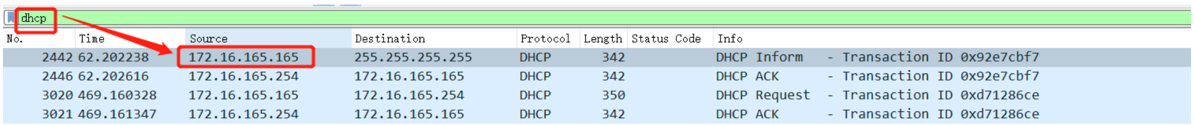
一级

1、虚拟机IP

```
# 答案
    172.16.165.165
```

```
# 分析过程
    虚拟机IP为本地DHCP服务器进行分配的，所以直接过滤"dhcp"，获取使用dhcp的虚拟机通信数据包；
虚拟机IP一般为内网的，172或者192开头的，也可以通过这个来看
```

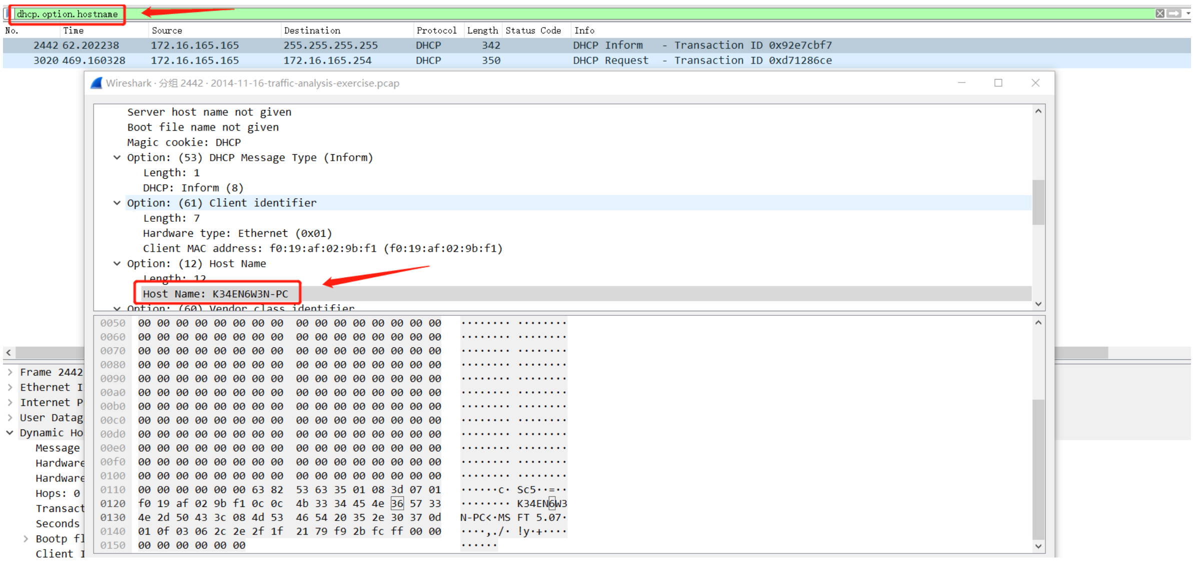


```
dhcp
No.   Time        Source          Destination      Protocol Length Status Code Info
 2442 62.202238   172.16.165.165  255.255.255.255  DHCP      342              DHCP Inform   - Transaction ID 0x92e7cbf7
 2446 62.202616   172.16.165.254  172.16.165.165   DHCP      342              DHCP ACK      - Transaction ID 0x92e7cbf7
 3020 469.160328  172.16.165.165  172.16.165.254   DHCP      350              DHCP Request  - Transaction ID 0xd71286ce
 3021 469.161347  172.16.165.254  172.16.165.165   DHCP      342              DHCP ACK      - Transaction ID 0xd71286ce
```

2、虚拟机主机名

```
# 答案
    K34EN6W3N-PC
```

```
# 分析过程
    过滤"dhcp.option.hostname"，直接查看到dhcp协议主机的hostname
```



```
dhcp.option.hostname
No.   Time        Source          Destination      Protocol Length Status Code Info
 2442 62.202238   172.16.165.165  255.255.255.255  DHCP      342              DHCP Inform   - Transaction ID 0x92e7cbf7
 3020 469.160328  172.16.165.165  172.16.165.254   DHCP      350              DHCP Request  - Transaction ID 0xd71286ce
```

Wireshark · 分组 2442 · 2014-11-16-traffic-analysis-exercise.pcap

```
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ˅ Option: (53) DHCP Message Type (Inform)
      Length: 1
      DHCP: Inform (8)
  ˅ Option: (61) Client identifier
      Length: 7
      Hardware type: Ethernet (0x01)
      Client MAC address: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
  ˅ Option: (12) Host Name
      Length: 12
      Host Name: K34EN6W3N-PC
  ˅ Option: (60) Vendor class identifier
```

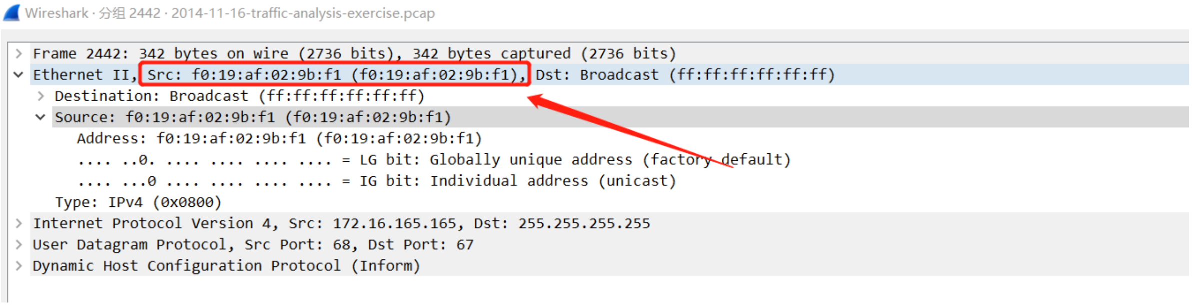
```
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 08 3d 07 01   ······c· Sc5··=··
0120  f0 19 af 02 9b f1 0c 0c  4b 33 34 45 4e 36 57 33   ········ K34EN6W3
0130  4e 2d 50 43 3c 08 4d 53  46 54 20 35 2e 30 37 0d   N-PC<·MS FT 5.07·
0140  01 0f 03 06 2c 2e 2f 1f  21 79 f9 2b fc ff 00 00   ····,./· !y·+····
0150  00 00 00 00 00 00                                  ······
```

```
> Frame 2442
> Ethernet I
> Internet P
> User Datag
˅ Dynamic Ho
    Message
    Hardware
    Hardware
    Hops: 0
    Transact
    Seconds
  > Bootp fl
    Client I
```

3、虚拟机MAC

```
# 答案
    f0:19:af:02:9b:f1
```

```
# 分析过程
    直接点击虚拟机相关的数据包，在数据链路层可以看到MAC地址
```



Wireshark · 分组 2442 · 2014-11-16-traffic-analysis-exercise.pcap

```
> Frame 2442: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
v Ethernet II, Src: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  v Source: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
      Address: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.16.165.165, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Inform)
```

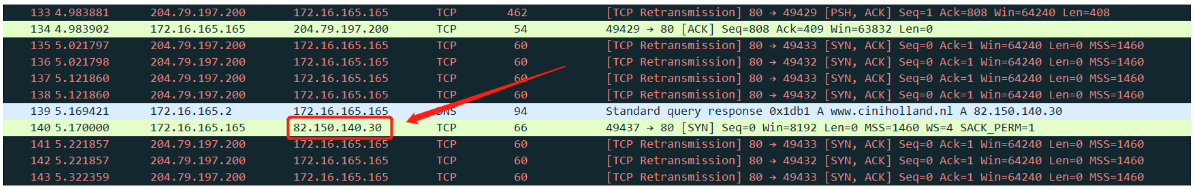
4、被入侵网站IP

答案

82.150.140.30

# 分析过程

前面信息收集，采用过滤器进行跳包。这里从头开始追包，前面基本都是本机与bing网站的交互，直到这里出现了一段DNS解析，随后出现了一个陌生的IP，之后频繁与该IP产生交互，初步确定该IP为被入侵的网站IP。且可还原出画像为，用户通过访问bing网站搜索到了该网站IP并产生交互。



```
133 4.983881   204.79.197.200   172.16.165.165   TCP   462   [TCP Retransmission] 80 → 49429 [PSH, ACK] Seq=1 Ack=808 Win=64240 Len=408
134 4.983902   172.16.165.165   204.79.197.200   TCP    54   49429 → 80 [ACK] Seq=808 Ack=409 Win=63832 Len=0
135 5.021797   204.79.197.200   172.16.165.165   TCP    60   [TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
136 5.021798   204.79.197.200   172.16.165.165   TCP    60   [TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
137 5.121860   204.79.197.200   172.16.165.165   TCP    60   [TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
138 5.121860   204.79.197.200   172.16.165.165   TCP    60   [TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
139 5.169421   172.16.165.2     172.16.165.165   DNS    94   Standard query response 0x1db1 A www.ciniholland.nl A 82.150.140.30
140 5.170000   172.16.165.165   82.150.140.30    TCP    66   49437 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
141 5.221857   204.79.197.200   172.16.165.165   TCP    60   [TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
142 5.221857   204.79.197.200   172.16.165.165   TCP    60   [TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
143 5.322359   204.79.197.200   172.16.165.165   TCP    60   [TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
```

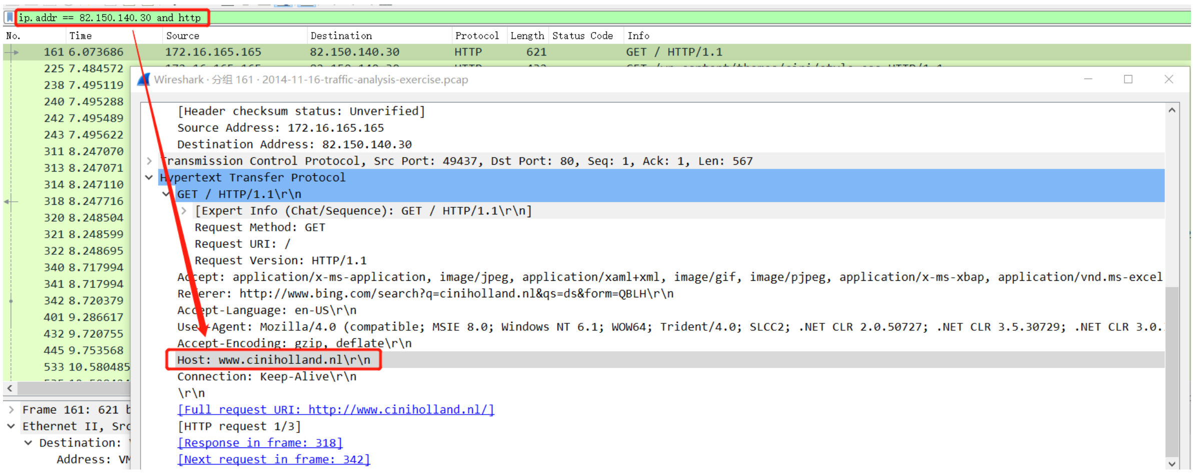
5、被入侵网站域名

答案

www.ciniholland.nl

# 分析过程

过滤"ip.addr == 82.150.140.30 and http"，定位关于被入侵IP的HTTP数据包



```
ip.addr == 82.150.140.30 and http

No.  Time          Source           Destination     Protocol  Length  Status Code  Info
161  6.073686      172.16.165.165   82.150.140.30   HTTP      621                  GET / HTTP/1.1
225  7.484572
238  7.495119
240  7.495288
242  7.495489
243  7.495622
311  8.247070
313  8.247071
314  8.247110
318  8.247716
320  8.248504
321  8.248599
322  8.248695
340  8.717994
341  8.717994
342  8.720379
401  9.286617
432  9.720755
445  9.753568
533  10.580485

> Frame 161: 621 b
v Ethernet II, Src
  v Destination:
      Address: VM
```

Wireshark · 分组 161 · 2014-11-16-traffic-analysis-exercise.pcap

```
    [Header checksum status: Unverified]
    Source Address: 172.16.165.165
    Destination Address: 82.150.140.30
> Transmission Control Protocol, Src Port: 49437, Dst Port: 80, Seq: 1, Ack: 1, Len: 567
v Hypertext Transfer Protocol
  v GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel
    Referer: http://www.bing.com/search?q=ciniholland.nl&qs=ds&form=QBLH\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.
    Accept-Encoding: gzip, deflate\r\n
    Host: www.ciniholland.nl\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://www.ciniholland.nl/]
    [HTTP request 1/3]
    [Response in frame: 318]
    [Next request in frame: 342]
```

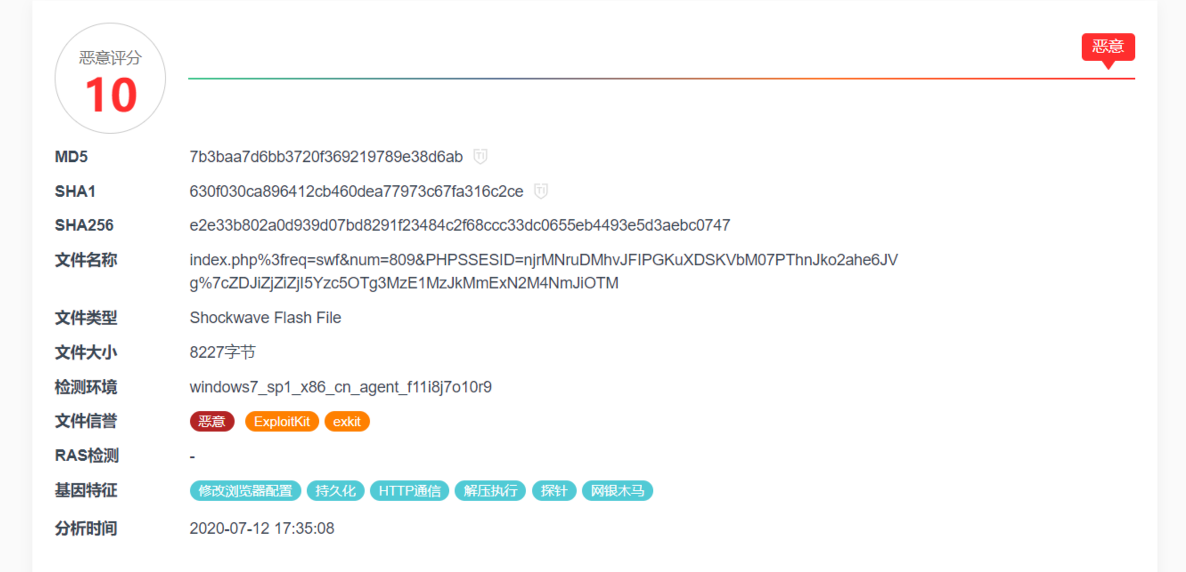
6、提供恶意软件的域名

答案

stand.trustandprobaterealty.com

# 分析过程

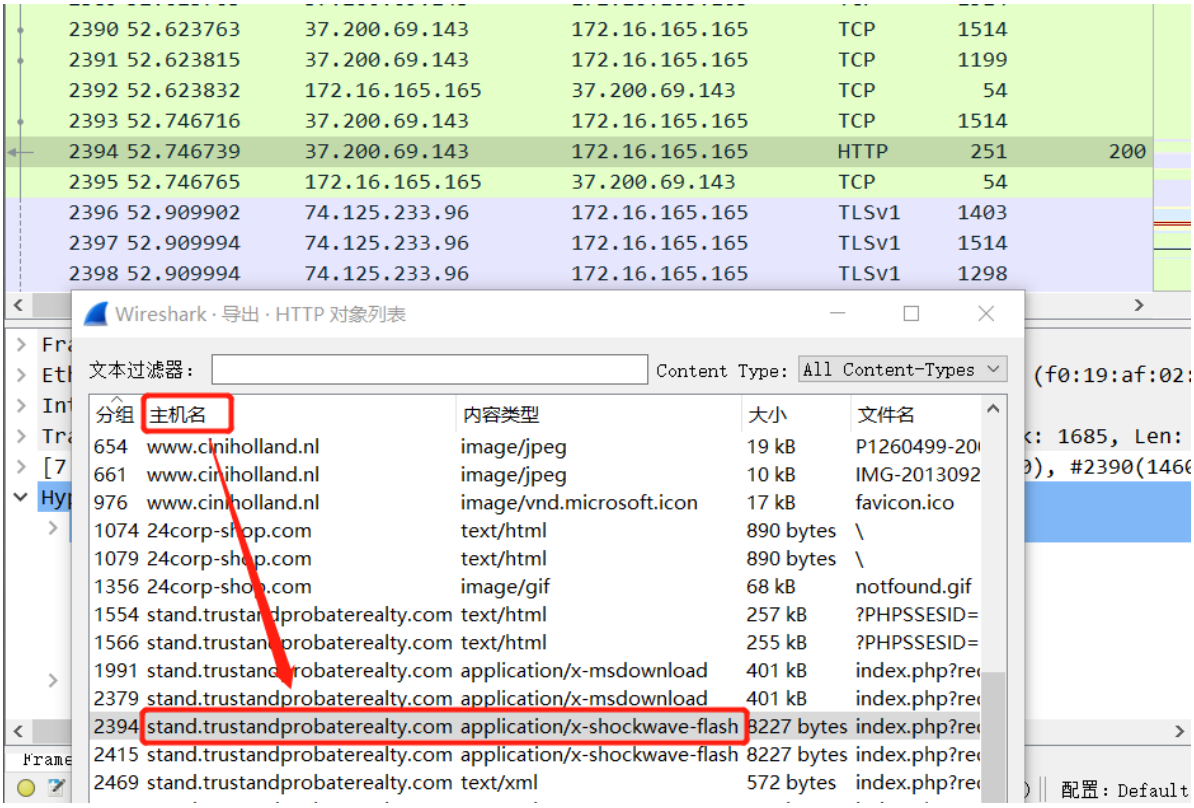
提供恶意软件的地址，首先定位到恶意软件，点击导出对象"HTTP"。发现其中存在一些不寻常的文件，如"application/x-msdownload"类型的文件，代表dll文件，"application/x-shockwave-flash"代表swf文件，"application/java-archive"代表jar文件，比较可疑。下载并分析，发现swf文件为恶意软件



MD5	7b3baa7d6bb3720f369219789e38d6ab
SHA1	630f030ca896412cb460dea77973c67fa316c2ce
SHA256	e2e33b802a0d939d07bd8291f23484c2f68ccc33dc0655eb4493e5d3aebc0747
文件名称	index.php%3freq=swf&num=809&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7cZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJiOTM
文件类型	Shockwave Flash File
文件大小	8227字节
检测环境	windows7_sp1_x86_cn_agent_f11i8j7o10r9
文件信誉	恶意 ExploitKit exkit
RAS检测	-
基因特征	修改浏览器配置 持久化 HTTP通信 解压执行 探针 网银木马
分析时间	2020-07-12 17:35:08

# 分析过程

定位该文件的数据包，发现恶意软件的域名为stand.trustandprobaterealty.com，IP为37.200.69.143



```
2390 52.623763   37.200.69.143    172.16.165.165   TCP     1514
2391 52.623815   37.200.69.143    172.16.165.165   TCP     1199
2392 52.623832   172.16.165.165   37.200.69.143    TCP       54
2393 52.746716   37.200.69.143    172.16.165.165   TCP     1514
2394 52.746739   37.200.69.143    172.16.165.165   HTTP     251      200
2395 52.746765   172.16.165.165   37.200.69.143    TCP       54
2396 52.909902   74.125.233.96    172.16.165.165   TLSv1   1403
2397 52.909994   74.125.233.96    172.16.165.165   TLSv1   1514
2398 52.909994   74.125.233.96    172.16.165.165   TLSv1   1298
```

Wireshark · 导出 · HTTP 对象列表

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

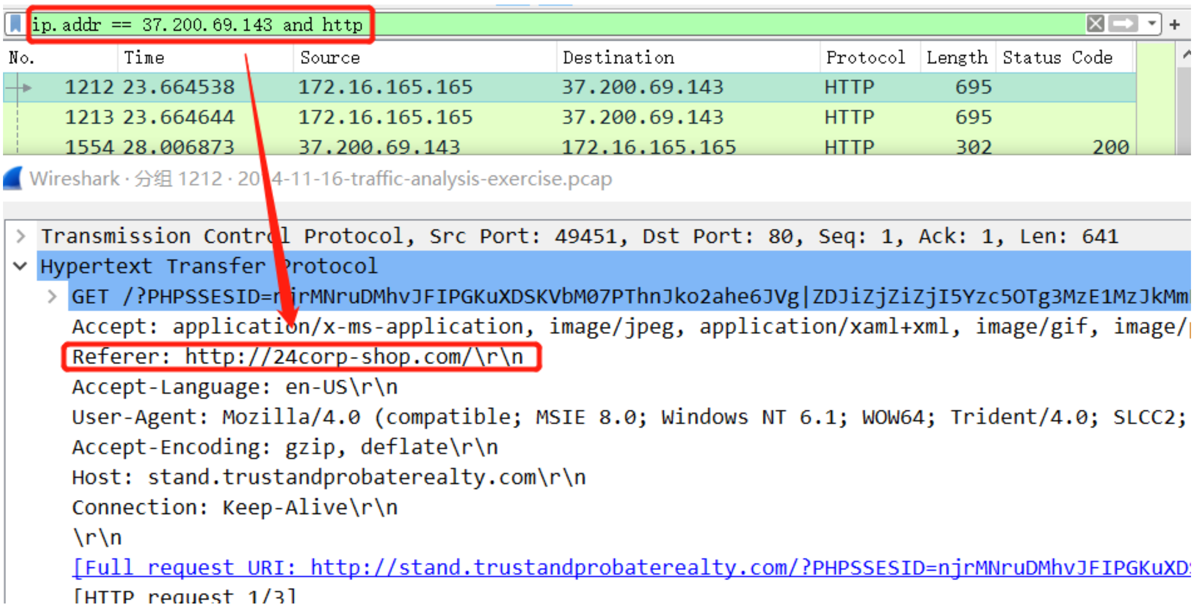
分组	主机名	内容类型	大小	文件名
654	www.ciniholland.nl	image/jpeg	19 kB	P1260499-20
661	www.ciniholland.nl	image/jpeg	10 kB	IMG-2013092
976	www.ciniholland.nl	image/vnd.microsoft.icon	17 kB	favicon.ico
1074	24corp-shop.com	text/html	890 bytes	\
1079	24corp-shop.com	text/html	890 bytes	\
1356	24corp-shop.com	image/gif	68 kB	notfound.gif
1554	stand.trustandprobaterealty.com	text/html	257 kB	?PHPSSESID=
1566	stand.trustandprobaterealty.com	text/html	255 kB	?PHPSSESID=
1991	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?re
2379	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?re
2394	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?re
2415	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?re
2469	stand.trustandprobaterealty.com	text/xml	572 bytes	index.php?re

二级

1、指向恶意软件登陆页面的重定向URL

```
# 答案
    http://24corp-shop.com/
```

```
# 分析过程
    已知恶意软件的IP为37.200.69.143，那么找重定向URL时，只需要找到第一次与37.200.69.143交互的HTTP数据包，并找到该数据包中的Referer，即重定向前的URL。过滤语法"ip.addr == 37.200.69.143 and http"
```



```
ip.addr == 37.200.69.143 and http

No.      Time          Source           Destination     Protocol  Length  Status Code
   1212 23.664538   172.16.165.165   37.200.69.143   HTTP      695
   1213 23.664644   172.16.165.165   37.200.69.143   HTTP      695
   1554 28.006873   37.200.69.143    172.16.165.165  HTTP      302         200
```

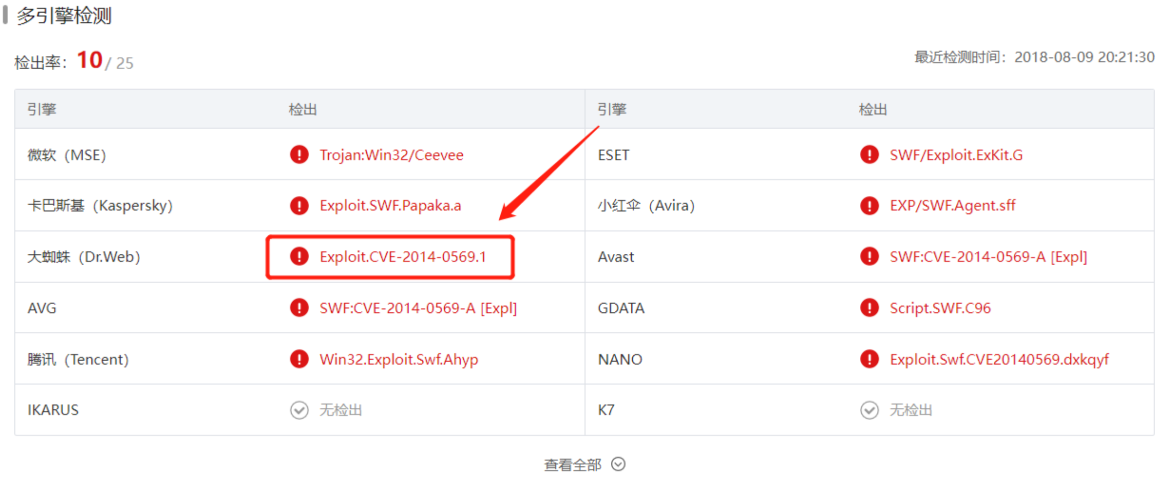
Wireshark · 分组 1212 · 2014-11-16-traffic-analysis-exercise.pcap

```
> Transmission Control Protocol, Src Port: 49451, Dst Port: 80, Seq: 1, Ack: 1, Len: 641
v Hypertext Transfer Protocol
  > GET /?PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMm
    Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/
    Referer: http://24corp-shop.com/\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2;
    Accept-Encoding: gzip, deflate\r\n
    Host: stand.trustandprobaterealty.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://stand.trustandprobaterealty.com/?PHPSSESID=njrMNruDMhvJFIPGKuXD
    [HTTP request 1/3]
```

2、出来登陆页面（CVE-2013-2551）之外，还发送了哪些其他漏洞利用

```
# 答案
    CVE-2012-0507
```

```
# 分析思路
    将恶意文件下载下来，放入病毒检测平台中检测，发现存在swf文件存在CVE-2014-0569漏洞，jar文件存在CVE-2012-0507漏洞
```

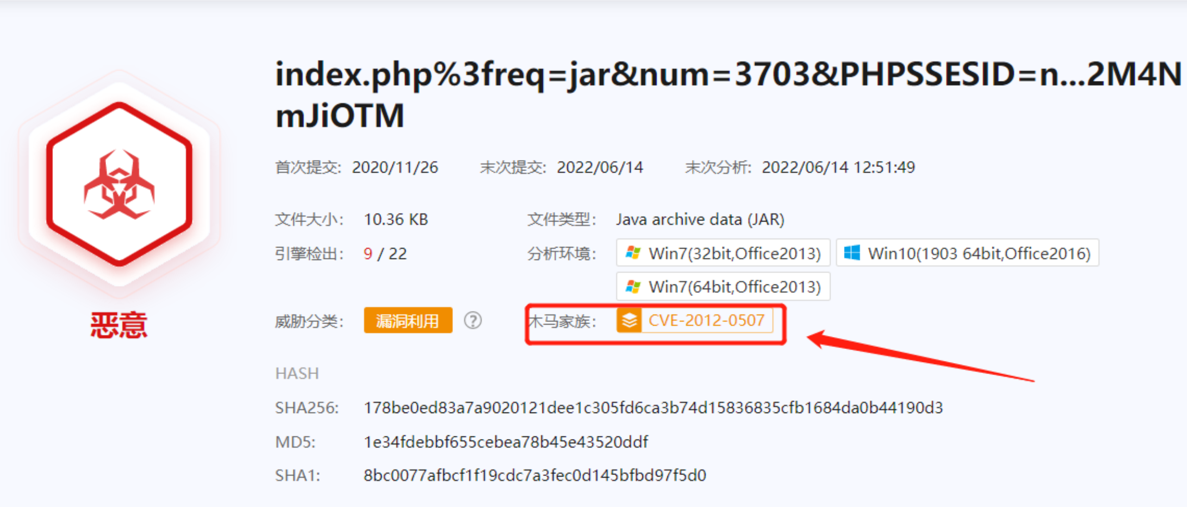


多引擎检测

检出率：10 / 25

最近检测时间：2018-08-09 20:21:30

引擎	检出	引擎	检出
微软（MSE）	Trojan:Win32/Ceevee	ESET	SWF/Exploit.ExKit.G
卡巴斯基（Kaspersky）	Exploit.SWF.Papaka.a	小红伞（Avira）	EXP/SWF.Agent.sff
大蜘蛛（Dr.Web）	Exploit.CVE-2014-0569.1	Avast	SWF:CVE-2014-0569-A [Expl]
AVG	SWF:CVE-2014-0569-A [Expl]	GDATA	Script.SWF.C96
腾讯（Tencent）	Win32.Exploit.Swf.Ahyp	NANO	Exploit.Swf.CVE20140569.dxkqyf
IKARUS	无检出	K7	无检出



index.php%3freq=jar&num=3703&PHPSSESID=n...2M4NmJiOTM

首次提交: 2020/11/26　　末次提交: 2022/06/14　　末次分析: 2022/06/14 12:51:49

文件大小: 10.36 KB　　文件类型: Java archive data (JAR)

引擎检出: 9 / 22　　分析环境: Win7(32bit,Office2013)　Win10(1903 64bit,Office2016)　Win7(64bit,Office2013)

威胁分类: 漏洞利用　　木马家族: CVE-2012-0507

HASH

SHA256: 178be0ed83a7a9020121dee1c305fd6ca3b74d15836835cfb1684da0b44190d3

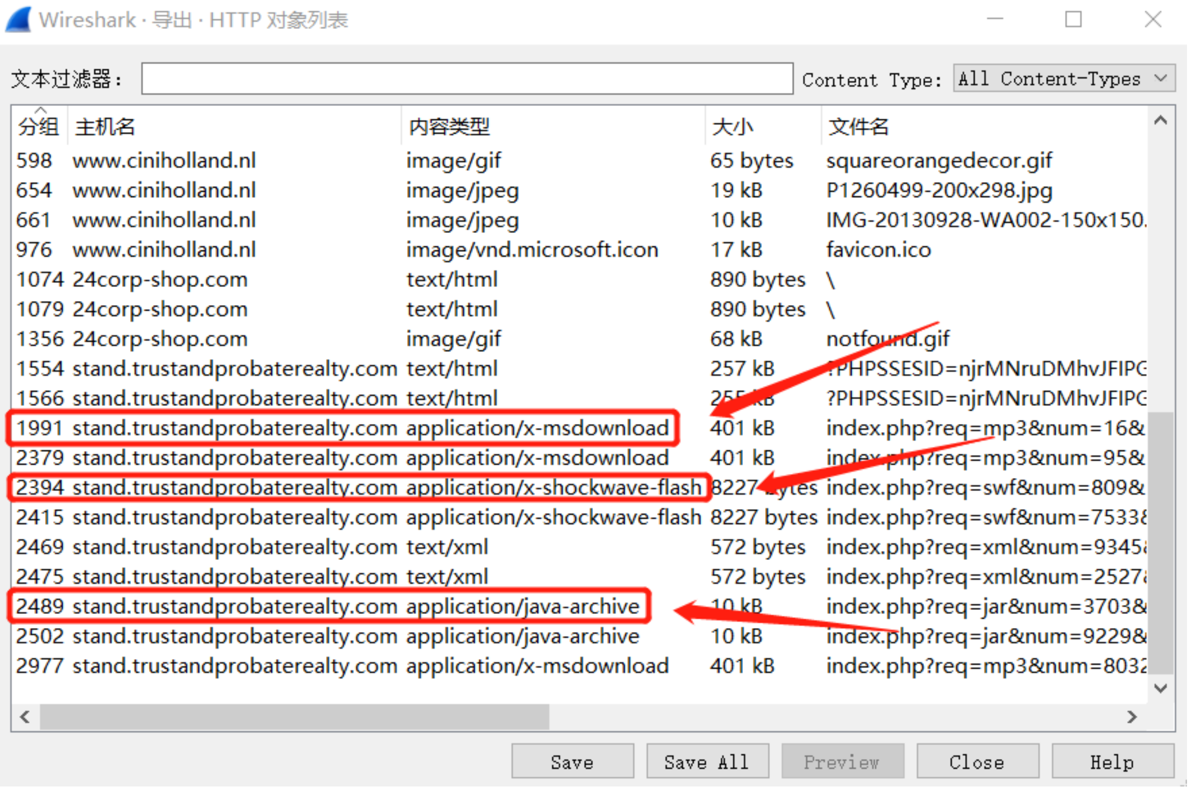
MD5: 1e34fdebbf655cebea78b45e43520ddf

SHA1: 8bc0077afbcf1f19cdc7a3fec0d145bfbd97f5d0

3、有效载荷传递了多少次

```
# 答案
    3次
```

```
# 分析思路
    查看恶意软件的个数
```



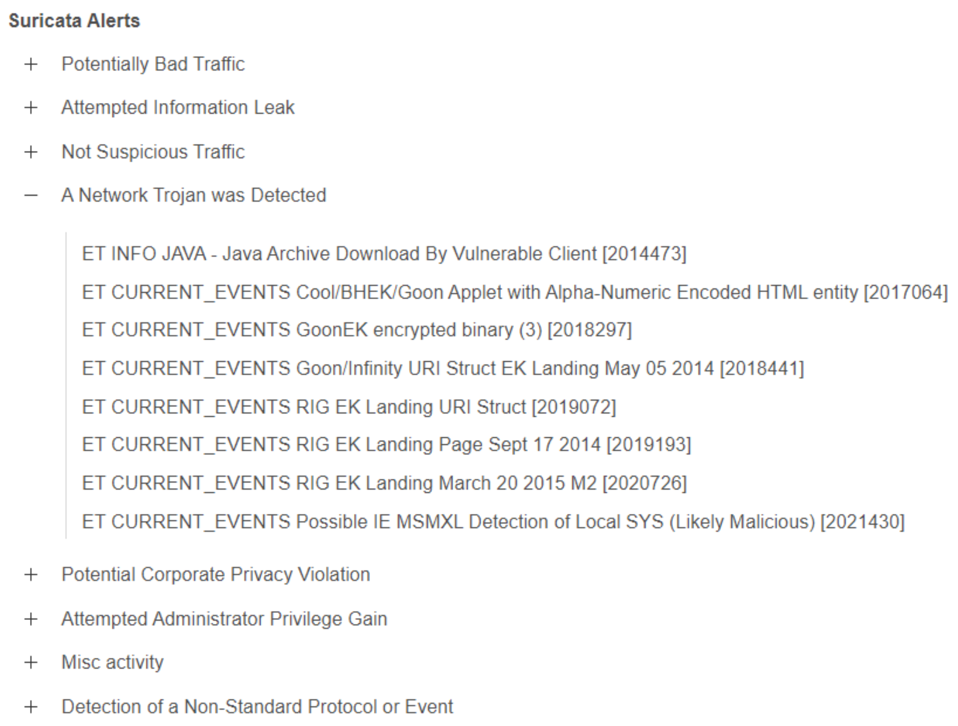
文本过滤器：　　Content Type: All Content-Types

分组	主机名	内容类型	大小	文件名
598	www.ciniholland.nl	image/gif	65 bytes	squareorangedecor.gif
654	www.ciniholland.nl	image/jpeg	19 kB	P1260499-200x298.jpg
661	www.ciniholland.nl	image/jpeg	10 kB	IMG-20130928-WA002-150x150.
976	www.ciniholland.nl	image/vnd.microsoft.icon	17 kB	favicon.ico
1074	24corp-shop.com	text/html	890 bytes	\
1079	24corp-shop.com	text/html	890 bytes	\
1356	24corp-shop.com	image/gif	68 kB	notfound.gif
1554	stand.trustandprobaterealty.com	text/html	257 kB	?PHPSSESID=njrMNruDMhvJFIPG
1566	stand.trustandprobaterealty.com	text/html	255 kB	?PHPSSESID=njrMNruDMhvJFIPG
1991	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=16&
2379	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=95&
2394	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=809&
2415	stand.trustandprobaterealty.com	application/x-shockwave-flash	8227 bytes	index.php?req=swf&num=7533
2469	stand.trustandprobaterealty.com	text/xml	572 bytes	index.php?req=xml&num=9345
2475	stand.trustandprobaterealty.com	text/xml	572 bytes	index.php?req=xml&num=2527
2489	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=3703&
2502	stand.trustandprobaterealty.com	application/java-archive	10 kB	index.php?req=jar&num=9229&
2977	stand.trustandprobaterealty.com	application/x-msdownload	401 kB	index.php?req=mp3&num=8032

4、将pcap提交给Virus Total并找到触发了哪些snort警报，Suricate警报中显示的EK名称是什么

```
# 答案
    ET INFO JAVA - Java Archive Download By Vulnerable Client [2014473]
    ET CURRENT_EVENTS Cool/BHEK/Goon Applet with Alpha-Numeric Encoded HTML entity [2017064]
    ET CURRENT_EVENTS GoonEK encrypted binary (3) [2018297]
    ET CURRENT_EVENTS Goon/Infinity URI Struct EK Landing May 05 2014 [2018441]
    ET CURRENT_EVENTS RIG EK Landing URI Struct [2019072]
    ET CURRENT_EVENTS RIG EK Landing Page Sept 17 2014 [2019193]
    ET CURRENT_EVENTS RIG EK Landing March 20 2015 M2 [2020726]
    ET CURRENT_EVENTS Possible IE MSMXL Detection of Local SYS (Likely Malicious) [2021430]
```

```
# 分析过程
    直接将该pcap拖到Virustotal网站，查看DETAILS模块
```



Suricata Alerts

- + Potentially Bad Traffic
- + Attempted Information Leak
- + Not Suspicious Traffic
- − A Network Trojan was Detected
  - ET INFO JAVA - Java Archive Download By Vulnerable Client [2014473]
  - ET CURRENT_EVENTS Cool/BHEK/Goon Applet with Alpha-Numeric Encoded HTML entity [2017064]
  - ET CURRENT_EVENTS GoonEK encrypted binary (3) [2018297]
  - ET CURRENT_EVENTS Goon/Infinity URI Struct EK Landing May 05 2014 [2018441]
  - ET CURRENT_EVENTS RIG EK Landing URI Struct [2019072]
  - ET CURRENT_EVENTS RIG EK Landing Page Sept 17 2014 [2019193]
  - ET CURRENT_EVENTS RIG EK Landing March 20 2015 M2 [2020726]
  - ET CURRENT_EVENTS Possible IE MSMXL Detection of Local SYS (Likely Malicious) [2021430]
- + Potential Corporate Privacy Violation
- + Attempted Administrator Privilege Gain
- + Misc activity
- + Detection of a Non-Standard Protocol or Event