 **Universidad Nacional   
 Autónoma de México**

Facultad de Ingeniería

Sistemas Operativos

**Integrantes del equipo:**

* Buendía Monroy Laura
* Trejo Vázquez Efren

**Profesor:** Gunnar Wolf

**“Rootkits”**

**Grupo:** 2

**Semestre:** 2018-2

ROOTKITS

**¿Qué son los rootkits?**

**Un rootkit** es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos. Hay rootkits para una amplia variedad de sistemas operativos, como Linux, Solaris o Microsoft Windows. Por ejemplo, el rootkit puede esconder una aplicación que lance una consola cada vez que el atacante se conecte al sistema a través de un determinado puerto. Los rootkits del kernel o núcleo pueden contener funcionalidades similares.

Un backdoor puede permitir también que los procesos lanzados por un usuario sin privilegios de administrador ejecuten algunas funcionalidades reservadas únicamente al superusuario. Todo tipo de herramientas útiles para obtener información de forma ilícita pueden ser ocultadas mediante rootkits.

Rootkit es una aplicación (o conjunto de aplicaciones), que oculta su presencia o la presencia de otra aplicación (virus, spyware, etc.) en el equipo, utilizando alguna de las capas más bajas del sistema operativo (redirección de la función API, utilización de las funciones OS no documentadas, etc.), lo que los convierte en casi indetectables para el software antimalware normal.

Tenga en cuenta que los rootkits pueden ser **legítimos** o **maliciosos**. Los rootkits correctos se pueden instalar como parte de una aplicación legítima. La lista de algunos rootkits conocidos se encuentra en Detección de rootkits legítimos conocidos. Por este motivo, es necesario prestar mucha atención a los resultados del AntiRootkit.

Un rootkit puede entrar en un equipo de varias formas. La más común es a través de algún troyano o del archivo adjunto de algún correo electrónico sospechoso. También navegar en internet puede dar como resultado la instalación de un rootkit, cuando por ejemplo se necesita un complemento "especial" (el cual se presenta como legítimo) para visualizar correctamente alguna página web, para ejecutar algún archivo, etc.

Los Rootkits aparecieron, por primera vez, hace 20 años. Estos programas permiten a los hackers acceder y robar la información de los equipos de los usuarios sin ser detectados. Este término se usa para diferentes herramientas de malware, diseñadas específicamente para permanecer ocultas, infectar los ordenadores y controlar el PC de forma remota. Para ayudar a los usuarios a comprender qué es un rootkit y cómo funciona.

**Definición de Rootkit**

Un rootkit es un término que se aplica a un tipo de malware, diseñado para infectar un PC, el cual permite al hacker instalar diferentes herramientas que le dan acceso remoto al ordenador. Este malware se oculta en la máquina, dentro del sistema operativo y sortea los obstáculos como aplicaciones antimalware o algunos productos de seguridad. El rootkit contiene diferentes herramientas maliciosas como un keylogger, un módulo para robar los números de tarjeta o cuentas bancarias, un bot para ataques DDoS y otras funciones que pueden desactivar el software de seguridad. Los rootkits actúan como un backdoor que permite al atacante infectar, de forma remota, al equipo y eliminar o instalar componentes específicos. Algunos ejemplos de rootkits de Windows, todavía activos, son TDSS, ZeroAccess, Alureon y  Necurs.

**Variantes de Rootkit**

Existen dos tipos principales de rootkits: user-mode y kernel-mode. Los primeros están diseñados para funcionar en el mismo lugar que opera el sistema operativo y las aplicaciones. Ejecutan sus funciones maliciosas hackeando las aplicaciones del equipo o reescribiendo la memoria que usan dichas aplicaciones. Este tipo de rootkit es el más habitual. En cambio, los kernel operan desde el núcleo y proporcionan al cracker los privilegios del equipo más importantes. Una vez el rootkit de núcleo está instalado, el hacker puede tener el control del ordenador infectado y hacer cualquier cosa que desee en él. Este tipo de malware es más complejo que el anterior y, por ende, menos habitual. Además, también es más difícil de detectar y eliminar.

También existen otras variantes, aunque menos comunes, como los bootkits. Estos programas se diseñan para modificar el bootloader (gestor de arranque) del ordenador, el software que funciona antes de que se cargue el sistema operativo. Recientemente, ha emergido una nueva clase de rootkits móviles cuyo objetivo son los smartphones, especialmente los dispositivos Android. Estos rootkits se asocian a una aplicación maliciosa que se descarga en foros o appstore de terceros.

**¿Cómo infecta al equipo?**

Los rootkits se pueden instalar siguiendo varios métodos, pero el más común es aprovechando una vulnerabilidad en el sistema operativo o en una aplicación del equipo. Los piratas informáticos dirigen sus atacantes contra vulnerabilidades conocidas y desconocidas en el sistema operativo y aplicaciones; usando un exploit que controle la máquina. Luego, instalan el rootkit y configuran unos componentes que proporcionan acceso remoto al PC. Los exploit se suelen alojar en una website, hackeada previamente. Otra forma de infección son los USB. Los atacantes dejan USB infectados en algún sitio donde una víctima los vea y los recoja: edificios de oficinas, cafeterías o centros de convenciones. En algunos casos, se realiza la instalación mediante vulnerabilidades de seguridad, pero en otros, se instala a partir de una aplicación o un archivo legal de un USB.

**Eliminación**

Es difícil detectar la presencia de un rootkit en un equipo, porque este tipo de malware permanece oculto y hace “su trabajo” a escondidas.  No obstante, existen herramientas diseñadas para buscar rootkits siguiendo sus patrones de comportamiento. Eliminar un rootkit es un proceso complejo, que requiere el uso de herramientas especiales como TDSSKiller; herramienta de Kaspersky Lab que puede detectar y eliminar el rootkit TDSS. A veces, puede ser necesario que la víctima reinstale el sistema operativo ya que el equipo está demasiado dañado.

Los rootkits son una amenaza de Internet de la que últimamente viene hablándose mucho, fundamentalmente desde que se ha hecho público que una gran empresaha distribuido un rootkit con sus productos. Pero, ¿qué es exactamente un rootkit? ¿Por qué es tan peligroso? ¿Es cierto que no pueden eliminarse de los sistemas? Vamos a intentar responder a estas preguntas y aclarar algunos mitos.

El término viene de la unión de “root” y de “kit”. “Root” se refiere al usuario con máximos derechos en sistemas tipo Unix (puede ser Unix, AIX, Linux, etc). Es el superusuario, el “administrador”, en definitiva, es la **expresión máxima de autoridad** sobre un determinado sistema informático. Por su parte, “kit” se refiere a un **conjunto de herramientas**, por lo que un rootkit se puede entender como un conjunto de herramientas con categoría de administrador de un sistema.

Los rootkits, en la práctica, son programas que una vez instalados en un sistema, efectúan las **modificaciones** necesarias para poder llevar a cabo las tareas que tiene programadas **sin que su presencia pueda ser detectada**. Fundamentalmente, los rootkits tratan de **encubrir** a otros procesos que están llevando a cabo acciones maliciosas en el sistema. Por ejemplo, si en el sistema hay una puerta trasera para llevar a cabo tareas de espionaje, el rootkit ocultará los puertos abiertos que delaten la comunicación; o si hay un sistema para enviar spam, ocultará la actividad del sistema de correo. La única limitación es la imaginación del creador.

Los rootkits, al estar diseñados para pasar desapercibidos, no pueden ser detectados. Si un usuario (o incluso el usuario root) intenta analizar el sistema para ver qué procesos están ejecutándose, el rootkit mostrará información falsa, mostrando todos los procesos excepto él mismo y los que está ocultando. O si se intenta ver un listado de los ficheros de un sistema, el rootkit hará que se muestre esa información pero ocultando la existencia del propio fichero del rootkit y de los procesos que esconde.

Cuando el antivirus haga una llamada al sistema operativo para comprobar qué ficheros hay, o cuando intente averiguar qué procesos están en ejecución,   
el rootkit falseará los datos y el antivirus no podrá recibir la información correcta para llevar a cabo la desinfección del sistema.

Además, los rootkits presentan un problema añadido: **no son códigos que se propaguen por sí solos**. Si un rootkit está en un sistema es porque ha sido introducido directamente, no porque se haya propagado a través de Internet como un gusano tradicional. Así, es muy posible que un determinado rootkit esté pensado y diseñado **para un sistema concreto**, no para una generalidad de ordenadores. Sus funciones y características dependen del sistema atacado, una solución hecha a medida para llevar a cabo acciones maliciosas en un determinado sistema.

**Los rootkits y los antivirus**

Con esta característica, los creadores de antivirus se encuentran con la inmensa dificultad de detectar un código que es difícil conocer. No hay propagación, por lo que **no pueden obtenerse muestras** del mismo, y su análisis se vuelve prácticamente imposible, puesto que además en el propio sistema afectado no se puede conseguir información sobre el rootkit, ya que él mismo se oculta.

En diversos medios han aparecido informaciones alertando sobre la gran peligrosidad de estos programas, y no les falta razón. El riesgo es muy elevado, y las consecuencias que generan pueden ser muy graves.

En primer lugar, para que un rootkit infecte un sistema, debe primero instalarse. Y mientras no se demuestre lo contrario, en lo ordenadores actuales para instalar un programa (sea un rootkit o un lector de correo electrónico) **debe copiarse** una serie de ficheros a un dispositivo de almacenamiento. Es decir, hay que utilizar el disco duro del sistema para introducir los ficheros del rootkit.

Desde hace muchos años, los antivirus vigilan la actividad del disco duro como principal mecanismo de defensa contra códigos maliciosos. Cara fichero que se guarda en el disco es analizado por el antivirus, y si se detecta una amenaza es eliminada. Así, si el rootkit es conocido, un antivirus sin grandes alardes técnicos puede al menos detectarlo, y en muchas ocasiones, además eliminarlo.

Pero tal y como comentábamos más arriba, los rootkits pueden ser **ejemplares únicos**, desarrollados en exclusiva para una máquina en particular. Esto impide claramente que los antivirus puedan tener un conocimiento previo del programa y listarlo entre las firmas de identificación de código malicioso.

E incluso podríamos llegar a pensar en un rootkit que no hiciera uso del disco duro, tal y como pasaba con el gusano SQLSlammer. En ese caso fracasarían estrepitosamente las soluciones de protección clásicas, como de hecho sucedió con el mencionado gusano. Por tanto, es necesario un sistema que vigile no se limite a vigilar la actividad de los ficheros en el disco, sino que vaya más allá. En lugar de analizar los ficheros byte a byte, debe vigilarse lo que hacen al ejecutarse.

**Las tecnologías preventivas**

Un rootkit necesita llevar a cabo unas tareas que podríamos considerar “**típicas**”, como adquirir derechos de *root*, modificar llamadas básicas al sistema operativo, falsear sistemas de reporte de datos del sistema… Todas estas tareas, una a una, entrañan poco peligro. Pero todas juntas, llevadas a cabo por el mismo programa, nos dan información clara de que algo extraño está pasando en el ordenador.

Si tal y como decíamos antes, las soluciones antivirus fracasan definitivamente a la hora de detectar un rootkit, las nuevas tecnologías de detección de amenazas por comportamiento tienen su mejor prueba de eficacia en la detección y bloqueo de rootkits. Estas tecnologías no basan su funcionamiento en condicionantes previamente aprendidos sobre patrones cerrados de identificación de amenazas. Su éxito se basa en la **investigación inteligente y automática** de la situación de un proceso en un ordenador.

Cuando una serie de acciones se llevan a cabo sobre el sistema y todas ellas (o, al menos, alguna) pueden suponer un**riesgo para la integridad** de la información o el correcto funcionamiento de la máquina, se evalúan una serie de factores que sirven para calificar la peligrosidad de esas tareas Por ejemplo, que un proceso quiera tomar derechos de administración en un sistema puede ser más o menos habitual. E implica un cierto riesgo, sin duda, pero no hay que alertar por ello. Un simple instalador para un juego puede necesitar solicitar derechos de administrador para poder llevar a cabo las modificaciones necesarias y poder ejecutarse correctamente.

También puede suceder que un determinado proceso deba permanecer oculto, ya que no existe posibilidad de interacción, o que un determinado proceso abra un puerto en concreto para comunicarse, o que registre pulsaciones de teclas. Pero todas esas características juntas hacen que el proceso se pueda considerar como una amenaza y sea necesario un análisis es profundidad para poder autorizar la ejecución de manera segura.

En este momento es cuando las tecnologías preventivas entran en acción, ya que su misión es precisamente **vigilar los procesos y evaluar la peligrosidad** de los mismos. En caso de que sean realmente dañinos, lo bloquearán y enviarán una muestra para su análisis.

**Desinfección de rootkits**

A pesar de lo que viene diciéndose, los rootkits**pueden eliminarse**, aunque no tan fácilmente como un “Viernes 13”. Tal y como hemos dicho, los rootkits se autoprotegen escondiéndose y evitando que ningún otro proceso (como un antivirus) pueda detectarlos. Pero para que ese proceso pueda ocultarse, debe estar en funcionamiento y activado en memoria.

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 CD. Así, si el rootkit es conocido, podrá eliminarse.

Sin embargo, si el rootkit no es conocido (es decir, si ha sido desarrollado específicamente para un sistema concreto), cualquier antivirus fracasará. Entonces, el problema informático es casi el menos importante: hay una persona que, intencionadamente, quiere hacer daño a su empresa y se ha molestado en entrar en el sistema para perjudicarle.

En este caso es necesario, además de una investigación policial, poder contar con un proveedor de seguridad que disponga de medios suficientes como para llevar a cabo una**investigación forense**sobre un disco y poder detectar y eliminar el rootkit.