

# Combatiendo a "Windows Intruder Detection Checklist"

Por SirDarckCat. sirdarckcat [at] gmail [.] com

<http://foro.elhacker.net/index.php/topic,109998.msg509057.html#msg509057>

Ayer estaba leyendo el documento que publico el CERT sobre detección de intrusos en Windows..  
1 palabra, decepcionante.

El documento inicia recomendando ciertas herramientas para detectar rootkits.  
Citar

- Rkdetect, available from <http://www.security.nnov.ru/soft/>
- RootKit Revealer, available from <http://www.sysinternals.com/Utilities/RootkitRevealer.html>
- VICE, a hooker detection tool, available from <http://www.rootkit.com> (registration required)

Una explicación de su funcionamiento puede ser encontrada en:  
<http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2004-05/0045.html>  
<http://www.sysinternals.com/Utilities/RootkitRevealer.html>

Sin embargo estos no son capaces de detectar la integridad del proceso.  
Es conocido que es posible anexas a un servicio en ejecución una sección extra de código, además de ser capaz de modificar las propiedades del servicio, métodos que saltan los análisis de estos 3 programas.

**Exploit de ejemplo y explicación que anexa código a un servicio. (WinXP sessmgr.exe, para Win2K utilman.exe).**

<http://foro.elhacker.net/index.php/topic,109365.msg507867.html#msg507867>

**Exploit ejemplo y explicación para modificar propiedades de un servicio para ejecutar código arbitrario.**

<http://foro.elhacker.net/index.php/topic,109000.0.html>

Después en este documento nos indican de estos 2 programas para ejecutar programas sin la influencia de cualquier troyano.

Citar

- BartPE, a bootable CD-based OS capable of running Win32 binaries: <http://www.nu2.ne/pebuilder/>
- WinPE, which is similar to BartPE, however there is no GUI support. See <http://www.microsoft.com/licensing/programs/sa/support/winpe.mspx> for availability information

Poco después nos hablan de leer los registros o "Logs", sin embargo las primeras cosas que hace un rootkit es borrar sus huellas, lo que hace poco útil este paso.

Después nos hablan de verificar la existencia de usuarios nuevos o extraños, sin embargo, los llamados rootkits e incluso algunos virus, se ejecutan en el contexto de SYSTEM o LocalService, y como ya mencionamos, en procesos reales de Windows.

El problema que veo aquí, es que al parecer toman como medida muy importante el buscar usuarios y grupos nuevos, cuando estos no son siempre la mejor manera de proceder.

Después nos hablan de ver aplicaciones que se ejecutan automáticamente en estas claves del registro:

Citar

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup
- HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows

- HKLM\System\CurrentControlSet\Control\Session Manager\KnownDLLs
- HKLM\System\ControlSet001\Control\Session Manager\KnownDLLs
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Windows\load
- HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Windows

y en C:\Documents and Settings\%username%\Start Menu\Programs\Startup

Sin embargo, si elegimos usar la carpeta de inicio de el usuario actual, normalmente se puede saltar al colocar "ATTRIB +S +H" como nombre un "espacio" o inclusive sin nombre, y un icono transparente.. aunque de todas formas, para iniciar automáticamente un programa, se usan mas las entradas del registro en HKLM..

En el documento explican que al acceder a las dichas claves, pueden ver los programas que se inician automáticamente, pero es sabido que se pueden esconder claves del registro usando "RegEnumValueW".

### Hide String value from Regedit by Hooking the RegEnumValueW API

<http://www.codeproject.com/system/hidereg.asp>

Después hablan de comparar los BINARIOS, es decir.. no el que se guarda en memoria, sino el que esta guardado, recordemos que nuestro método de inicialización, era meter en el parámetro de ejecución del servicio nuestro programa, y después anexarnos al proceso del servicio.

Es decir una vez que logramos acceder, esto no nos sirve de NADA.

Poco después hablan de verificar que las configuraciones de red no estén corruptas, pero nuestro programa ya debe estar entrenado para desactivar las configuraciones que uso, cuando no las use, y cuando las este usando, no dejar que netstat las rastree.

Esto se logra así:

Entramos a "%windir%\system32\drivers\etc\services"

Agregamos esta entrada al final del archivo:

Citar

.	1337/tcp
---	----------

y netstat listara la conexión sin el puerto, sino con un punto, tambien podriamos usar esto:

Citar

80/http	1337/tcp
---------	----------

y se listara como conexión típica http

después modificamos "%windir%\system32\drivers\etc\hosts"

y en este agregamos una entrada asi.

Citar

servidor.atacante	:
-------------------	---

y cuando netstat busque, pondrá "dos puntos" en lugar de el atacante..

Después nos hablan de ver los discos compartidos, pero si ya tenemos una shell es poco probable que usemos algun tipo de recurso compartido.

De todas formas, suponiendo que accedamos a través de NetBios, o algún familiar..

Podemos usar siempre C\$ o Admin\$, que son comúnmente compartidas aunque piden autenticación, pero ya quedamos en que si tenemos shell, no necesitamos este tipo de conexión, es como decir que hay que cerrar muy bien las ventanas, pero dejamos la puerta abierta.

Después nos piden que limpiemos las tareas programadas.

Sin embargo podemos dejar nuestro rootkit que al ser eliminado deje un batch ejecutandose en memoria y ejecute un comando, o incluso un archivo VBS o JS, o que al finalizar cree el comando "AT".

Y suponiendo que el Administrador finalizo todo.. se vería algo asi:

Código:

```
C:\WINDOWS\system32>at
No hay entradas en la lista.
```

```
C:\WINDOWS\system32>at 04:27 /INTERACTIVE /every:Lunes "cmd"
Se ha agregado un nuevo trabajo con identificador = 1
```

```
C:\WINDOWS\system32>at
Estado ID Día Hora Línea de comando
-----
1 Cada L 04:27 cmd
```

```
C:\WINDOWS\system32>at /delete
Esta operación eliminará todos los trabajos planificados.
¿Desea continuar esta operación? (S/N) [N]: s
```

```
C:\WINDOWS\system32>
```

Esta mal hecho el comando, solo fue de ejemplo..

Sin embargo, la terminación COM se ejecuta antes que los EXE, es decir si creamos un programa llamado AT.com se ejecutara este en lugar de at.exe

Se crea asi:

Código:

```
C:\WINDOWS\system32>debug
```

```
-A
0C9C:0100 JMP 121
0C9C:0102 DB "No hay entradas en la lista.",0d,0a,"$"
0C9C:0121 mov ah,9
0C9C:0123 mov dx,102
0C9C:0126 int 21
0C9C:0128 int 20
0C9C:012A
-rcx
CX 0000
:129
-n at.com
-w
Escribiendo 00129 bytes
-q
```

```
C:\WINDOWS\system32>
```

De esta forma siempre que escribamos at, se ejecutara at.com, sin tener que modificar ningún binario, y pasar la prueba de integridad.

Después nos dicen que busquemos por procesos no autorizados, sin embargo repito, como nuestro shellcode esta anexo en un proceso legítimo, es imposible detectarlo, por estos métodos.

Después nos hablan sobre buscar en archivos ocultos.

Es decir con ATTRIB +S +H o inclusive solo con +H

Sin embargo, usando un programa sin extensión, y como nombre un carácter invisible,

Código:

```
C:\ff>echo HOLA>". "
C:\ff>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 9CBB-4F6A
```

Directorio de C:\ff

```
20/02/2006 04:41 p.m. <DIR> .
20/02/2006 04:41 p.m. <DIR> ..
20/02/2006 04:41 p.m. 6 .
1 archivos 6 bytes
2 dirs 70,575,153,152 bytes libres
```

nuestro archivo es ese 6 que esta ahí. Sin nombre, sin nada, solo esta ahí..

Ahora dado que cmd ejecuta los archivos según su cabecera, si nuestro archivo fantasma es un

ejecutable se ejecutara como ejecutable.

Además, su eliminación, no solo es difícil, porque el archivo no tiene un nombre normal, sino que normalmente pasa desapercibido.

Aunque recordemos, que nuestro rootkit/virus/etc.. moderno es realmente un comando, así que no hay nada que esconder xD

Después nos dicen que verifiquemos los permisos a los usuarios, sin embargo una de 2 o nuestro proceso ya tiene acceso como el usuario actual o como system, por lo que no necesitamos cambiar las directivas locales.

Después nos hablan de verificar si no estamos en otro dominio, esto es para ataques en redes empresariales comúnmente, así que suponiendo que necesitamos unirnos a otro dominio, el nuevo lo usaremos como proxy al viejo, por lo que la computadora nunca se dará cuenta de que cambiamos de dominio.

Por ultimo nos recomiendan auditar para ver que acciones se han hecho en el sistema.. esta ultima, debo reconocer que es talvez el único paso que cuesta trabajo saltarse, aunque una eliminación de los registros es posible, probablemente levantara sospechas, lo mejor que un atacante puede hacer es especificar que registros desea conservar y cuales borrar, pero ese trabajo ya es demasiado, pero posible.

Ah se me olvidaba, y también sugieren usar software para detectar intrusiones, nos sugieren estos:

1.

Citar

Freeware/shareware Intrusion Detection Systems

- The COAST Intrusion Detection System Resources web page has a list of some freeware/shareware intrusion detection systems.

<http://www.cerias.purdue.edu/coast/ids/>

- GFI System Integrity Monitor

<http://www.gfi.com/downloads/downloads.asp?pid=9&vid=1&lid=1>

2. Commercial Intrusion Detection Systems

- Tripwire

<http://www.tripwire.com>

- Real Secure Server Sensor

[http://www.iss.net/products\\_services/enterprise\\_protection/rsserver/protector\\_server.php](http://www.iss.net/products_services/enterprise_protection/rsserver/protector_server.php)

- eEye SecureIIS

<http://www.eeye.com/html/products/secureiis/>

- Intact

<http://pedestalsoftware.com/products/>

Para los cuales, cada uno es un caso diferente, por lo que no me pondre a explicarlos.. ya eso le corresponderá a otros.

En conclusión quiero dejar que este documento creado por la CERT solo levanta falsas esperanzas y como dice ANELKAOS, un experto, no dejara tantas huellas.

Si quieren estar seguros, hagan todo minuciosamente, y si quieren atacar algo seguro, atáquenlo mas municiosamente.

Es todo, Saludos!!