SELECTED STADIUM

SOLUTIONS

Category: Network Traffic Analysis
Bracket: Silver
Title: HTTP 1 Challenge **SOLUTION**

This challenge evaluates the participant's ability to understand a packet capture containing Hypertext Transfer Protocol (HTTP) traffic - https://www.dropbox.com/s/3umosjquz1j0i9d/NCL-2015-HTTP1.pcap?dl=0. During the game, it was suggested to use the Wireshark program to solve the challenge.

1. What was the compromised website?	**php.net**
2. What version of PHP were they using?	**5.4.16**
3. What version of Apache were they using?	**2.2.21**
4. In what year was this capture made?	**2013**
5. What domain serves up the malicious files?	**zivvgmyrwy.3razbave.info**
6. What is the IP address of the malicious domain?	**144.76.192.102**
7. At what packet number is the first request for a malicious .SWF made?	**177**
8. At what packet number is the second request for a malicious .SWF made?	**180**
9. At what packet number is the first request to download a malicious executable made?	**213**

SELECTED STADIUM SOLUTIONS

Questions 1-4 can be solved by applying the filter below and then following the TCP stream for the first matched packet:

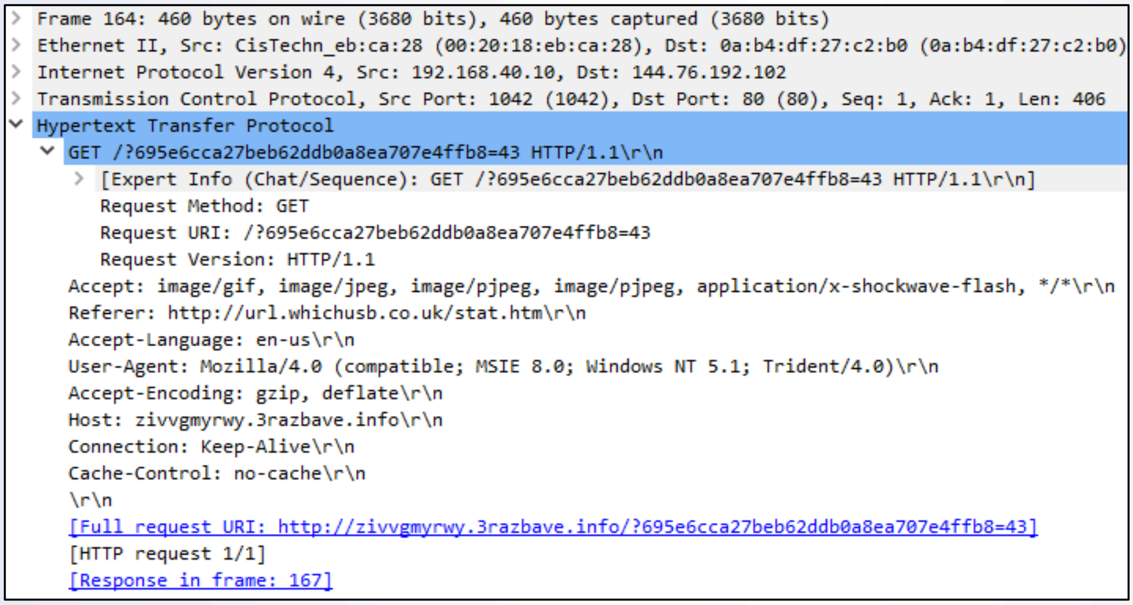
http.request

This will yield the request/response to/from the compromised website:

```
GET / HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg,
application/x-
shockwave-flash, */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT
5.1; Trident/4.0)
Accept-Encoding: gzip, deflate
Host: php.net
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 22 Oct 2013 19:27:52 GMT
Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21
OpenSSL/0.9.8q PHP/5.4.16-dev
X-Powered-By: PHP/5.4.16-dev
Content-language: en
Set-Cookie: COUNTRY=USA%2C64.235.155.80; expires=Tue, 29-
Oct-2013 19:27:52
GMT; path=/; domain=.php.net
Last-Modified: Wed, 23 Oct 2013 01:00:14 GMT
Vary: User-Agent,Accept-Encoding
Content-Encoding: gzip
Content-Length: 6507
Connection: close
Content-Type: text/html;charset=utf-8
```

Questions 5-6 can be solved by looking for suspicious HTTP requests. One such request is packet #164, which contains a series of hexadecimal characters in the URL and an even more suspicious host, *zivvgmyrwy.3razbave.info*. By following the stream, the response can be seen to contain HTML that attempts to retrieve a .SWF file. These factors indicate that the request was made to a malicious host.



```
> Frame 164: 460 bytes on wire (3680 bits), 460 bytes captured (3680 bits)
> Ethernet II, Src: CisTechn_eb:ca:28 (00:20:18:eb:ca:28), Dst: 0a:b4:df:27:c2:b0 (0a:b4:df:27:c2:b0)
> Internet Protocol Version 4, Src: 192.168.40.10, Dst: 144.76.192.102
> Transmission Control Protocol, Src Port: 1042 (1042), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 406
v Hypertext Transfer Protocol
    v GET /?695e6cca27beb62ddb0a8ea707e4ffb8=43 HTTP/1.1\r\n
        > [Expert Info (Chat/Sequence): GET /?695e6cca27beb62ddb0a8ea707e4ffb8=43 HTTP/1.1\r\n]
          Request Method: GET
          Request URI: /?695e6cca27beb62ddb0a8ea707e4ffb8=43
          Request Version: HTTP/1.1
      Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, */*\r\n
      Referer: http://url.whichusb.co.uk/stat.htm\r\n
      Accept-Language: en-us\r\n
      User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)\r\n
      Accept-Encoding: gzip, deflate\r\n
      Host: zivvgmyrwy.3razbave.info\r\n
      Connection: Keep-Alive\r\n
      Cache-Control: no-cache\r\n
      \r\n
      [Full request URI: http://zivvgmyrwy.3razbave.info/?695e6cca27beb62ddb0a8ea707e4ffb8=43]
      [HTTP request 1/1]
      [Response in frame: 167]
```

Questions 7-8 can be solved be extrapolating data from the response in packet #164. The filter below can be used to help remove noise and to help find requests made after packet #164:

```
http.request
```

Note that the first request returns a 404 error and the other may trigger antivirus programs when you view the TCP stream.

Question 9 can be found by following TCP streams for various HTTP requests. The executable will contain the string, “This program cannot be run in DOS mode.”