Category
Network Forensics

Challenge Name
To the “future” direction - 2

Message given to challengers
Your task is to understand Mirai protocol to obtain a DDoS attack command from the C2 server “mirai-c2.trend:23”, and find DDoS attack to “10.192.0.10”.
For evidence of your understanding, we request you to create the flag string like “CSG_FLAG{<type number>:<target port>:<attack duration>}”.
Ex.) If you find a command which means “30 second UDP flood attack to port 80” to “10.192.0.10”, the flag will be “CSG_FLAG{0:80:30}”

Warning: You might know the Mirai C2 server has a buffer overflow vulnerability, but it is not PWN challenge. Trying compromise C2 server may crash the server and then you cannot get the flag until the entire challenge environment (including other challenges) is restored.

Objective
You can learn how you can use open-source information to network forensics, and how to get commands from C&C server.

Detailed Instructions
To emulate the communication, you must write a program to send the followings to the C&C server:
- “00 00 00 01 <1 byte of bot id length> < botid>” (login packet)
- “00 00” (ping packet)

If you ignore to respond pong packet, you will be disconnected from the C&C server.

Then, to find the necessary information you need to parse the Mirai protocol.
- Packet length (2 bytes from offset 0)
- Attack duration (4 bytes from offset 2)
- Attack type (1 byte from offset 6)
- Number of targets (1 byte from offset 7)
- Target IP/ IP network mask (5 bytes for each target, from offset 8)
- Number of flags (1 byte after target IP-mask list)

- Other flags (various length)
  - Flag type (1 byte)
  - Flag data size (1 byte)
  - Flag data (various length)

Sometimes you need to shave first 2 bytes before parse when the message starts from “00 00”. It must be parsed as ping(s) and DDoS command.

The C&C server replies many DDoS attack commands. But if you check IP address only, it will fail to find the flag. You will receive two command packets once in 3 minutes, respectively, where “oolong-tea.ajccbc-cyber-sea-game.net” is resolved to “10.192.0.10”.

1. “40 seconds of HTTP attack to port 8080 of oolong-tea.ddns.net”
2. “60 seconds of DNS query flood that queries ‘oolong-tea. ajccbc-cyber-sea-game.net’ to 192.168.0.1, 172.16.0.1, 127.0.0.1, and 10.192.0.10”

But you must take a deeper look at the source code. The HTTP attack is targeted to the specified host with a header “Host: oolong-tea. ajccbc-cyber-sea-game.net”. So, we cannot say this query is target to the server. On the other hand, the DNS attack explicitly intends to overload the server “10.192.0.10”.

Finally, you can create the flag “CSG_FLAG{2:53:60}”.

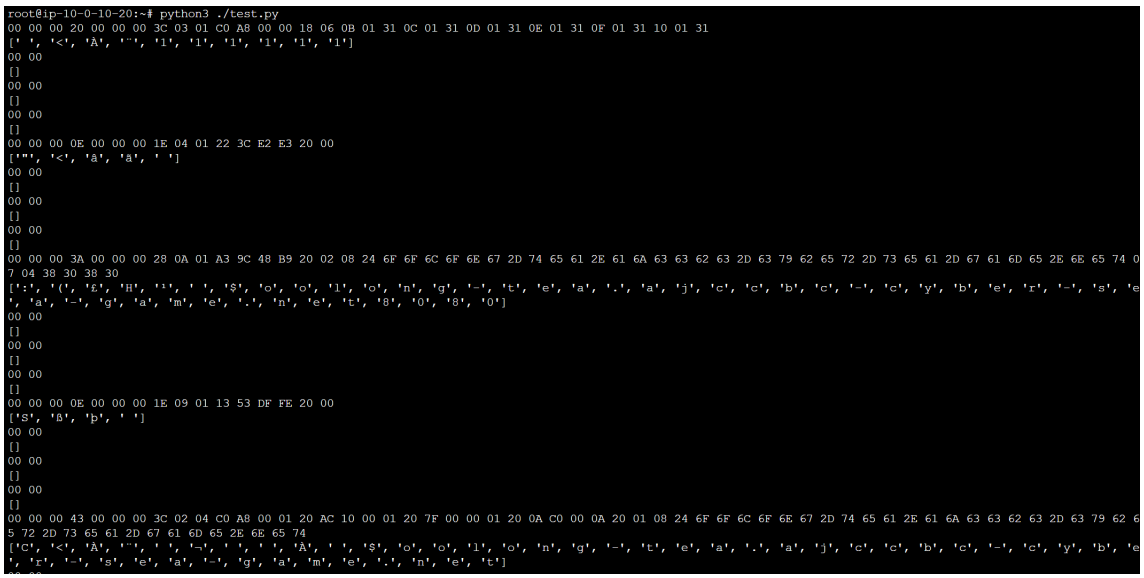
Simple sample code in python: you need install hexdump by “python3 -m pip install hexdump”

```
import socket
import hexdump
import time

# Connection inititialization
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((‘mirai-c2.trend’, 23))
s.send(b‘¥x00¥x00¥x00¥x01’)    # Hello
time.sleep(1)
s.send(b‘¥x03abc’)    # login with botid
time.sleep(1)

while True:
      s.send(b’¥x00¥x00’) # ping
      time.sleep(5)
      packet = s.recv(1024)
      # Remove trailing pong packets.
      while packet[:2] == ‘¥x00¥x00’:
            packet = packet[2:]
      # Read the packet...    In this answer key, we do not implement mirai protocol
parser
      print(hexdump.dump(packet))
      print([chr(i) for i in packet if chr(i).isprintable()])
```

The program can get hex code like this from C2 server, for example.



You can see two DDoS commands indicate:

1. “40 seconds of HTTP attack to port 8080 of oolong-tea.ddns.net”
2. “60 seconds of DNS query flood that queries ‘oolong-tea. ajccbc-cyber-sea-game.net’ to 192.168.0.1, 172.16.0.1, 127.0.0.1, and 10.192.0.10”

References

Documents

Mirai-Source-Code https://github.com/jgamblin/Mirai-Source-Code

Mirai (DDoS) Source Code Review https://medium.com/@cjbarker/mirai-ddos-source-code-review-57269c4a68f

Understanding the Mirai Botnet https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf