Sony, Rootkits y Gestión de Derechos Digitales ido demasiado lejos

La semana pasada cuando estaba probando la última versión de RootkitRevealer (RKR) me encontré con un análisis sobre uno de mis sistemas y se sorprendió al ver la evidencia de un rootkit. Los rootkits son tecnologías de camuflaje que oculta los archivos, claves de registro, y otros objetos del sistema de diagnóstico y software de seguridad, y generalmente son empleadas por el malware tratando de mantener oculta su aplicación (véase mi "Desenterrando Rootkits" artículo de thre edición de junio de Windows IT Pro Revista para obtener más información sobre rootkits). La ventana de resultados reportados RKR un directorio oculto, varios controladores de dispositivos ocultos y una aplicación oculta:



Teniendo en cuenta el hecho de que soy cuidadoso en mis hábitos de navegación y sólo instalar el software de fuentes confiables que no tenía idea de lo que había recogido un rootkit real, y si no fuera por los nombres de sospechosos de los archivos enumerados me hubiera sospechado RKR haber un error. De inmediato corrió Process Explorer y Autoruns para buscar evidencia de código que se activaría el rootkit cada arranque, pero me encontré vacío con ambas herramientas. Me pasó a ocuparse LiveKd, una herramienta que escribí para el interior de Windows 2000 y que le permite explorar las interioridades de un sistema en vivo utilizando el depurador de núcleo de Microsoft, para determinar qué componente era responsable de la ocultación.

Los rootkits que ocultan archivos, directorios y claves de registro o bien puede ejecutar en modo de usuario mediante parches API de Windows en cada proceso que las aplicaciones utilizan para acceder a esos objetos, o en modo kernel, interceptando las API asociadas modo de núcleo. Una forma común para interceptar la aplicación en modo de núcleo API es parchear la tabla del kernel del sistema de servicios, una técnica que yo iniciamos con Bryce para Windows en 1996 cuando escribió la primera versión de Regmon. Todos los servicios del kernel que se exporta para ser utilizado por las aplicaciones de Windows tiene un puntero en una tabla que se indexan con el número de un servicio interno de Windows asigna a la API. Si un conductor sustituye a una entrada en la tabla con un puntero a su propia función entonces el núcleo invoca la función de controlador cualquier momento se ejecuta una aplicación de la API y el conductor puede controlar el comportamiento de la API.

Es relativamente fácil de detectar la llamada al sistema de enganche simplemente volcar el contenido de la tabla de servicios: todas las entradas deben apuntar en direcciones que se encuentran dentro del núcleo de Windows, cualquier que no son funciones "parcheada". Dumping en la mesa LiveKd reveló varias funciones parche:



Hice una lista de una de las funciones interceptar y vio que era parte del controlador de dispositivo Aries.sys, que fue una de las imágenes que había visto envuelta en el directorio $ sys $ filesystem:



Armados con el conocimiento de lo que implementó el controlador de encubrimiento salí a ver si podía desactivar la capa y exponer los procesos ocultos, archivos, directorios, y los datos del Registro. Aunque RKR indicó que el \ Windows \ System32 \ $ sys $ filesystem directorio oculto de la API de Windows, es común que los rootkits para ocultar directorios de una lista de directorios, pero no para evitar un directorio oculto de ser abierto directamente. Por lo tanto, seleccionados para ver si podía examinar los archivos en el directorio oculto al abrir un símbolo del sistema y los cambios en el directorio oculto. Efectivamente, tuve la oportunidad de entrar y acceder a la mayoría de los archivos ocultos:


Tal vez el cambio de nombre del controlador y reiniciar eliminaría la capa, pero también quería ver si estaba haciendo Aries.sys más de encubrimiento por lo que se copia en un directorio uncloaked y lo cargó en IDA Pro, un desensamblador de gran alcance que utilizo en mi exploración de Windows internos. Aquí está una captura de pantalla de la AIF Pro desmontaje del código que calcula las entradas de la tabla de servicios del sistema que corresponden a las funciones que quiere manipular:



He estudiado la función del controlador de inicialización, confirmó que los parches varias funciones a través de la tabla de llamadas al sistema y vio que su camuflaje esconde código de cualquier archivo, directorio, clave del Registro o proceso cuyo nombre comience por "$ sys $". Para comprobar que hice una copia de Notepad.exe llamada $ sys $ notepad.exe y desapareció de la vista. Además de ser indiscriminada sobre los objetos que capas, otras partes del código de Aries muestran una falta de sofisticación por parte del programador. Nunca es seguro descargar un controlador que los parches de la tabla de llamadas al sistema, ya que algunos hilos, podría estar a punto de ejecutar la primera instrucción de una función enganchó cuando se descarga el controlador, si eso pasa el hilo saltará a memoria no válida. No hay manera de que el conductor la protección contra esta ocurrencia, pero el piloto de Aries descarga apoya y trata de mantener un seguimiento de si los hilos se ejecute su código. El programador no tuvo en cuenta la condición de carrera que he descrito. Van a tener que subir con un nuevo enfoque a sus rootkit más pronto o más tarde todos modos, desde la llamada al sistema de enganche no funciona en absoluto en las versiones x64 de 64-bit de Windows.

Después de que terminé estudiando el código del conductor me reinicia el sistema. El manto se había ido como esperaba y pude ver todos los archivos que hayan sido escondidos en el Explorador y claves de registro en Regedit. Yo dudaba de que los archivos tenido información de la versión, pero pasé la utilidad Sigcheck en ellas de todos modos. Para mi sorpresa, la mayoría tenía la identificación de productos, archivos y cadenas de la compañía. Yo ya había reconocido Dbghelp.dll y unicows.dll como Microsoft Windows DLL por sus nombres. Los otros archivos afirmó ser parte de la "Essential System Tools" producto de una empresa llamada "First 4 Internet":



Entré en el nombre de la empresa en la barra de direcciones de mi navegador de Internet y se fue a http://www.first4internet.com/. He buscado tanto para el nombre del producto y Aries.sys, pero se quedó vacío. Sin embargo, el hecho de que la compañía vende una tecnología llamada XCP me hizo pensar que tal vez los archivos que había encontrado eran parte de algún esquema de protección de contenidos. Busqué en Google el nombre de la empresa y me encontré con este artículo, lo que confirma el hecho de que tienen ofertas con varias discográficas, como Sony, para la aplicación Digital Rights Management (DRM) de CDs.

La referencia DRM me acuerdo de haber comprado un CD recientemente que sólo se puede reproducir utilizando el reproductor multimedia que viene en el CD sí mismo y que lo limita a un máximo de 3 copias. Yo scrounged a través de mi CD y lo encontró, Sony BMG estar bien con el Hombre (el nombre es irónico, dadas las circunstancias) CD de los hermanos Van Zant. No me había dado cuenta cuando compré el CD en Amazon.com que está protegido con el software DRM, pero si me había mirado más de cerca el texto de la página web de Amazon.com me hubiera conocido:



La siguiente fase de mi investigación sería para comprobar que el rootkit y los archivos ocultos estaban relacionadas con que la protección de CD's copia, por lo inserté el CD en la unidad y haga doble clic en el icono para iniciar el software del reproductor, que tiene iconos para hacer hasta tres CDs protegidos contra copia de copia de seguridad:



Process Explorer muestra el reproductor de Macromedia como, pero he notado un aumento en el uso de CPU por $ sys $ DRMServer.exe, una de las imágenes previamente envuelta, cuando apreté el botón de reproducción. Un vistazo a la ficha Servicios de su proceso de diálogo de propiedades muestra que contiene un servicio llamado "administrador Plug and Play de dispositivos", que es obviamente un intento de engañar al usuario ocasional que tropieza con ella en el SNAPin MMC Servicios (services.msc) en pensando que es una parte esencial de Windows:



Cerré el jugador y espera $ sys $ DRMServer de uso de CPU para bajar a cero, pero quedó consternado al ver que seguía consumiendo entre uno y dos por ciento. Al parecer, yo estaba pagando una pena de CPU desconocido para sólo tener el proceso activo en mi sistema. Lancé Filemon y Regmon para ver lo que podría estar haciendo y Filemón la traza mostró que escanea los ejecutables correspondientes a los procesos que se ejecutan en el sistema cada dos segundos, la información básica sobre la consulta de archivos, incluyendo su tamaño, ocho veces cada escaneo. Yo estaba perdiendo rápidamente el respeto de los desarrolladores del software:



Todavía tenía que confirmar la conexión entre el proceso y el reproductor de CD, así que tomé una mirada más atenta a cada proceso. Sobre la base de la canalización con nombre maneja vi cada uno de ellos se había abierto cuando miré en el explorador de procesos de manejar vista sospeché que sistema el jugador y $ $ DRMServer comunicada a través de canalizaciones con nombre y lo puse en marcha Filemón, comprobado de canalizaciones con nombre en el menú de volúmenes, y confirmó mi teoría:



En ese momento me di cuenta de manera concluyente que el rootkit y sus archivos asociados se relacionaron con el First 4 Internet buques derechos digitales del software de Sony en sus CDs. No contento de haber solapado y software escrito descuidadamente en mi sistema busqué una forma de desinstalarlo. Sin embargo, no encontré ninguna referencia a ella en el Panel de control lista de Agregar o quitar programas, ni tampoco he encontrado ningún utilidad de desinstalación o instrucciones en el CD o el primer sitio de Internet 4. Comprobé el EULA y no veía ninguna mención al hecho de que yo era de aceptar que el software puesto en mi sistema que no ha podido desinstalar. Ahora yo estaba loco.

I deleted the driver files and their Registry keys, stopped the $sys$DRMServer service and deleted its image, and rebooted. As I was deleting the driver Registry keys under He eliminado los archivos del controlador y de sus claves de registro, se detuvo el servicio de $ sys $ DRMServer y eliminar su imagen, y se reinicie. Como yo era eliminar las claves del Registro del conductor en HKLM \ System \ CurrentControlSet \ Services noté que estaban configurarse como controladores de inicio de arranque o de los miembros de los grupos enumerados por su nombre en la clave HKLM \ System \ CurrentControlSet \ subclaves Control \ SafeBoot, lo que significa que carga incluso en modo seguro, lo que hace extremadamente difícil la recuperación del sistema, si alguno de ellos tiene un error que impide que el sistema se inicie.

Cuando entré de nuevo, descubrí que la unidad de CD no figura en el Explorador. Eliminación de los pilotos han tenido las personas con discapacidad CD. Ahora estaba muy enojado. Windows es compatible con el dispositivo "filtrado", que permite a un conductor de insertarse por debajo o por encima de otra para que pueda ver y modificar las E / S peticiones dirigidas a la que quiere filtrar. Sé por mi trabajo pasado con los controladores de dispositivo controlador de filtro que si borra la imagen de un controlador de filtro, Windows no puede iniciar el controlador de destino. Abrí el Administrador de dispositivos, muestra las propiedades de mi dispositivo de CD-ROM, y vio a uno de los conductores envueltos, Crater.sys (otro nombre irónico, ya que había "cráteres" mi CD), registrada como un filtro más bajo:



Por desgracia, aunque se pueden ver los nombres de los controladores de filtro registrados en los filtros de "Alto" y "filtros de bajar" las entradas de los detalles de un dispositivo ficha en el Administrador de dispositivos, no hay interfaz de administración para eliminar filtros. Filtrar registros se almacenan en el Registro en HKLM \ System \ CurrentControlSet \ Enum así que abrí Regedit y consultado por $ sys $ en esa clave. He encontrado la configuración de la entrada inferior del filtro de la Conferencia


He eliminado la entrada, pero me salió un error de acceso denegado. Estas teclas tienen permisos de seguridad que sólo permiten la cuenta Sistema local para modificarlas, por lo que relanzó Regedit en la cuenta de sistema local usando PsExec: PsExec-s-i-d regedit.exe. Me vuelve a intentar el borrado, tuvo éxito, y consultado por $ sys $ otra vez. Siguiente He encontrado una entrada de configurar otro de los conductores, Cor.sys (internamente llamado Corvus), como un filtro superior para el dispositivo de canal IDE y también eliminado. YO ligar de nuevo y mi CD estaba de vuelta.

Toda la experiencia fue frustrante e irritante. No sólo se había puesto Sony software en mi sistema que utiliza técnicas comúnmente usadas por el malware para ocultar su presencia, el software está mal escrita y no proporciona los medios para la desinstalación. Peor aún, la mayoría de los usuarios que toparse con los archivos disfrazado con capa RKR exploración paralizar su ordenador si intentan el paso obvio de borrar los archivos ocultos.

Aunque creo en el derecho de la industria de medios de utilizar los mecanismos de protección anticopia para evitar la copia ilegal, no creo que hemos encontrado el equilibrio correcto de uso leal y la protección de copia, todavía. Este es un caso claro de Sony DRM tomando demasiado lejos.