

# 一、基本问题

## 1、被感染的Windows虚拟机的IP

# 答案

172.16.165.132

# 分析思路

通过过滤"http.request", 找到所有发起http请求的主机, 发现只有172这台主机

2014-11-23-traffic-analysis-exercise.pcap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

http.request

No.	Time	Source	Destination	Protocol	Length	Status Code	Info
1	0.000000	172.16.165.132	74.125.230.120	HTTP	743		GET /url?sa=t&rct=j&q=&esrc=s&frm=1&source=...
4	0.332042	172.16.165.132	74.125.230.120	HTTP	514		GET /favicon.ico HTTP/1.1
18	1.187319	172.16.165.132	192.30.138.146	HTTP	525		GET / HTTP/1.1
23	1.578633	172.16.165.132	192.30.138.146	HTTP	365		GET /wp-content/themes/comicpress-hijink...
48	1.962023	172.16.165.132	192.30.138.146	HTTP	384		GET /wp-content/plugins/eshop-order-ema...
50	1.962196	172.16.165.132	192.30.138.146	HTTP	397		GET /wp-content/themes/comicpress-hijink...
52	1.962330	172.16.165.132	192.30.138.146	HTTP	380		GET /wp-content/plugins/wp-lightbox-2/st...
54	1.962505	172.16.165.132	192.30.138.146	HTTP	366		GET /wp-content/plugins/jetpack/css/jetp...
69	2.202491	172.16.165.132	88.221.134.170	HTTP	355		GET /button/buttons.js HTTP/1.1
74	2.225348	172.16.165.132	192.30.138.146	HTTP	373		GET /wp-content/plugins/comic-easel/css/...
78	2.226140	172.16.165.132	192.30.138.146	HTTP	386		GET /wp-content/plugins/comic-easel/ima...
80	2.226657	172.16.165.132	192.30.138.146	HTTP	354		GET /wp-content/uploads/eshop_files/esh...
83	2.325533	172.16.165.132	192.30.138.146	HTTP	382		GET /wp-content/plugins/mf-gig-calendar...
125	2.570113	172.16.165.132	192.30.138.146	HTTP	381		GET /wp-includes/js/jquery/jquery.js?ver...

## 2、受感染虚拟机的MAC地址

# 答案

00:50:56:f3:ca:52

# 分析思路

查看关于IP172.16.165.132数据包中数据链路层的MMAC地址

78	2.226140	172.16.165.132	192.30.138.146	HTTP	386	GET /wp-content/
80	2.226657	172.16.165.132	192.30.138.146	HTTP	354	GET /wp-content/
83	2.325533	172.16.165.132	192.30.138.146	HTTP	382	GET /wp-content/
125	2.570113	172.16.165.132	192.30.138.146	HTTP	381	GET /wp-includes
133	2.572244	172.16.165.132	192.30.138.146	HTTP	392	GET /wp-includes
134	2.572356	172.16.165.132	192.30.138.146	HTTP	412	GET /wp-content/
163	2.693527	172.16.165.132	192.30.138.146	HTTP	409	GET /assets/misc
165	2.693706	172.16.165.132	192.30.138.146	HTTP	353	GET /jumpbar.js
167	2.693861	172.16.165.132	192.30.138.146	HTTP	440	GET /wp-content/
172	2.716778	172.16.165.132	192.30.138.146	HTTP	434	GET /wp-content/

<

> Frame 54: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits)

> Ethernet II, Src: VMware\_c5:b7:a1:00:0c:29:c5:b7:a1, Dst: VMware\_f3:ca:52 (00:50:56:f3:ca:52)

> Internet Protocol Version 4, Src: 172.16.165.132, Dst: 192.30.138.146

> Transmission Control Protocol, Src Port: 49371, Dst Port: 80, Seq: 1, Ack: 1, Len: 312

> Hypertext Transfer Protocol

## 3、受感染网站的IP地址

# 答案

192.30.138.146

## # 分析过程

前面的分析均为跳包模式，现在从头开始追包，可以看到序号1-5包一直与IP 74.125.230.120进行交互，在序号6包、序号11包时出现了一条192.30.138.146的DNS解析记录，之后频繁与该IP进行交互，初步确认为受感染的IP

The figure displays a Wireshark packet capture of a DNS transaction. The packet list on the left shows a DNS query (packet 6) and a response (packet 11). The packet details pane on the right shows the structure of the DNS query, including the question section with a query for 192.30.138.146.

No.	Time	Source	Destination	Protocol	Length	Status	Code	Info
1	0.000000	172.16.165.132	74.125.230.120	HTTP	743	GET		/url?sa=t&rc=t&j&q=&src=s&frm=1&source=web&cd=1&ved=0CCEQFjAA&url=h
2	0.000192	74.125.230.120	172.16.165.132	TCP	60	80 → 49361 [ACK]		Seq=1 Ack=690 Win=64240 Len=0
3	0.306675	74.125.230.120	172.16.165.132	HTTP	880	200 HTTP/1.1	200 OK	(text/html)
4	0.332042	172.16.165.132	74.125.230.120	HTTP	514	GET		/favicon.ico HTTP/1.1
5	0.332197	74.125.230.120	172.16.165.132	TCP	60	80 → 49361 [ACK]		Seq=827 Ack=1150 Win=64240 Len=0
6	0.351533	172.16.165.132	172.16.165.2	DNS	76	Standard query		0xf082 A hijinksense.com
7	0.644953	74.125.230.120	172.16.165.132	TCP	1409	80 → 49361 [PSH, ACK]		Seq=827 Ack=1150 Win=64240 Len=1355 [TCP segment
8	0.745024	74.125.230.120	172.16.165.132	TCP	1409	[TCP Retransmission] 80 → 49361 [PSH, ACK]		Seq=827 Ack=1150 Win=64240 L
9	0.745049	172.16.165.132	74.125.230.120	TCP	54	49361 → 80 [ACK]		Seq=1150 Ack=2182 Win=64240 Len=0
10	0.766567	74.125.230.120	172.16.165.132	HTTP	87	200 HTTP/1.1	200 OK	(image/x-icon)
11	0.766620	172.16.165.2	172.16.165.132	DNS	92	Standard query response		0xf082 A hijinksense.com A 192.30.138.146
12	0.767192	172.16.165.132	192.30.138.146	TCP	66	49366 → 80 [SYN]		Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	0.767331	172.16.165.132	192.30.138.146	TCP	66	49367 → 80 [SYN]		Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	0.866550	74.125.230.120	172.16.165.132	TCP	87	[TCP Retransmission] 80 → 49361 [PSH, ACK]		Seq=2182 Ack=1150 Win=64240
15	0.866570	172.16.165.132	74.125.230.120	TCP	54	49361 → 80 [ACK]		Seq=1150 Ack=2215 Win=64207 Len=0
16	1.185297	192.30.138.146	172.16.165.132	TCP	60	80 → 49367 [SYN, ACK]		Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
17	1.185343	172.16.165.132	192.30.138.146	TCP	54	49367 → 80 [ACK]		Seq=1 Ack=1 Win=64240 Len=0
18	1.187319	172.16.165.132	192.30.138.146	HTTP	525	GET		/ HTTP/1.1
19	1.187484	192.30.138.146	172.16.165.132	TCP	60	80 → 49367 [ACK]		Seq=1 Ack=472 Win=64240 Len=0
20	1.305954	192.30.138.146	172.16.165.132	TCP	60	80 → 49366 [SYN, ACK]		Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

Packet 6 details:

```

.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0x15d7 (5591)
> Flags: 0x40, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x48b3 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.16.165.132
  Destination Address: 192.30.138.146
  
```

#### 4、被入侵网站的域名

## # 答案

hijinksensue.com

## # 分析过程

查看关于上面IP的DNS记录或HTTP数据包中的Host值，可以看到域名为hijinksensue.com

1	0.000000	172.16.165.132	74.125.230.120	HTTP	743	GET /url?sa=t&rt=j&q=&src=s&frm=1&source=web&cd=1&ved=0CCEQFjAA&url=http://www.google.co.uk/
2	0.000192	74.125.230.120	172.16.165.132	TCP	60	80 → 49361 [ACK] Seq=1 Ack=690 Win=64240 Len=0
3	0.306675	74.125.230.120	172.16.165.132	HTTP	880	200 HTTP/1.1 200 OK (text/html)
4	0.332042	172.16.165.132	74.125.230.120	HTTP	514	GET /favicon.ico HTTP/1.1
5	0.332197	74.125.230.120	172.16.165.132	TCP	60	80 → 49361 [ACK] Seq=827 Ack=1150 Win=64240 Len=0
6	0.351353	172.16.165.132	172.16.165.2	DNS	76	Standard query 0xf082 A hijinksense.com
7	0.644953	74.125.230.120	172.16.165.132	TCP	1409	80 → 49361 [PSH, ACK] Seq=827 Ack=1150 Win=64240 Len=1355 [TCP segment of a set already received by peer 172.16.165.2:80]
8	0.745024	74.125.230.120	172.16.165.132	TCP	1409	[TCP Retransmission] 80 → 49361 [PSH, ACK] Seq=827 Ack=1150 Win=64240 Len=1355 [TCP segment of a set already received by peer 172.16.165.2:80]
9	0.745049	172.16.165.132	74.125.230.120	TCP	54	49361 → 80 [ACK] Seq=1150 Ack=2182 Win=64240 Len=0
10	0.766567	74.125.230.120	172.16.165.132	HTTP	87	200 HTTP/1.1 200 OK (image/x-icon)
11	0.766620	172.16.165.2	172.16.165.132	DNS	92	Standard query response 0xf082 A hijinksense.com A 192.30.138.146
12	0.767192	172.16.165.132	192.30.138.146	TCP	66	49366 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	0.767331	172.16.165.132	192.30.138.146	TCP	66	49367 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	0.767551	172.16.165.132	192.30.138.146	TCP	60	49367 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	0.866550	74.125.230.120	172.16.165.132	TCP	87	[TCP Retransmission] 80 → 49361 [PSH, ACK] Seq=2182 Ack=49366 Win=64240 Len=0
16	0.866570	172.16.165.132	74.125.230.120	TCP	54	49361 → 80 [ACK] Seq=1150 Ack=2215 Win=64207 Len=0
17	1.185297	192.30.138.146	172.16.165.132	TCP	60	80 → 49367 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
18	1.185343	172.16.165.132	192.30.138.146	TCP	54	49367 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
19	1.187319	172.16.165.132	192.30.138.146	HTTP	525	GET / HTTP/1.1
20	1.187484	192.30.138.146	172.16.165.132	TCP	60	80 → 49367 [ACK] Seq=1 Ack=472 Win=64240 Len=0
21	1.187551	192.30.138.146	172.16.165.132	TCP	60	80 → 49367 [ACK] Seq=1 Ack=472 Win=64240 Len=0

5、提供恶意软件的IP地址和域名

### # 答案

37.143.15.180

g.trinketking.com:51439

### # 分析过程1

导出值 -> http, 可以看到一个文件类型为"**application/octet-stream**"的文件, 导出时直接被安全软件查杀了, 其他文件均为正常的图片/文档。可以看到该恶意软件提供的主机名为"**h.trinketking.com:51439**"



发现1项病毒威胁, 已自动处理



cars.php%3fhonda=1185&proxy=24...

后门病毒 (Backdoor/Qbot)

详情

Wireshark · 导出 · HTTP 对象列表

文本过滤器:

Content Type: All Content-Types

分组	主机名	内容类型	大小	文件名
1652	pixel.wp.com	image/gif	50 bytes	url%3Fsa
1675	hijinksensue.com	image/png	2790 bytes	prev.png
1680	hijinksensue.com	image/jpeg	33 kB	saf-quid
1691	hijinksensue.com	image/png	10 kB	amazon_
1692	g.trinketking.com:51439	text/html	137 kB	birds.ph
1703	hijinksensue.com	image/png	3034 bytes	lastin.pn
1705	ads.thehiveworks.com	application/javascript	6707 bytes	fl.js
1706	wd-edge.sharethis.com	text/javascript	162 bytes	getAllAq
1710	hijinksensue.com	image/png	2731 bytes	next.png
2143	h.trinketking.com:51439	application/octet-stream	369 kB	cars.php
2154	wd-edge.sharethis.com	text/javascript	22 bytes	checkO/
2201	g.trinketking.com:51439	text/html	9 bytes	ENFWA/
2230	tag.contextweb.com	application/x-javascript	535 bytes	getjs.as
2231	seg.sharethis.com	text/html	549 bytes	getSegr
2236	tag.contextweb.com	application/x-javascript	535 bytes	getjs.as
2239	tag.contextweb.com	application/x-javascript	534 bytes	getjs.as
2257	w.sharethis.com	text/css	24 kB	buttons.

Save

Save All

Preview

Close

Help

### # 分析过程2

定位该数据包, 可以看到该恶意软件提供的IP

No.	Time	Source	Destination	Protocol	Length
2143	13.957799	37.143.15.180	172.16.165.132	HTTP	74
2144	13.957829	172.16.165.132	37.143.15.180	TCP	54
2145	14.363839	172.16.165.132	37.143.15.180	HTTP	41

  

Wireshark · 导出 · HTTP 对象列表

文本过滤器:  Content Type: All Content-Types

分组	主机名	内容类型	大小	文件名
2143	h.trinketking.com:51439	application/octet-stream	369 kB	cars.php
2154	wd-edge.sharethis.com	text/javascript	22 bytes	checkO/
2201	g.trinketking.com:51439	text/html	9 bytes	ENFWA/
2230	tag.contextweb.com	application/x-javascript	535 bytes	getjs.as
2231	seg.sharethis.com	text/html	549 bytes	getSegr
2236	tag.contextweb.com	application/x-javascript	535 bytes	getjs.as
2239	tag.contextweb.com	application/x-javascript	534 bytes	getjs.as
2257	w.sharethis.com	text/css	24 kB	buttons.
2274	ads.contextweb.com	application/x-javascript	8564 bytes	getjs.sta
2284	edge.sharethis.com	text/html	12 kB	index.af
2299	ads.contextweb.com	application/x-javascript	1253 bytes	GetAd.a
2319	w.sharethis.com	application/x-javascript	103 kB	st.b6e4c
2328	ads.contextweb.com	application/x-javascript	1410 bytes	GetAd.a
2335	ads.contextweb.com	application/x-javascript	1253 bytes	GetAd.a
2383	pagead2.google syndication.com	text/javascript	23 kB	adsbygc
2388	ads.thehiveworks.com	image/gif	43 bytes	lg.php?t
2389	pixel.quantserve.com	image/gif	35 bytes	p-01-0V

Save Save All Preview Close Help

## 二、高级问题

### 1、传递恶意软件的EK

#### # 答案

1.exe

#### # 分析过程

下载刚刚上面那个文件，传入病毒检测网站，发现为木马文件



**恶意**

### 1.exe

首次提交: 2020/08/01 末次提交: 2021/04/24 末次分析: 2021/04/24 20:56:52

文件大小: 360.41 KB 文件类型: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows

引擎检出: 19 / 25 分析环境: Win7(32bit,Office2013) WinXP(SP3,exe)

威胁分类: 木马 木马家族: SpyEyes

HASH

SHA256: cc185105946c202d9fd0ef18423b078cd8e064b1e2a87e93ed1b3d4f2cbdb65d

MD5: 1408275c2e2c8fe5e83227ba371ac6b3

SHA1: dac3d479ce4af6d2ffd5314191e768543acfe32d

下载样本 下载PCAP 下载报告 收藏报告 重新分析

### 2、指向EK登陆页面的重定向URL

#### # 答案

hijinksensue.com/assets/misc/facebook.png

### # 分析过程

通过查看恶意软件IP出现的第一个HTTP数据包（没有发现Referer头），在其之上虚拟机做了一次DNS解析与该IP进行连接，在该DNS解析前向192.30.138.146发出了请求，初步判断是从该位置跳转过来的

1251	5.957324	192.30.138.146	172.16.165.132	HTTP	1307	200 HTTP/1.1 200 OK (PNG)
1252	5.957699	172.16.165.132	192.30.138.146	HTTP	380	GET /assets/misc/facebook.png HTTP/1.1
1253	5.957767	172.16.165.2	172.16.165.132	DNS	96	Standard query response 0x3d8a A ads.thehiveworks.com A 199.167.132.217
1254	5.957822	192.30.138.146	172.16.165.132	TCP	60	80 → 49366 [ACK] Seq=101529 Ack=2345 Win=64240 Len=0
1255	5.958374	172.16.165.132	199.167.132.217	TCP	66	49392 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1256	5.965727	192.30.138.146	172.16.165.132	TCP	1409	80 → 49370 [PSH, ACK] Seq=154251 Ack=1385 Win=64240 Len=1355 [TCP segment of a reassembled PDU]
1257	5.966009	192.30.138.146	172.16.165.132	TCP	1409	80 → 49370 [PSH, ACK] Seq=155606 Ack=1385 Win=64240 Len=1355 [TCP segment of a reassembled PDU]
1258	5.966021	172.16.165.132	192.30.138.146	TCP	54	49370 → 80 [ACK] Seq=1385 Ack=156961 Win=64240 Len=0
1259	5.967216	192.30.138.146	172.16.165.132	TCP	1409	80 → 49370 [PSH, ACK] Seq=156961 Ack=1385 Win=64240 Len=1355 [TCP segment of a reassembled PDU]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x9d98 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

> [Timestamps]

> [SEQ/ACK analysis]

TCP payload (326 bytes)

▼ Hypertext Transfer Protocol

▼ GET /assets/misc/facebook.png HTTP/1.1\r\n

> [Expert Info (Chat/Sequence): GET /assets/misc/facebook.png HTTP/1.1\r\n]

Request Method: GET

Request URI: /assets/misc/facebook.png

Request Version: HTTP/1.1

### 3、指向EK登录页面的重定向URL的IP

### # 答案

192.30.138.146

### # 分析过程

取上一个答案的IP

1251	5.957324	192.30.138.146	172.16.165.132	HTTP	1307	200 HTTP/1.1 200 OK (PNG)
1252	5.957699	172.16.165.132	192.30.138.146	HTTP	380	GET /assets/misc/facebook.png HTTP/1.1
1253	5.957767	172.16.165.2	172.16.165.132	DNS	96	Standard query response 0x3d8a A ads.thehiveworks.com A 199.167.132.217
1254	5.957822	192.30.138.146	172.16.165.132	TCP	60	80 → 49366 [ACK] Seq=101529 Ack=2345 Win=64240 Len=0
1255	5.958374	172.16.165.132	199.167.132.217	TCP	66	49392 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1256	5.965727	192.30.138.146	172.16.165.132	TCP	1409	80 → 49370 [PSH, ACK] Seq=154251 Ack=1385 Win=64240 Len=1355 [TCP segment of a reassembled PDU]
1257	5.966009	192.30.138.146	172.16.165.132	TCP	1409	80 → 49370 [PSH, ACK] Seq=155606 Ack=1385 Win=64240 Len=1355 [TCP segment of a reassembled PDU]
1258	5.966021	172.16.165.132	192.30.138.146	TCP	54	49370 → 80 [ACK] Seq=1385 Ack=156961 Win=64240 Len=0
1259	5.967216	192.30.138.146	172.16.165.132	TCP	1409	80 → 49370 [PSH, ACK] Seq=156961 Ack=1385 Win=64240 Len=1355 [TCP segment of a reassembled PDU]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x9d98 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

> [Timestamps]

> [SEQ/ACK analysis]

TCP payload (326 bytes)

▼ Hypertext Transfer Protocol

▼ GET /assets/misc/facebook.png HTTP/1.1\r\n

> [Expert Info (Chat/Sequence): GET /assets/misc/facebook.png HTTP/1.1\r\n]

Request Method: GET

Request URI: /assets/misc/facebook.png

Request Version: HTTP/1.1

### 4、pcap提交Virus Total并触发的snort警报

#### Snort Alerts

- Sensitive Data
  - (spp\_sdf) SDF Combination Alert [1]
- Potentially Bad Traffic
  - (http\_inspect) LONG HEADER [19]
  - PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority [254]
- Attempted Administrator Privilege Gain
  - SERVER-WEBAPP Checkpoint Firewall-1 HTTP parsing format string vulnerability attempt [2381]
  - SERVER-APACHE Apache Struts wildcard matching OGNL remote code execution attempt [29639]
- Attempted User Privilege Gain
  - BROWSER-PLUGINS AcroPDF.PDF ActiveX clsid access attempt [13913]
  - BROWSER-IE Microsoft Internet Explorer XHTML element memory corruption attempt [13974]
  - BROWSER-IE Microsoft Internet Explorer HTML DOM invalid DHTML textnode creation attempt [16301]
  - PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt [19187]
  - INDICATOR-OBfuscation Multiple character encodings detected [29509]
  - POLICY-OTHER PDF ActiveX CLSID access detected [38038]
  - FILE-IMAGE Apple PICT Quickdraw image converter packType 4 buffer overflow attempt [44455]
  - SERVER-OTHER Beutel Connection Manager username buffer overflow attempt [44679]
- + Potential Corporate Privacy Violation
- + A Network Trojan was detected
- + Detection of a Denial of Service Attack

## 5、提取恶意软件的Payload，MD5或SHA256哈希是什么

### # 答案

MD5:1408275c2e2c8fe5e83227ba371ac6b3

SHA256:cc185105946c202d9fd0ef18423b078cd8e064b1e2a87e93ed1b3d4f2cbdb65d

### # 分析过程

提交该恶意软件到病毒分析平台，可直接查看到分析出的MD5值和SHA256值等

恶意评分

10

恶意

MD5	1408275c2e2c8fe5e83227ba371ac6b3
SHA1	dac3d479ce4af6d2ffd5314191e768543acfe32d
SHA256	cc185105946c202d9fd0ef18423b078cd8e064b1e2a87e93ed1b3d4f2cbdb65d
文件名称	cars.php%3fhonda=1185&proxy=2442&timeline=4&jobs=823&image=171&join=757&iist=679
文件类型	PE32 Executable for MS Windows (EXE)
文件大小	369056字节
检测环境	Windows 7 x86
文件信誉	恶意 Trojan Mint
RAS检测	en-US Signed_PE
基因特征	修改浏览器配置 持久化 HTTP通信 解压执行 探针 检测沙箱 存在网络地址 可疑命令行 检测虚拟机 可疑程序 窃密软件 注入 shellcode 网银木马 联网行为
分析时间	2022-06-15 11:24:10

