DRAFT

IT Consultores **Diciembre, 2009**

Algunas cosas que debe conocer sobre RootKits.

(Condensado del documento 10 (+) cosas que debe conocer sobre RootKits.)

Rootkits son amenazas altamente complejas y siempre cambiantes lo cual hace difícil de entender con exactitud a que nos estamos enfrentando. Son posiblemente las peores armas que el Cibercrimen emplea ya que como veremos, sus alcances significan sin lugar a dudas "ceder" el control de nuestros sistemas… sin saberlo.

Para aprender un poco, miremos algunos puntos sobre ellos…

1. Que es un RootKit.

Separando el término *rootkit* en sus dos palabras componentes: root – kit, podemos visualizar la major manera de definirlo . *Root* es un término del ambiente UNIX/Linux utilizado para definir a un usuario equivalente al (para algunos conocido) … Administrador en Windows. (!!) El término *kit* denota <programas>. .. los cuales permiten a alguien tener acceso del nivel root/Administrador en una computadora o Servidor, al ejecutar los programas contenidos en el Kit.

Atención: ...todo lo anterior puede ser hecho sin el consentimiento o conocimiento del usuario real o propietario del sistema!!

2. Porqué y para que usar un RootKit.

Un RootKits tienen dos funciones: Comando/Control remoto (backdoor) y Software -furtivo-. Un RootKit permite a alguien -legítimo o nó- controlar una computadora/server con derechos de administrador : Accesar o visualizar bitácoras (logs), monitorear la actividad del usuario, ejecutar archivos de cualquier tipo y mas aún, cambiar la configuración de un sistema.

Como vemos, un RootKit es de las peores amenazas que pueden afectar la vulnerabilidad de nuestros sistemas ya que significa tanto o mas derechos que sus usuarios propietarios; En un sentido estricto, incluso versiones VNC (Virtual Network Computing) son consideradas como RootKit. Esto podría sorprender a algunos que piensen que todo RootKit es malware ya que un VNC es una herramienta mas en ambiente de TI sin embargo, la característica de Controlar remotamente un sistema lo ubica como tal en el mundo de los sistemas de seguridad ya que un sistema que funja como cliente VNC, de caer eventualmente en manos no autorizadas sería un medio para ejecutar acciones maliciosas.

Un caso famoso (o infame según puntos de vista...) de uso de RootKit fue hecho por Sony BMG en su intento de prevenir violaciones al copywright. Sony BMG no notificó a ninguno de sus clientes que estaban colocando software DRM en algunas computadoras personales a manera de monitorear el uso de CD´s de audio/video. Como ejemplo de que tan bueno fué su software, podemos decir que <ninguna> aplicación antivirus/Antispyware logró detectarlo...

3.Propagación 4. Tipos 5. Síntomas 6. Polimorfismo 7. Detección/Remoción (?)..10(+)

Un RootKit no se auto***propaga***; para esto por lo general lo hace formando parte de una mezcla o coctel de amenazas (Blended Treats) que se ubican en redes sociales (Facebook, Hi5, etc) entre otros...

Sobre ***tipos***, hay desde el menos difícil de detectar (User-Mode RootKit) hasta los mas sofisticados del tipo Firmware (Usa el Firmware de tarjetas periféricas como video, Ethernet, etc) hasta los virtuales...

Un RootKit implica un trabajo duro aún para un experto; esto es debido a que por su diseño es difícil determinar si tenemos un sistema con uno de ellos rondando por allí. Con todo, hay ciertos ***síntomas*** observables que nos pueden ayudar...

Sumado a lo anterior y a pesar de que el ***polimorfismo*** no es un tópico específico de un RootKit, se aprovecha del mismo para "mimetizarse" en un sistema. Muchos de ellos instalan su propio antivirus para confundir aún mas...

Detección/Remoción: Si bién hay aplicaciones que nos ayudan a esta tarea, en general y para los tipos mas sofisticados casi podríamos decir que no hay garantía de remoción. (Hay divergencia en este tema)...

El documento completo forma parte de nuestros programas de entrenamiento a manera de ayudarle a establecer un sistema de seguridad y control basado tanto en el soporte tecnológico, como en la <culturización> del recurso humano el cual es pieza clave o fundamental para el éxito de un programa de Seguridad en su Departamento de Tecnología de la información. Hace poco una nota en un medio de Internet decía: ... ""Hay una mentalidad global que tiene que ver con creer que los casos de brechas de seguridad y robo de información sólo suceden en la televisión", afirmó en entrevista el director de Investigación de la estadounidense, Bryan Sartin."" cnnexpansion.com de Dic/16/2008. No vea este tópico como un costo, No lo vea como algo ajeno o lejano a sus bienes confidenciales que maneja en su sistema informático; Hoy el cibercriminal no es un tipo solitario aislado en algún cuarto en alguna parte del mundo, no Señor; Es crimen organizado cuyo blanco o target ES cualquier sistema conectado, esté donde esté geográficamente hablando.

Un término ahora usado comunmente en el ambiente de seguridad en tecnologías de la Información es: "Out in the wild"; es decir "Afuera en la Jungla" para referirse al espacio global en el cual se mueve o almacena Su Información. Precisamente porque ahora es nuestra obligación extender nuestros esquemas de seguridad ya no a nuestro mundo real cada día mas inestable socialmente hablando sino a la comunidad mundial que es Internet, en la cual el delincuente puede ser cualquier tipo en cualquier parte del planeta tocando a su puerta .

Mil gracias por su visita!!

La Seguridad no es solo un proceso tecnológico.... es un proceso organizacional!

2da Calle, 2da etapa No. 37, Jardines del Valle, 504- 50334 504-98401996
www.econsultores.biz ** email: helpdesk@econsultores.biz**