

## Rootkits evasivos: el mejor amigo del código malicioso y el peor enemigo de Windows

### Introducción

A lo largo de los últimos años, se ha hablado mucho acerca de los *rootkits*. Esa forma particularmente peligrosa de código malicioso al que le es posible esconderse en el sistema operativo huésped y que, por medio de tecnologías ocultas, puede permitir que programas espía y otras formas más obvias de código realicen alguna actividad dañina, al mismo tiempo que permanece indetectable.

Una vez que el *rootkit* obtuvo acceso al ordenador, es muy difícil rastrearlo y eliminarlo.

La amenaza de los *rootkits*, ha estado presente desde hace un cierto tiempo, pero se está usando con más frecuencia en la actualidad.

Comentaremos qué se debe tener en cuenta, cómo evitar ser infectado y, en caso de haber sucedido, cómo limpiar el sistema.

### Antecedentes

El término *rootkit* (un conjunto de herramientas para obtener acceso raíz (*root*), o del tipo administrador, al sistema objetivo del ataque) se originó en el mundo de Unix, donde el acceso al sistema raíz implicaba el mayor nivel disponible de privilegios de control sobre el sistema, que se otorgaba únicamente a administradores.

Los *rootkits* de Unix permitieron a los piratas escalar el nivel de acceso hasta la cuenta raíz y, prácticamente, realizar cualquier tipo de acción en el sistema, controlando ese equipo y amenazando otros sistemas que podrían estar conectados. Recientemente, los *rootkits* han invadido el mundo de Windows, donde se los reconoce (y teme) por su capacidad para ocultar al sistema operativo, partes del sistema de archivos, entradas de registro y otros objetos internos. Al trabajar en segundo plano, los *rootkits* pueden continuar actuando con impunidad hasta que el sistema se formatea por completo o se utiliza tecnología igual de astuta para soportar su ataque.

*Kit*, la segunda parte de la palabra, implica que existen conjuntos de herramientas que cualquier persona puede obtener gratuitamente o por una cuota y posteriormente adaptar, para ser utilizados junto con su propio código malicioso y encubrir las actividades de este mismo programa.

Algunas veces, los *rootkits* se distribuyen en un formato de código abierto (*open source*), lo que significa que incluso el programador menos habilidoso puede modificar fácilmente el código del *rootkit* existente. Por ejemplo, se puede utilizar para evitar la detección por parte de una aplicación antivirus que busque firmas de virus, ya que el *rootkit* las escondería.

### ¿Qué puede hacer un rootkit?

Por sí solo, un *rootkit* es casi inofensivo. Si no está programado para realizar una actividad maliciosa, puede brindar funcionalidad adicional a cualquier tipo de programa.

Los usos legítimos de la tecnología de *rootkits* podría incluir, por ejemplo, a un proveedor de antivirus que protege los binarios de dicho programa contra potenciales ataques, es decir ocultándolos al sistema operativo. Esta "cualidad" podría haber sido el concepto original tras la idea de Symantec de utilizar las características similares a la de los *rootkits* en su conjunto de aplicaciones SystemWorks. Sin embargo, la empresa se vio forzada a lanzar rápidamente un parche para eliminar al *rootkit* debido a que se suponía que un programa malicioso podría explotar esta técnica para esconderse.

Recientemente, el último programa de gestión de derechos digitales de Sony, sufrió el mismo problema. En este caso, los piratas sí encontraron la forma de instalar un troyano y transformarlo en indetectable utilizando la aplicación de gestión como cubierta.

El motivo por el cual los *rootkits* son tan peligrosos, es porque los programas maliciosos pueden utilizarlos para esconder cualquier archivo, proceso, carpeta o claves de registro de cualquier programa contra código malicioso. Esto hace imposible que un analizador de seguridad pueda reparar el daño una vez que el sistema ha sido infectado. Los *rootkits* sofisticados, incluso instalan servicios y unidades invisibles que pueden transmitir datos personales a los piratas y/o secuestrar el ordenador para ataques *botnets*, falsificación de sitios y distribución de correo no deseado.

## Tipos de rootkits

Existen cuatro tipos de *rootkits*.

La siguiente lista los ordena por su grado de sofisticación:

### 1. Virtualizados

Los *rootkits* virtualizados son casi imposibles de detectar porque tienen un acceso de nivel muy bajo al *kernel* del sistema operativo. Estos *rootkits* modifican la forma en que el equipo inicia el sistema operativo. Como resultado, pueden crear un entorno virtual, y hacer que el ordenador considere al *rootkit* como un sistema operativo huésped que esté ejecutando el sistema operativo original como invitado.

En consecuencia, el sistema huésped (el *rootkit* virtualizado en este caso) tiene el control casi total sobre el ordenador. Puede realizar cualquier tipo de cambio, en la forma en que los procesos en ejecución o los listados de directorios, se enumeran en el sistema operativo invitado al interceptar las llamadas al equipo realizadas en el invitado. El *rootkit* experimental SubVirt, recientemente creado con el apoyo de Microsoft, es un ejemplo de este tipo de amenaza.

### 2. A nivel de kernel

Estos *rootkits* modifican el *kernel* del sistema operativo, de forma tal que todo el sistema se encuentre bajo el control del *rootkit*. Esta no es una tarea sencilla, pero una vez lograda, el *rootkit* puede realizar cualquier tipo de actividad en el ordenador sin ser detectado. Esto no solamente compromete la seguridad del equipo, sino también tendrá un impacto drástico sobre la estabilidad y futura viabilidad del sistema.

### 3. A nivel de librerías

Estos *rootkits*, por lo general, emparchan, adhieren o reemplazan llamadas del sistema con versiones que esconden información acerca del agresor. Estas instancias pueden modificar la forma en que se comporta un programa legítimo al hacerlo realizar funciones adicionales, para el cual no está autorizado a realizar, como por ejemplo, abrir una nueva conexión y transmitir datos confidenciales utilizando permisos de acceso del programa legítimo.

### 4. A nivel de aplicación

Estos *rootkits* reemplazan archivos binarios de aplicaciones legítimas, con archivos maliciosos. También pueden secuestrar programas legítimos y realizar acciones maliciosas en su nombre. Este tipo de *rootkit* emparcha un programa legítimo, de forma tal que pueda realizar operaciones adicionales, por lo general ilegítimas.

## Detección y eliminación

Los *rootkits* deben combatirse de manera proactiva, antes que puedan infiltrarse realmente en el sistema, de lo contrario, eliminarlos es mucho más difícil.

Como siempre, las medidas comunes de precaución para evitar la infección con un *rootkit*, incluyen el uso de aplicaciones antivirus y contra programas espías que cuenten con la última actualización, la aplicación de los últimos parches y un programa cortafuegos configurado adecuadamente. Todos los usuarios deben asegurarse que también tienen un conocimiento básico de la seguridad en Windows.

Existe un par de programas especializados que pueden detectar si un *rootkit* está presente en un sistema:

RootkitRevealer (<http://www.sysinternals.com/Utilities/RootkitRevealer.html>) y IceSword (<http://www.xfocus.org/>).

Otro producto prometedor que apunta a evitar que el *rootkit* ingrese en el equipo objetivo es SocketShield (<http://www.explabs.net/ss/index.html>), que complementa a los cortafuegos, al controlar el tráfico para explotar descargas conducidas que usualmente vienen en la forma de *rootkit*.

Estos programas utilizan diferentes técnicas para localizar *rootkits*, pero ambos han sido efectivos al tratar con instancias recientes de muestras de los mismos. No obstante, siempre existen ejemplos más modernos y más audaces de código malicioso que van surgiendo, por lo tanto esto se convierte en el juego del gato y el ratón, y lo que atrapa las amenazas de hoy puede no atrapar las de mañana.

Si se siente seguro, o si tiene un amigo o colega que lo pueda hacer, sería útil iniciar, a menudo, el equipo desde un sistema operativo diferente (por medio de una unidad USB, de discos compactos o disco duro externo) y ejecutar una verificación junto con un análisis con uno de los programas antes mencionados para asegurarse que su ordenador no contiene ningún tipo de *rootkit*.

## Conclusión

Los *rootkits* pueden causar serios daños al sistema y, si se los deja tomar el control puede obligar al usuario a formatear por completo su ordenador. Sin embargo, si se toman precauciones razonables de seguridad y se cuenta con sistemas operativos y aplicaciones con sus correspondientes parches y un programa de seguridad actualizado, se hará mucho para evitar que los *rootkits* obtengan acceso a su sistema.

Autor: Igor Pankov, Agnitum Ltd.

Traducción y adaptación al español: Ontinet.com, S.L.