Reto: Análisis de Malware Básico & Medio/Alto

Hector Fabio Jimenez aka c1b3rh4ck

c1b3rh4ck@gmail.com

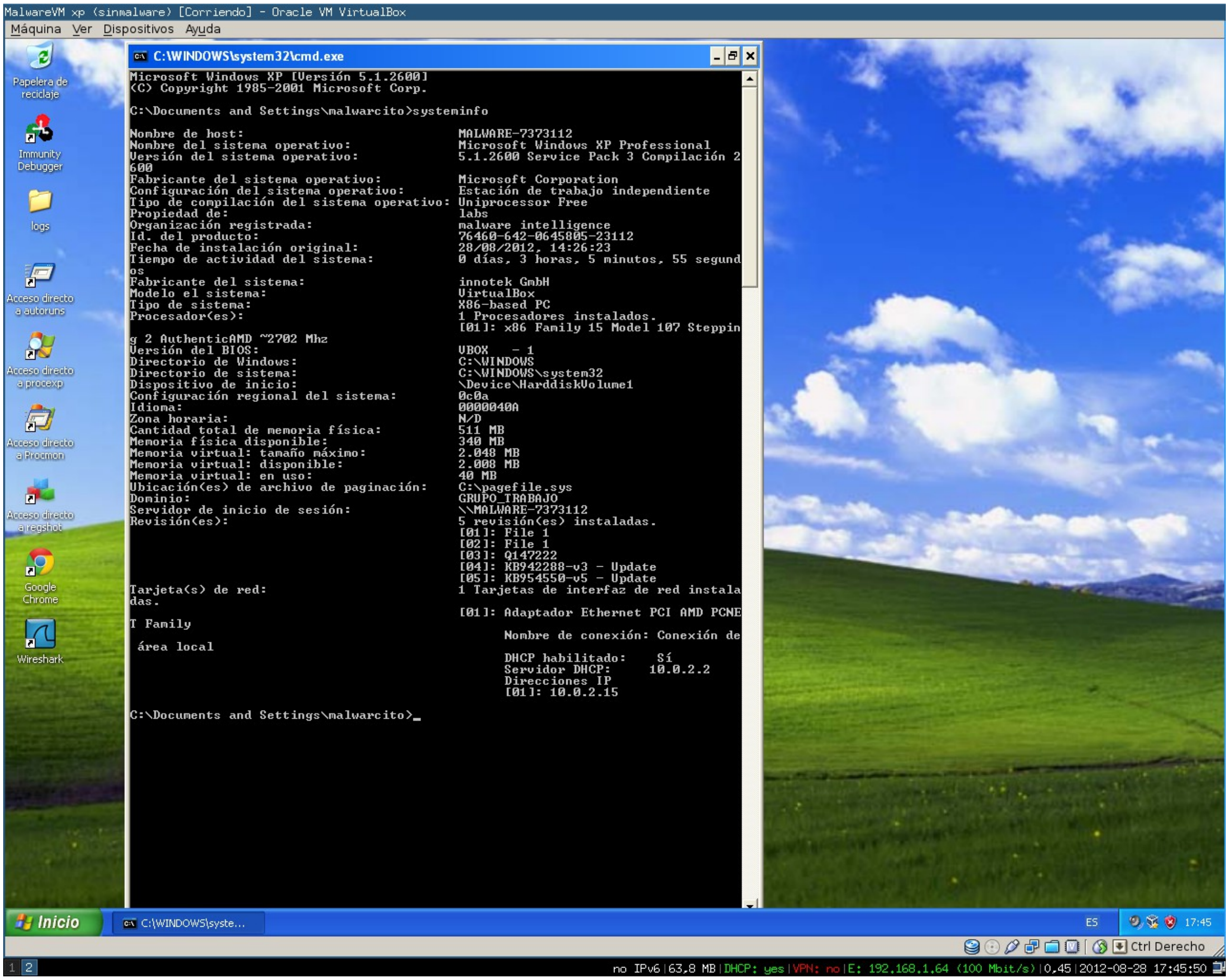
Sec Track

The "Do" to Security

Sec-track.org

Virtual Machine Details :

This paper aims to describe some steps and my methodology to solve this challenge,i'm not a professional in malware analisys,i'm an enthusiast so if you make a better job please share with me,document it into the wiki,my contact details are below.Being said that the first thing to do is set up a controlled virtual machine,in this case i'll use Windows Xp Professional SP3 as a virtual machine,in addittion to that i'm going to use “Tomar instantaneas” or snapshots of the vm.The vm has this features :



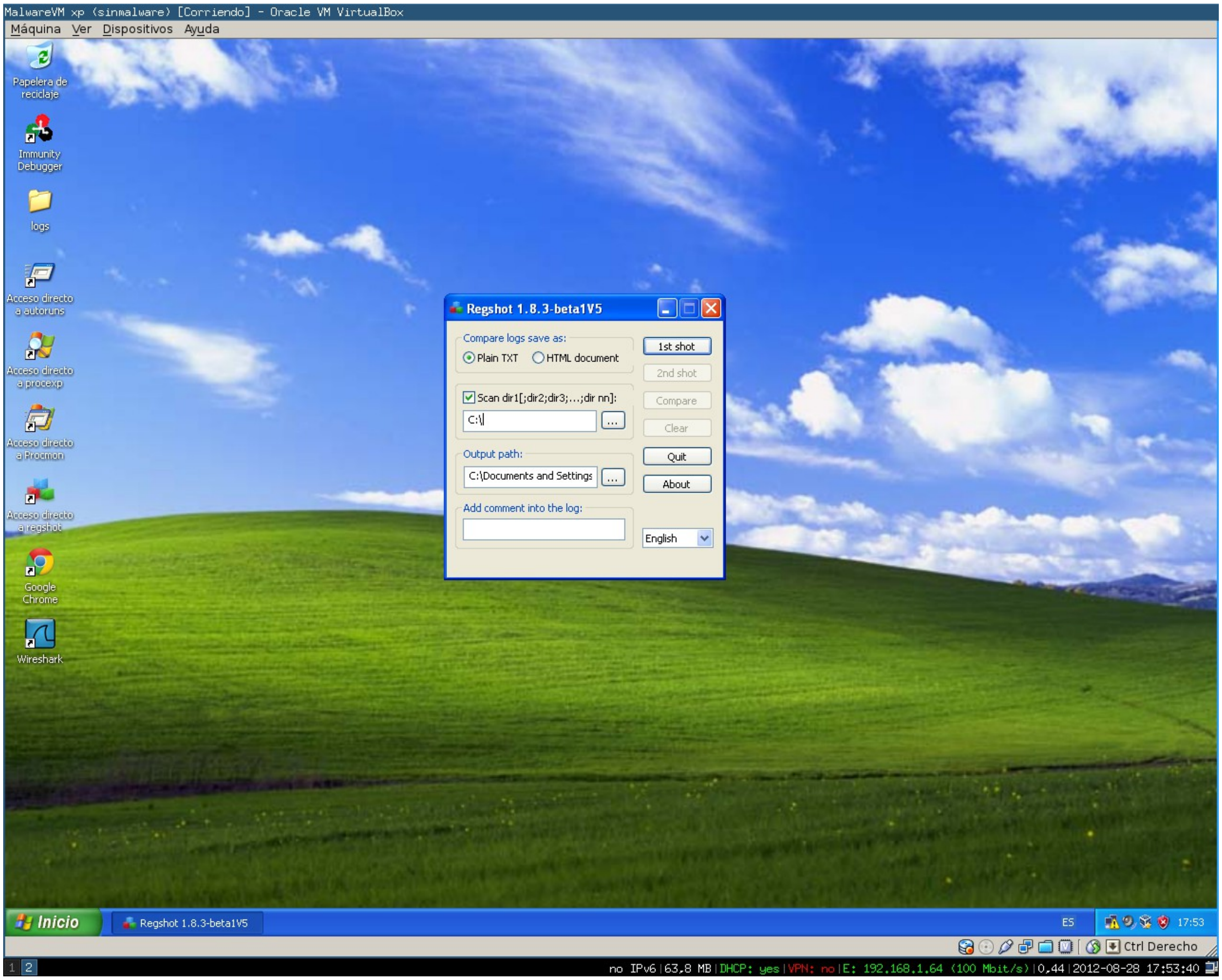
MalwareVM xp (sinmalware) [Corriendo] - Oracle VM VirtualBox
Máquina
Ver
Dispositivos
Ayuda
C:\WINDOWS\system32\cmd.exe
Papelera de reciclaje
Immunity Debugger
logs
Acceso directo a autoruns
Acceso directo a procexp
Acceso directo a Procmon
Acceso directo a regshot
Google Chrome
Wireshark
Inicio
C:\WINDOWS\syste...
ES
17:45
Ctrl Derecho
1
2
no IPv6 | 63.8 MB | DHCP: yes | VPN: no | E: 192.168.1.64 (100 Mbit/s) | 0.45 | 2012-08-28 17:45:50

```
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\malwarcito>systeminfo

Nombre de host:                            MALWARE-7373112
Nombre del sistema operativo:              Microsoft Windows XP Professional
Versión del sistema operativo:             5.1.2600 Service Pack 3 Compilación 2
600
Fabricante del sistema operativo:          Microsoft Corporation
Configuración del sistema operativo:       Estación de trabajo independiente
Tipo de compilación del sistema operativo: Uniprocessor Free
Propiedad de:                              labs
Organización registrada:                   malware intelligence
Id. del producto:                          76460-642-0645805-23112
Fecha de instalación original:             28/08/2012, 14:26:23
Tiempo de actividad del sistema:           0 días, 3 horas, 5 minutos, 55 segund
os
Fabricante del sistema:                    innotek GmbH
Modelo el sistema:                         VirtualBox
Tipo de sistema:                           X86-based PC
Procesador(es):                            1 Procesadores instalados.
                                           [01]: x86 Family 15 Model 107 Steppin
g 2 AuthenticAMD ~2702 Mhz
Versión del BIOS:                          VBOX   - 1
Directorio de Windows:                     C:\WINDOWS
Directorio de sistema:                     C:\WINDOWS\system32
Dispositivo de inicio:                     \Device\HarddiskVolume1
Configuración regional del sistema:        0c0a
Idioma:                                    0000040A
Zona horaria:                              N/D
Cantidad total de memoria física:          511 MB
Memoria física disponible:                 340 MB
Memoria virtual: tamaño máximo:            2.048 MB
Memoria virtual: disponible:               2.008 MB
Memoria virtual: en uso:                   40 MB
Ubicación(es) de archivo de paginación:    C:\pagefile.sys
Dominio:                                   GRUPO_TRABAJO
Servidor de inicio de sesión:              \\MALWARE-7373112
Revisión(es):                              5 revisión(es) instaladas.
                                           [01]: File 1
                                           [02]: File 1
                                           [03]: Q147222
                                           [04]: KB942288-v3 - Update
                                           [05]: KB954550-v5 - Update
Tarjeta(s) de red:                         1 Tarjetas de interfaz de red instala
das.
                                           [01]: Adaptador Ethernet PCI AMD PCNE
T Family
                                                 Nombre de conexión: Conexión de
 área local
                                                 DHCP habilitado:    Sí
                                                 Servidor DHCP:     10.0.2.2
                                                 Direcciones IP
                                                 [01]: 10.0.2.15


C:\Documents and Settings\malwarcito>_
```

Pic 1: basic set up for vm

with a little amount of software installed on it(reader,java,flash,chrome..etc),it could be used for our analysis.

For perform behavioral analysis in this vm i'm going to take my first registry shot using regshot[1],this tool let to take an entire shot of the register keys and other things inside him,also it has the capacibilities to make a quick diff between on and two files .



MalwareVM xp (sinmalware) [Corriendo] - Oracle VM VirtualBox

Regshot 1.8.3-beta1V5

Compare logs save as: ● Plain TXT ○ HTML document

☑ Scan dir1[;dir2;dir3;...;dir nn]:

C:\

Output path:

C:\Documents and Settings

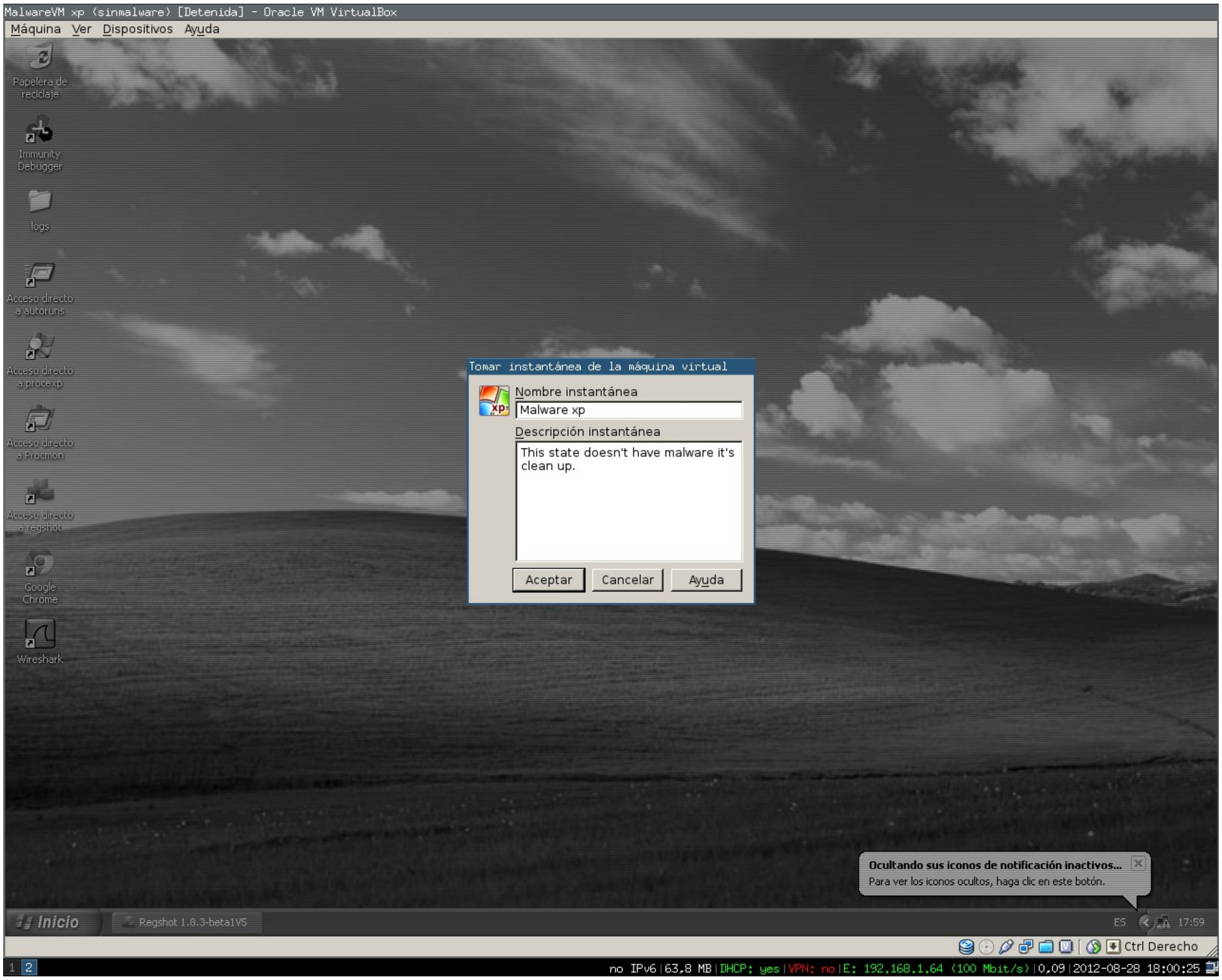
Add comment into the log:

English

no IPv6 | 63.8 MB | DHCP: yes | VPN: no | E: 192.168.1.64 (100 Mbit/s) | 0.44 | 2012-08-28 17:53:40

Pic 2: Using regshot for got snapshot

Our next step to do is take one snapshot in case of you need to revert the vm for repeat the behavior in the same,off course you can use other tools like norton ghost utility but this option is quick and efficient.



MalwareVM xp (sinmalware) [Detenida] - Oracle VM VirtualBox

Tomar instantánea de la máquina virtual

Nombre instantánea: Malware xp

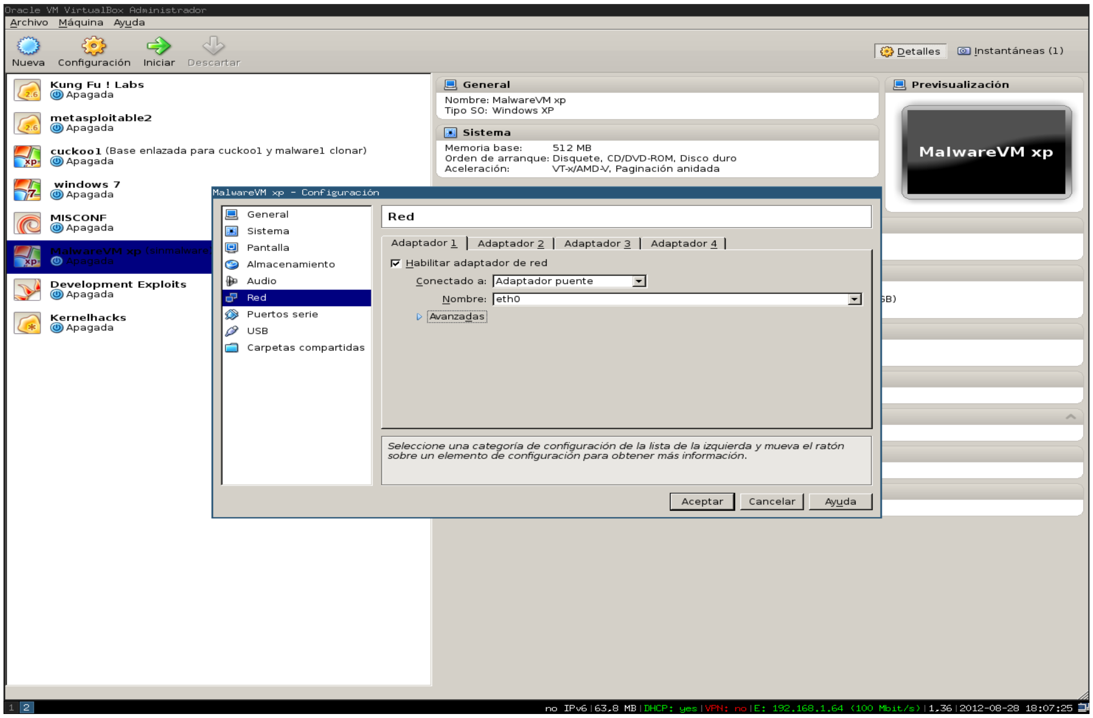
Descripción instantánea: This state doesn't have malware it's clean up.

Ocultando sus iconos de notificación inactivos...
Para ver los iconos ocultos, haga clic en este botón.

```
no IPv6 | 63.8 MB | DHCP: yes | VPN: no | E: 192.168.1.64 (100 Mbit/s) | 0.09 | 2012-08-28 18:00:25
```

Pic 3: Taking snapshot to revert to good state

The final step to this vm is set up the network configuration; for this lab i used two network interfaces,the first is in bridge and the second is used as internal network.



General
Nombre: MalwareVM xp
Tipo SO: Windows XP

Sistema
Memoria base: 512 MB
Orden de arranque: Disquete, CD/DVD-ROM, Disco duro
Aceleración: VT-x/AMD-V, Paginación anidada

MalwareVM xp - Configuración

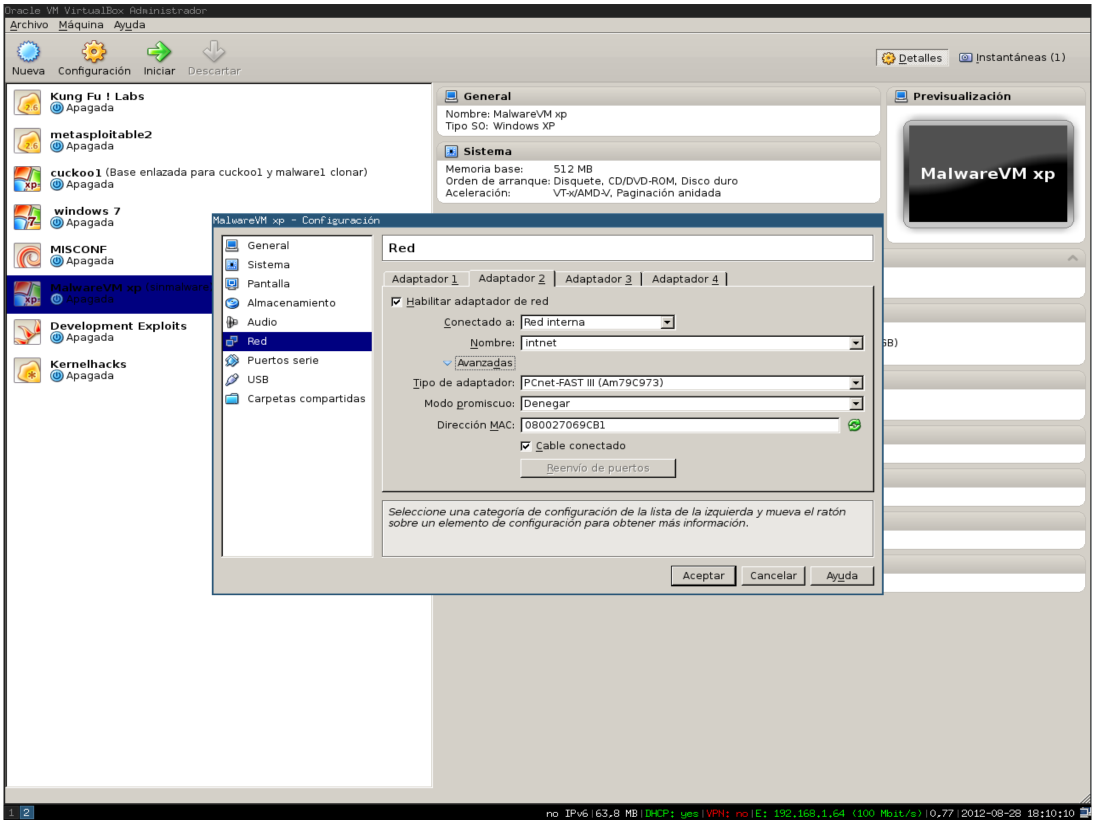
Red

☑ Habilitar adaptador de red
Conectado a: Adaptador puente
Nombre: eth0
▷ Avanzadas

Seleccione una categoría de configuración de la lista de la izquierda y mueva el ratón sobre un elemento de configuración para obtener más información.

```
no IPv6 | 63.8 MB | DHCP: yes | VPN: no | E: 192.168.1.64 (100 Mbit/s) | 1.36 | 2012-08-28 18:07:25
```

Pic 4:Network Interfaces Setup



General
Nombre: MalwareVM xp
Tipo SO: Windows XP

Sistema
Memoria base: 512 MB
Orden de arranque: Disquete, CD/DVD-ROM, Disco duro
Aceleración: VT-x/AMD-V, Paginación anidada

MalwareVM xp - Configuración

Red

☑ Habilitar adaptador de red
Conectado a: Red interna
Nombre: intnet
▽ Avanzadas
Tipo de adaptador: PCnet-FAST III (Am79C973)
Modo promiscuo: Denegar
Dirección MAC: 080027069CB1
☑ Cable conectado

Seleccione una categoría de configuración de la lista de la izquierda y mueva el ratón sobre un elemento de configuración para obtener más información.

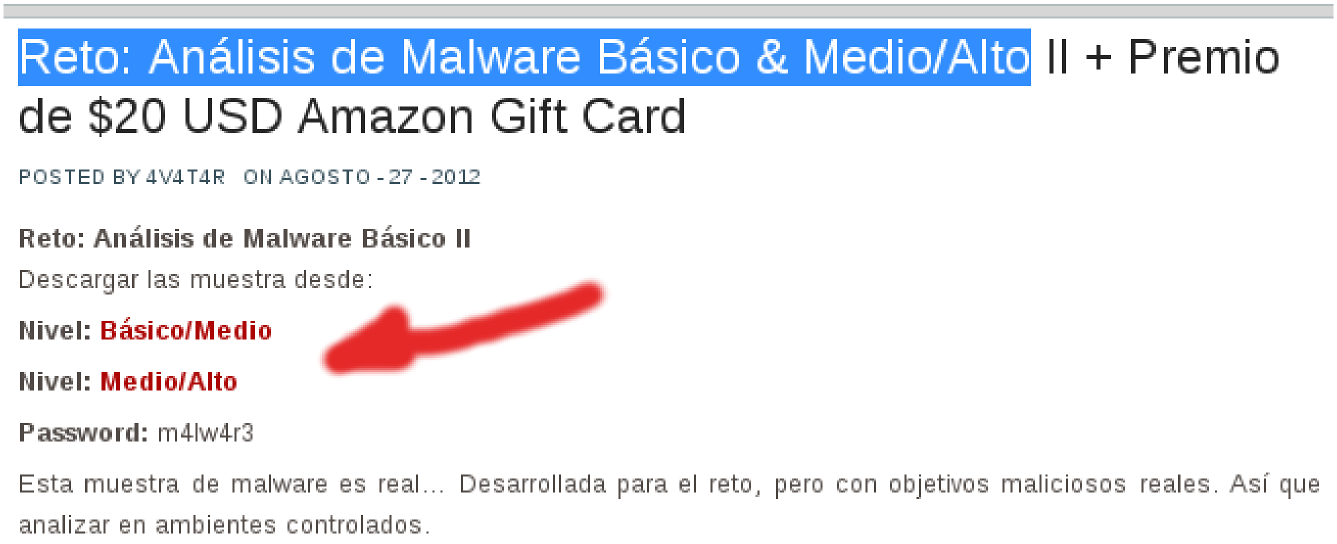
```
no IPv6 | 63.8 MB | DHCP: yes | VPN: no | E: 192.168.1.64 (100 Mbit/s) | 0.77 | 2012-08-28 18:10:10
```

Pic 5: Network Interfaces Setup

As a final addittion we need to have all the tools in the virtual machine for the behavioral analysis,tools like sysinternals,wireshark,ollydbg,capturebat and others really useful.

Identification of the Specimens:

Now we have the virtual machine done,we need to identify our specimens,in sec-track.org we find two links :



Reto: Análisis de Malware Básico & Medio/Alto II + Premio de $20 USD Amazon Gift Card

POSTED BY 4V4T4R ON AGOSTO - 27 - 2012

Reto: Análisis de Malware Básico II

Descargar las muestra desde:

Nivel: Básico/Medio

Nivel: Medio/Alto

Password: m4lw4r3

Esta muestra de malware es real... Desarrollada para el reto, pero con objetivos maliciosos reales. Así que analizar en ambientes controlados.

c

The first is "Basico/Medio" correspond to smss.rar and the second file "Medio/Alto" correspond to winlogon.rar,i download,and check the md5sums :

```
hector@Osiris:/tmp/analisis/smss$ md5sum smss.rar
c667c9ba336708ccda8fc562f0807359  smss.rar
```

```
hector@Osiris:/tmp/analisis/winlogon$ md5sum winlogon.rar
cdb997e8e823eda3176268130ced9e1b  winlogon.rar
```

being downloaded the couple of files ,i'm going to identify some special details of each one,details like peid,strings,sections,note at this point is posible to use a dynamic code analysis or static code analysis,if is necesary .

Let me identify the file inside smss.rar.

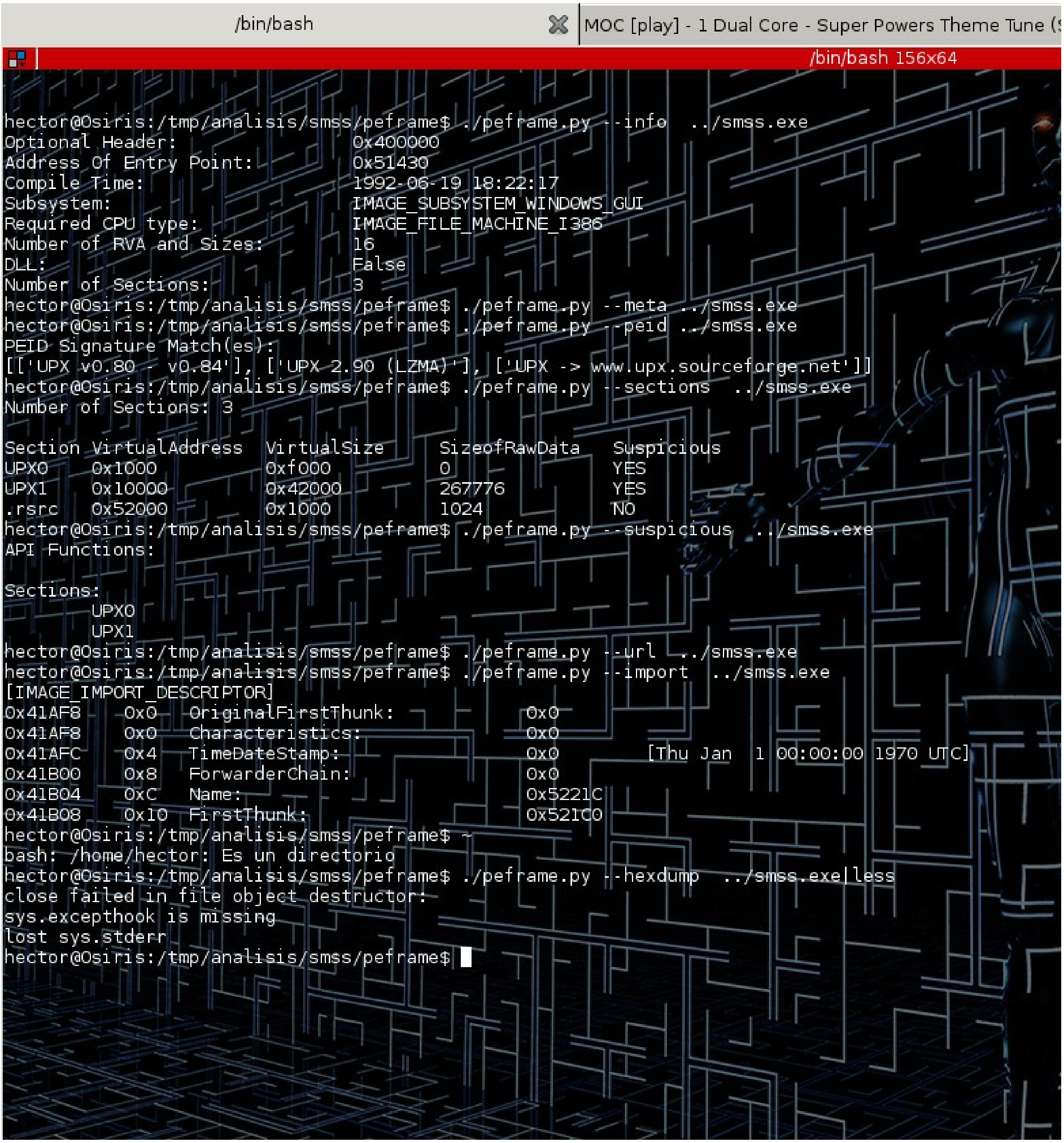
1.Extract the file in smss.rar

```
hector@Osiris:/tmp/analisis/smss$ unrar x smss.rar

UNRAR 4.10 freeware      Copyright (c) 1993-2012 Alexander Roshal

Enter password (will not be echoed) for smss.rar:

Extracting from smss.rar
smss.exe already exists. Overwrite it ?
[Y]es, [N]o, [A]ll, n[E]ver, [R]ename, [Q]uit y

Extracting  smss.exe                                             OK
All OK
```

2. verify the md5 and sha1 :

```
hector@Osiris:/tmp/analisis/smss$ md5sum smss.exe && sha1sum smss.exe
c970a9dd758fc1620684f85731610d4d  smss.exe
3ed34887b65f48daea269ca49d0a31edc99bf0f2  smss.exe

hector@Osiris:/tmp/analisis/smss$ file smss.exe
smss.exe: PE32 executable (GUI) Intel 80386, for MS Windows, U0PX compressed

hector@Osiris:/tmp/analisis/smss$ stat  smss.exe
  Fichero: «smss.exe»
  Tamaño: 269824       Bloques: 530        Bloque E/S: 1024   fichero regular
Dispositivo: 808h/2056d       Nodo-i: 30506       Enlaces: 1
Acceso: (0644/-rw-r--r--)  Uid: ( 1000/  hector)   Gid: ( 1000/  hector)
      Acceso: 2012-08-29 06:25:05.000000000 -0500
Modificación: 2012-08-24 22:00:54.000000000 -0500
      Cambio:    2012-08-29 06:22:34.000000000 -0500
    Creación: -
```

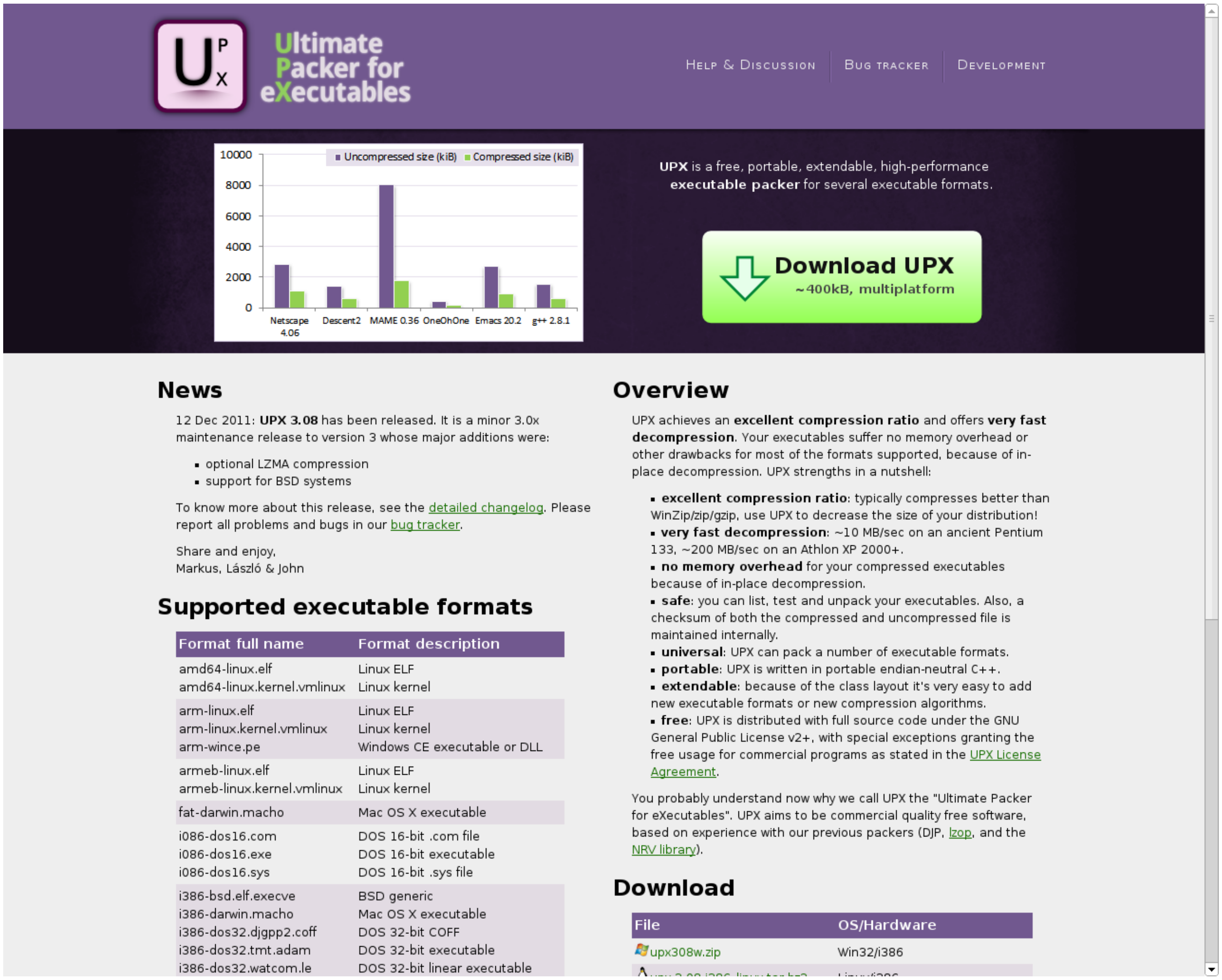
at this point i use peframe an awesome tool write in python for static analysis of malware[2]
you can find summary of functions,information,peid,extract the urls,strings ...etc[2]



```
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --info  ../smss.exe
Optional Header:                0x400000
Address Of Entry Point:         0x51430
Compile Time:                   1992-06-19 18:22:17
Subsystem:                      IMAGE_SUBSYSTEM_WINDOWS_GUI
Required CPU type:              IMAGE_FILE_MACHINE_I386
Number of RVA and Sizes:        16
DLL:                            False
Number of Sections:             3
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --meta ../smss.exe
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --peid ../smss.exe
PEID Signature Match(es):
[['UPX v0.80 - v0.84'], ['UPX 2.90 (LZMA)'], ['UPX -> www.upx.sourceforge.net']]
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --sections  ../smss.exe
Number of Sections: 3

Section VirtualAddress  VirtualSize     SizeofRawData   Suspicious
UPX0    0x1000          0xf000          0               YES
UPX1    0x10000         0x42000         267776          YES
.rsrc   0x52000         0x1000          1024            NO
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --suspicious  ../smss.exe
API Functions:

Sections:
        UPX0
        UPX1
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --url  ../smss.exe
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --import  ../smss.exe
[IMAGE_IMPORT_DESCRIPTOR]
0x41AF8    0x0   OriginalFirstThunk:            0x0
0x41AF8    0x0   Characteristics:               0x0
0x41AFC    0x4   TimeDateStamp:                 0x0        [Thu Jan  1 00:00:00 1970 UTC]
0x41B00    0x8   ForwarderChain:                0x0
0x41B04    0xC   Name:                          0x5221C
0x41B08    0x10  FirstThunk:                    0x521C0
hector@Osiris:/tmp/analisis/smss/peframe$ ~
bash: /home/hector: Es un directorio
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --hexdump  ../smss.exe|less
close failed in file object destructor:
sys.excepthook is missing
lost sys.stderr
hector@Osiris:/tmp/analisis/smss/peframe$ 
```

Pic 6: Using Peframe for smss.exe

Are you thinking what i'm thinking?
What's about upx ?



UPX is a free, portable, extendable, high-performance **executable packer** for several executable formats.

News

12 Dec 2011: **UPX 3.08** has been released. It is a minor 3.0x maintenance release to version 3 whose major additions were:

- optional LZMA compression
- support for BSD systems

To know more about this release, see the detailed changelog. Please report all problems and bugs in our bug tracker.

Share and enjoy,
Markus, László & John

Supported executable formats

Format full name	Format description
amd64-linux.elf	Linux ELF
amd64-linux.kernel.vmlinux	Linux kernel
arm-linux.elf	Linux ELF
arm-linux.kernel.vmlinux	Linux kernel
arm-wince.pe	Windows CE executable or DLL
armeb-linux.elf	Linux ELF
armeb-linux.kernel.vmlinux	Linux kernel
fat-darwin.macho	Mac OS X executable
i086-dos16.com	DOS 16-bit .com file
i086-dos16.exe	DOS 16-bit executable
i086-dos16.sys	DOS 16-bit .sys file
i386-bsd.elf.execve	BSD generic
i386-darwin.macho	Mac OS X executable
i386-dos32.djgpp2.coff	DOS 32-bit COFF
i386-dos32.tmt.adam	DOS 32-bit executable
i386-dos32.watcom.le	DOS 32-bit linear executable

Overview

UPX achieves an **excellent compression ratio** and offers **very fast decompression**. Your executables suffer no memory overhead or other drawbacks for most of the formats supported, because of in-place decompression. UPX strengths in a nutshell:

- **excellent compression ratio**: typically compresses better than WinZip/zip/gzip, use UPX to decrease the size of your distribution!
- **very fast decompression**: ~10 MB/sec on an ancient Pentium 133, ~200 MB/sec on an Athlon XP 2000+.
- **no memory overhead** for your compressed executables because of in-place decompression.
- **safe**: you can list, test and unpack your executables. Also, a checksum of both the compressed and uncompressed file is maintained internally.
- **universal**: UPX can pack a number of executable formats.
- **portable**: UPX is written in portable endian-neutral C++.
- **extendable**: because of the class layout it's very easy to add new executable formats or new compression algorithms.
- **free**: UPX is distributed with full source code under the GNU General Public License v2+, with special exceptions granting the free usage for commercial programs as stated in the UPX License Agreement.

You probably understand now why we call UPX the "Ultimate Packer for eXecutables". UPX aims to be commercial quality free software, based on experience with our previous packers (DJP, lzop, and the NRV library).

Download

File	OS/Hardware
upx308w.zip	Win32/i386
upx-3.08-i386_linux.tar.bz2	Linux/i386

Pic 7: What about upx packer ?

It seems upx is an other interesting packer,we can unpack the smss.exe,but wait a minute we need to make a smss.exe backup.

```
hector@Osiris:/tmp$ cp smss.exe originalsmss.exe
hector@Osiris:/tmp$ md5sum originalsmss.exe && md5sum smss.exe
c970a9dd758fc1620684f85731610d4d  originalsmss.exe
c970a9dd758fc1620684f85731610d4d  smss.exe
hector@Osiris:/tmp$ diff -u originalsmss.exe smss.exe
```

now let me unpack smss.exe using upx utility.

```
hector@Osiris:/tmp$ upx -d smss.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2011
UPX 3.08        Markus Oberhumer, Laszlo Molnar & John Reiser   Dec 12th 2011

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    282624 <-    269824   95.47%    win32/pe     smss.exe

Unpacked 1 file.
```

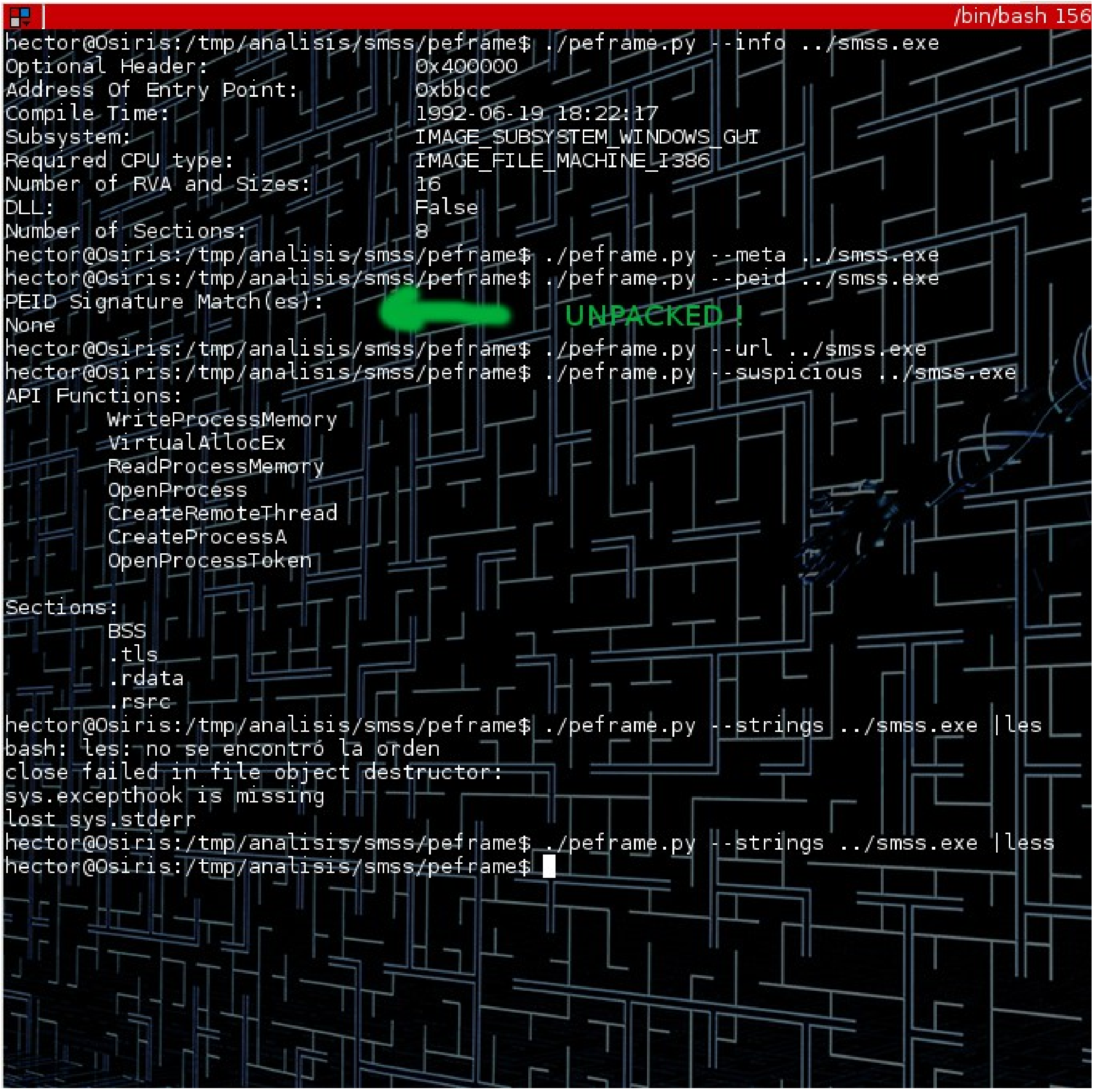
```
hector@Osiris:/tmp/analisis/smss$ diff -u originalsmss.exe smss.exe
Los ficheros binarios originalsmss.exe y smss.exe son distintos

hector@Osiris:/tmp/analisis/smss$  md5sum originalsmss.exe && md5sum smss.exe
c970a9dd758fc1620684f85731610d4d  originalsmss.exe /original
23463920f354766fd6f38009b9258491  smss.exe    /unpacked
```

doing a quick diff of the strings :

```
hector@Osiris:/tmp/analisis/smss$ strings smss.exe |wc -l
3346
hector@Osiris:/tmp/analisis/smss$ strings originalsmss.exe |wc -l
2563
```

Note the diference when it is unpacked if i could'nt unpack this,with upx utility i had loaded into olly.

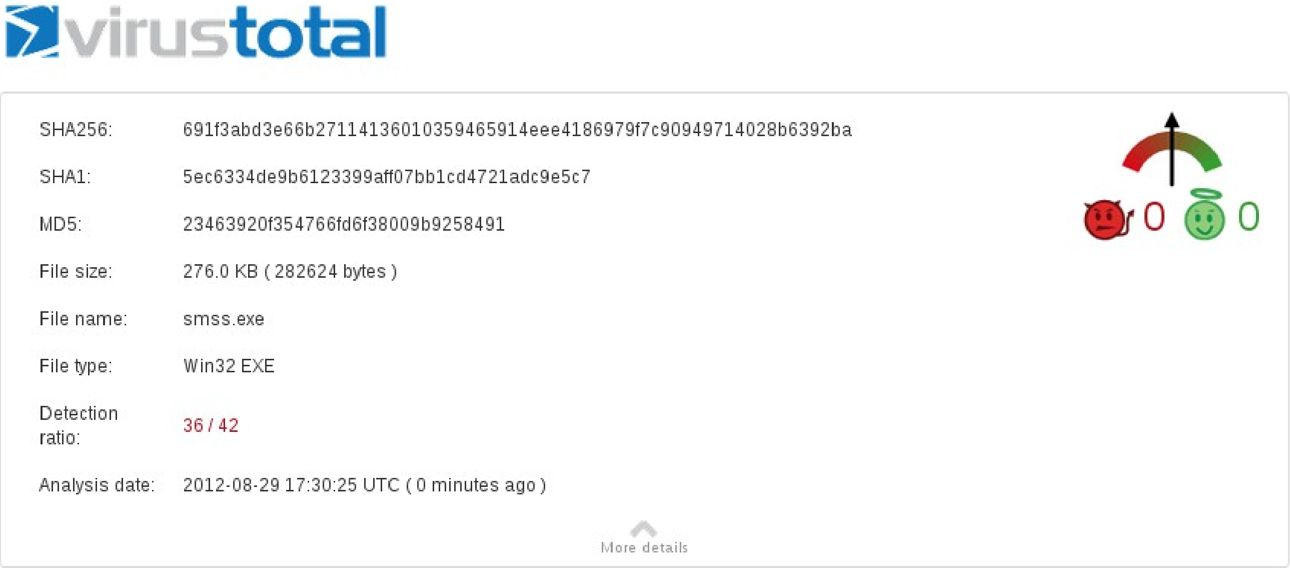
again i can use peframe for functions and suspicious :)



```
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --info ../smss.exe
Optional Header:                0x400000
Address Of Entry Point:         0xbbcc
Compile Time:                   1992-06-19 18:22:17
Subsystem:                      IMAGE_SUBSYSTEM_WINDOWS_GUI
Required CPU type:              IMAGE_FILE_MACHINE_I386
Number of RVA and Sizes:        16
DLL:                            False
Number of Sections:             8
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --meta ../smss.exe
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --peid ../smss.exe
PEID Signature Match(es):
None
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --url ../smss.exe
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --suspicious ../smss.exe
API Functions:
        WriteProcessMemory
        VirtualAllocEx
        ReadProcessMemory
        OpenProcess
        CreateRemoteThread
        CreateProcessA
        OpenProcessToken

Sections:
        BSS
        .tls
        .rdata
        .rsrc
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --strings ../smss.exe |les
bash: les: no se encontró la orden
close failed in file object destructor:
sys.excepthook is missing
lost sys.stderr
hector@Osiris:/tmp/analisis/smss/peframe$ ./peframe.py --strings ../smss.exe |less
hector@Osiris:/tmp/analisis/smss/peframe$ 
```

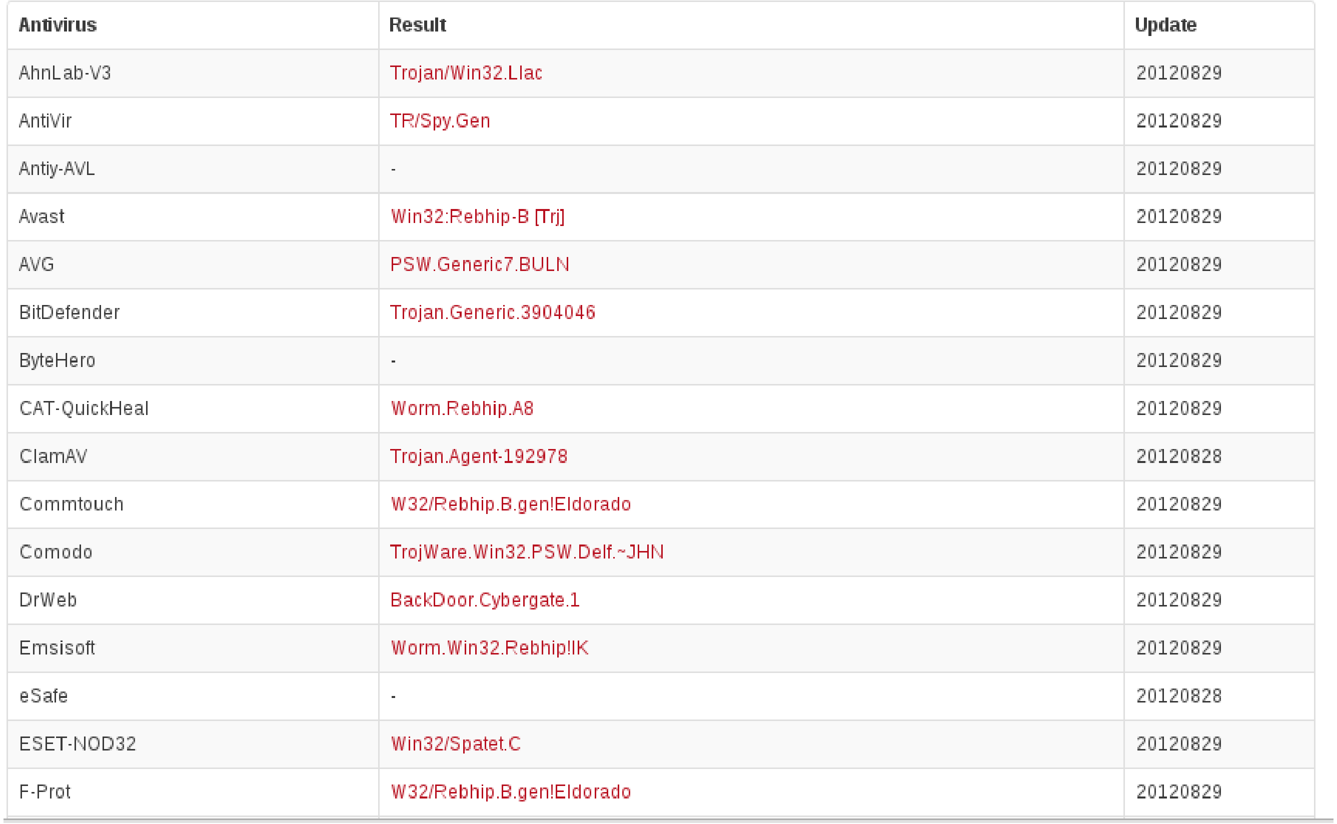
Pic 8:Peframe in action –suspicious argument changed drastically note .rdata,.rsrc.

We need to check the antivirus detection rate :P :



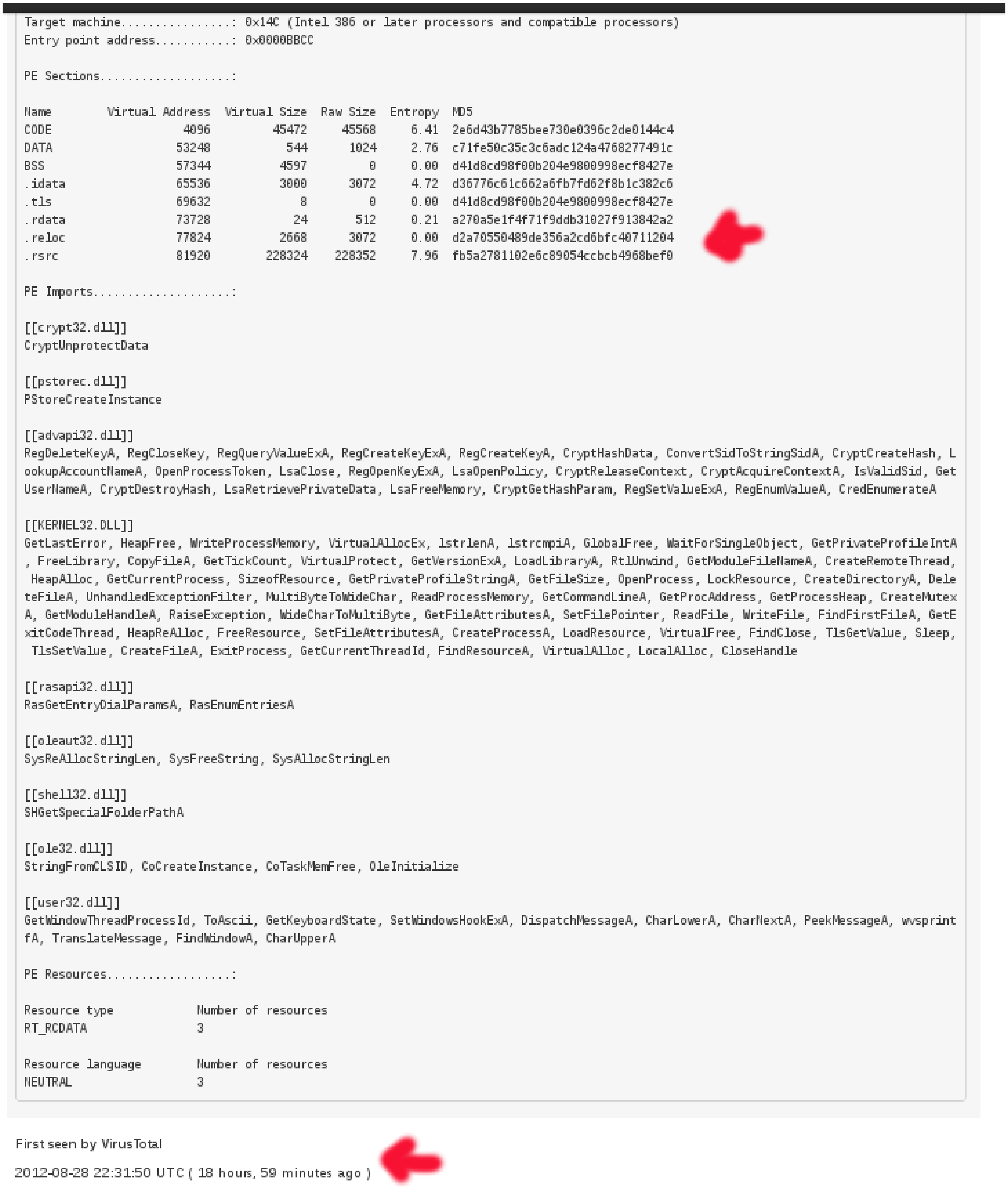
SHA256:	691f3abd3e66b27114136010359465914eee4186979f7c90949714028b6392ba
SHA1:	5ec6334de9b6123399aff07bb1cd4721adc9e5c7
MD5:	23463920f354766fd6f38009b9258491
File size:	276.0 KB (282624 bytes)
File name:	smss.exe
File type:	Win32 EXE
Detection ratio:	36 / 42
Analysis date:	2012-08-29 17:30:25 UTC (0 minutes ago)

Pic 9:virustotal.com report



Antivirus	Result	Update
AhnLab-V3	Trojan/Win32.Llac	20120829
AntiVir	TR/Spy.Gen	20120829
Antiy-AVL	-	20120829
Avast	Win32:Rebhip-B [Trj]	20120829
AVG	PSW.Generic7.BULN	20120829
BitDefender	Trojan.Generic.3904046	20120829
ByteHero	-	20120829
CAT-QuickHeal	Worm.Rebhip.A8	20120829
ClamAV	Trojan.Agent-192978	20120828
Commtouch	W32/Rebhip.B.gen!Eldorado	20120829
Comodo	TrojWare.Win32.PSW.Delf.~JHN	20120829
DrWeb	BackDoor.Cybergate.1	20120829
Emsisoft	Worm.Win32.Rebhip!IK	20120829
eSafe	-	20120828
ESET-NOD32	Win32/Spatet.C	20120829
F-Prot	W32/Rebhip.B.gen!Eldorado	20120829

Pic 10:virustotal.com result

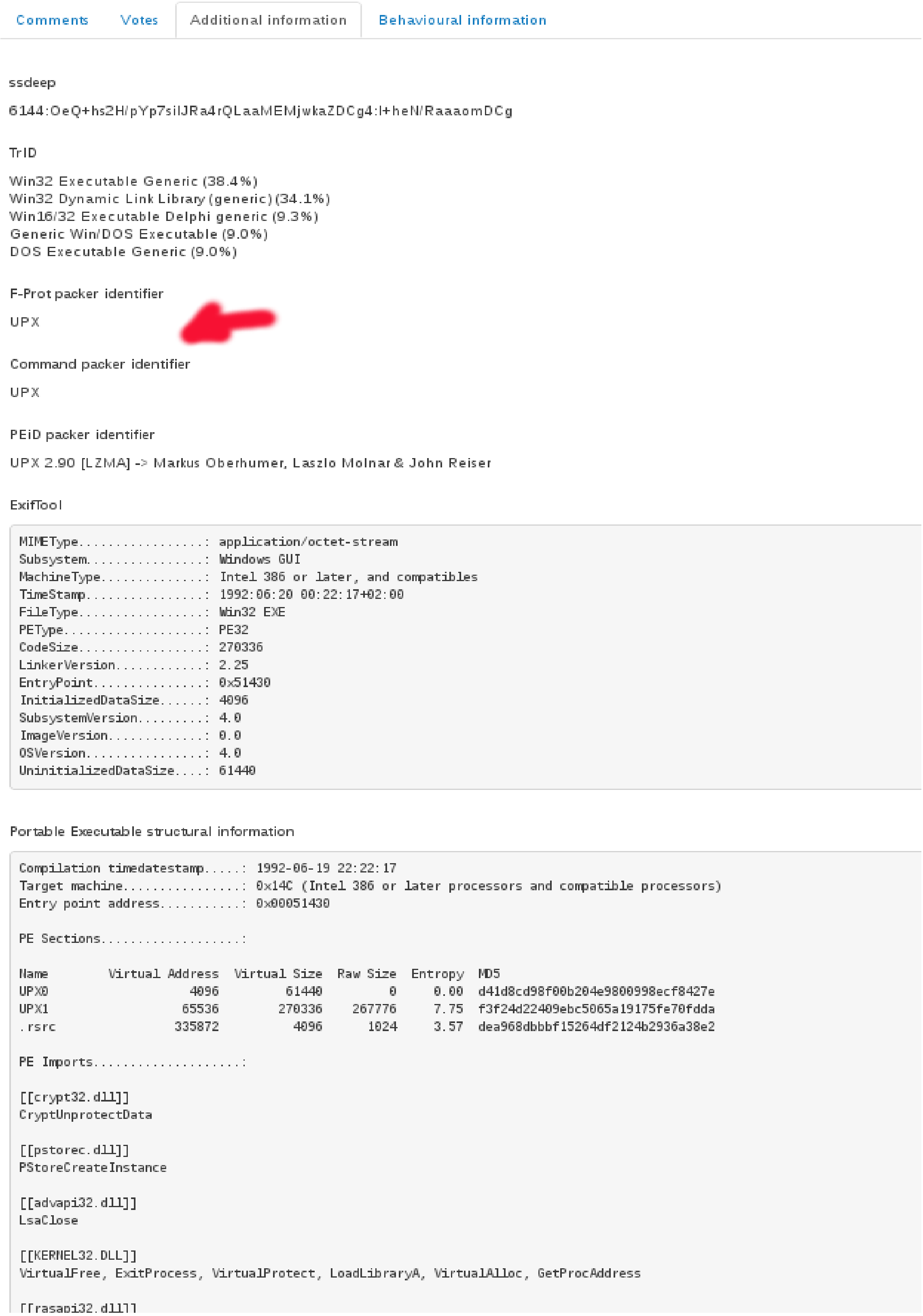


```
Target machine................: 0x14C (Intel 386 or later processors and compatible processors)
Entry point address...........: 0x0000BBCC

PE Sections...................:

Name        Virtual Address  Virtual Size  Raw Size  Entropy  MD5
CODE                   4096         45472     45568     6.41  2e6d43b7785bee730e0396c2de0144c4
DATA                  53248           544      1024     2.76  c71fe50c35c3c6adc124a4768277491c
BSS                   57344          4597         0     0.00  d41d8cd98f00b204e9800998ecf8427e
.idata                65536          3000      3072     4.72  d36776c61c662a6fb7fd62f8b1c382c6
.tls                  69632             8         0     0.00  d41d8cd98f00b204e9800998ecf8427e
.rdata                73728            24       512     0.21  a270a5e1f4f71f9ddb31027f913842a2
.reloc                77824          2668      3072     0.00  d2a70550489de356a2cd6bfc40711204
.rsrc                 81920        228324    228352     7.96  fb5a2781102e6c89054ccbcb4968bef0

PE Imports....................:

[[crypt32.dll]]
CryptUnprotectData

[[pstorec.dll]]
PStoreCreateInstance

[[advapi32.dll]]
RegDeleteKeyA, RegCloseKey, RegQueryValueExA, RegCreateKeyExA, RegCreateKeyA, CryptHashData, ConvertSidToStringSidA, CryptCreateHash, L
ookupAccountNameA, OpenProcessToken, LsaClose, RegOpenKeyExA, LsaOpenPolicy, CryptReleaseContext, CryptAcquireContextA, IsValidSid, Get
UserNameA, CryptDestroyHash, LsaRetrievePrivateData, LsaFreeMemory, CryptGetHashParam, RegSetValueExA, RegEnumValueA, CredEnumerateA

[[KERNEL32.DLL]]
GetLastError, HeapFree, WriteProcessMemory, VirtualAllocEx, lstrlenA, lstrcmpiA, GlobalFree, WaitForSingleObject, GetPrivateProfileIntA
, FreeLibrary, CopyFileA, GetTickCount, VirtualProtect, GetVersionExA, LoadLibraryA, RtlUnwind, GetModuleFileNameA, CreateRemoteThread,
 HeapAlloc, GetCurrentProcess, SizeofResource, GetPrivateProfileStringA, GetFileSize, OpenProcess, LockResource, CreateDirectoryA, Dele
teFileA, UnhandledExceptionFilter, MultiByteToWideChar, ReadProcessMemory, GetCommandLineA, GetProcAddress, GetProcessHeap, CreateMutex
A, GetModuleHandleA, RaiseException, WideCharToMultiByte, GetFileAttributesA, SetFilePointer, ReadFile, WriteFile, FindFirstFileA, GetE
xitCodeThread, HeapReAlloc, FreeResource, SetFileAttributesA, CreateProcessA, LoadResource, VirtualFree, FindClose, TlsGetValue, Sleep,
 TlsSetValue, CreateFileA, ExitProcess, GetCurrentThreadId, FindResourceA, VirtualAlloc, LocalAlloc, CloseHandle

[[rasapi32.dll]]
RasGetEntryDialParamsA, RasEnumEntriesA

[[oleaut32.dll]]
SysReAllocStringLen, SysFreeString, SysAllocStringLen

[[shell32.dll]]
SHGetSpecialFolderPathA

[[ole32.dll]]
StringFromCLSID, CoCreateInstance, CoTaskMemFree, OleInitialize

[[user32.dll]]
GetWindowThreadProcessId, ToAscii, GetKeyboardState, SetWindowsHookExA, DispatchMessageA, CharLowerA, CharNextA, PeekMessageA, wvsprint
fA, TranslateMessage, FindWindowA, CharUpperA

PE Resources..................:

Resource type            Number of resources
RT_RCDATA                3

Resource language        Number of resources
NEUTRAL                  3
```

First seen by VirusTotal

2012-08-28 22:31:50 UTC (18 hours, 59 minutes ago)

Pic 11:virustotal.com detailled analysis[3] come back to the virustotal to analyse the original smss.exe and check the behavioural information



ssdeep

6144:OeQ+hs2H/pYp7silJRa4rQLaaMEMjwkaZDCg4:l+heN/RaaaomDCg

TrID

Win32 Executable Generic (38.4%)
Win32 Dynamic Link Library (generic) (34.1%)
Win16/32 Executable Delphi generic (9.3%)
Generic Win/DOS Executable (9.0%)
DOS Executable Generic (9.0%)

F-Prot packer identifier

UPX

Command packer identifier

UPX

PEiD packer identifier

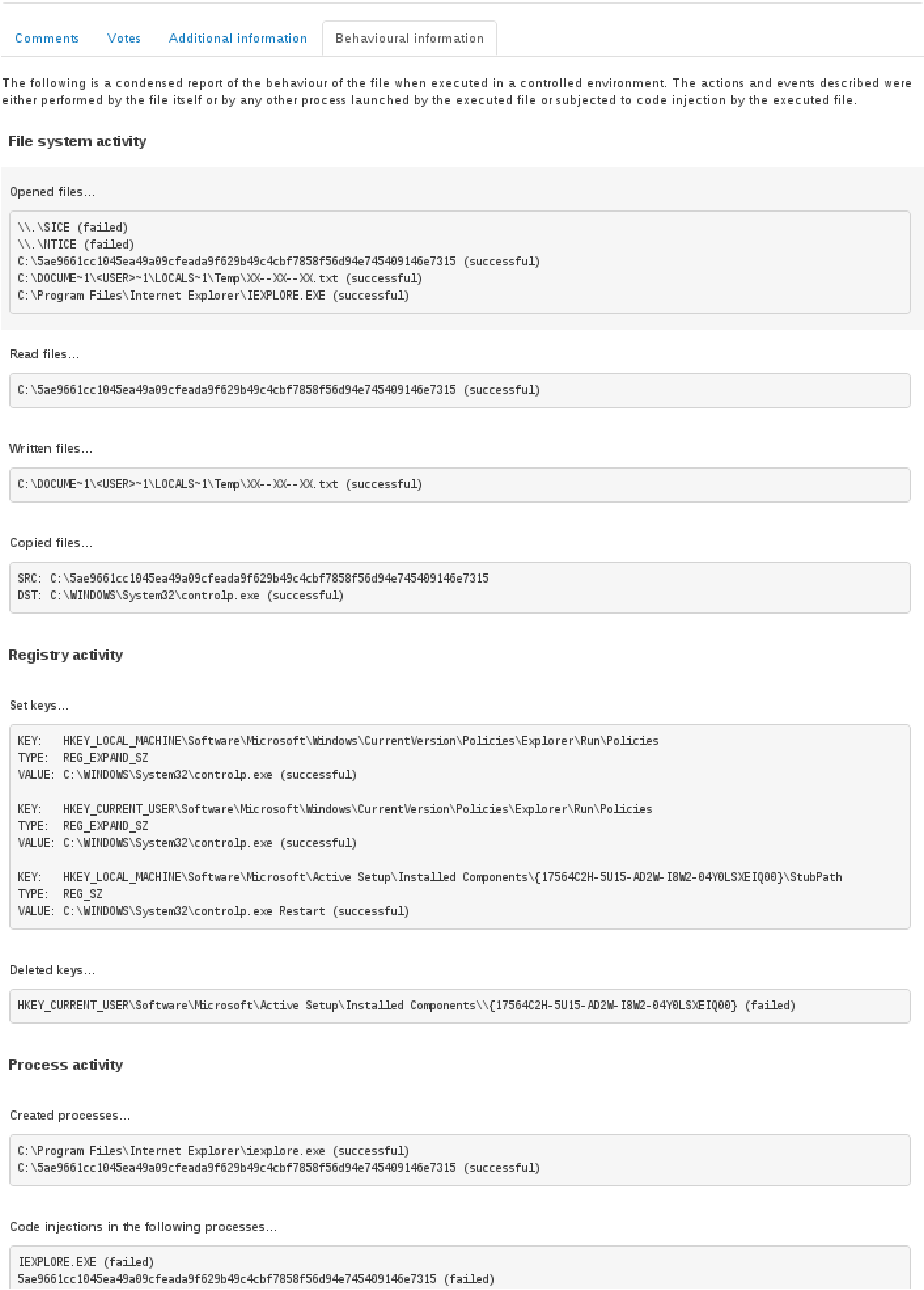
UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser

ExifTool

```
MIMEType.................: application/octet-stream
Subsystem................: Windows GUI
MachineType..............: Intel 386 or later, and compatibles
TimeStamp................: 1992:06:20 00:22:17+02:00
FileType.................: Win32 EXE
PEType...................: PE32
CodeSize.................: 270336
LinkerVersion............: 2.25
EntryPoint...............: 0x51430
InitializedDataSize......: 4096
SubsystemVersion.........: 4.0
ImageVersion.............: 0.0
OSVersion................: 4.0
UninitializedDataSize....: 61440
```

Portable Executable structural information

```
Compilation timedatestamp.....: 1992-06-19 22:22:17
Target machine................: 0x14C (Intel 386 or later processors and compatible processors)
Entry point address...........: 0x00051430

PE Sections...................:

Name        Virtual Address  Virtual Size  Raw Size  Entropy  MD5
UPX0                   4096         61440         0     0.00  d41d8cd98f00b204e9800998ecf8427e
UPX1                  65536        270336    267776     7.75  f3f24d22409ebc5065a19175fe70fdda
.rsrc                335872          4096      1024     3.57  dea968dbbbf15264df2124b2936a38e2

PE Imports....................:

[[crypt32.dll]]
CryptUnprotectData

[[pstorec.dll]]
PStoreCreateInstance

[[advapi32.dll]]
LsaClose

[[KERNEL32.DLL]]
VirtualFree, ExitProcess, VirtualProtect, LoadLibraryA, VirtualAlloc, GetProcAddress

[[rasapi32.dll]]
```



The following is a condensed report of the behaviour of the file when executed in a controlled environment. The actions and events described were either performed by the file itself or by any other process launched by the executed file or subjected to code injection by the executed file.

File system activity

Opened files...

```
\\.\SICE (failed)
\\.\NTICE (failed)
C:\5ae9661cc1045ea49a09cfeada9f629b49c4cbf7858f56d94e745409146e7315 (successful)
C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\XX--XX--XX.txt (successful)
C:\Program Files\Internet Explorer\IEXPLORE.EXE (successful)
```

Read files...

```
C:\5ae9661cc1045ea49a09cfeada9f629b49c4cbf7858f56d94e745409146e7315 (successful)
```

Written files...

```
C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\XX--XX--XX.txt (successful)
```

Copied files...

```
SRC: C:\5ae9661cc1045ea49a09cfeada9f629b49c4cbf7858f56d94e745409146e7315
DST: C:\WINDOWS\System32\controlp.exe (successful)
```

Registry activity

Set keys...

```
KEY:   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Policies
TYPE:  REG_EXPAND_SZ
VALUE: C:\WINDOWS\System32\controlp.exe (successful)

KEY:   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Policies
TYPE:  REG_EXPAND_SZ
VALUE: C:\WINDOWS\System32\controlp.exe (successful)

KEY:   HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\{17564C2H-5U15-AD2W-I8W2-04Y0LSXEIQ00}\StubPath
TYPE:  REG_SZ
VALUE: C:\WINDOWS\System32\controlp.exe Restart (successful)
```

Deleted keys...

```
HKEY_CURRENT_USER\Software\Microsoft\Active Setup\Installed Components\\{17564C2H-5U15-AD2W-I8W2-04Y0LSXEIQ00} (failed)
```

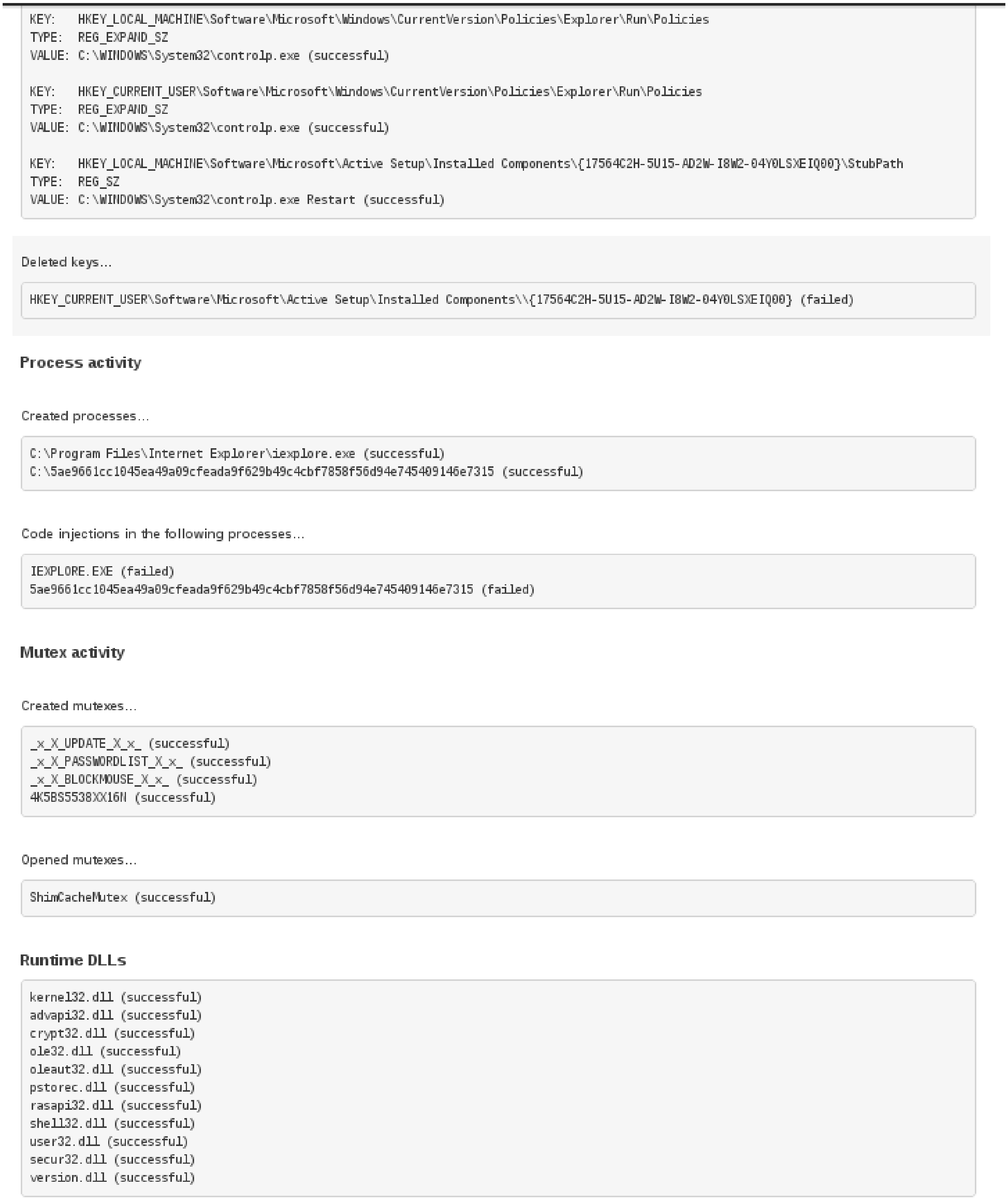
Process activity

Created processes...

```
C:\Program Files\Internet Explorer\iexplore.exe (successful)
C:\5ae9661cc1045ea49a09cfeada9f629b49c4cbf7858f56d94e745409146e7315 (successful)
```

Code injections in the following processes...

```
IEXPLORE.EXE (failed)
5ae9661cc1045ea49a09cfeada9f629b49c4cbf7858f56d94e745409146e7315 (failed)
```



```
KEY:   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Policies
TYPE:  REG_EXPAND_SZ
VALUE: C:\WINDOWS\System32\controlp.exe (successful)

KEY:   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Policies
TYPE:  REG_EXPAND_SZ
VALUE: C:\WINDOWS\System32\controlp.exe (successful)

KEY:   HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\{17564C2H-5U15-AD2W-I8W2-04Y0LSXEIQ00}\StubPath
TYPE:  REG_SZ
VALUE: C:\WINDOWS\System32\controlp.exe Restart (successful)
```

Deleted keys...

```
HKEY_CURRENT_USER\Software\Microsoft\Active Setup\Installed Components\\{17564C2H-5U15-AD2W-I8W2-04Y0LSXEIQ00} (failed)
```

Process activity

Created processes...

```
C:\Program Files\Internet Explorer\iexplore.exe (successful)
C:\5ae9661cc1045ea49a09cfeada9f629b49c4cbf7858f56d94e745409146e7315 (successful)
```

Code injections in the following processes...

```
IEXPLORE.EXE (failed)
5ae9661cc1045ea49a09cfeada9f629b49c4cbf7858f56d94e745409146e7315 (failed)
```

Mutex activity

Created mutexes...

```
_x_X_UPDATE_X_x_ (successful)
_x_X_PASSWORDLIST_X_x_ (successful)
_x_X_BLOCKMOUSE_X_x_ (successful)
4K5BS5538XX16N (successful)
```

Opened mutexes...

```
ShimCacheMutex (successful)
```

Runtime DLLs

```
kernel32.dll (successful)
advapi32.dll (successful)
crypt32.dll (successful)
ole32.dll (successful)
oleaut32.dll (successful)
pstorec.dll (successful)
rasapi32.dll (successful)
shell32.dll (successful)
user32.dll (successful)
secur32.dll (successful)
version.dll (successful)
```

Pic 12,13,14:Analysing the original smss.exe in the pic 12 it's packed,behaviour is analysed in pic 13,,pic 14

Time to show in the virtual machine :) but first :

check the internet conectivity :

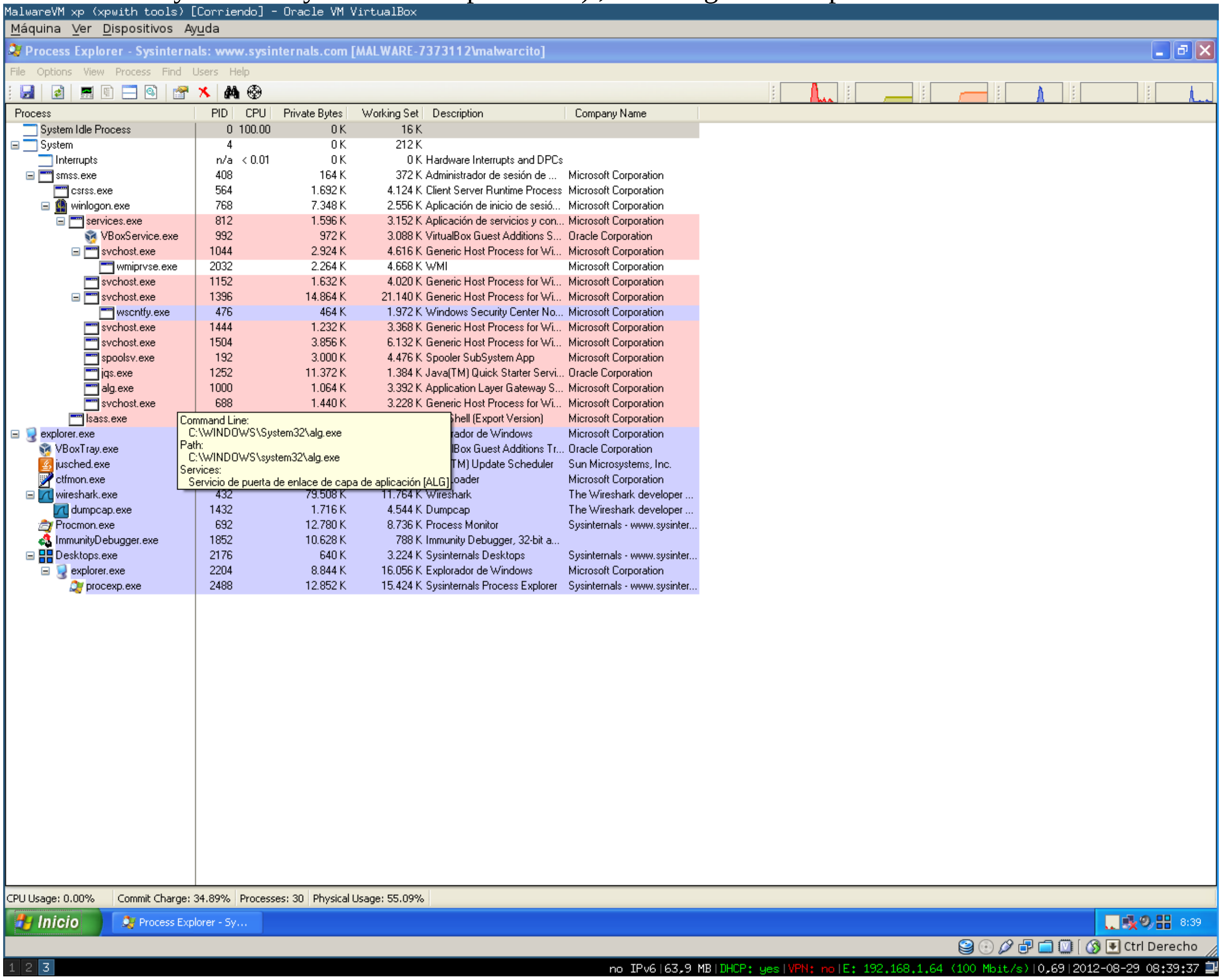
nping google.com or ping google.com

open wireshark for network events.

Open process monitor.

open process explorer,and if you want you could use capturedbat,

And after that you're ready for run the specimen :) ,don't forget the snapshots in the vm.


MalwareVM xp (xpwith tools) [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
Process Explorer - Sysinternals: www.sysinternals.com [MALWARE-7373112\malwarcito]
File Options View Process Find Users Help
Inicio
Process Explorer - Sy...
8:39
Ctrl Derecho
1 2 3

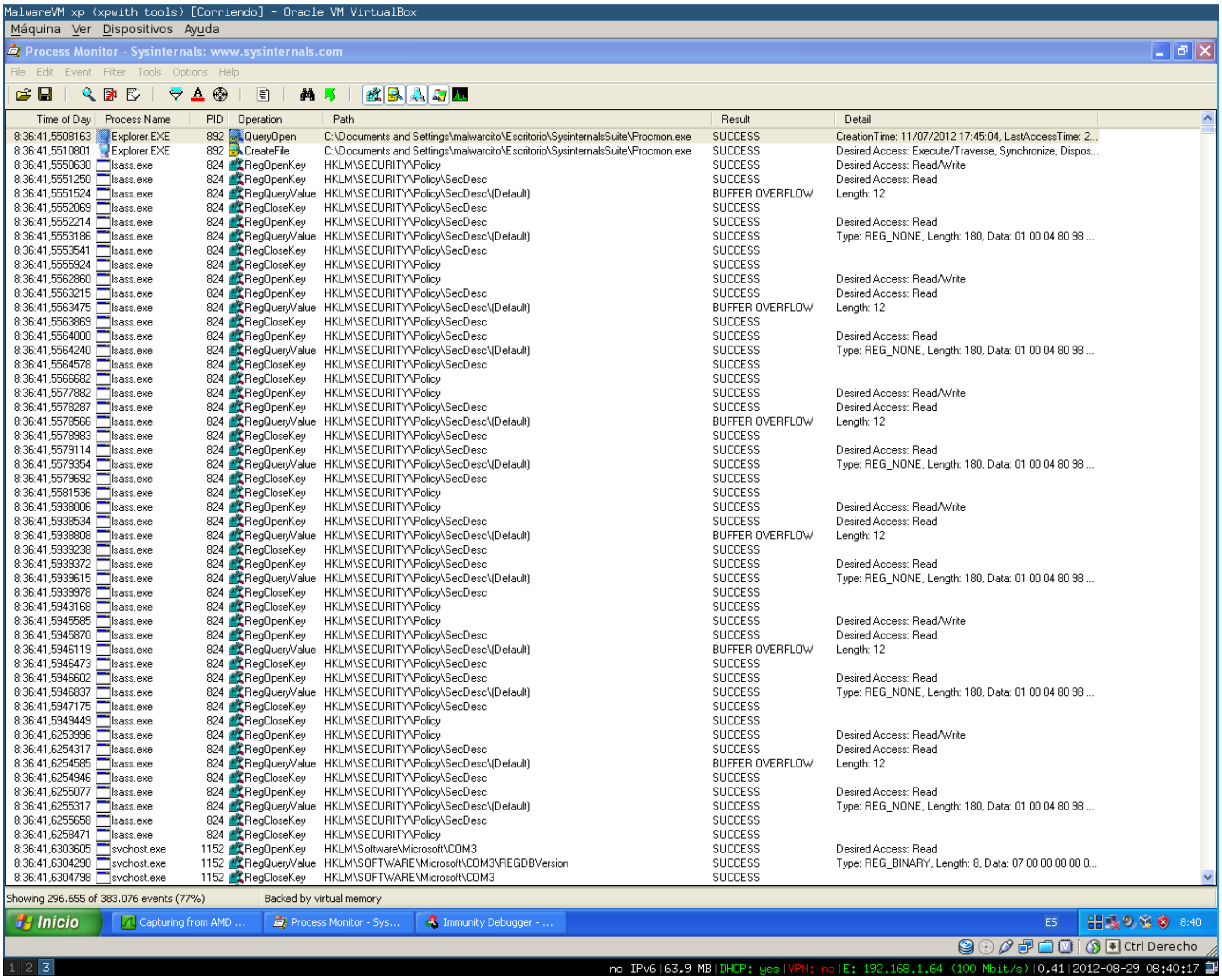
Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	100.00	0 K	16 K		
System	4		0 K	212 K		
Interrupts	n/a	< 0.01	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	408		164 K	372 K	Administrador de sesión de ...	Microsoft Corporation
csrss.exe	564		1.692 K	4.124 K	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	768		7.348 K	2.556 K	Aplicación de inicio de sesió...	Microsoft Corporation
services.exe	812		1.596 K	3.152 K	Aplicación de servicios y con...	Microsoft Corporation
VBoxService.exe	992		972 K	3.088 K	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe	1044		2.924 K	4.616 K	Generic Host Process for Wi...	Microsoft Corporation
wmiprvse.exe	2032		2.264 K	4.668 K	WMI	Microsoft Corporation
svchost.exe	1152		1.632 K	4.020 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1396		14.864 K	21.140 K	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe	476		464 K	1.972 K	Windows Security Center No...	Microsoft Corporation
svchost.exe	1444		1.232 K	3.368 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1504		3.856 K	6.132 K	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe	192		3.000 K	4.476 K	Spooler SubSystem App	Microsoft Corporation
jqs.exe	1252		11.372 K	1.384 K	Java(TM) Quick Starter Servi...	Oracle Corporation
alg.exe	1000		1.064 K	3.392 K	Application Layer Gateway S...	Microsoft Corporation
svchost.exe	688		1.440 K	3.228 K	Generic Host Process for Wi...	Microsoft Corporation
lsass.exe					Shell (Export Version)	Microsoft Corporation
explorer.exe					rador de Windows	Microsoft Corporation
VBoxTray.exe					Box Guest Additions Tr...	Oracle Corporation
jusched.exe					TM) Update Scheduler	Sun Microsystems, Inc.
ctfmon.exe					oader	Microsoft Corporation
wireshark.exe	432		79.508 K	11.764 K	Wireshark	The Wireshark developer ...
dumpcap.exe	1432		1.716 K	4.544 K	Dumpcap	The Wireshark developer ...
Procmon.exe	692		12.780 K	8.736 K	Process Monitor	Sysinternals - www.sysinter...
ImmunityDebugger.exe	1852		10.628 K	788 K	Immunity Debugger, 32-bit a...	
Desktops.exe	2176		640 K	3.224 K	Sysinternals Desktops	Sysinternals - www.sysinter...
explorer.exe	2204		8.844 K	16.056 K	Explorador de Windows	Microsoft Corporation
procexp.exe	2488		12.852 K	15.424 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...

```
Command Line:
  C:\WINDOWS\System32\alg.exe
Path:
  C:\WINDOWS\system32\alg.exe
Services:
  Servicio de puerta de enlace de capa de aplicación [ALG]
```

CPU Usage: 0.00% | Commit Charge: 34.89% | Processes: 30 | Physical Usage: 55.09%

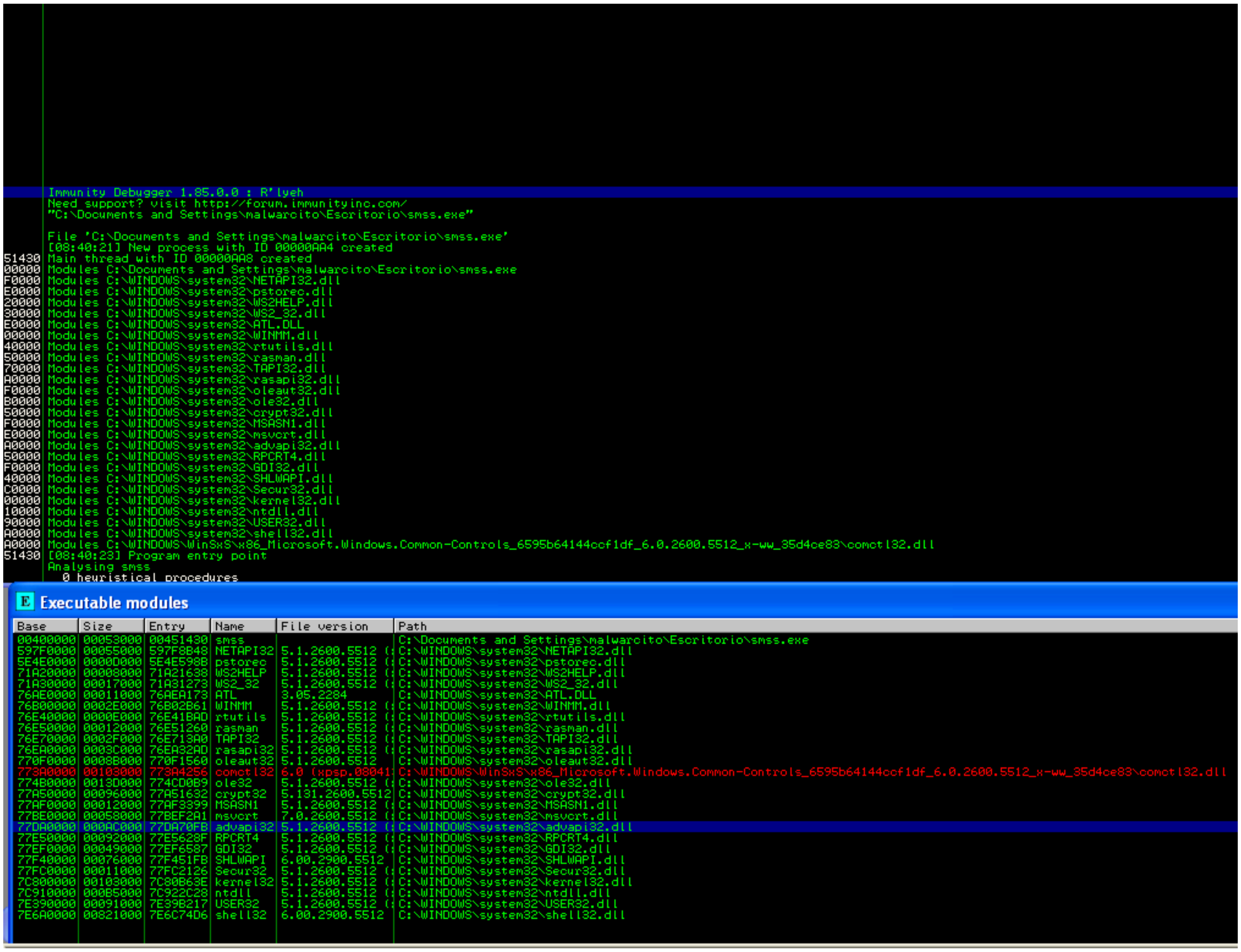
no IPv6 | 63,9 MB | DHCP: yes | VPN: no | E: 192.168.1.64 (100 Mbit/s) | 0,69 | 2012-08-29 08:39:37

Pic 15: process explorer before start the specimen


MalwareVM xp (xpwith tools) [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Inicio
Capturing from AMD ...
Process Monitor - Sys...
Immunity Debugger - ...
ES
8:40
Ctrl Derecho
1 2 3

```
Time of Day       Process Name  PID   Operation      Path                                                                          Result           Detail
8:36:41,5508163   Explorer.EXE  892   QueryOpen      C:\Documents and Settings\malwarcito\Escritorio\SysinternalsSuite\Procmon.exe SUCCESS          CreationTime: 11/07/2012 17:45:04, LastAccessTime: 2...
8:36:41,5510801   Explorer.EXE  892   CreateFile     C:\Documents and Settings\malwarcito\Escritorio\SysinternalsSuite\Procmon.exe SUCCESS          Desired Access: Execute/Traverse, Synchronize, Dispos...
8:36:41,5550630   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy                                                          SUCCESS          Desired Access: Read/Write
8:36:41,5551250   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS          Desired Access: Read
8:36:41,5551524   lsass.exe     824   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                                        BUFFER OVERFLOW  Length: 12
8:36:41,5552069   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS
8:36:41,5552214   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS          Desired Access: Read
8:36:41,5553186   lsass.exe     824   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                                        SUCCESS          Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 ...
8:36:41,5553541   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS
8:36:41,5555924   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy                                                          SUCCESS
8:36:41,5562860   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy                                                          SUCCESS          Desired Access: Read/Write
8:36:41,5563215   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS          Desired Access: Read
8:36:41,5563475   lsass.exe     824   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                                        BUFFER OVERFLOW  Length: 12
8:36:41,5563869   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS
8:36:41,5564000   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS          Desired Access: Read
8:36:41,5564240   lsass.exe     824   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                                        SUCCESS          Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 ...
8:36:41,5564578   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS
8:36:41,5566682   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy                                                          SUCCESS
8:36:41,5577882   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy                                                          SUCCESS          Desired Access: Read/Write
8:36:41,5578287   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS          Desired Access: Read
8:36:41,5578566   lsass.exe     824   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                                        BUFFER OVERFLOW  Length: 12
8:36:41,5578983   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS
8:36:41,5579114   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS          Desired Access: Read
8:36:41,5579354   lsass.exe     824   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                                        SUCCESS          Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 ...
8:36:41,5579692   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS
8:36:41,5581536   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy                                                          SUCCESS
8:36:41,5938006   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy                                                          SUCCESS          Desired Access: Read/Write
8:36:41,5938534   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS          Desired Access: Read
8:36:41,5938808   lsass.exe     824   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                                        BUFFER OVERFLOW  Length: 12
8:36:41,5939238   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS
8:36:41,5939372   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS          Desired Access: Read
8:36:41,5939615   lsass.exe     824   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                                        SUCCESS          Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 ...
8:36:41,5939978   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS
8:36:41,5943168   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy                                                          SUCCESS
8:36:41,5945585   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy                                                          SUCCESS          Desired Access: Read/Write
8:36:41,5945870   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS          Desired Access: Read
8:36:41,5946119   lsass.exe     824   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                                        BUFFER OVERFLOW  Length: 12
8:36:41,5946473   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS
8:36:41,5946602   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS          Desired Access: Read
8:36:41,5946837   lsass.exe     824   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                                        SUCCESS          Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 ...
8:36:41,5947175   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS
8:36:41,5949449   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy                                                          SUCCESS
8:36:41,6253996   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy                                                          SUCCESS          Desired Access: Read/Write
8:36:41,6254317   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS          Desired Access: Read
8:36:41,6254585   lsass.exe     824   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                                        BUFFER OVERFLOW  Length: 12
8:36:41,6254946   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS
8:36:41,6255077   lsass.exe     824   RegOpenKey     HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS          Desired Access: Read
8:36:41,6255317   lsass.exe     824   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                                        SUCCESS          Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 ...
8:36:41,6255658   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy\SecDesc                                                  SUCCESS
8:36:41,6258471   lsass.exe     824   RegCloseKey    HKLM\SECURITY\Policy                                                          SUCCESS
8:36:41,6303605   svchost.exe   1152  RegOpenKey     HKLM\Software\Microsoft\COM3                                                  SUCCESS          Desired Access: Read
8:36:41,6304290   svchost.exe   1152  RegQueryValue  HKLM\SOFTWARE\Microsoft\COM3\REGDBVersion                                     SUCCESS          Type: REG_BINARY, Length: 8, Data: 07 00 00 00 00 0...
8:36:41,6304798   svchost.exe   1152  RegCloseKey    HKLM\SOFTWARE\Microsoft\COM3                                                  SUCCESS

Showing 296.655 of 383.076 events (77%)    Backed by virtual memory

no IPv6|63,9 MB|DHCP: yes|VPN: no|E: 192.168.1.64 (100 Mbit/s)|0,41|2012-08-29 08:40:17
```

Pic 16: process monitor before start the binary specimen

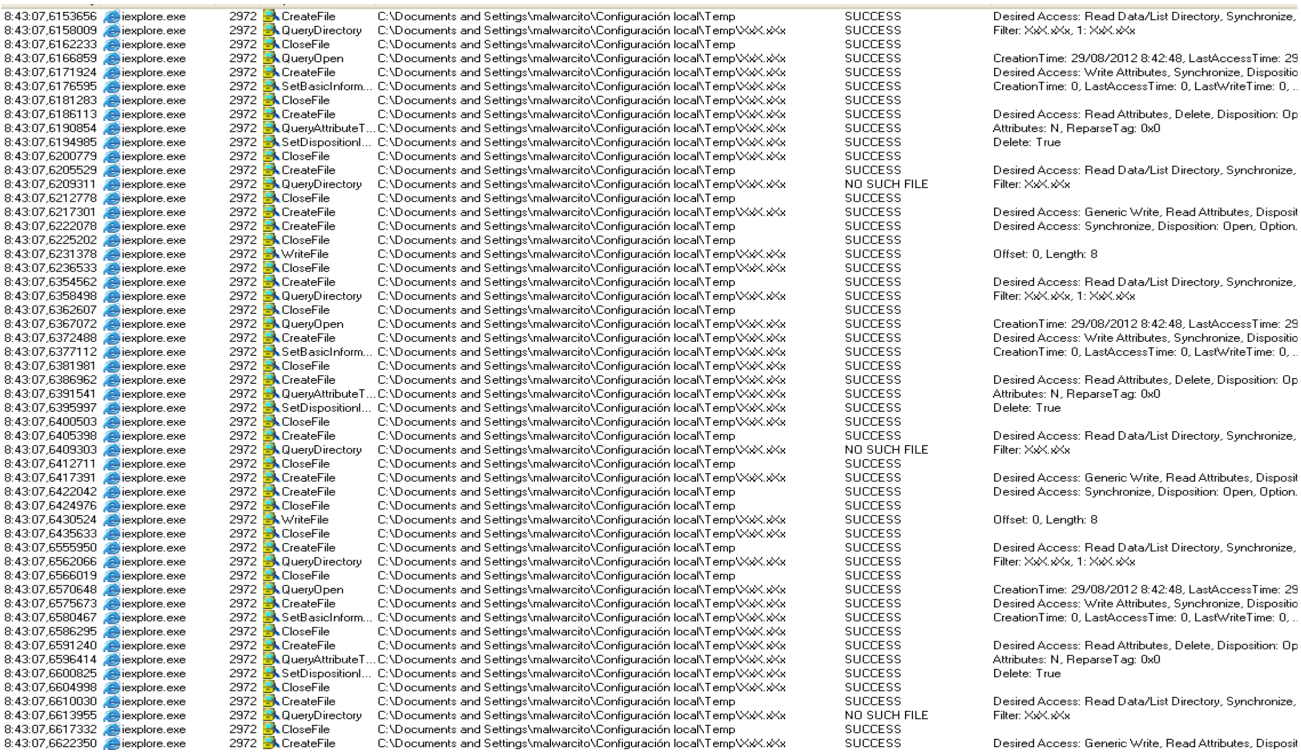


```
      Immunity Debugger 1.85.0.0 : R'lyeh
      Need support? visit http://forum.immunityinc.com/
      "C:\Documents and Settings\malwarcito\Escritorio\smss.exe"

      File 'C:\Documents and Settings\malwarcito\Escritorio\smss.exe'
      [08:40:21] New process with ID 00000AA4 created
51430 Main thread with ID 00000AA8 created
00000 Modules C:\Documents and Settings\malwarcito\Escritorio\smss.exe
F0000 Modules C:\WINDOWS\system32\NETAPI32.dll
E0000 Modules C:\WINDOWS\system32\pstorec.dll
20000 Modules C:\WINDOWS\system32\WS2HELP.dll
30000 Modules C:\WINDOWS\system32\WS2_32.dll
E0000 Modules C:\WINDOWS\system32\ATL.DLL
00000 Modules C:\WINDOWS\system32\WINMM.dll
40000 Modules C:\WINDOWS\system32\rtutils.dll
50000 Modules C:\WINDOWS\system32\rasman.dll
70000 Modules C:\WINDOWS\system32\TAPI32.dll
A0000 Modules C:\WINDOWS\system32\rasapi32.dll
F0000 Modules C:\WINDOWS\system32\oleaut32.dll
B0000 Modules C:\WINDOWS\system32\ole32.dll
50000 Modules C:\WINDOWS\system32\crypt32.dll
F0000 Modules C:\WINDOWS\system32\MSASN1.dll
E0000 Modules C:\WINDOWS\system32\msvcrt.dll
A0000 Modules C:\WINDOWS\system32\advapi32.dll
50000 Modules C:\WINDOWS\system32\RPCRT4.dll
F0000 Modules C:\WINDOWS\system32\GDI32.dll
40000 Modules C:\WINDOWS\system32\SHLWAPI.dll
C0000 Modules C:\WINDOWS\system32\Secur32.dll
00000 Modules C:\WINDOWS\system32\kernel32.dll
10000 Modules C:\WINDOWS\system32\ntdll.dll
90000 Modules C:\WINDOWS\system32\USER32.dll
A0000 Modules C:\WINDOWS\system32\shell32.dll
A0000 Modules C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
51430 [08:40:23] Program entry point
      Analysing smss
        0 heuristical procedures
```

Executable modules

```
Base     Size     Entry    Name     File version     Path
00400000 00053000 00451430 smss                      C:\Documents and Settings\malwarcito\Escritorio\smss.exe
597F0000 00055000 597F8B48 NETAPI32 5.1.2600.5512 (  C:\WINDOWS\system32\NETAPI32.dll
5E4E0000 0000D000 5E4E598B pstorec  5.1.2600.5512 (  C:\WINDOWS\system32\pstorec.dll
71A20000 00008000 71A21638 WS2HELP  5.1.2600.5512 (  C:\WINDOWS\system32\WS2HELP.dll
71A30000 00017000 71A31273 WS2_32   5.1.2600.5512 (  C:\WINDOWS\system32\WS2_32.dll
76AE0000 00011000 76AEA173 ATL      3.05.2284        C:\WINDOWS\system32\ATL.DLL
76B00000 0002E000 76B02B61 WINMM    5.1.2600.5512 (  C:\WINDOWS\system32\WINMM.dll
76E40000 0000E000 76E41BAD rtutils  5.1.2600.5512 (  C:\WINDOWS\system32\rtutils.dll
76E50000 00012000 76E51260 rasman   5.1.2600.5512 (  C:\WINDOWS\system32\rasman.dll
76E70000 0002F000 76E713A0 TAPI32   5.1.2600.5512 (  C:\WINDOWS\system32\TAPI32.dll
76EA0000 0003C000 76EA32AD rasapi32 5.1.2600.5512 (  C:\WINDOWS\system32\rasapi32.dll
770F0000 0008B000 770F1560 oleaut32 5.1.2600.5512    C:\WINDOWS\system32\oleaut32.dll
773A0000 00103000 773A4256 comctl32 6.0 (xpsp.08041  C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
774B0000 0013D000 774CD0B9 ole32    5.1.2600.5512 (  C:\WINDOWS\system32\ole32.dll
77A50000 00096000 77A51632 crypt32  5.131.2600.5512  C:\WINDOWS\system32\crypt32.dll
77AF0000 00012000 77AF3399 MSASN1   5.1.2600.5512 (  C:\WINDOWS\system32\MSASN1.dll
77BE0000 00058000 77BEF2A1 msvcrt   7.0.2600.5512 (  C:\WINDOWS\system32\msvcrt.dll
77DA0000 000AC000 77DA70FB advapi32 5.1.2600.5512 (  C:\WINDOWS\system32\advapi32.dll
77E50000 00092000 77E5628F RPCRT4   5.1.2600.5512 (  C:\WINDOWS\system32\RPCRT4.dll
77EF0000 00049000 77EF6587 GDI32    5.1.2600.5512 (  C:\WINDOWS\system32\GDI32.dll
77F40000 00076000 77F451FB SHLWAPI  6.00.2900.5512   C:\WINDOWS\system32\SHLWAPI.dll
77FC0000 00011000 77FC2126 Secur32  5.1.2600.5512 (  C:\WINDOWS\system32\Secur32.dll
7C800000 00103000 7C80B63E kernel32 5.1.2600.5512 (  C:\WINDOWS\system32\kernel32.dll
7C910000 000B5000 7C922C28 ntdll    5.1.2600.5512 (  C:\WINDOWS\system32\ntdll.dll
7E390000 00091000 7E39B217 USER32   5.1.2600.5512 (  C:\WINDOWS\system32\USER32.dll
7E6A0000 00821000 7E6C74D6 shell32  6.00.2900.5512   C:\WINDOWS\system32\shell32.dll
```

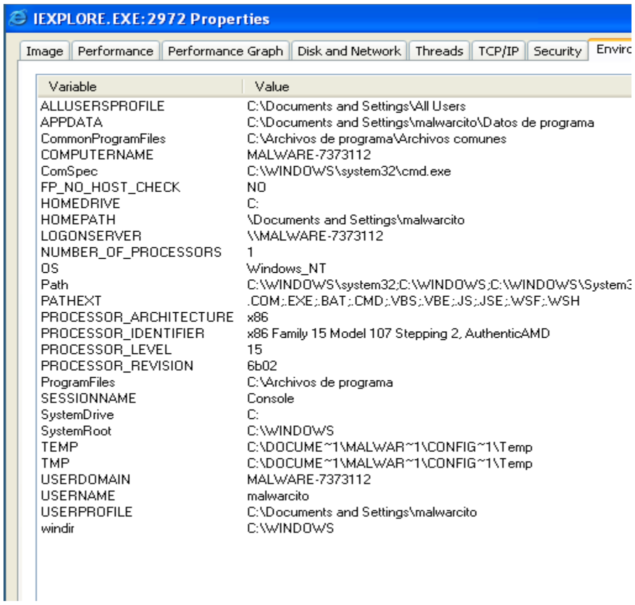
Pic 17: Loading immunity debugger smss.exe after run the specimen in the vm ,i've noticed some actions,internet explorer is open,it creates new files in the temporal folder. %temp%



```
8:43:07,6153656  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS        Desired Access: Read Data/List Directory, Synchronize,
8:43:07,6158009  iexplore.exe  2972  QueryDirectory      C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Filter: XxX.xXx, 1: XxX.xXx
8:43:07,6162233  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS
8:43:07,6166859  iexplore.exe  2972  QueryOpen           C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        CreationTime: 29/08/2012 8:42:48, LastAccessTime: 29
8:43:07,6171924  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Desired Access: Write Attributes, Synchronize, Dispositio
8:43:07,6176595  iexplore.exe  2972  SetBasicInform...   C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        CreationTime: 0, LastAccessTime: 0, LastWriteTime: 0, ..
8:43:07,6181283  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS
8:43:07,6186113  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Desired Access: Read Attributes, Delete, Disposition: Op
8:43:07,6190854  iexplore.exe  2972  QueryAttributeT...  C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Attributes: N, ReparseTag: 0x0
8:43:07,6194985  iexplore.exe  2972  SetDispositionI...  C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Delete: True
8:43:07,6200779  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS
8:43:07,6205529  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS        Desired Access: Read Data/List Directory, Synchronize,
8:43:07,6209311  iexplore.exe  2972  QueryDirectory      C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  NO SUCH FILE   Filter: XxX.xXx
8:43:07,6212778  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS
8:43:07,6217301  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Desired Access: Generic Write, Read Attributes, Disposit
8:43:07,6222078  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS        Desired Access: Synchronize, Disposition: Open, Option.
8:43:07,6225202  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS
8:43:07,6231378  iexplore.exe  2972  WriteFile           C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Offset: 0, Length: 8
8:43:07,6236533  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS
8:43:07,6354562  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS        Desired Access: Read Data/List Directory, Synchronize,
8:43:07,6358498  iexplore.exe  2972  QueryDirectory      C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Filter: XxX.xXx, 1: XxX.xXx
8:43:07,6362607  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS
8:43:07,6367072  iexplore.exe  2972  QueryOpen           C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        CreationTime: 29/08/2012 8:42:48, LastAccessTime: 29
8:43:07,6372488  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Desired Access: Write Attributes, Synchronize, Dispositio
8:43:07,6377112  iexplore.exe  2972  SetBasicInform...   C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        CreationTime: 0, LastAccessTime: 0, LastWriteTime: 0, ..
8:43:07,6381981  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS
8:43:07,6386962  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Desired Access: Read Attributes, Delete, Disposition: Op
8:43:07,6391541  iexplore.exe  2972  QueryAttributeT...  C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Attributes: N, ReparseTag: 0x0
8:43:07,6395997  iexplore.exe  2972  SetDispositionI...  C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Delete: True
8:43:07,6400503  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS
8:43:07,6405398  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS        Desired Access: Read Data/List Directory, Synchronize,
8:43:07,6409303  iexplore.exe  2972  QueryDirectory      C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  NO SUCH FILE   Filter: XxX.xXx
8:43:07,6412711  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS
8:43:07,6417391  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Desired Access: Generic Write, Read Attributes, Disposit
8:43:07,6422042  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS        Desired Access: Synchronize, Disposition: Open, Option.
8:43:07,6424976  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS
8:43:07,6430524  iexplore.exe  2972  WriteFile           C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Offset: 0, Length: 8
8:43:07,6435633  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS
8:43:07,6555950  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS        Desired Access: Read Data/List Directory, Synchronize,
8:43:07,6562066  iexplore.exe  2972  QueryDirectory      C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Filter: XxX.xXx, 1: XxX.xXx
8:43:07,6566019  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS
8:43:07,6570648  iexplore.exe  2972  QueryOpen           C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        CreationTime: 29/08/2012 8:42:48, LastAccessTime: 29
8:43:07,6575673  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Desired Access: Write Attributes, Synchronize, Dispositio
8:43:07,6580467  iexplore.exe  2972  SetBasicInform...   C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        CreationTime: 0, LastAccessTime: 0, LastWriteTime: 0, ..
8:43:07,6586295  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS
8:43:07,6591240  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Desired Access: Read Attributes, Delete, Disposition: Op
8:43:07,6596414  iexplore.exe  2972  QueryAttributeT...  C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Attributes: N, ReparseTag: 0x0
8:43:07,6600825  iexplore.exe  2972  SetDispositionI...  C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Delete: True
8:43:07,6604998  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS
8:43:07,6610030  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS        Desired Access: Read Data/List Directory, Synchronize,
8:43:07,6613955  iexplore.exe  2972  QueryDirectory      C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  NO SUCH FILE   Filter: XxX.xXx
8:43:07,6617332  iexplore.exe  2972  CloseFile           C:\Documents and Settings\malwarcito\Configuración local\Temp          SUCCESS
8:43:07,6622350  iexplore.exe  2972  CreateFile          C:\Documents and Settings\malwarcito\Configuración local\Temp\XxX.xXx  SUCCESS        Desired Access: Generic Write, Read Attributes, Disposit
```

Pic 18: Analysing process monitor changes made by itself (smss.exe)

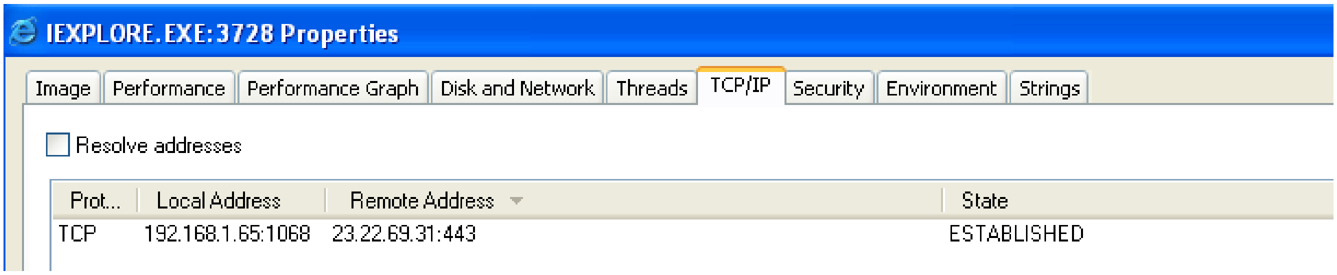
in the other hand i check the process explorer,and the new IEXPLORE.EXE launched by smss.exe :



Variable	Value
ALLUSERSPROFILE	C:\Documents and Settings\All Users
APPDATA	C:\Documents and Settings\malwarcito\Datos de programa
CommonProgramFiles	C:\Archivos de programa\Archivos comunes
COMPUTERNAME	MALWARE-7373112
ComSpec	C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK	NO
HOMEDRIVE	C:
HOMEPATH	\Documents and Settings\malwarcito
LOGONSERVER	\\MALWARE-7373112
NUMBER_OF_PROCESSORS	1
OS	Windows_NT
Path	C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System3
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE	x86
PROCESSOR_IDENTIFIER	x86 Family 15 Model 107 Stepping 2, AuthenticAMD
PROCESSOR_LEVEL	15
PROCESSOR_REVISION	6b02
ProgramFiles	C:\Archivos de programa
SESSIONNAME	Console
SystemDrive	C:
SystemRoot	C:\WINDOWS
TEMP	C:\DOCUME~1\MALWAR~1\CONFIG~1\Temp
TMP	C:\DOCUME~1\MALWAR~1\CONFIG~1\Temp
USERDOMAIN	MALWARE-7373112
USERNAME	malwarcito
USERPROFILE	C:\Documents and Settings\malwarcito
windir	C:\WINDOWS

Pic 19:IEXPLORE.EXE process launched by smss.exe . Properties

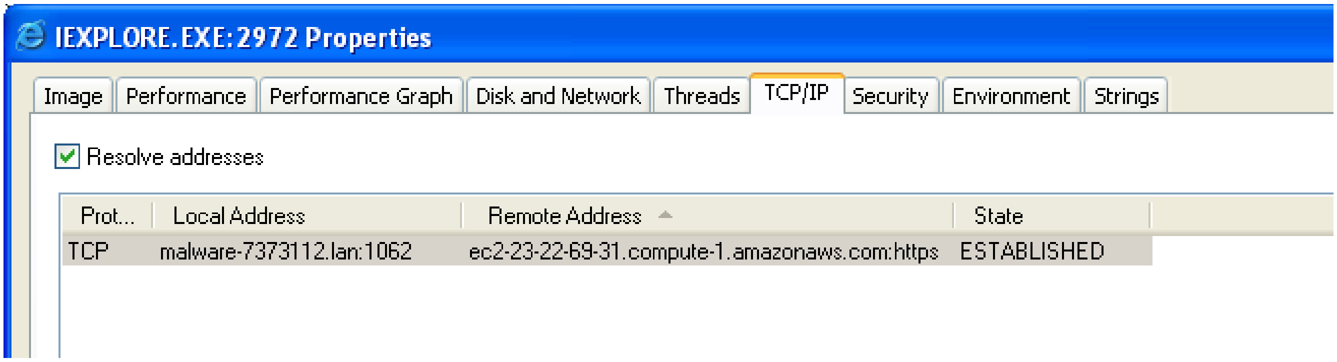
Besides of that the network activity :



□ Resolve addresses

Prot...	Local Address	Remote Address	State
TCP	192.168.1.65:1068	23.22.69.31:443	ESTABLISHED

Pic 20:Network activity without resolve the address



☑ Resolve addresses

Prot...	Local Address	Remote Address	State
TCP	malware-7373112.lan:1062	ec2-23-22-69-31.compute-1.amazonaws.com:https	ESTABLISHED

Pic 21:Network activity without resolving the address,wow amazon ec2

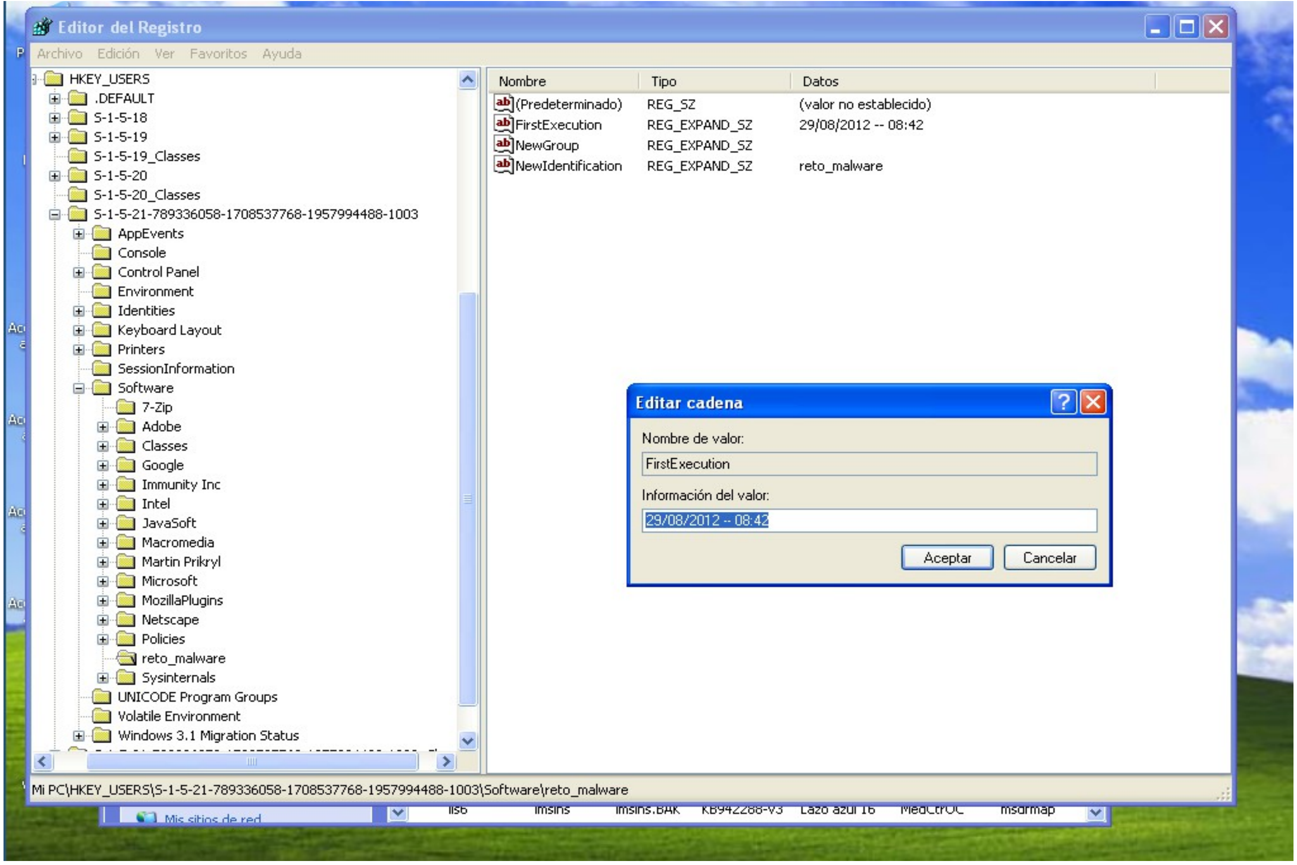
Until now we have a little bit information ,maybe we can know about process and files changed in the registry,using regshot,or other tools.

```
----------------------------------
Keys added:149
---------------------------------- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\Policies:
"C:\WINDOWS\System32\controlp.exe"



----------------------------------
Values added:712
----------------------------------

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\Policies:
"C:\WINDOWS\System32\controlp.exe"
```

regshot is great but i decided to probe anubis an online tool,it can gives me a nice report is much more clean than regshot [4],but it depend of the situation,is more human readable :P.

```
[=========================================================================]
   3.a) IEXPLORE.EXE - Registry Activities
[===========================================================================
============]
[-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
   Registry Keys Created:
[-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
      Key: [ HKU\S-1-5-21-842925246-1425521274-308236825-500\SOFTWARE\reto_malware ]
      Key: [ HKLM\SYSTEM\CurrentControlSet\Control\MediaResources\msvideo ]
```

checking this keys using regedit :



Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
FirstExecution	REG_EXPAND_SZ	29/08/2012 -- 08:42
NewGroup	REG_EXPAND_SZ	
NewIdentification	REG_EXPAND_SZ	reto_malware

Nombre de valor: FirstExecution

Información del valor: 29/08/2012 -- 08:42

Mi PC\HKEY_USERS\S-1-5-21-789336058-1708537768-1957994488-1003\Software\reto_malware

Pic 22:Checking regedit keys

```
[-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
   Files Modified:
[-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
      File Name: [ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\XX--XX--XX.txt ]
      File Name: [ C:\WINDOWS\System32\controlp.exe ]

[-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
   Files Deleted:
[-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
      File Name: [ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\UuU.uUu ]
      File Name: [ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\XX--XX--XX.txt ] //una hora !
      File Name: [ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\XxX.xXx ]
```

```
        File Name: [ C:\smss.exe ]

[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
    Files Created:
[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
        File Name: [ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\UuU.uUu ]
        File Name: [ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\XxX.xXx ]
        File Name: [ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\teste.vbs ]
        File Name: [ C:\Documents and Settings\Administrator\Application Data\cglogs.dat ]

[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
    Files Read:
[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
        File Name: [ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\XX--XX--XX.txt ]
        File Name: [ C:\Documents and Settings\Administrator\Application Data\cglogs.dat ]
        File Name: [ C:\Documents and Settings\Administrator\My Documents\desktop.ini ]
        File Name: [ C:\Documents and Settings\All Users\Documents\desktop.ini ]
        File Name: [ C:\WINDOWS\Registration\R000000000000b.clb ]
        File Name: [ C:\WINDOWS\System32\controlp.exe ]
        File Name: [ C:\WINDOWS\system32\cscript.exe ]
        File Name: [ PIPE\lsarpc ]
        File Name: [ PIPE\wkssvc ]


[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
    Files Modified:
[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
        File Name: [ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\UuU.uUu ] this files are created by controlp.exe
        File Name: [ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\XxX.xXx ] it contains the hour time...
        File Name: [ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\teste.vbs ]  it is called by cscript.exe !
        File Name: [ C:\Documents and Settings\Administrator\Application Data\cglogs.dat ]
        File Name: [ Ip ]
        File Name: [ MountPointManager ]
        File Name: [ PIPE\lsarpc ]
        File Name: [ PIPE\wkssvc ]
        File Name: [ \Device\Afd\Endpoint ]
        File Name: [ \Device\Ip ]
        File Name: [ \Device\RasAcd ]
        File Name: [ \Device\Tcp ]
```

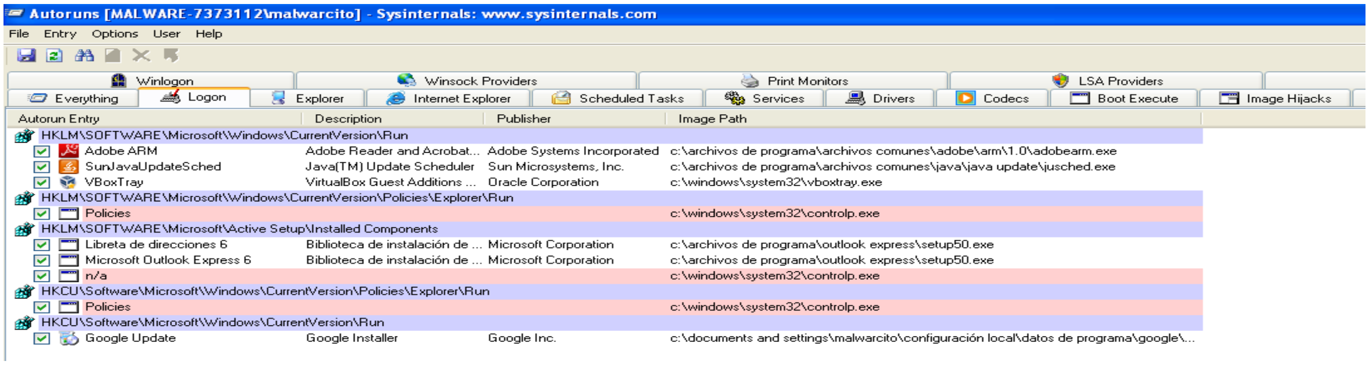
cscript interpret the vbs files in this case teste.vbs

```
[=================================================================================]
    5.b) cscript.exe - File Activities
[=================================================================================]
[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
    Files Read:
[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
        File Name: [ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\teste.vbs ]
        File Name: [ C:\Documents and Settings\Administrator\Local Settings\Temp\teste.vbs ]
        File Name: [ C:\WINDOWS\Registration\R000000000000b.clb ]
        File Name: [ C:\WINDOWS\system32\cscript.exe ]
        File Name: [ C:\WINDOWS\system32\rsaenh.dll ]
        File Name: [ PIPE\lsarpc ]

[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
    Files Modified:
[=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=]
```

```
File Name: [ PIPE\lsarpc ]
```

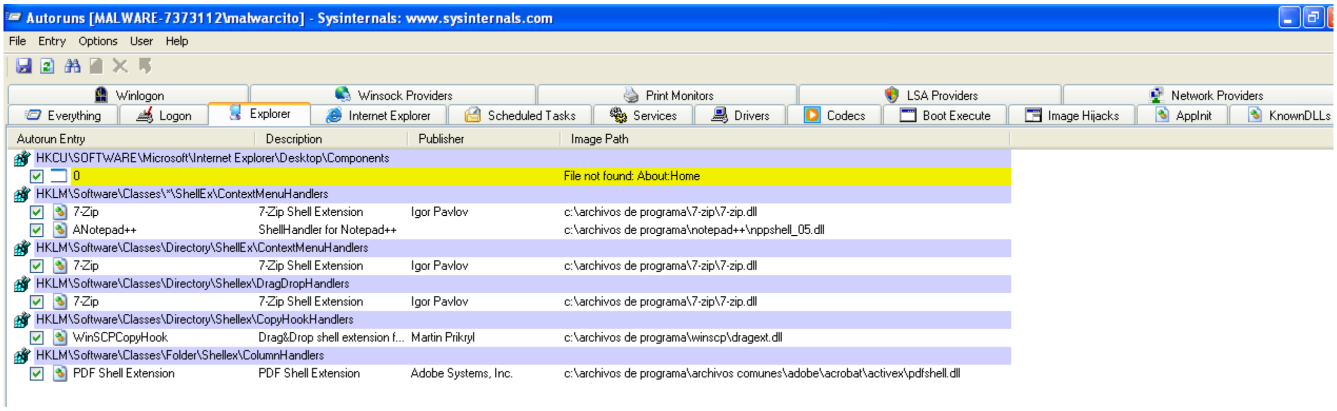
Administrator account is not visible in the system for check this we need to log out and press ctrl + alt + sup and write Administrator in the user account. When you go through this way you won't find the File Name: [C:\Documents and Settings\Administrator\Local Settings\Temp\teste.vbs]...mmm strange ..

I'd like to check the autoruns,the process IEXPLORE creates new keys



Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ Adobe ARM	Adobe Reader and Acrobat...	Adobe Systems Incorporated	c:\archivos de programa\archivos comunes\adobe\arm\1.0\adobearm.exe
☑ SunJavaUpdateSched	Java(TM) Update Scheduler	Sun Microsystems, Inc.	c:\archivos de programa\archivos comunes\java\java update\jusched.exe
☑ VBoxTray	VirtualBox Guest Additions ...	Oracle Corporation	c:\windows\system32\vboxtray.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run			
☑ Policies			c:\windows\system32\controlp.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
☑ Libreta de direcciones 6	Biblioteca de instalación de ...	Microsoft Corporation	c:\archivos de programa\outlook express\setup50.exe
☑ Microsoft Outlook Express 6	Biblioteca de instalación de ...	Microsoft Corporation	c:\archivos de programa\outlook express\setup50.exe
☑ n/a			c:\windows\system32\controlp.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run			
☑ Policies			c:\windows\system32\controlp.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run			
☑ Google Update	Google Installer	Google Inc.	c:\documents and settings\malwarcito\configuración local\datos de programa\google\...

Pic 23:changes in registry



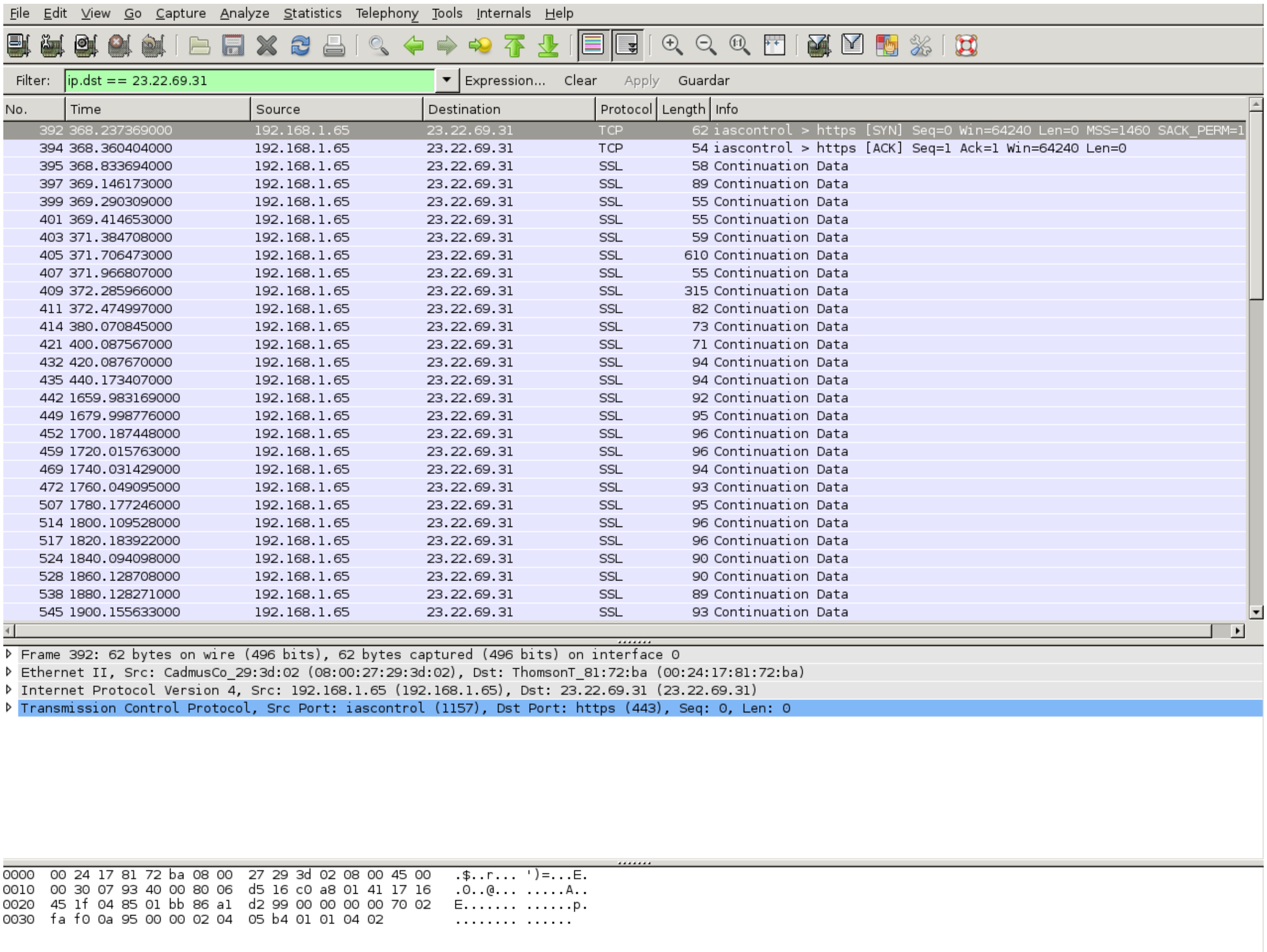
Autorun Entry	Description	Publisher	Image Path
HKCU\SOFTWARE\Microsoft\Internet Explorer\Desktop\Components			
☑ 0			File not found: About:Home
HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers			
☑ 7-Zip	7-Zip Shell Extension	Igor Pavlov	c:\archivos de programa\7-zip\7-zip.dll
☑ ANotepad++	ShellHandler for Notepad++		c:\archivos de programa\notepad++\nppshell_05.dll
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers			
☑ 7-Zip	7-Zip Shell Extension	Igor Pavlov	c:\archivos de programa\7-zip\7-zip.dll
HKLM\Software\Classes\Directory\Shellex\DragDropHandlers			
☑ 7-Zip	7-Zip Shell Extension	Igor Pavlov	c:\archivos de programa\7-zip\7-zip.dll
HKLM\Software\Classes\Directory\Shellex\CopyHookHandlers			
☑ WinSCPCopyHook	Drag&Drop shell extension f...	Martin Prikryl	c:\archivos de programa\winscp\dragext.dll
HKLM\Software\Classes\Folder\Shellex\ColumnHandlers			
☑ PDF Shell Extension	PDF Shell Extension	Adobe Systems, Inc.	c:\archivos de programa\archivos comunes\adobe\acrobat\activex\pdfshell.dll

Pic 24:changes made in internet explorer

at this point we can conclude :

Whe you run smss.exe it creates a new process and inject inside IEXPLORE,it has the capacibilities to create files in tmp folder,also it creates a network conection with 23.22.69.31 in port 443,using ssl for conection,also download files like controlp.exe that generates a file again in %tmp% with the hour note that we can't see the folder [C:\WINDOWS\system32\ ] we need to write absolute path,and off course controlp.exe you can't see it,you need to open a cmd.

The network activity for this specimen is doing a conection with 23.22.69.31 in port 443 i did a quick look up using the filter : ip.dst == 23.22.69.31 as you can see the most packets are under ssl .


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Guardar

Filter: ip.dst == 23.22.69.31

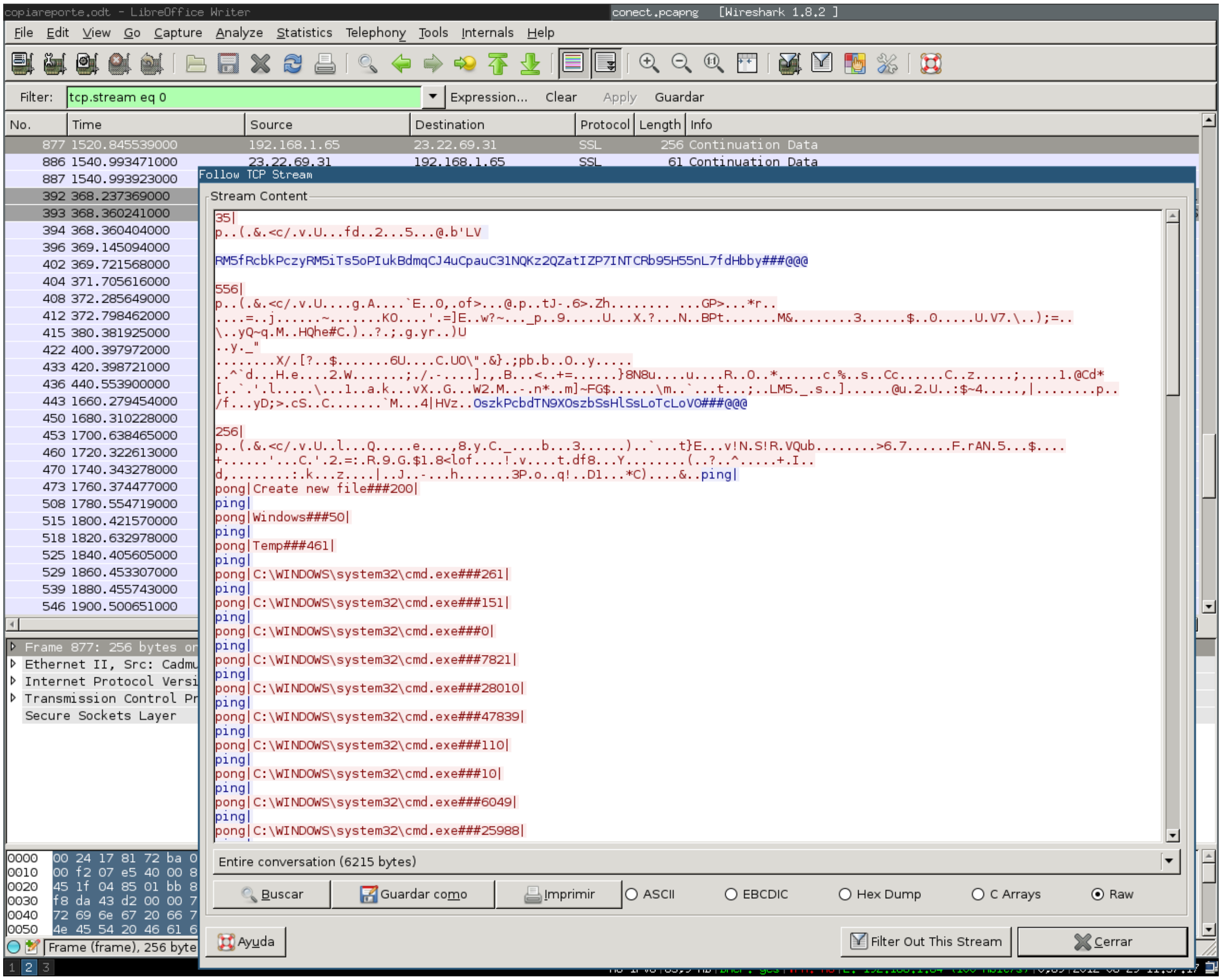
```
No.  Time             Source        Destination  Protocol Length Info
 392 368.237369000    192.168.1.65  23.22.69.31  TCP        62 iascontrol > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 394 368.360404000    192.168.1.65  23.22.69.31  TCP        54 iascontrol > https [ACK] Seq=1 Ack=1 Win=64240 Len=0
 395 368.833694000    192.168.1.65  23.22.69.31  SSL        58 Continuation Data
 397 369.146173000    192.168.1.65  23.22.69.31  SSL        89 Continuation Data
 399 369.290309000    192.168.1.65  23.22.69.31  SSL        55 Continuation Data
 401 369.414653000    192.168.1.65  23.22.69.31  SSL        55 Continuation Data
 403 371.384708000    192.168.1.65  23.22.69.31  SSL        59 Continuation Data
 405 371.706473000    192.168.1.65  23.22.69.31  SSL       610 Continuation Data
 407 371.966807000    192.168.1.65  23.22.69.31  SSL        55 Continuation Data
 409 372.285966000    192.168.1.65  23.22.69.31  SSL       315 Continuation Data
 411 372.474997000    192.168.1.65  23.22.69.31  SSL        82 Continuation Data
 414 380.070845000    192.168.1.65  23.22.69.31  SSL        73 Continuation Data
 421 400.087567000    192.168.1.65  23.22.69.31  SSL        71 Continuation Data
 432 420.087670000    192.168.1.65  23.22.69.31  SSL        94 Continuation Data
 435 440.173407000    192.168.1.65  23.22.69.31  SSL        94 Continuation Data
 442 1659.983169000   192.168.1.65  23.22.69.31  SSL        92 Continuation Data
 449 1679.998776000   192.168.1.65  23.22.69.31  SSL        95 Continuation Data
 452 1700.187448000   192.168.1.65  23.22.69.31  SSL        96 Continuation Data
 459 1720.015763000   192.168.1.65  23.22.69.31  SSL        96 Continuation Data
 469 1740.031429000   192.168.1.65  23.22.69.31  SSL        94 Continuation Data
 472 1760.049095000   192.168.1.65  23.22.69.31  SSL        93 Continuation Data
 507 1780.177246000   192.168.1.65  23.22.69.31  SSL        95 Continuation Data
 514 1800.109528000   192.168.1.65  23.22.69.31  SSL        96 Continuation Data
 517 1820.183922000   192.168.1.65  23.22.69.31  SSL        96 Continuation Data
 524 1840.094098000   192.168.1.65  23.22.69.31  SSL        90 Continuation Data
 528 1860.128708000   192.168.1.65  23.22.69.31  SSL        90 Continuation Data
 538 1880.128271000   192.168.1.65  23.22.69.31  SSL        89 Continuation Data
 545 1900.155633000   192.168.1.65  23.22.69.31  SSL        93 Continuation Data
```

```
Frame 392: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: CadmusCo_29:3d:02 (08:00:27:29:3d:02), Dst: ThomsonT_81:72:ba (00:24:17:81:72:ba)
Internet Protocol Version 4, Src: 192.168.1.65 (192.168.1.65), Dst: 23.22.69.31 (23.22.69.31)
Transmission Control Protocol, Src Port: iascontrol (1157), Dst Port: https (443), Seq: 0, Len: 0
```

```
0000  00 24 17 81 72 ba 08 00  27 29 3d 02 08 00 45 00   .$..r... ')=...E.
0010  00 30 07 93 40 00 80 06  d5 16 c0 a8 01 41 17 16   .0..@... .....A..
0020  45 1f 04 85 01 bb 86 a1  d2 99 00 00 00 00 70 02   E....... ......p.
0030  fa f0 0a 95 00 00 02 04  05 b4 01 01 04 02         ........ ......
```

Pic 25:Tracking the source 23.22.69.31

But what we can see in the follow tcp stream ?


copiareporte.odt - LibreOffice Writer
conect.pcapng [Wireshark 1.8.2]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Guardar
Follow TCP Stream
Entire conversation (6215 bytes)
Buscar
Guardar como
Imprimir
○ ASCII
○ EBCDIC
○ Hex Dump
○ C Arrays
● Raw
Ayuda
Filter Out This Stream
Cerrar

Filter: tcp.stream eq 0

```
No.  Time             Source          Destination     Protocol Length Info
 877 1520.845539000   192.168.1.65    23.22.69.31     SSL         256 Continuation Data
 886 1540.993471000   23.22.69.31     192.168.1.65    SSL          61 Continuation Data
 887 1540.993923000
 392 368.237369000
 393 368.360241000
 394 368.360404000
 396 369.145094000
 402 369.721568000
 404 371.705616000
 408 372.285649000
 412 372.798462000
 415 380.381925000
 422 400.397972000
 433 420.398721000
 436 440.553900000
 443 1660.279454000
 450 1680.310228000
 453 1700.638465000
 460 1720.322613000
 470 1740.343278000
 473 1760.374477000
 508 1780.554719000
 515 1800.421570000
 518 1820.632978000
 525 1840.405605000
 529 1860.453307000
 539 1880.455743000
 546 1900.500651000
```

```
Frame 877: 256 bytes or
Ethernet II, Src: Cadmu
Internet Protocol Versi
Transmission Control Pr
Secure Sockets Layer
```

```
0000  00 24 17 81 72 ba 0
0010  00 f2 07 e5 40 00 8
0020  45 1f 04 85 01 bb 8
0030  f8 da 43 d2 00 00 7
0040  72 69 6e 67 20 66 7
0050  4e 45 54 20 46 61 6
```

Frame (frame), 256 byte

Stream Content

```
35|
p..(.&.<c/.v.U...fd..2...5...@.b'LV

RM5fRcbkPczyRM5iTs5oPIukBdmqCJ4uCpauC31NQKz2QZatIZP7INTCRb95H55nL7fdHbby###@@@

556|
p..(.&.<c/.v.U....g.A....`E..O,.of>...@.p..tJ-.6>.Zh........ ...GP>...*r..
....=..j......~.......KO....'.=]E..w?~..._p..9.....U...X.?...N..BPt.......M&........3......$..O.....U.V7.\..);=..
\..yQ~q.M..HQhe#C.)..?.;.g.yr..)U
..y._"
........X/.[?..$.......6U....C.UO\".&}.;pb.b..O..y.....
..^`d...H.e....2.W.......;./.-....].,.B...<..+=......}8N8u....u....R..O..*......c.%..s..Cc......C..z.....;.....1.@Cd*
[..`.'.l.....\...1..a.k...vX..G...W2.M..-.n*..m]~FG$......\m..`...t...;..LM5._.s..]......@u.2.U..:$~4.....,|........p..
/f...yD;>.cS..C.......`M...4|HVz..OszkPcbdTN9XOszbSsHlSsLoTcLoVO###@@@

256|
p..(.&.<c/.v.U..l...Q.....e....,8.y.C._....b...3......)..`...t}E...v!N.S!R.VQub........>6.7......F.rAN.5...$....
+......'...C.'.2.=:.R.9.G.$1.8<lof....!.v....t.df8...Y........(..?..^.....+.I..
d,........:.k...z....|..J..-...h.......3P.o..q!..D1...*C)....&..ping|
pong|Create new file###200|
ping|
pong|Windows###50|
ping|
pong|Temp###461|
ping|
pong|C:\WINDOWS\system32\cmd.exe###261|
ping|
pong|C:\WINDOWS\system32\cmd.exe###151|
ping|
pong|C:\WINDOWS\system32\cmd.exe###0|
ping|
pong|C:\WINDOWS\system32\cmd.exe###7821|
ping|
pong|C:\WINDOWS\system32\cmd.exe###28010|
ping|
pong|C:\WINDOWS\system32\cmd.exe###47839|
ping|
pong|C:\WINDOWS\system32\cmd.exe###110|
ping|
pong|C:\WINDOWS\system32\cmd.exe###10|
ping|
pong|C:\WINDOWS\system32\cmd.exe###6049|
ping|
pong|C:\WINDOWS\system32\cmd.exe###25988|
```

Pic 25:Tracking the source 23.22.69.31 follow tcp stream ping pong... XD

wow they're using ssl but what happend if i use my favorite tool to check the services in the server?

```
hector@Osiris:~$ sudo proxychains nmap -sS -sV -T4 -A 23.22.69.31

Starting Nmap 6.00 ( http://nmap.org ) at 2012-08-29 11:42 COT
Nmap scan report for ec2-23-22-69-31.compute-1.amazonaws.com (23.22.69.31)
Host is up (0.12s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd 0.9.41 beta
443/tcp  open  spy-net       Spy-Net or CyberGate backdoor (**BACKDOOR**)
3389/tcp open  ms-wbt-server Microsoft Terminal Service

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista
OS CPE: cpe:/o:microsoft:windows_vista::sp2
OS details: Microsoft Windows Vista SP2
Network Distance: 14 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   62.28 ms  …..........................
2   38.65 ms  …..........................
3   47.15 ms  …..........................
4   40.74 ms  …..........................
5   39.75 ms  …..........................
6   101.80 ms xe-0-1-0.mia10.ip4.tinet.net
7   129.31 ms xe-10-1-0.was14.ip4.tinet.net
8   127.75 ms vadata-gw.ip4.tinet.net
9   129.32 ms …........................
10  126.67 ms …...........................
11  122.88 ms 216.182.224.27
12  .125.13 ms …......................
14  122.19 ms ec2-23-22-69-31.compute-1.amazonaws.com (23.22.69.31)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 93.08 seconds
```

mmmm we have this situation,searching in the web about spy-net the most popular site for rats and similar tools in spanish :
http://troyanosyvirus.com.ar/2008/09/spy-net-rat-01.html

Now we could do some cool sutff with this level of knowledge,in fact we could run a nessus season and use metasploit,but for this purpouse is for my educational and learning process in malware analysis.

Now let me continue with the Second specimen in other moment winlogon.exe,it seems more dificult because we need to use the dynamic code analysis while it runs ,so lets do it later.

Sec-track.org

References :

[1]http://sourceforge.net/projects/regshot/
[2]https://upx.sourceforget.net
[3]peframe analysis tool code.google.com
[4]http://anubis.iseclab.org/?action=result&task_id=14d6c1eb13443bdc4b9884489aacd29d2&format=txt

If you've any question , contact details :

@c1b3rh4ck

c1b3rh4ck@gmail.com

irc.freenode.org #social-engineer,backtrack-es,pulpa

Useful Resources :

1.http://blogs.technet.com/b/markrussinovich/ Mark Russinovich blog
2.http://technet.microsoft.com/en-us/sysinternals/gg618529.aspx
3.http://technet.microsoft.com/en-us/sysinternals/gg618529.aspx
4.http://www.karmany.net/index.php/ingenieria-inversa/