ANALIZANDO ARCHIVOS. BUSCANDO CODIGOS MALICIOSOS

[Paper publicado en http://www.mipistus.blogspot.com]

Jorge Alejandro Mieres
jamieres@gmail.com

©2007 Jorge Alejandro Mieres

ESTE “PAPER” SE PUBLICA BAJO UNA LICENCIA CREATIVE COMMONS BY-NC-SA 2.5 AR.

Por lo tanto, usted es libre de: 1) copiar, distribuir, exhibir, y ejecutar la obra. 2) Hacer obras derivadas. Bajo las siguientes condiciones: 1) Debe dar atribución mencionando el nombre del autor. 2) Usted no puede usar esta obra con fines comerciales. 3) Si usted altera, transforma, o crea sobre estos textos, sólo podrá distribuir la obra derivada resultante bajo una licencia idéntica a ésta.
Ante cualquier reutilización o distribución, usted debe dejar claro a los otros los términos de la licencia de esta obra. Cualquiera de estas condiciones puede dispensarse si usted obtiene permiso del titular de los derechos de autor. Nada en esta licencia menoscaba o restringe los derechos morales del autor.

BUSCANDO CODIGOS MALICIOSOS

En este paper veremos que tan fácil es caer en las garras de los malware que se esconden dentro de páginas de descarga de archivos o programas del tipo P2P a la espera de que algún cibernauta las agarre y deposite su confianza en ellos.

Hay muchas personas que están acostumbradas a descargar cuanto pueden de Internet o probar todos los programas que se cruzan por delante, utilizando programas como emule o páginas de descarga directa como rapidshare, 4shared, etc., sin tomarse la molestia de escanear los archivos para ver si algún bichito se esconde entre las ranuras del archivo zipeado.

La página web que se utilizó para buscar archivos fue *www.4shared.com*, 4shared es un site que nos ofrece en forma gratuita 1Gb de espacio para alojar lo que queramos, archivos de texto, programas, videos, etc. La verdad que es una herramienta bastante útil, el tema es que de la misma manera que encontramos cosas buenas también nos podemos encontrar con cualquier tipo de plaga.

La palabra clave que se utilizó para la búsqueda fue “Hotmail”, (*¿quien no vio en algún foro, “necesito hackear la cuenta de Hotmail de mi novia, me pueden ayudar?”*). Como si se pudiera violar la seguridad de la empresa de software mas grande del mundo. De los 15 archivos analizados 9 contenían algún código malicioso.

Vamos a ver un ejemplo utilizando la herramienta online de Virustotal, la cual busca en los archivos códigos maliciosos utilizando un motor de escaneo de 31 antivirus, y la herramienta gratuita Process Explorer de Sysinternals sobre un archivo llamado **“hotmailaccount.zip”**.

AhnLab-V3	2007.3.17.0	16.03.2007	no ha encontrado virus
AntiVir	7.3.1.43	17.03.2007	TR/Glukonat
Authentium	4.93.8	17.03.2007	is a security risk or a "backdoor" program
Avast	4.7.936.0	16.03.2007	Win32:Trojan-gen. {VC}
AVG	7.5.0.447	17.03.2007	Downloader.Glukonat.A
BitDefender	7.2	17.03.2007	Trojan.Downloader.Glukonat.D
CAT-QuickHeal	9.00	15.03.2007	TrojanDownloader.Glukonat.a
ClamAV	0.90.1	17.03.2007	no ha encontrado virus
DrWeb	4.33	17.03.2007	Trojan.DownLoader.10435
eSafe	7.0.14.0	16.03.2007	Win32.Hacktool
eTrust-Vet	30.6.3486	16.03.2007	no ha encontrado virus
Ewido	4.0	17.03.2007	Downloader.Glukonat.a
FileAdvisor	1	17.03.2007	no ha encontrado virus
Fortinet	2.85.0.0	17.03.2007	Download/Glukonat
F-Prot	4.3.1.45	17.03.2007	W32/Malware!62f8
F-Secure	6.70.13030.0	16.03.2007	Trojan-Downloader.Win32.Glukonat.a
Ikarus	T3.1.1.3	17.03.2007	Trojan-Downloader.Win32.Glukonat.A
Kaspersky	4.0.2.24	17.03.2007	Trojan-Downloader.Win32.Glukonat.a
McAfee	4986	16.03.2007	Generic.ca
Microsoft	1.2306	17.03.2007	TrojanDownloader:Win32/Glukonat
NOD32v2	2123	17.03.2007	Win32/TrojanDownloader.Glukonat.A
Norman	5.80.02	16.03.2007	W32/Smalltroj.COY
Panda	9.0.0.4	17.03.2007	Trojan Horse
Prevx1	V2	17.03.2007	Trojan:W32:(Gotecom)
Sophos	4.15.0	13.03.2007	Troj/Glukona-A
Sunbelt	2.2.907.0	16.03.2007	no ha encontrado virus
Symantec	10	17.03.2007	Hacktool
TheHacker	6.1.6.076	15.03.2007	Trojan/Downloader.Glukonat.a
UNA	1.83	16.03.2007	TrojanDownloader.Win32.Glukonat.545A
VBA32	3.11.2	16.03.2007	Trojan.Win32.TrojanDownloader.Glukonat.A
VirusBuster	4.3.7:9	17.03.2007	no ha encontrado virus

Como podrán observar en la imagen, de los 31 antivirus consultados, 25 detectaron algo raro. Veamos de que se trata. El archivo es en realidad un troyano del tipo rootkit llamado ***"Trojan.Downloader.Glukonat"*** que utiliza técnicas stealth para ocultarse y trabajar como backdoor *(para ver que son los backdoors y rootkit puede consultar el paper* ***"Malware. Programas maliciosos"****)*, todos los otros nombres son alias y dependen del nombre que le den las firmas antivirus.

Una vez que el troyano se instala, suele dejar tres archivos en los equipos infectados, cuyos nombres son seleccionados al azar. Por ejemplo:

```
c:\windows\system32\conf.com
c:\windows\system32\confmser.dll
c:\windows\system32\confmsur.dll
```

Además cada vez que se reinicia el sistema, crea una clave en el registro similar a la siguiente:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Conf.com = c:\windows\system32\conf.com
```

Cabe aclarar que la limpieza de este tipo de troyanos, no pasa solo por quitar los archivos que crea en el sistema, y evitar su ejecución en cada reinicio. Por la naturaleza de sus acciones (backdoors que permiten que uno o más intrusos hagan lo que deseen en el equipo infectado), la única forma de dejar totalmente seguro y limpio al sistema es borrar y reinstalar todo el sistema operativo y los programas necesarios.

Otra línea roja que aparece en la imagen es la que identifica a otro malware. En este caso es el ***"W32/Smalltroj.COY"***, también se trata de un troyano pero con características del tipo dropper (ejecutable que contiene varios virus en su interior) que instala un componente keylogger (captura y registra todo lo que se ingresa mediante el teclado) con la capacidad de registrar, entre otras cosas, nuestras contraseñas y enviarlas a un atacante o página controlada por éste.

Otros bichitos encontrados en los otros archivos analizados son:

- **Trojan-Spy.Win32.Banker.to:** se trata de un troyano tipo spy (espiá) que se instala en el registro del sistema y roba información de sitios web de bancos online, cuando se instala por primera vez se copia en: ***C:\Windows\svchosts.exe***, y deja una clave en el registro: ***HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\svchosts.***

F-Secure	6.70.13030.0	16.03.2007	no ha encontrado virus
Ikarus	T3.1.1.3	17.03.2007	Trojan-Spy.Win32.Banker.to
Kaspersky	4.0.2.24	17.03.2007	no ha encontrado virus

- **Backdoor.Small:** es un troyano que tiene como fin dar acceso remoto a un atacante a la maquina infectada. Se instala en el sistema como un servicio llamado *hwclock* (mostrando el nombre *Hardware Clock Driver*) y se conecta a un canal IRC y espera una orden del usuario remoto. Puede descargar otros troyanos, y también puede explotar una de las vulnerabilidades de red en Windows para penetrar a otras máquinas de la misma red.

DrWeb	4.33	17.03.2007	BackDoor.Generic.1060
eSafe	7.0.14.0	16.03.2007	Win32.Small.cib
eTrust-Vet	30.6.3486	16.03.2007	no ha encontrado virus
Ewido	4.0	17.03.2007	Backdoor.Small
FileAdvisor	1	17.03.2007	no ha encontrado virus
Fortinet	2.85.0.0	17.03.2007	no ha encontrado virus
F-Prot	4.3.1.45	17.03.2007	no ha encontrado virus
F-Secure	6.70.13030.0	17.03.2007	no ha encontrado virus
Ikarus	T3.1.1.3	17.03.2007	Backdoor.Generic.1060
Kaspersky	4.0.2.24	17.03.2007	no ha encontrado virus

Otros archivos contenían algún otro tipo de códigos maliciosos, como por ejemplo, el “180solutions”, un adware que se encarga de monitorear las actividades del navegador y muestra publicidad pop-up e incluye funcionalidad para descargar, instalar y ejecutarse en forma silenciosa.

Para realizar este análisis he puesto como ejemplo la descarga de archivos desde una página que se ha vuelto bastante popular como lo es 4shared, pero este ejemplo sirve para otras páginas de este tipo como rapidshare o megaunpload, además se debería tener el mismo criterio con la utilización de programas de intercambio de archivos del tipo P2P como Emule, Kazaa, FileScope, Ares, etc.

Cabe aclarar que no se esta poniendo en tela de juicio los servicios que ofrecen estas páginas o la utilidad que se les da a los programas P2P, sino que sí son propensos, evidentemente por su naturaleza, a ser usados como “nido de bichos”.

EL ANALISIS

Hasta aquí vimos que tan fácil es diseminar archivos infectados utilizando servicios de consumo masivo, veamos ahora, de una forma mas detallada y con un ejemplo real, cuales son los pasos y mecanismos utilizados por un troyano para infectar una computadora.

En principio, vamos a hacer un escaneo online utilizando la herramienta del site virustotal para comprobar que realmente estamos en presencia de un troyano, el resultado es el siguiente:

Antivirus	Version	Actualización	Resultado
AhnLab-V3	2007.3.17.0	16.03.2007	no ha encontrado virus
AntiVir	7.3.1.43	17.03.2007	TR/Barrio.10
Authentium	4.93.8	17.03.2007	could be a corrupted executable file
Avast	4.7.936.0	16.03.2007	Win32:Barok-B
AVG	7.5.0.447	18.03.2007	PSW.Generic.BBT
BitDefender	7.2	18.03.2007	Trojan.Pws.Barok.B
CAT-QuickHeal	9.00	15.03.2007	Trojan.PSW.Barok.10
ClamAV	0.90.1	18.03.2007	Trojan.PSW.Barok.10
DrWeb	4.33	18.03.2007	Trojan.Barok.10
eSafe	7.0.14.0	16.03.2007	Win32.PSW.Barok.10
eTrust-Vet	30.6.3486	16.03.2007	no ha encontrado virus
Ewido	4.0	18.03.2007	Trojan.Barok.10
FileAdvisor	1	18.03.2007	no ha encontrado virus
Fortinet	2.85.0.0	18.03.2007	W32/PWS_Barok!tr
F-Prot	4.3.1.45	17.03.2007	W32/Malware!2d3c
F-Secure	6.70.13030.0	18.03.2007	Trojan-PSW.Win32.Barok.10
Ikarus	T3.1.1.3	18.03.2007	Trojan-PWS.Win32.Barok.10
Kaspersky	4.0.2.24	18.03.2007	Trojan-PSW.Win32.Barok.10
McAfee	4986	16.03.2007	PWS-Barok
Microsoft	1.2306	18.03.2007	PWS:Win32/Barok
NOD32v2	2125	18.03.2007	PSW.Barok.A
Norman	5.80.02	16.03.2007	no ha encontrado virus
Panda	9.0.0.4	18.03.2007	Trj/PSW.Barok.10

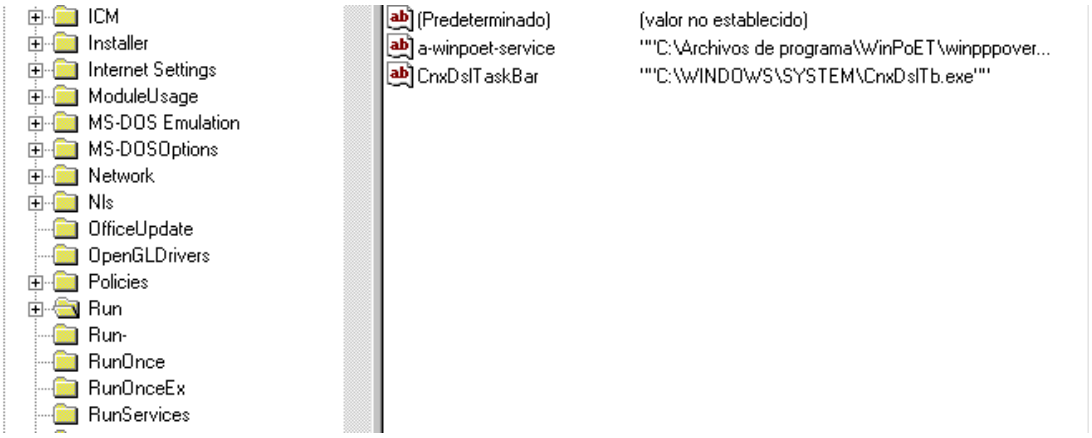
Evidentemente, estamos en presencia de un archivo infectado, en este caso, se trata de un troyano diseñado para obtener las contraseñas de la máquina infectada para luego enviar la información a una dirección elegida por el atacante. Veamos si esto es cierto.

Supongamos que nos hemos bajado de la web un archivo zipeado que supuestamente contiene un programa cualquiera; como con todo programa que queremos instalar en Windows, le damos doble click.

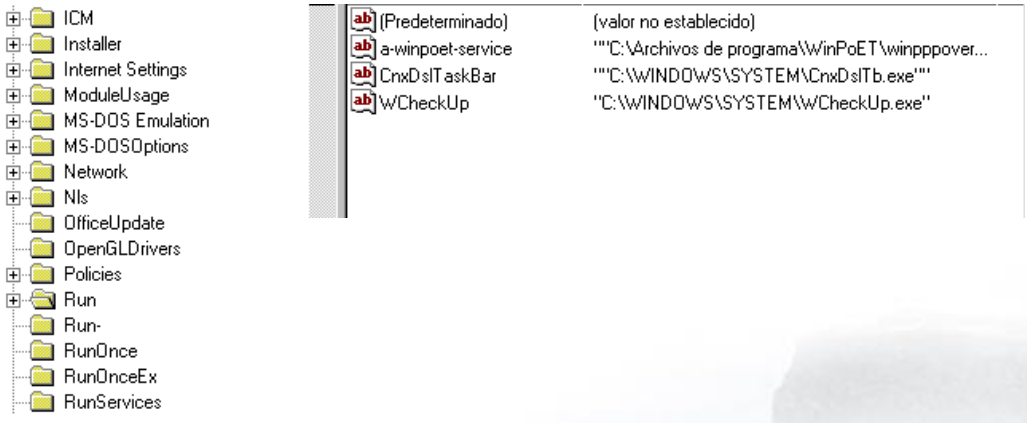
Para realizar el seguimiento de las actividades de este troyano y para hacerlo un poco más didáctico, mostraré capturas de lo que nuestro bichito vaya haciendo.

Luego de ejecutar nuestro archivo infectado, lo primero que hace el troyano es agregar una clave al registro en la siguiente dirección: **HKLM\Software\Microsoft\Windows\CurrentVersion\Run**, esto lo hace para poder ejecutarse automáticamente en cada reinicio del sistema (la mayoría de los malware crean una clave en esta dirección del registro). En el paper ***"Malware. Programas maliciosos"*** podrá encontrar más información sobre las claves del registro que comúnmente son manipuladas por los malware al hacer referencia a los backdoors.

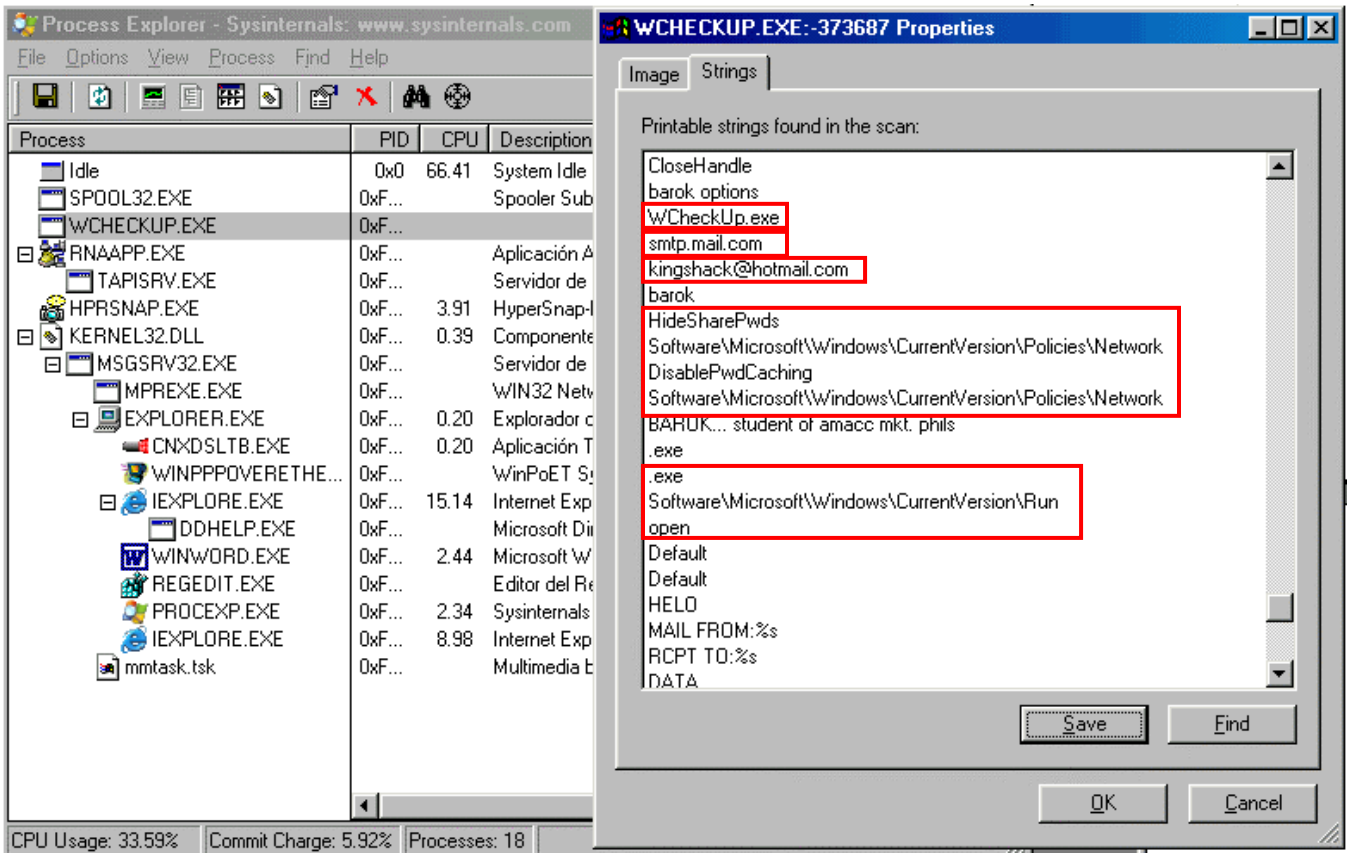
La siguiente imagen muestra una captura de esta clave del registro tomada antes de que el troyano infecte nuestra máquina.



En esta otra imagen vemos claramente una clave que antes no estaba bajo el nombre ***"WCheckUp"*** ubicada en la carpeta ***"SYSTEM"*** del sistema.



Ahora veamos que procesos están corriendo en nuestro sistema, para ello, ejecutamos la herramienta gratuita "*Process Explorer"* de Systernals.
http://www.microsoft.com/technet/sysinternals/utilities/ProcessExplorer.mspx



En la imagen podemos notar que tenemos un proceso que corre bajo el mismo nombre mostrado en la clave del registro que el troyano había creado, hacemos doble click sobre el mismo para entrar a sus propiedades y desde allí nos dirigimos a la solapa *Strings* para ver que contiene el proceso.

Vemos entonces que el troyano, además de agregar una clave en el registro nos desactiva el caché de contraseñas ***"Software\Microsoft\Windows\CurrentVersion\Policies\Network DisablePwdCaching"***, y la opción de evitar claves ocultas con ***HideSharePwds***.

Además vemos otra vez el nombre del ejecutable creado e inmediatamente después vemos las siguientes líneas: ***smtp.mail.com*** (SMTP es el protocolo utilizado para enviar e-mail) y ***kinghack@hotmail.com*** (dirección de e-mail), esto nos indica claramente que el troyano, en algún momento, intentará enviar un correo electrónico a ésta dirección de correo, seguramente, con las contraseñas almacenadas en nuestra máquina.

Resumiendo el tema en cuestión, pudimos ver que el primer paso realizado por el troyano fue el de asegurarse que su proceso (***WchekUp.exe***) se ejecute automáticamente en cada reinicio del sistema como si fuese parte del núcleo del mismo, vimos también que el mecanismo utilizado para lograrlo fue el de manipular el registro, agregando una clave y desactivando otras.

Por otro lado, también pudimos ver que el troyano incorpora su propio servido SMTP, el cual utiliza para enviar la información robada a una determinada casilla de e-mail establecida previamente por el atacante.

Recuerden que un troyano es una aplicación maligna que aparenta ser útil y benigna, y que está constituido básicamente por dos archivos, un archivo cliente y un archivo servidor, donde el servidor es el encargado de abrir un puerto en la computadora (archivo infectado que ejecutamos) para que el atacante, por intermedio del archivo cliente, pida los datos en forma remota, en este caso, contraseñas y demás datos importantes.

Esta forma de analizar los procesos que ejecuta un malware es genérica, es decir, casi siempre crean una clave en la dirección del registro mencionada en este ejemplo, y también levantan uno o varios procesos que podemos ver fácilmente si utilizamos las herramientas correctas.

ESTE “PAPER” SE PUBLICA BAJO UNA LICENCIA CREATIVE COMMONS BY-NC-SA 2.5 AR.

Por lo tanto, usted es libre de: 1) copiar, distribuir, exhibir, y ejecutar la obra. 2) Hacer obras derivadas. Bajo las siguientes condiciones: 1) Debe dar atribución mencionando el nombre del autor. 2) Usted no puede usar esta obra con fines comerciales. 3) Si usted altera, transforma, o crea sobre estos textos, sólo podrá distribuir la obra derivada resultante bajo una licencia idéntica a ésta.
Ante cualquier reutilización o distribución, usted debe dejar claro a los otros los términos de la licencia de esta obra. Cualquiera de estas condiciones puede dispensarse si usted obtiene permiso del titular de los derechos de autor. Nada en esta licencia menoscaba o restringe los derechos morales del autor.