IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers

Xiaolu Zhang, Oren Upton, Nicole Lang Beebe, Kim-Kwang Raymond Choo
Department of Information Systems and Cyber Security, University of Texas at San Antonio
Most important features of Mirai

- An IoT malware and a centralized Botnet
- Caused those most famous IoT DDoS attacks
- Open sourced and fast-growing
Mirai botnet structure

- (192.168.1.1) Attacker’s terminal
- (192.168.1.3) CNC
- (192.168.1.4) MySQL database
- Scan receiver
- Loading server
- DNS server (192.168.1.7)
- (192.168.4.2) Infected IoT
- Vulnerable IoT (192.168.4.3)
- (192.168.4.4) Victim of DDoS attack
Motivation

• Many investigations/research of Mirai to date have focused on a traditional malware analysis of the executable code found on infected IoT devices.

• As Mirai is open sourced, there has been increasing abuse of Mirai’s source code. Someone lacking the expertise to write an IoT botnet can easily build their own Mirai botnet for a DDoS attack. In this case, a forensic investigator might be involved in a case where the control server of a Mirai botnet is captured.
Research questions

• What forensic approaches could work on the botnet servers?
• What evidence is retrievable from the servers?
• Where is the evidence located?
• What investigative information could be obtained from the evidence?
Methodology

• Build our own local Mirai botnet.
• Acquire data from the file system, RAM, and network traffic for each physical server.
• Apply manual analysis on the data source acquired in the preceding step. Specifically targeting:
  1. The historical record of the achieved attacks
  2. The victim/target of the DDoS attack
  3. The information about the infected bots
• Incorporate the findings into a Road Map.
The road map for Mirai botnet server forensics
Key findings on CNC server

• CNC source code (Unlikely) → User credentials of the Database

• CNC executable (Disk image) → User credentials of the Database

• CNC live process (Memory dump) → Bot list
CNC source code

User credentials of the Database

/Mirai-Source-Code/mirai/cnc/main.go

```go
const DatabaseAddr string = "192.168.1.4"
const DatabaseUser string = "db-login-usrname"
const DatabasePass string = "db-login-passwd"
const DatabaseTable string = "mirai"
```
CNC executable

→ User credentials of the Database

• By reverse engineering CNC executable (written in Go Lang), we proposed how to recover the Database server’s user credentials.
CNC live process

→ Bot list

• CNC server retains a queue of live Bots in RAM only.

• By tracking the “Bot” data structure in RAM the IP address of the live bots could be recovered.
Key findings on Database server

CNC User credentials and Command history

- If the database server is captured, CNC is accessible remotely.
The road map for Mirai botnet server forensics
Key findings on Scan Receiver & Loader

→ Bot list
  • The standard output stream (or ‘stdout’) is where the Loader acquires the information of a vulnerable IoT device reported by a bot

```
64 65 62 75 67 23 20 2E 2F 73 63 61 6E 4C 69 73
74 65 6D 20 0A 31 39 32 2E 31 36 38 2E 34 2E 33
3A 32 33 20 72 6F 6F 74 3A 70 61 73 73 0A 31 39
32 2E 34 2E 33 33 20 72 6F 6F 74 3A 70 61 73 73 0A 31 39
74 3A 70 61 73 73 0A 0A 00 00 00 00 00 00 00 00
```

debug# ./scanListen 192.168.4.3
:23 root:pass
2.168.4.3:23 root:pass

→ Bot Executable
  • a Loader must store bot executables for infecting the vulnerable IoT devices
The road map for Mirai botnet server forensics
Key findings on DNS server

➔ CNC server and the Scan Receiver’s IP address
➔ Client (bot) list

Aug 16 16:55:22 cnc named[515]: client @0x7ff9140c72a0 192.168.4.2#42576
Aug 16 16:55:50 cnc named[515]: client @0x7ff9140c72a0 192.168.4.2#55160
(report.mirai.com): query: report.mirai.com IN A + (192.168.1.7)

A Bot who queried the CNC’s IP address.
CNC’s domain name
Scan Receiver’s domain name
Summary

• This research intends to fill the gap where no existing study has performed a digital forensic analysis on IoT botnet servers.
• This research provides findings tactically useful to forensic investigators, not only from the perspective of what data could be obtained but also important information about which device they should target for acquisition and investigation to obtain the most investigatively useful information.
Thank you

Xiaolu Zhang  xiaolu.zhang@utsa.edu
Oren Upton  oren.upton@utsa.edu
Nicole Lang Beebe  nicole.beebe@utsa.edu
Kim-Kwang Raymond Choo  raymond.choo@fulbrightmail.org

The Cyber Center for Security & Analytics