encode the real part of the code in hexadecimal and obfuscate with junk characters in between

- Using CyberChef, let's remove hexadecimal characters 0-9, a-f
- Then convert the characters back to Ascii



- The output shows the familiar malicious URL
- The redirect URL and IP address:
  - **static.charlotteretirementcommunities.com/k?tstmp=3701802802**
  - **50.87.149.90**

6) What is the IP address of the compromised web site?

- Let's work back to that last HTTP stream and find the Referrer

```
GET /k?tstmp=3701802802 HTTP/1.1
Accept: application/javascript, */*;q=0.8
Referer: http://hijinksensue.com/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Accept-Encoding: gzip, deflate
Host: static.charlotteretirementcommunities.com
Connection: Keep-Alive
```

7) What is the domain name of the compromised web site?

http.host == hijinksensue.com

o.	Time	Src Add	Src Port	Dst Add	Dst Port	Protocol	Stream	Host
18	2014-11-23 00:58:41	172.16.165.132	49367	192.30.138.146	80	HTTP	2	hijinksensue.com
23	2014-11-23 00:58:42	172.16.165.132	49366	192.30.138.146	80	HTTP	1	hijinksensue.com
48	2014-11-23 00:58:42	172.16.165.132	49368	192.30.138.146	80	HTTP	3	hijinksensue.com