La verdad sobre el software «congelador»

tic_pereda@yahoo.es

Fuente: **La verdad sobre el software "reinicie y restaure"**

Existe un tipo de software llamado "reinicie y restaure" (reboot and restore) que sirve para proteger la integridad de los datos de un disco duro o una partición, permitiendo que los datos permanezcan inalterables a los cambios. Una vez que el software ha sido instalado y activado cualquier modificación hecha en los ficheros se deshará en cuanto se reinicie el sistema.

En principio este sistema de protección se inventó para ser empleado en colegios, universidades, aulas de colegio, bibliotecas y centros similares para evitar que los usuarios hiciesen modificaciones al sistema operativo y así evitar que hubiese que estar reinstalándolo continuamente. En principio también resultó ser un sistema eficaz para evitar las infecciones de virus y malwares; aunque un virus infectase un sistema sólo con reiniciar bastaba para que el virus desapareciera.

❍ Lo que promete la publicidad

Son varias las compañías que desarrollan este tipo de software, siendo probablemente la más famosa Faronics y su Deep Freeze.

Por ejemplo Faronics anuncia el Deep Freeze con la siguiente publicidad:

*Faronics Deep Freeze hace a los ordenadores **indestructibles** y previene contra cambios no deseados en las estaciones de trabajo, ya sean accidentales o maliciosos.*

Returnil anuncia así su producto:

*RVS 2010 usa una avanzada tecnología anti-malware y de virtualización. Clona (copia) tu sistema operativo y crea un entorno virtual para tu PC. En vez de leer el sistema operativo nativo, un clon es leído que te permite correr tus aplicaciones y hacer tus actividades online en un entorno absolutamente aislado. De esta forma tu sistema operativo **nunca** se ve afectado por virus, troyanos, malwares y otras amenazas maliciosas.*

El resto de compañías anuncian su software en los mismos términos. La **promesa que hacen es que, pase lo que pase, cuando reinicies el sistema todo volverá a estar como antes**.

❍ El talón de Aquiles

En el año 2006, se cree que un coder chino, escribió un malware conocido como "Robot Dog". Una de las características de este malware era que hacía lo que se suponía que era imposible: sobrevivía al reinicio en las máquinas en las que Deep Freeze estaba instalado.

Desde ese año las casas desarrolladoras de software saben que existe un problema en el software de "reinicie y restaure". Marco Giulani, analista de malware que trabaja para PrevX, escribió un artículo en el que comenta:

Disk.sys is not the last driver invoked by an IRP request of reading/writing to the disk. After disk.sys has finished its job, it forward the request to next lower devices until it reaches the atapi.sys driver, which is the real responsible of communicating between the system and physical hard drives.

So, try to guess what would happen if a malware is able to communicate directly to atapi.sys, sending commands directly to this driver without following the usual chain of drivers.

Nos quedamos con la parte en la que dice: "Así que intenta imaginar qué pasaría si un malware es capaz de comunicarse directamente con atapi.sys, enviando comandos directamente a este driver sin seguir la habitual cadena de drivers".

Pues ahí está la vulnerabilidad del software de "reinice y restaure". Existe un tipo de **malwares que son capaces de comunicarse directamente con el driver atapi.sys para poder escribir a disco, saltándose el driver de filtrado** que el software de "reininice y restaure" utiliza para deshacer los cambios en disco. Probablemente exista algún método más para escribir directamente a disco.

❍ Negando la evidencia

Con este artículo se demuestra que los desarrolladores de software de "reinicie y restaure" estaban al tanto del problema. De hecho unos cuantos desarrolladores, la mayoría chinos y cuyo software se usaba en los cybercafés de ese país, abandonaron el mercado después de la aparición del malware "Robot Dog", debido a que su software era incapaz de restaurar el sistema y no dejar rastro de la infección.

Desaparecieron algunos productos pero no desaparecieron todos. ¿Qué hicieron las compañías que siguieron en el mercado? Pues básicamente **ignorar y/o negar el problema cuando se le preguntaba por él** y tratar de buscar soluciones que mitigasen el problema. Entre esas soluciones está lo que se conoce como AE: anti-execution.

La idea es que si el malware no se ejecuta no puede causar problemas. El problema de esta solución es que al final la responsabilidad recae sobre el usuario, que es quien debe decidir si ejecuta un fichero o no. Una vez que se ejecuta el fichero, es como saltar sin red porque el software de "reinicie y restaure" podría no servir para nada.

Este problema, que en el usuario recaiga la responsabilidad de decidir qué ejecuta, se agrava aún más debido a la publicidad que usan las compañías, ya que hacen pensar al usuario que está completamente (al 100%) protegido cuando en realidad no lo está. Un ejemplo de eso se puede ver aquí, en la publicidad del HDGuard. "Seguridad: 100%" dice.

❍ Haciendo pruebas

Para comprobar que el software de "reinicie y restaure" no es eficaz en absoluto he usado dos muestras de malware, una del SafeSys y otra del TDSS. Como "host OS" usé un Windows XP y como "guest OS" otro Windows XP corriendo bajo VirtualPC 2007.

En las pruebas se partía de un sistema operativo limpio, se instalaba el producto y se activaba la protección. Luego se comprobaba que la protección estaba activada borrando un fichero, reiniciando el sistema y comprobando que el fichero volvía a estar en su sitio.

Una vez hecha esta comprobación se ejecutaba el malware y se reiniciaba el sistema.

Si la protección hubiese funcionado el malware no debería estar instalado en el sistema, tras reiniciar pero los resultados mostraban que el malware seguía instalado.

Para comprobar la presencia de los malwares utilicé el DrWeb CureIt! y una utilidad específica de Kaspersky Labs para la detección del TDSS.

Todos los productos que aparecen listados a continuación fallaron el test, o sea, fueron incapaces de restaurar al reiniciar:

- Deep Freeze 7.00.020.3172
- Returnil 2010 3.1.8774.5254-REL
- Wondershare Time Freeze 1.0.0 & 2.0.0
- Windows SteadyState 2.5
  Comodo Time Machine 2.6.138262.166
- Eax-Fix / Rollback Rx 9.1 build 2695223310
- HDGuard 8
  Drive Vaccine PC Restore Plus 9.0
- PowerShadow 2.6

En esta lista se encuentra la práctica totalidad de los programas de "reinice y restaure" del mercado. **Sólo hay un producto que superó las pruebas: el Shadow Defender**.

No se sabe muy bien por qué (el autor se encuentra desaparecido) el Shadow Defender consiguió que los malwares no se instalasen en el sistema. Se desconoce si los malwares hubiesen conseguido sobrevivir al reinicio en caso de que se hubiesen instalado pero probablemente así habría sido, como pasa en el resto de productos.

Estas pruebas que yo he realizado fueron hechas por otros usuarios usando las mismas muestrad de malwares y presentando los mismos resultados.

❍ ¿Fraude?

Si las empresas tenían conocimiento del problema, ¿por qué han continuado vendiendo sus productos como un software inexpugnable, robusto y 100% seguro?

Personalmente considero que ha habido mala fe. Incluso se puede hablar de fraude ya que han vendido sus productos sabiendo que no hacía lo que decían.

Se han dedicado a ignorar e incluso negar el problema. Por ejemplo Faronics en el año 2007 respondía a la pregunta de un usuario sobre el SafeSys en los siguientes términos:

Faronics está al tanto del informe que dice que un gusano llamado "W32.SafeSys.Worn" es capaz de saltarse a Deep Freeze y otros productos de la competencia. De todas formas nosotros no hemos sido capaces de confirmar la exactitud del informe y en este momento hemos sido incapaces de reproducir estos resultados en nuestro laboratorio.

En principio incluso negaban la existencia del SafeSys.

Yo la semana pasada me puse en contacto con Faronics para preguntarles por el SafeSys y ésta fue su respuesta:

Gracias por el email; nuestros desarrolladores están investigando esta pieza de malware y en este momento no tenemos una actualización suya sobre el status de esta incidencia.

¡Es increíble! **3 años después y siguen dándole vueltas al problema** cuando cualquier persona con el Deep Freeze instalado y una muestra del malware SafeSys puede reproducir el fallo de seguridad.

❍ Soluciones provisionales

¿Existe alguna solución al problema **o los productos de "reinicie y restaure" son completamente ineficaces** contra este tipo de malwares?

Estos malwares necesitan que se los ejecute con privilegios de administrador para poder saltarse la protección de los sistemas de "reinicie y restaure". Si son ejecutados desde una cuenta LUA (Limited User Account) no podrán saltársela.

Evidentemente si se utiliza un sistema AE (anti-execution) los malwares no podrán ejecutarse. El problema es dedicir cuándo podemos confiar en un programa y cuándo no. Es posible que un programa en el que confiemos esté infectado.

Personalmente creo que la solución pasa por utilizar diferentes capas de protección (antivirus + software de virtualización y/o reinicie y restaure + anti-execution) y en último caso disponer siempre de una copia de seguridad con la que podamos restaurar el sistema. Siempre existe la posibilidad de volver a instalar el sistema operativo o restaurarlo desde una imagen pero para eso debemos ser conscientes de que estamos infectados.

*****