T-ZINE

Trojan Magazine

BY ANTRAX

ANTRAX@E-R00T.NET

ANALISIS DE MALWARES

Existen distintos tipos de Softwares para la identificación de archivos infectados, y no solo programas, sino también webs dedicadas a la exanimación de dichos archivos.

WEBS DE ANALISIS:

Una de esas webs es: http://www.cwsandbox.org/?page=submit&action=verify

Esta Web pide un correo (Obviamente el nuestro) ya que envía los resultados del análisis por mail.

RESPUESTA AL MAIL:

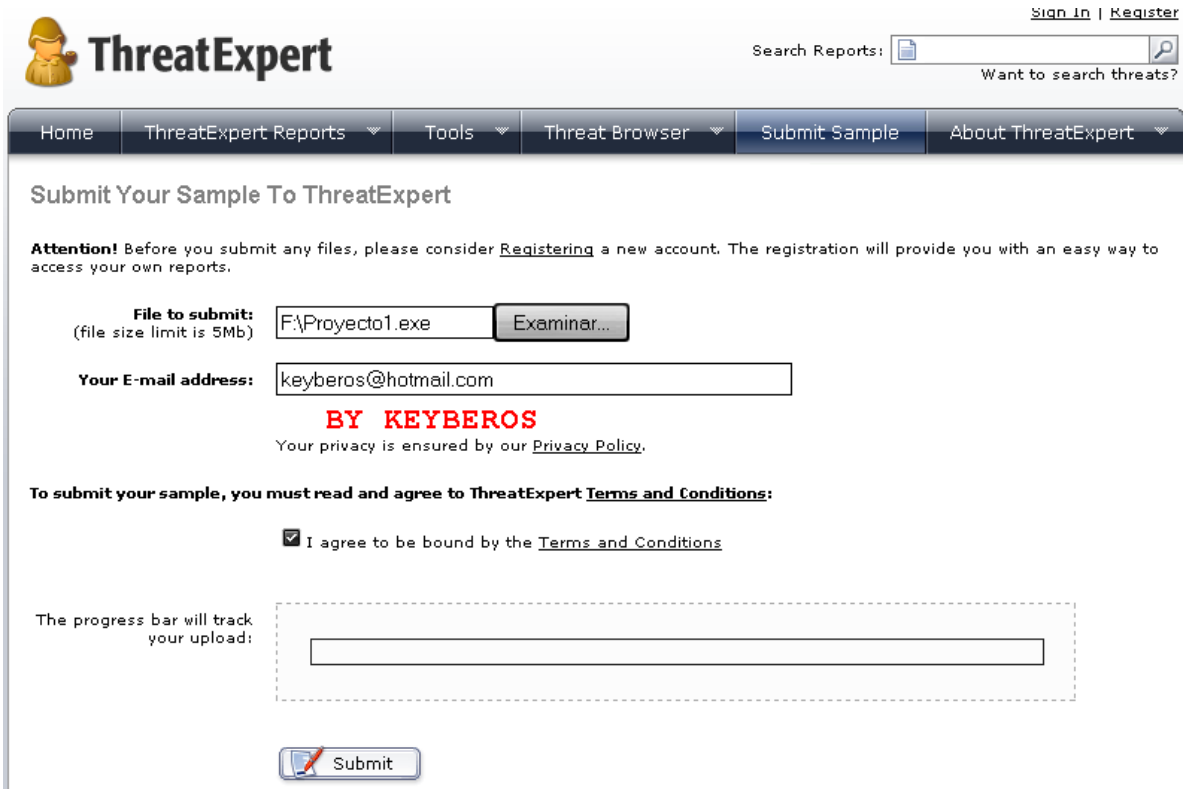
```
Submitted file: Proyecto1.exe
Analysis ID: 1041772
Sample ID: 730031
Submission ID: 424556
Your comment:
Analysis result: Processed


Your submitted sample has been successfully analyzed.
You can find the report at https://cwsandbox.org/?page=samdet&id=730031&password=cgykr.

----------
This analysis was created by CWSandbox (c) CWSE GmbH / Sunbelt Software
```

BY KEYBEROS

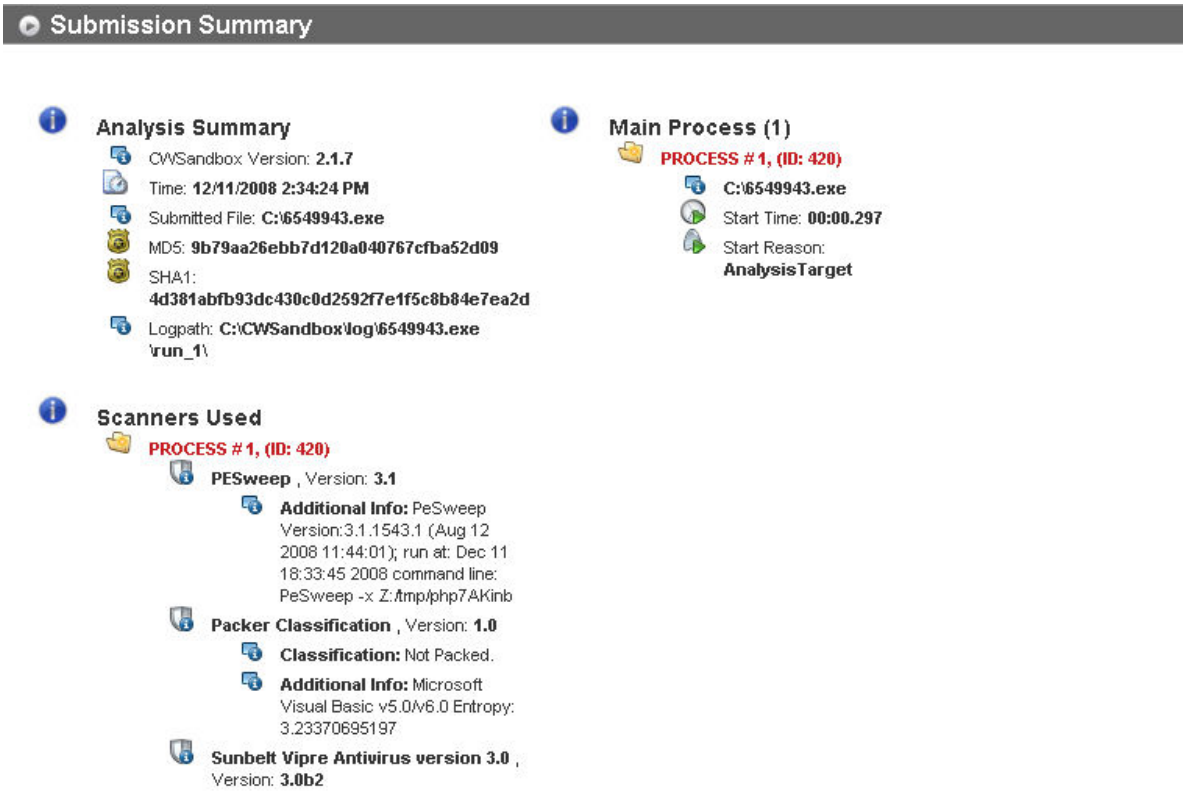
Otras de las Webs es: http://www.threatexpert.com/submit.aspx



Es muy similar a la anterior, solamente que dice un poco mas de información detallada del archivo examinado.

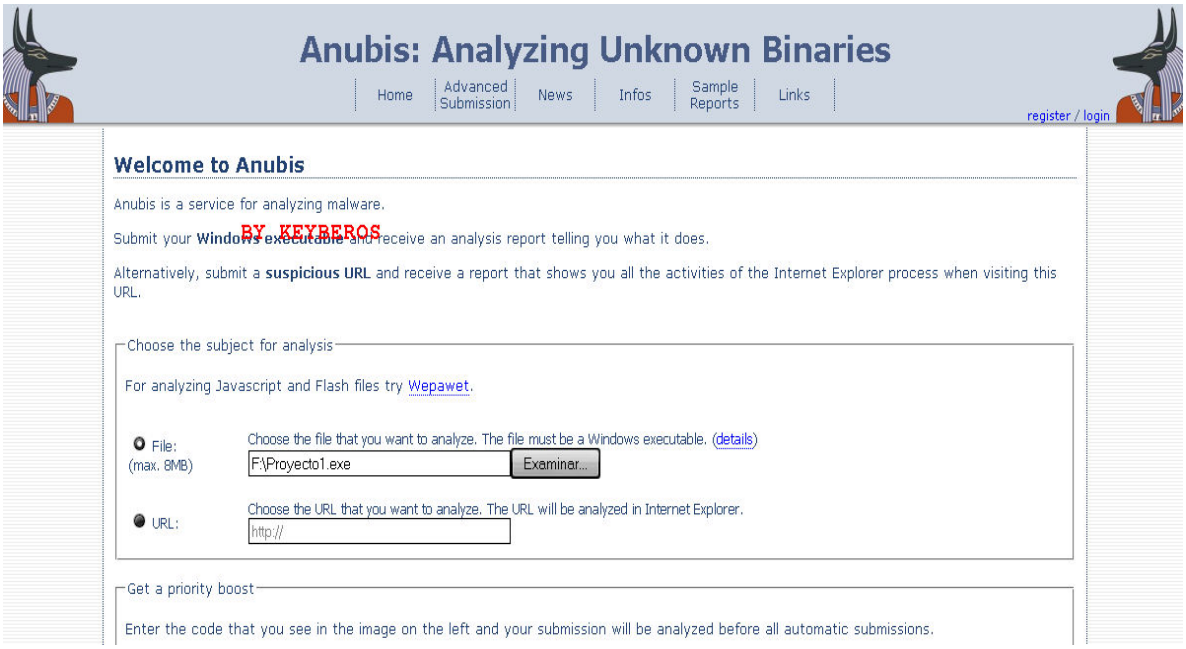
Otra Web: http://research.sunbelt-software.com/Submit.aspx

Esta web cómodamente dice hasta con que empaquetador fue empaquetado y compilado el archivo.



Obviamente que también nos dice si se ejecuta algún archivo o proceso, o si hace algún tipo de modificación

Últimamente tenemos a la mas conocida: http://analysis.seclab.tuwien.ac.at/



Analysis Report for Proyecto1.exe

Comment on this report

Summary:

Description	BY KEYBEROS	Risk
Performs Registry Activities: The executable reads and modifies register values. It also creates and monitors register keys.		

Table of Contents

expand all collapse all
General information
sample.exe

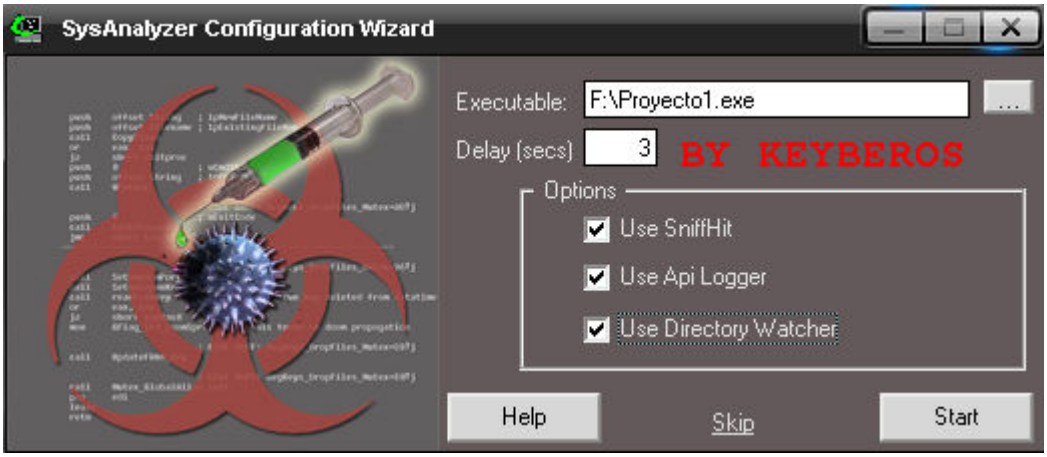
1. General Information

- Information about Anubis' invocation	
Time needed:	37 s
Report created:	01/13/09, 23:08:11 UTC
Termination reason:	All tracked processes have exited
Program version:	1.67.0

Sin duda una de las mejores, examen completo del archivo. Es una de las más utilizadas en todos lados a la hora de examinar un archivo.

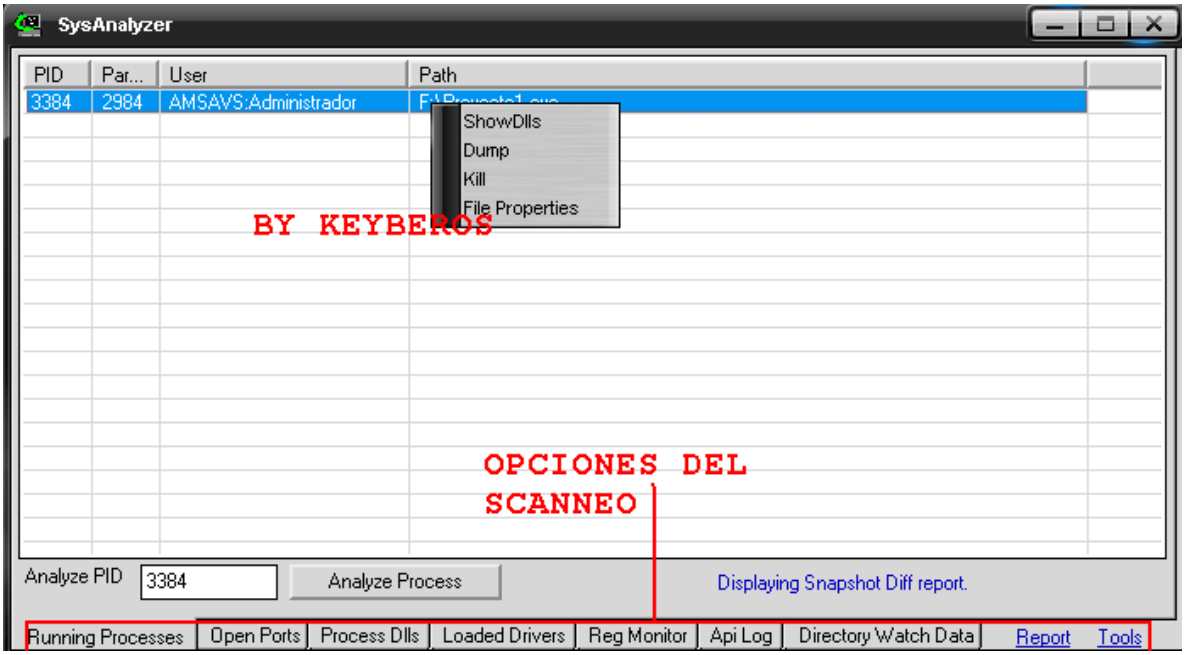
Como aclare al principio, no solo hay webs, sino también programas que pueden ser buscados en www.google.com o para más información y comentar dudas de los mismos, pueden ingresar a www.e-r00t.net o a www.indetectables.net o en el foro de donde lo descargaste.

El primer programa que evaluaremos será el: SysAnalizer



El SysAnalizer es un programa que nos dice los cambio que ocasiona el archivo sospechoso en la PC, Sniffea conexiones entrantes, cambios en el equipo, procesos, y seguimiento de Apis.

Al ejecutarlo, se nos abrirá una ventana como lo siguiente:

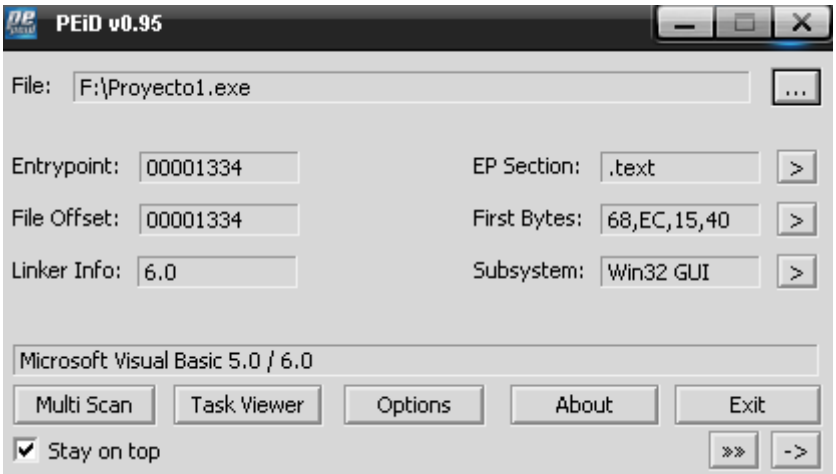


Como podemos ver tenemos muchas opciones abajo como remarca el recuadro rojo.

En cada una de esas pestañas, podremos ver distintos tipos de logs informativos del programa que estamos examinando.

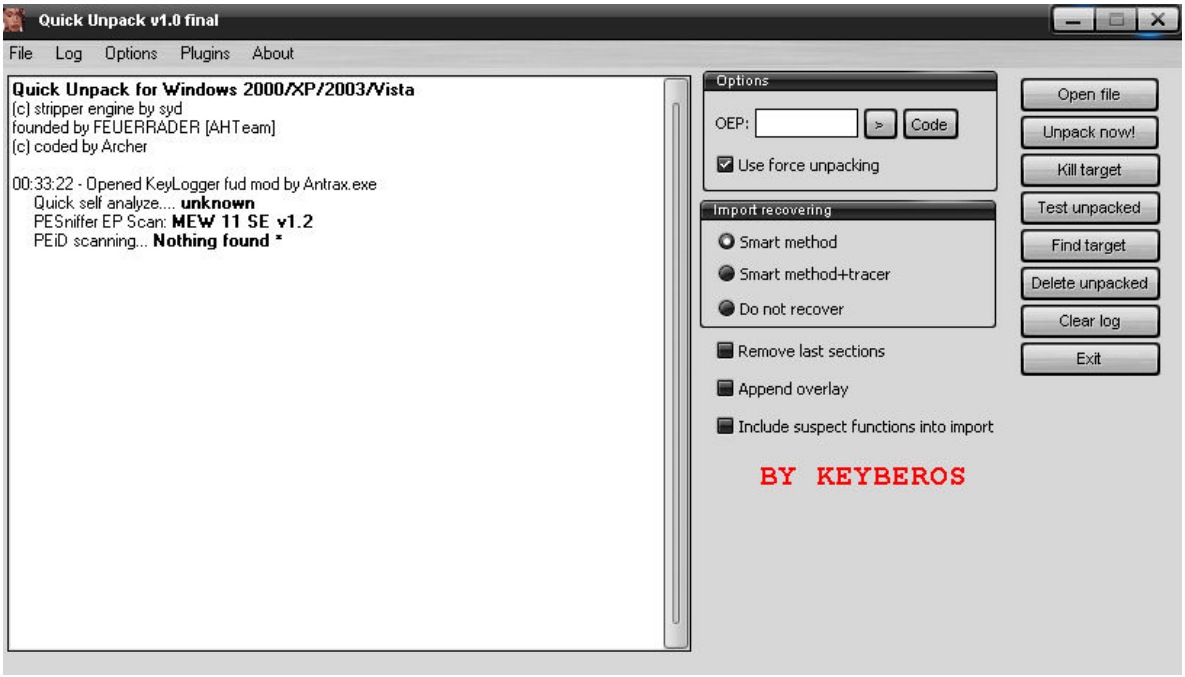
Por otro lado, existen distintos tipos de de programas para hacer un análisis individual de los Malwares, según lo que queramos saber sobre el.

Uno de esos programas es el: [PEiD]



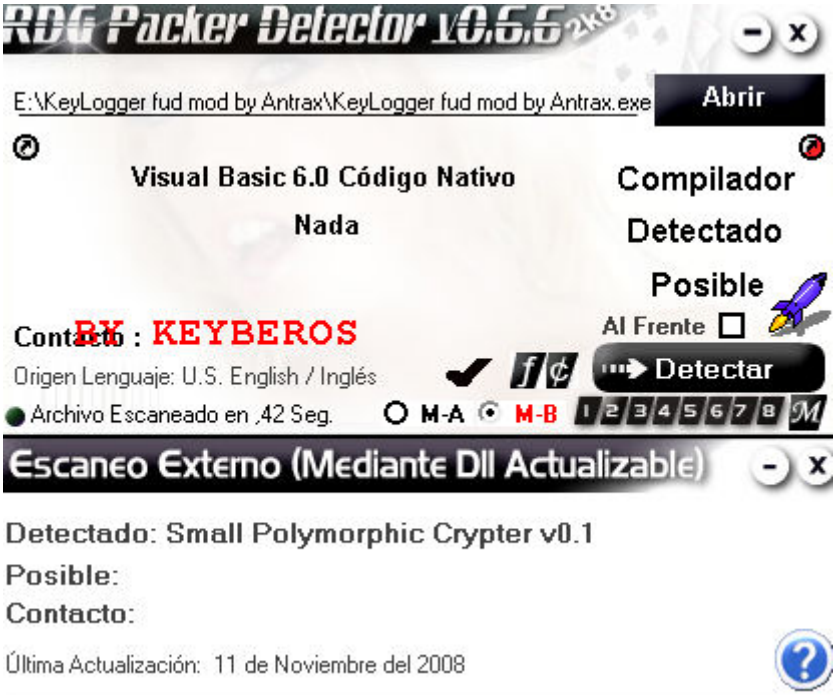
En este caso la información que nos dice la imagen es de con que esta compilado el archivo, y en caso de estar empaquetado, dice cual fue el empaquetador.

Otro programa similar es: [QuickUnpack]



Otro programa similar, que nos dice con que fue empaquetado el archivo que estamos escaneando.

Y por ultimo tenemos a: [RGD Packer detector]



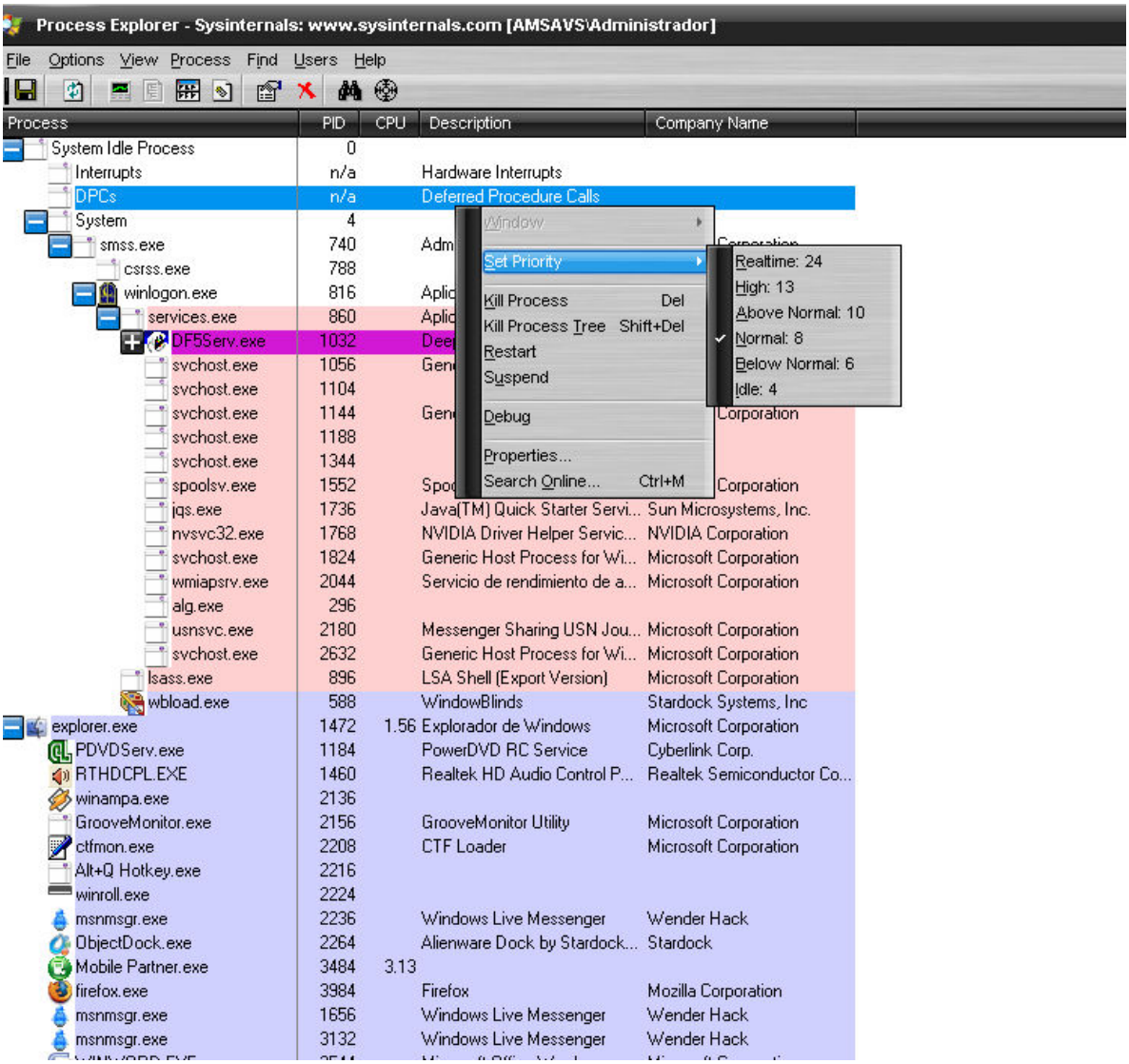
Uno de los mas completos, cómodo y fácil de usar.

Estos tres programitas mencionados anteriormente, nos da información como por ejemplo con que esta empaquetado, si tiene alguna protección, a demás de esto,

contienen una sencilla interfaz de des empaquetamiento. En caso de no poder desempaquetarlo con estos programas, se debe recurrir a un proceso mas complejo para realizarlo utilizando debuggers. Para esto se deben tener conocimientos en ASM e Ingeniería Inversa.

Todos los programas, incluyendo los Malwares, al ser ejecutados pueden abrir uno o más procesos. Para ver este tipo de comportamiento, existen distintos tipos de programas. Entre ellos:

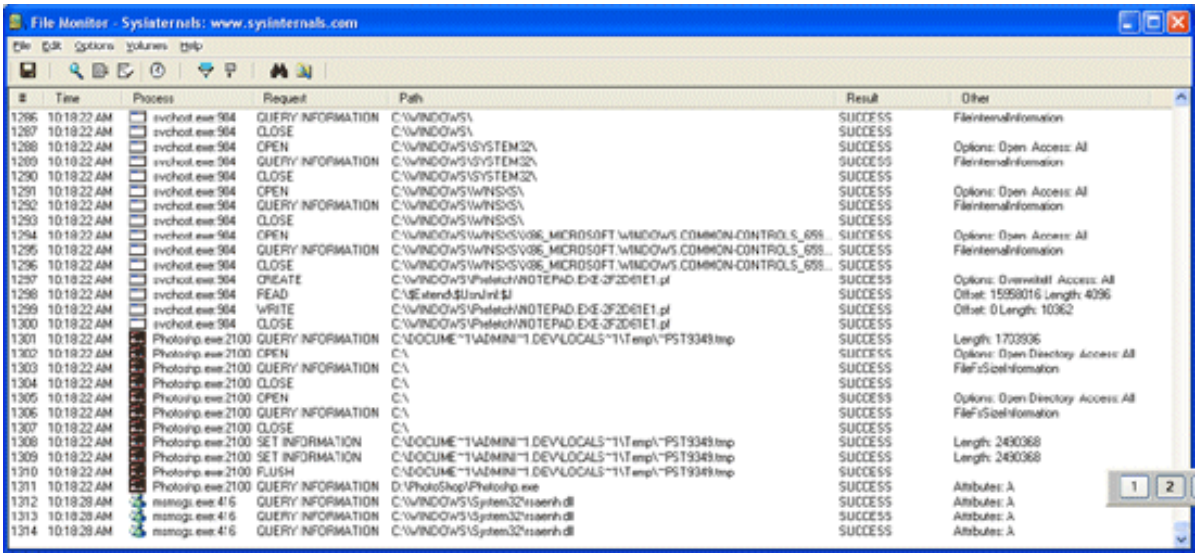
Process Explorer



Con este programa, podremos ver los procesos que se abren al iniciar el programa. A demás, este programa trae varias opciones, y nos dice todo tipo de información relacionados a ese proceso. Es bueno saber que proceso se activo o que proceso se abrió al iniciar el programa para ver y evaluar si es malicioso o no, y de esta manera poder analizarlo a fondo.

Análisis en los cambios de Archivos

Hay muchos malwares que al ser ejecutados producen cambios, crean o modifican archivos, etc. Es por eso que existe el llamado FileMon



Este programa se encarga de monitorear dichas modificaciones en archivos. Es muy útil para tener un control total de de todo lo que ocurre en nuestra PC.

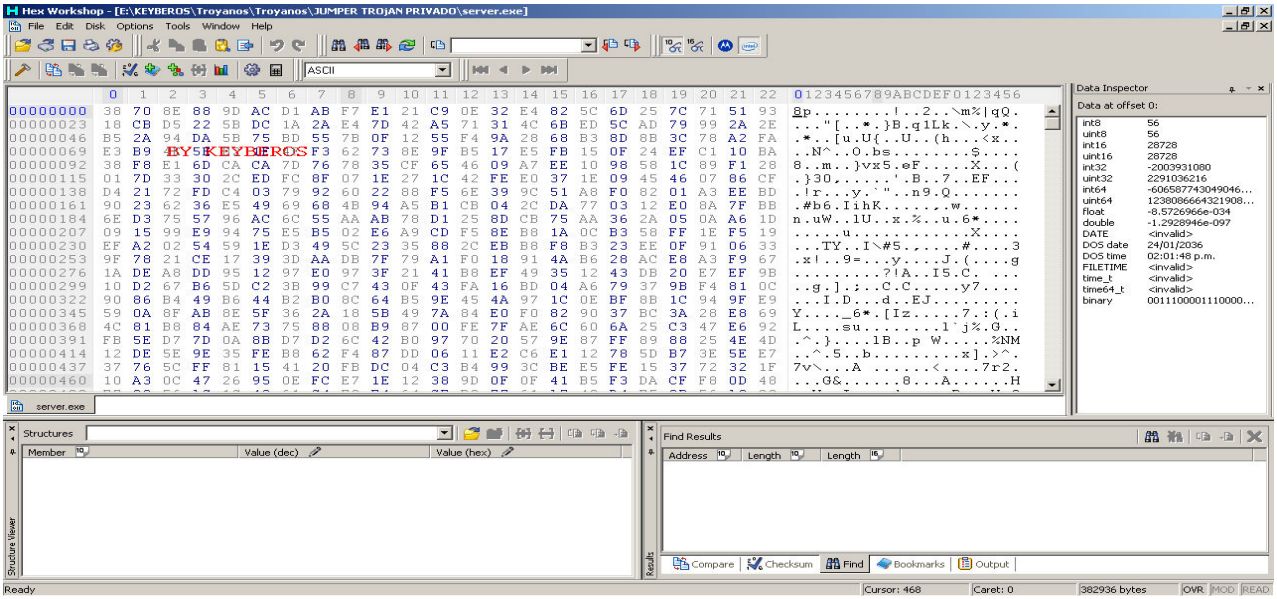
Análisis por medio de un Editor Hexadecimal

Muchas veces es muy útil utilizar un editor hexadecimal para ver las cadenas de textos visibles que contiene y así poder ver su funcionamiento.

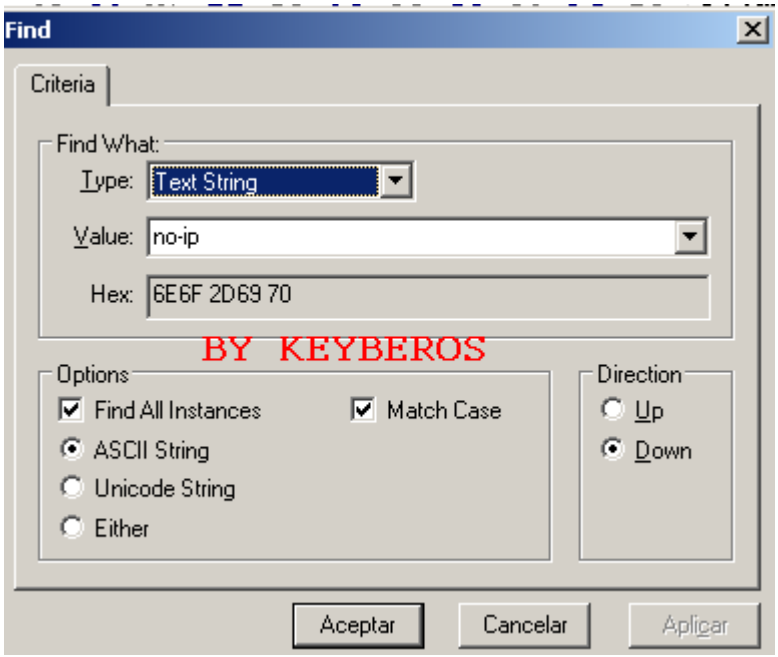
En este caso les mostrare una manera fácil de detectar una no-ip en un archivo que lo lleva visible:

Para empezar necesitamos un editor hexadecimal. Yo utilizo el Hex WorkShop que lo pueden conseguir en su web oficial: http://www.hexworkshop.com/

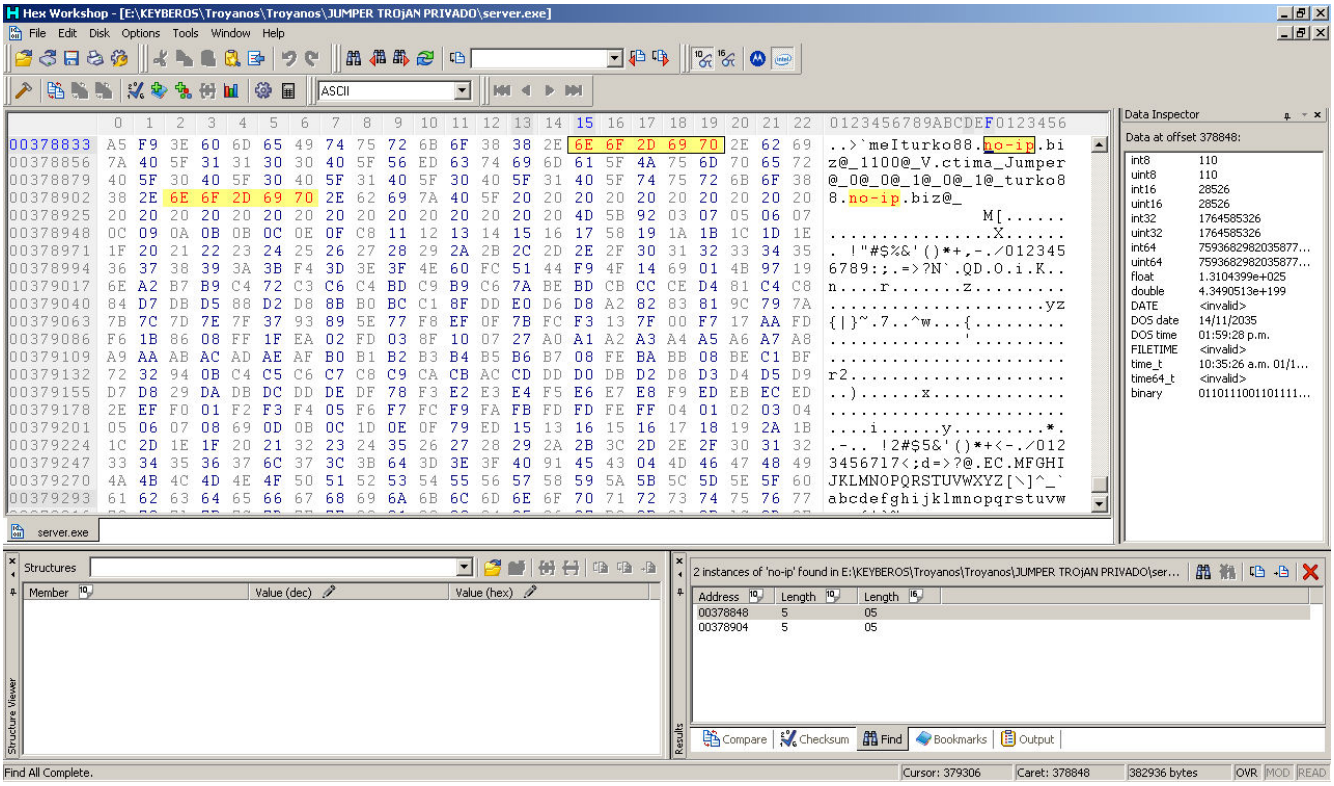
Una vez instalado, abrimos el archivo sospechoso con el editor y veremos algo así:



Una vez abierto tecleamos "CTRL + F" y veremos algo así:



Dejamos las opciones tal cual esta la imagen y le damos a aceptar. Inmediatamente nos llevara a la no-ip (si es que hay)

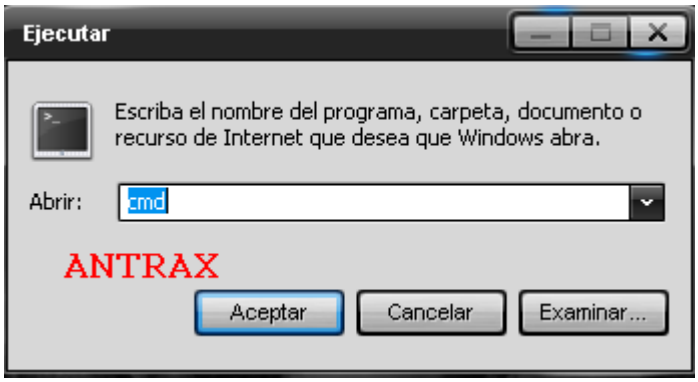


De esta manera determinamos que el programa conecta con esas no-ip como esta mostrando la imagen en ese punto resaltado en amarillo.

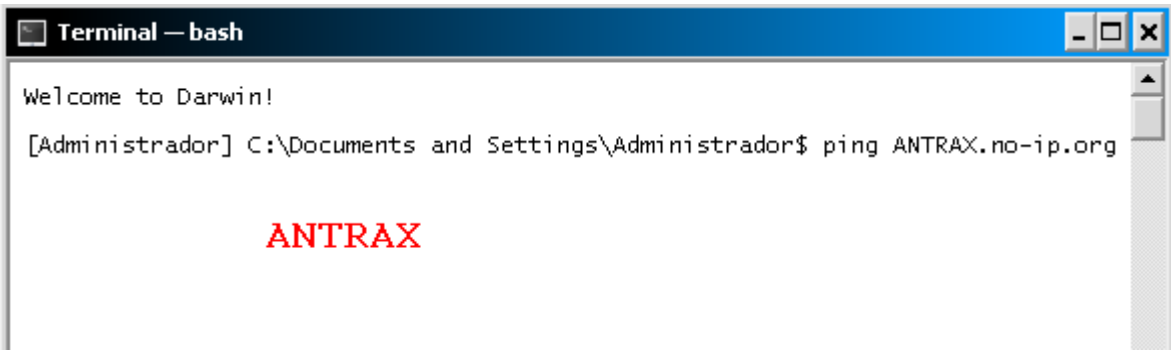
Para saber la ip de esa no ip, es muy sencillo. Solamente vamos a:

INICIO > EJECUTAR

Y tecleamos: "cmd" en Windows XP, o "command" en Windows 98 (Recuerda no escribir con comillas)



Una vez ahí, se abrirá la consola de Windows como esta o similar:



Escribimos: "ping lanoip.no-ip.org" (La no-ip varia dependiendo la que tengamos, solo puse esa de ejemplo)

Al darle en ENTER saldrá algo así:

Haciendo ping a XXX.XXX.XXX.XXX con 32 bytes de datos:

Respuesta desde XXX.XXX.XXX.XXX: bytes=32 tiempo<1m TTL=128

Respuesta desde XXX.XXX.XXX.XXX: bytes=32 tiempo<1m TTL=128

Respuesta desde XXX.XXX.XXX.XXX: bytes=32 tiempo<1m TTL=128

Respuesta desde XXX.XXX.XXX.XXX: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para XXX.XXX.XXX.XXX:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0

(0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 0ms, Máximo = 0ms, Media = 0ms

Con esto saldrá la IP de la PC que esta usando esa persona para acceder a tu PC.

En donde XXX.XXX.XXX.XXX es la IP de esa persona que nos tiene bajo su poder.

Para saber la ubicación geográfica de esa persona, Favor de leer mi tutorial de rastreo o traceo, en donde muestra como llegar a encontrar a una persona mediante su IP.