

ROOTKITS

Escondiéndose del Administrador



Presentado por:

Victor Eduardo Valdez Isidro

Sistemas Operativos

Grupo

Semestre 2018-1





Temas a tratar:

- ¿Qué son los *Rootkits* ?
- ¿Para qué sirven?
- ¿Cómo perjudican?
- ¿Cómo infectan al equipo?
- ¿Cómo prevenirse de los *Rootkits* ?
- ¿Se pueden eliminar los *Rootkits* ?
- Relación con el Sistema Operativo

¿Qué son los Rootkits?

Los *rootkits* son una colección de herramientas utilizadas por intrusos para mantener tanto a usuarios legítimos y administradores de un sistema comprometidos, en cuanto a seguridad y privacidad se refiere, y casi siempre se desconoce su presencia.





¿Para qué sirven?

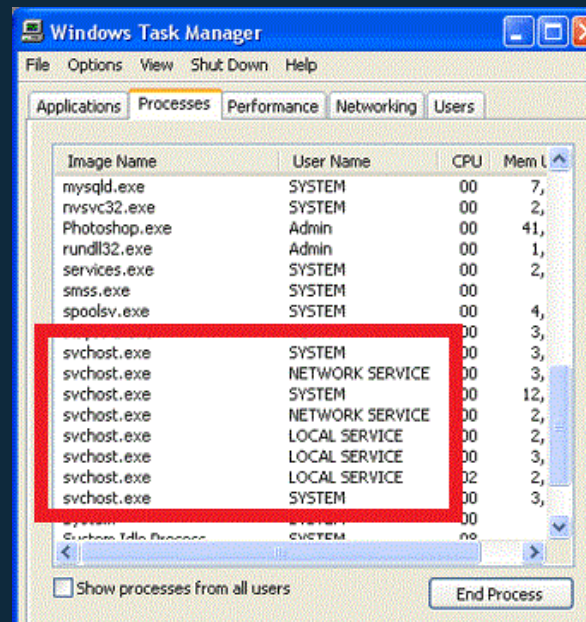
Estas herramientas sirven para esconder procesos, y archivos que permiten al intruso mantener el acceso al sistema con fines maliciosos, esconder conexiones de red, así como accesos a *root* (control total del sistema operativo).



¿Cómo perjudican?



Puerta trasera o *backdoor*



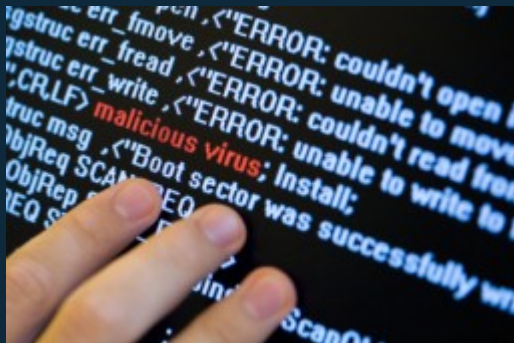
Ocultando procesos maliciosos al software antivirus, haciendo pasar un proceso 'maligno' por uno normal. Tenemos por ejemplo, en Microsoft Windows, el proceso svchost.exe



¿Cómo infectan al equipo?

Normalmente los *rootkits* se aprovechan de las vulnerabilidades del sistema operativo:

- Agujeros de seguridad, los cuales se solucionan instalando los debidos parches de seguridad (actualizaciones)

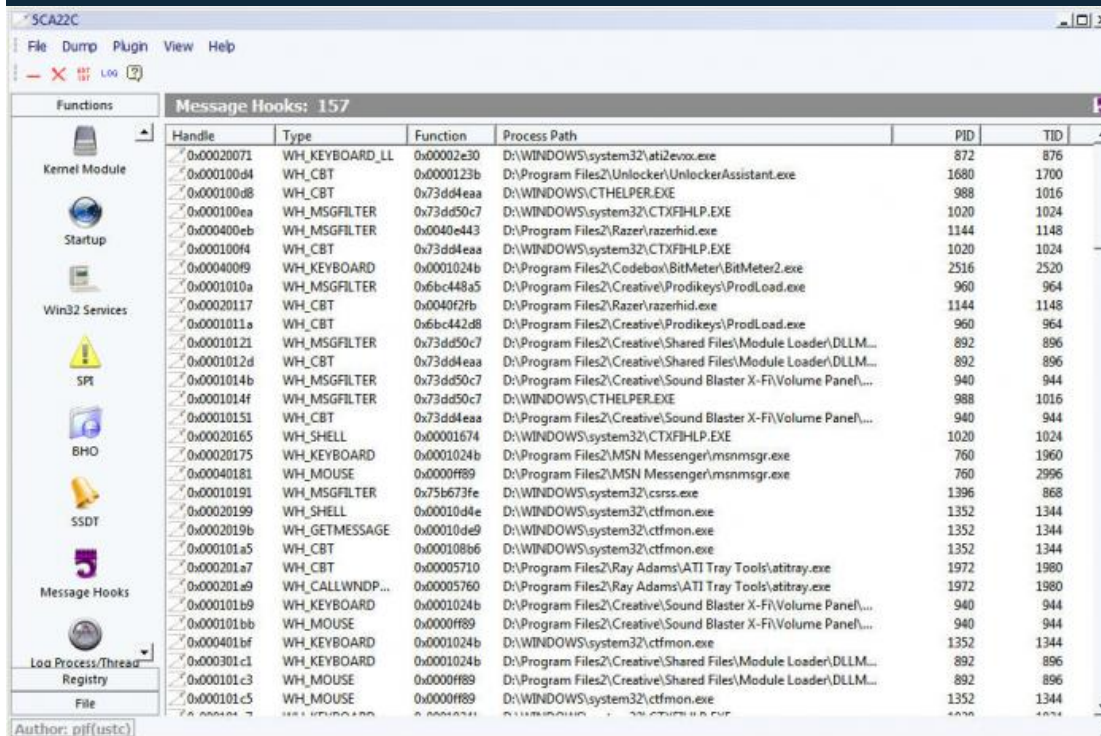


- De forma manual



¿Cómo prevenirse?

Es necesario un sistema que vigile no únicamente la actividad de los archivos en el disco, sino que vaya más allá. En lugar de analizar los archivos byte a byte, debe vigilarse lo que hacen al ejecutarse.



Handle	Type	Function	Process Path	PID	TID
0x00020071	WH_KEYBOARD_LL	0x0002e30	D:\WINDOWS\system32\ati2evxx.exe	872	876
0x000100d4	WH_CBT	0x000123b	D:\Program Files2\Unlocker\UnlockerAssistant.exe	1680	1700
0x000100d8	WH_CBT	0x73dd4ea	D:\WINDOWS\CTHELPER.EXE	988	1016
0x000100ea	WH_MSGFILTER	0x73dd50c7	D:\WINDOWS\system32\CTXFIHLP.EXE	1020	1024
0x000400eb	WH_MSGFILTER	0x0040e443	D:\Program Files2\Razer\razerhid.exe	1144	1148
0x000100f4	WH_CBT	0x73dd4ea	D:\WINDOWS\system32\CTXFIHLP.EXE	1020	1024
0x000400f9	WH_KEYBOARD	0x0001024b	D:\Program Files2\Codebox\BitMeter\BitMeter2.exe	2516	2520
0x0001010a	WH_MSGFILTER	0x6bc448a5	D:\Program Files2\Creative\Prodikeys\ProdLoad.exe	960	964
0x00020117	WH_CBT	0x0040f2fb	D:\Program Files2\Razer\razerhid.exe	1144	1148
0x0001011a	WH_CBT	0x6bc442d8	D:\Program Files2\Creative\Prodikeys\ProdLoad.exe	960	964
0x00010121	WH_MSGFILTER	0x73dd50c7	D:\Program Files2\Creative\Shared Files\Module Loader\DLLM...	892	896
0x0001012d	WH_CBT	0x73dd4ea	D:\Program Files2\Creative\Shared Files\Module Loader\DLLM...	892	896
0x0001014b	WH_MSGFILTER	0x73dd50c7	D:\Program Files2\Creative\Sound Blaster X-Fi\Volume Panel...	940	944
0x0001014f	WH_MSGFILTER	0x73dd50c7	D:\WINDOWS\CTHELPER.EXE	988	1016
0x00010151	WH_CBT	0x73dd4ea	D:\Program Files2\Creative\Sound Blaster X-Fi\Volume Panel...	940	944
0x00020165	WH_SHELL	0x0001674	D:\WINDOWS\system32\CTXFIHLP.EXE	1020	1024
0x00020175	WH_KEYBOARD	0x0001024b	D:\Program Files2\MSN Messenger\msnmgr.exe	760	1960
0x00040181	WH_MOUSE	0x0000ff89	D:\Program Files2\MSN Messenger\msnmgr.exe	760	2996
0x00010191	WH_MSGFILTER	0x75b673fe	D:\WINDOWS\system32\csrss.exe	1396	868
0x00020199	WH_SHELL	0x00010d4e	D:\WINDOWS\system32\ctfmon.exe	1352	1344
0x0002019b	WH_GETMESSAGE	0x00010de9	D:\WINDOWS\system32\ctfmon.exe	1352	1344
0x000101a5	WH_CBT	0x000108b6	D:\WINDOWS\system32\ctfmon.exe	1352	1344
0x000201a7	WH_CBT	0x00005710	D:\Program Files2\Ray Adams\ATI Tray Tools\atitray.exe	1972	1980
0x000201a9	WH_CALLWNDP...	0x00005760	D:\Program Files2\Ray Adams\ATI Tray Tools\atitray.exe	1972	1980
0x000101b9	WH_KEYBOARD	0x0001024b	D:\Program Files2\Creative\Sound Blaster X-Fi\Volume Panel...	940	944
0x000101bb	WH_MOUSE	0x0000ff89	D:\Program Files2\Creative\Sound Blaster X-Fi\Volume Panel...	940	944
0x000401bf	WH_KEYBOARD	0x0001024b	D:\WINDOWS\system32\ctfmon.exe	1352	1344
0x000301c1	WH_KEYBOARD	0x0001024b	D:\Program Files2\Creative\Shared Files\Module Loader\DLLM...	892	896
0x000101c3	WH_MOUSE	0x0000ff89	D:\Program Files2\Creative\Shared Files\Module Loader\DLLM...	892	896
0x000101c5	WH_MOUSE	0x0000ff89	D:\WINDOWS\system32\ctfmon.exe	1352	1344

Existe, para Microsoft Windows, un software que hace un monitoreo a los procesos del sistema operativo: Icesword Anti-Rootkit

Rootkits: Escondiéndose del administrador

¿Se pueden eliminar?

La mejor manera de evitar que el proceso entre en acción, es evitar el arranque del sistema operativo en el disco en el que se encuentra el *rootkit*, utilizando un disco diferente al del sistema infectado; como puede ser un *Live CD*. Así, si el *rootkit* es conocido, podrá eliminarse.

Hostname: PartedMagic
Linux Kernel: 3.14.2-pmagic
CPU Details: i686, 1333(MHz)

CPU History: [Bar chart showing CPU usage history]

CPU Usage: 22% [Bar chart]

RAM Usage: 159MiB (15%) [Bar chart]
Available RAM: 939MiB

ACPI Battery: 11 49% [Bar chart]
Remaining time: 2h 47m 25s

Processes: 134 Running: 1
(top 5 sorted by CPU usage)

NAME	PID	CPU%	MEM%
lxpanel	1324	3.03	1.37
Xorg	1297	2.52	1.02
parcellite	1358	0.30	0.85
kuonker/1:1	4264	0.10	0.00
kuonker/0:1	3444	0.10	0.00

Processes: 134 Running: 1
(top 5 sorted by MEM usage)

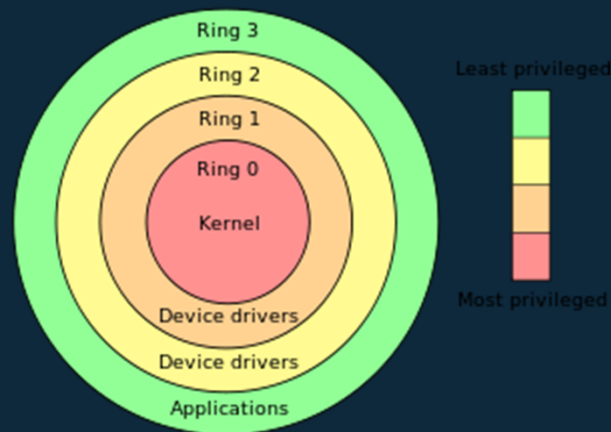
NAME	PID	CPU%	MEM%
Blender-applet	1473	0.00	2.12
PartedMagic	1472	0.00	1.87
gnome-udisks2-vo	1380	0.00	1.56
pcmanfm	1357	0.10	1.41
lxpanel	1324	3.03	1.37

System Uptime: 0h 24m 46s

PARTED Magic
partition | clone | rescue

10:25pm

Relación con el S.O



Dominios de protección jerárquica (anillos de protección para el procesador x86)

Los anillos están dispuestos en una jerarquía desde los más privilegiados (de más confianza), usualmente numerado cero, hasta el menos privilegiado (de menos confianza), usualmente con el mayor número de anillo. En la mayoría de sistemas operativos, el anillo 0 (Ring-0) es el nivel con la mayoría de los privilegios e interactúa más directamente con el hardware físico, como el CPU y la memoria.



Relación con el S.O

Tipos de *rootkits*

Rootkits en Espacio de Usuario. Estos se ejecutan en el anillo 3 (Ring-3), y modifican librerías, o archivos de configuración, e inclusive ejecutables (ls y ps en GNU/Linux).

Rootkits en Espacio de *Kernel*. Estos se ejecutan en el anillo 0 (Ring-0), y modifican estructuras del núcleo del sistema operativo o *kernel* y atrapan llamadas al sistema operativo (*hijacking syscall-table*). Podemos tenerlos como LKM's o como parches al núcleo *patch to kernel* ejecutando: `/dev/kmem` en GNU/Linux.





¡Gracias por tu atención!

