Simarks™ BestSafe™

White Paper

Simarks Software - cybersecurity

Índice

Simarks™ BestSafe™

Aviso Legal

Garantías

ESTE DOCUMENTO SE PROPORCIONA "TAL COMO ESTÁ" Y SE EXCLUYEN TODAS LAS CONDICIONES, REPRESENTACIONES Y GARANTÍAS EXPRESAS O IMPLÍCITAS, INCLUIDAS CUALQUIER GARANTÍA IMPLÍCITA DE COMERCIABILIDAD, ADECUACIÓN A UN FIN DETERMINADO O NO INFRACCIÓN, EXCEPTO EN LA MEDIDA EN QUE TALES DECLARACIONES DE RESPONSABILIDAD PUDIERAN SER LEGALMENTE INVÁLIDAS. SIMARKS NO SERÁ RESPONSABLE POR LOS DAÑOS INCIDENTALES O CONSECUENTES EN RELACIÓN CON EL USO DE ESTE DOCUMENTO. LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO ESTÁ SUJETA A CAMBIOS SIN PREVIO AVISO.

Simarks Software S.L.
Centro de Negocios Al Andalus
C/ Copenhague 6
28232 Las Rozas de Madrid - Spain.

www.simarks.com

Introducción

La lucha contra todo tipo de *malware* se ha caracterizado principalmente por la utilización de métodos de tipo reactivo. De hecho el nombre de "virus" se otorga precisamente porque para poder combatir las amenazas primero deben conocerse sus propiedades y sus diferentes formas de infección y propagación.

Además de los programas Anti-Virus tradicionales que se instalan en los puestos finales también se ha intentado combatir el *malware* con la llamada protección del perímetro que consiste principalmente en proporcionar inteligencia en materia de ciber-seguridad a los equipos conectados a la red (routers, firewalls, etc.) y que se encargan de la detección temprana e impedir que el *malware* penetre en los sistemas que se desean proteger.

Pero la realidad es que, independientemente de todos los recursos que se destinen a la protección y detección de las ciber-amenazas, muchas de ellas consiguen el objetivo de llegar a los sistemas finales. En especial las de tipo de *ransomware* que, aunque ya se producían desde muchos años antes, es a partir de 2013 cuando experimentan su mayor crecimiento siendo hoy en día el tipo de ciber-ataque más lucrativo y con más posibilidades de éxito.

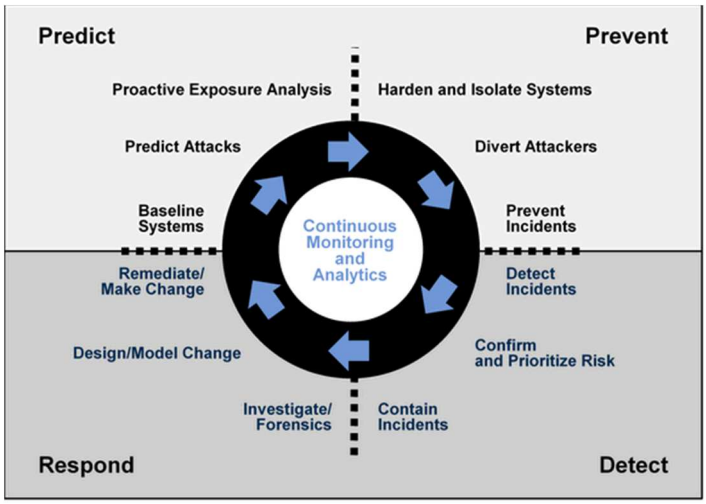
El método más utilizado por estas herramientas es el análisis y detección mediante reconocimiento de patrones heurísticos que hasta hace muy poco tiempo ofrecía unos resultados muy aceptables. Pero con la aparición del *ransomware* y las técnicas de ingeniería social este tipo de herramientas han dejado de ser efectivas y actualmente solo tienen éxito frente aproximadamente la mitad del *malware* existente en la red.

¿Qué es BestSafe™?

BestSafe es una solución modular cuya característica principal es la gestión de privilegios basada en sencillas reglas y de muy fácil aplicación que ofrece las siguientes funcionalidades:

- ✓ Gestión de privilegios a nivel de aplicación.
- ✓ Gestión de privilegios a nivel de usuario.
- ✓ Gestión de contraseñas de usuarios administradores locales.
- ✓ Estadística de uso de aplicaciones.
- ✓ Control de uso del equipo.
- ✓ Control del uso de aplicaciones.

En el informe "*Designing an Adaptive Security Architecture for Protection From Advanced Attacks*", Gartner recomienda una arquitectura de seguridad ante amenazas avanzadas y ZeroDay basada en cuatro etapas: Prevención, Detección, Retrospección y Predicción.



https://www.gartner.com/doc/reprints?id=1-279SLRJ&ct=150109&st=sb

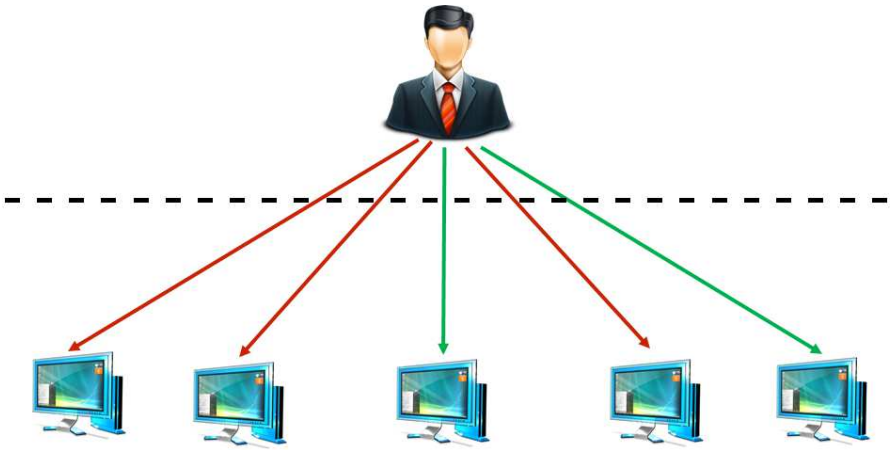
BestSafe es una herramienta que se posiciona perfectamente en la primera etapa, la de Prevención, que el informe define como: "*el conjunto de políticas, productos y procesos que deben tenerse en cuenta para prevenir los ciber-ataques. El objetivo clave de esta etapa es elevar el nivel de protección para reducir la superficie atacada y bloquear el mayor número de amenazas antes de que impacten en la organización*".

Gestión de privilegios

Dentro de una organización existen multitud de tareas administrativas que requieren de privilegios elevados para poder llevarse a cabo. La gestión de estos permisos ha sido, y sigue siendo una de las responsabilidades de las áreas de IT y Seguridad Informática más relevantes. Por otro lado, la correcta asignación de privilegios a los usuarios de un sistema ha demostrado ser una de las mejores medidas en la protección ante cualquier tipo de *malware*.

Tradicionalmente, las herramientas de Gestión de Privilegios se han especializado en dotar al personal de estas áreas de la posibilidad de realizar ésta gestión de una manera ágil y con sistemas de aprobación basadas en tickets de forma que el usuario solicita la asignación de los permisos necesarios para realizar una tarea, siendo el sistema, después de superar el flujo de aprobación, quién se encarga de otorgar al usuario los privilegios necesarios y de retirárselos cuando la autorización expira. Es decir, la asignación se realiza a nivel de usuario en un marco temporal durante el cual la exposición al *malware* sigue siendo total.

Además de ofrecer gestión de privilegios a nivel de usuario, BestSafe va mucho más allá y también es capaz de asignar privilegios a nivel de aplicación (o proceso), independientemente de los privilegios que en ese momento tenga el usuario que ejecuta la aplicación.



Con BestSafe se pueden definir, de forma simultánea:

- Listas Blancas.
  Muchas aplicaciones o procesos necesitan de privilegios de administrador para su correcta ejecución. En estas ocasiones la única opción que ofrece el sistema operativo es elevar las credenciales del usuario. Sin embargo, con BestSafe es posible asignar esas credenciales solamente al proceso o aplicación sin necesidad de otorgarle esos permisos al usuario.
- Listas Grises.
  Si, por cualquier circunstancia, es necesario otorgar permisos de administrador a determinados usuarios, con BestSafe es posible proteger a estos usuarios asignando permisos restringidos a todas aquellas aplicaciones que tengan conectividad con internet, como navegadores, clientes de correo electrónico, etc.
- Listas Negras.
  BestSafe permite bloquear la ejecución de determinadas aplicaciones y procesos que cumplan con unas determinadas reglas y ofrece la posibilidad de mostrar o no un mensaje al usuario que puede personalizarse por la organización en función de la aplicación.

Uso de BestSafe en la lucha contra el ransomware

¿Qué es el *Ransomware*?

Este tipo de ciber-amenazas se caracterizan por “secuestrar” los documentos del usuario, encriptando su contenido y posteriormente solicitando un “rescate” de una cantidad de dinero, generalmente en Bitcoins, si el usuario quiere obtener la clave con la que se han encriptado los ficheros y recuperar la información.

¿Por qué el *ransonware* está siendo tan efectivo? Hasta su aparición, la gran mayoría de las ciber-amenazas requerían que la vulnerabilidad del programa que se deseaba explotar, sobre todo navegadores y clientes de correo electrónico, se hubieran ejecutado con credenciales de usuario administrador del equipo. Microsoft asegura que más del 92% de las ciber-amenazas actuales no tienen efecto si el usuario que las ejecuta no posee credenciales de administrador del equipo.

Pero el *ransonware* no necesita de esta característica para conseguir su objetivo ya que los documentos que encripta son los documentos a los que el usuario tiene acceso, independientemente de sus credenciales de seguridad.

En Simarks utilizamos tanto técnicas de ingeniería social como análisis forense para combatir los ciber-ataques. Estos análisis se realizan en tres fases:

A. Análisis de los sistemas y vías de infección y propagación de las amenazas desde su origen. Principalmente vía correo electrónico y páginas web comprometidas.
B. Análisis del comportamiento humano cuando recibe la amenaza.
   Acciones que realiza el usuario final cuando recibe el correo electrónico o accede a una página web (abrir ficheros adjuntos, pulsar sobre enlaces, etc.).
C. Análisis del funcionamiento del sistema operativo ante el comportamiento del usuario.
   Dónde se guardan los ficheros adjuntos de correo cuando el usuario lo abre y qué aplicación se ejecuta, o qué ficheros y procesos se generan cuando se pulsa en un enlace, etc.

A través de la gestión de privilegios a nivel de aplicación y de los resultados de estos análisis, BestSafe permite confeccionar sencillas reglas de diferentes tipos, como por ejemplo:

- Ejecutar en modo restringido cualquier navegador, independientemente de las credenciales del usuario.
- Ejecutar en modo restringido cualquier aplicación del paquete de Microsoft Office.
- Si el usuario abre un documento de Microsoft Word desde el correo electrónico, asegurar que Word se ejecuta con las macros deshabilitadas, independientemente de la configuración del Centro de Seguridad. Si aun así el usuario pulsa el botón “Habilitar Contenido” bloquear cualquier proceso que se ejecute a través de las macros de Word.
- Bloquear cualquier proceso que se ejecute desde el directorio temporal del usuario dependiendo de la sucesión de procesos que se han ejecutado antes.

La confección de estas reglas se realiza de forma muy sencilla y normalmente solo son necesarias un número muy pequeño de reglas para conseguir un alto nivel de protección en toda la organización.

Estas técnicas proporcionan un excelente resultado en la fase de prevención que dan como resultado un porcentaje de amenazas bloqueadas cercano al 100%, incluido las de tipo *ransomware*.

Gestión de contraseñas

La mayoría de las organizaciones dotan a su personal de ordenadores portátiles o tabletas para realizar sus trabajos sometidos a situaciones de movilidad. En un entorno donde los usuarios no son, por regla general, usuarios administradores de sus equipos, se produce la siguiente problemática:

Si el usuario no es administrador y tiene algún problema que le impide usar el equipo no tiene otra opción que ponerse en contacto con el personal de soporte. Pero en muchas ocasiones el personal de soporte no puede conectarse al equipo por lo que se hace necesario el habilitar una cuenta de administrador local cuya contraseña debe facilitar al usuario final para que se conecte al equipo y siga sus instrucciones.

Dependiendo del número de equipos con movilidad y del tipo de usuarios, la gestión de la contraseña de estas cuentas locales genera un serio problema que lleva, en no pocas ocasiones, a establecer la misma contraseña para cada equipo, lo que se traduce en una brecha de seguridad considerable.

El módulo de Gestión de Contraseñas de BestSafe ofrece una gestión automática de la contraseña de estas cuentas y establece una contraseña diferente por día y máquina en función de una semilla corporativa que el administrador de BestSafe configura. Además, registras las modificaciones no autorizadas y la reestablece a la que le corresponda.

El personal autorizado puede obtener cualquier contraseña de cualquier equipo de la red mediante un sencillo módulo, y sin necesidad de estar conectado a la red.

Estadística de uso de aplicaciones

El administrador de BestSafe puede configurar aquellas aplicaciones (o procesos) cuyo uso en los *endpoints* desee monitorizar. BestSafe enviará un evento al correspondiente SIEM cada vez que la aplicación sea ejecutada en cualquier equipo que tenga el agente instalado.

Control de Uso del equipo

Mediante el módulo de "Control de Uso del Equipo" el administrador de BestSafe tiene la posibilidad de generar sencillas reglas para establecer en que franjas horarias un determinado usuario, o grupo de usuarios, está autorizado a conectarse a un determinado equipo, o grupo de equipos, como por ejemplo:

- ✓ Permitir el uso del equipo por un determinado usuario solamente durante las siguientes dos horas.
- ✓ Permitir el uso del equipo solamente en fines de semana.
- ✓ Permitir el uso del equipo durante 3 horas reales de conexión sin tomar en cuenta el tiempo que el usuario no lo está utilizando.

Control de Uso de aplicaciones

Mediante el módulo de "Control de Uso de Aplicaciones" el administrador de BestSafe tiene la posibilidad de generar sencillas reglas para establecer en que franjas horarias un determinado usuario, o grupo de usuarios, está autorizado a utilizar determinadas aplicaciones, como por ejemplo:

- ✓ Permitir la utilización de una determinada aplicación solamente los días laborables y solo en horario de oficina.
- ✓ Permitir la utilización de una determinada aplicación durante las próximas 2 horas.
- ✓ Permitir la utilización de las aplicaciones contenidas a partir de un determinado directorio solamente en fines de semana.

¿Cómo funciona BestSafe™?

BestSafe actúa sobre los procesos y cuentas locales del *endpoint* en el momento de su ejecución analizando si debe aplicar alguna de las reglas sobre un proceso y, en tal caso, aplica el contexto de seguridad establecido en la regla de manera completamente transparente para el usuario final.

El impacto en el rendimiento del equipo es completamente imperceptible y no requiere de elementos adicionales (servidores, bases de datos, etc.) para su funcionamiento.

Las reglas se generan con la herramienta de Administración de BestSafe.

Aunque la inteligencia de BestSafe reside en el *endpoint*, dependiendo de la edición el funcionamiento de BestSafe varía. BestSafe se ofrece en las siguientes ediciones:

Edición Empresarial. La configuración se almacena en Directorio Activo. El *endpoint* obtiene su configuración de reglas particular desde el controlador de dominio más cercano y lo almacena en la caché local. Esta edición va dirigida a organizaciones de cualquier tamaño y que dispongan de Directorio Activo. Solamente los administradores designados podrán confeccionar y aplicar reglas. La Herramienta de Administración está basada en Microsoft Management Console.

Edición Elite. La configuración se almacena en el propio *endpoint*. No obstante existe la posibilidad de conectarse al servicio de reglas de Simarks desde donde se pueden descargar tanto reglas genéricas como reglas particulares a la organización. El usuario administrador del *endpoint* puede editar y modificar las reglas. Va dirigida tanto a empresas de cualquier tamaño que no dispongan de Directorio Activo como a usuarios individuales que desean administrar ellos mismos las reglas. La edición Elite puede considerarse como la versión "*stand-alone*" de la edición empresarial.

Edición Estándar. Va dirigida a usuarios sin conocimientos informáticos y es adecuada para el uso doméstico. Las reglas se descargan del servicio de reglas de Simarks.

Integración con SIEM

Cualquier acción realizada, tanto por el usuario administrador como por el agente del *endpoint*, es enviada a un servidor de *logs* desde donde pueden extraerse todo tipo de estadísticas y realizar análisis forense. BestSafe no proporciona servicio de SIEM per se, sino que se integra con cualquier SIEM existente en la organización a través de un nombre DNS (o dirección IP) y tipo y número de puerto.

Requerimientos

BestSafe no necesita de infraestructura adicional. La Edición Enterprise solamente requiere de Directorio Activo en modo nativo. Soporta todas las versiones de Windows Server a partir de Windows Server 2003.

El agente que se instala en los *endpoints* soporta desde Windows XP hasta Windows 10, 32 y 64 bits y desde Windows Server 2008 hasta Windows 2016, 32 y 64 bits.

BestSafe™ es una solución de Gestión de Privilegios tanto a nivel de usuario como a nivel de aplicación. Nuestra tecnología innovadora permite un nuevo enfoque en la asignación de privilegios, permitiendo realizarlo a nivel de cada aplicación o programa que el ordenador vaya a ejecutar, independientemente de los privilegios que tenga el usuario que ejecuta la aplicación.

Anexo I. Ejemplo práctico de Gestión de Privilegios a nivel de aplicación.

Al iniciar la consola de administración de BestSafe™ Privilege Management se muestra una vista del Directorio Activo corporativo que incluye solamente los objetos de tipo "*computer*" y los de tipo contenedor tal y como muestra la Figura A1.

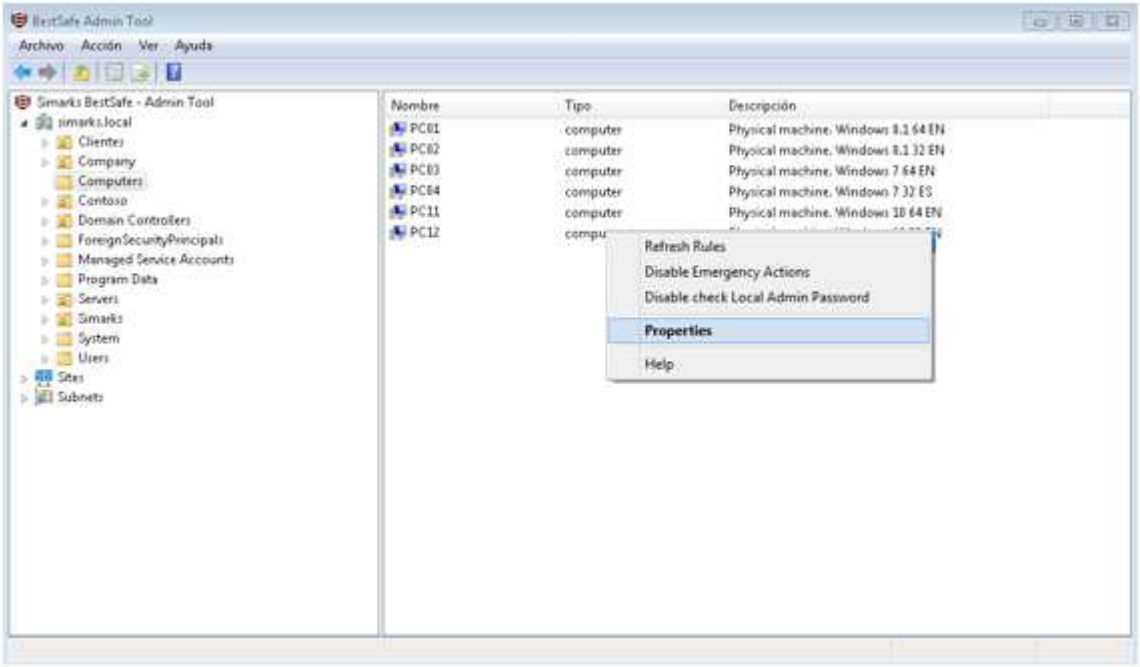


Figura A1

Al pulsar el botón derecho sobre un equipo y seleccionando la opción "Propiedades" del menú contextual se muestra la pantalla de edición de reglas. La Figura A2 muestra un ejemplo de configuración de varias reglas donde se detallan tanto las opciones globales para el objeto, como la descripción y opciones particulares para cada regla.

1) El objeto de Directorio Activo sobre el que se aplican las reglas de BestSafe™ es el objeto "computer". Las reglas se pueden asignar sobre un equipo particular, sobre un grupo de equipos, o a los equipos contenidos en los siguientes contenedores: unidad organizativa, contenedor, dominio, subred y *site*.
2) Descripción de la regla: ejecutar la aplicación "chrome.exe" de forma restringida para cualquier usuario que haga *logon (%WinBuiltinUsersSid%)* en el equipo, independientemente de las credenciales del usuario.
3) Descripción de la regla: bloquear cualquier fichero ejecutable que se lance desde el cualquier dispositivo extraíble para cualquier usuario que ha *logon (%WinBuiltinUsersSid%)* en el equipo.

4) Descripción de la regla: independientemente de las credenciales del usuario, ejecutar la aplicación Microsoft Word con privilegios restringidos para cualquier usuario que haga *logon (%WinBuiltinUsersSid%)* en el equipo.

5) Descripción de la regla: permitir cambiar la configuración del plan de energía del equipo al "Usuario1".

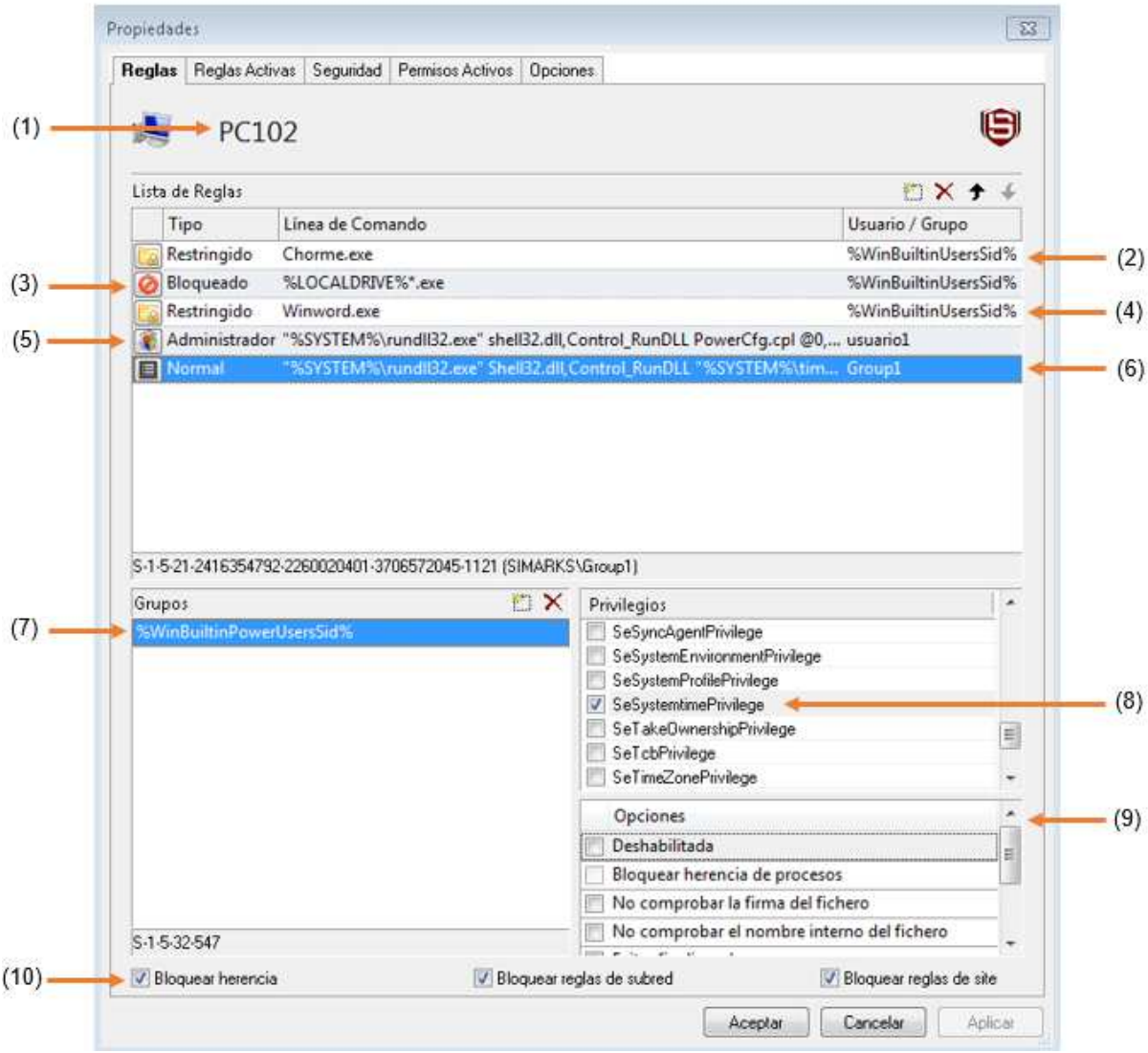


Figura A2

6) Descripción de la regla: permitir cambiar la fecha y hora del reloj del equipo a los usuarios pertenecientes al grupo "Grupo1" de Directorio Activo.

BestSafe permite una gran granularidad al confeccionar las reglas. Por ejemplo, hay ocasiones en las que no es necesario otorgar permisos de administrador sobre un proceso para realizar una tarea administrativa sino que es suficiente añadir el proceso al grupo local correspondiente **(7)** y/o asignar al proceso el privilegio Windows necesario **(8)**.

Esta regla significa: Cuando un usuario que pertenece al Grupo1 del Directorio Activo se conecte al equipo y ejecute el proceso de cambio de hora, ejecutar el proceso con las propias credenciales

del usuario añadiendo el proceso al grupo “Usuarios Avanzados” local, y asignándole el privilegio Windows “*SeSystemtimePrivilege*”.

Esta configuración es suficiente para permitir que un usuario sin privilegios pueda cambiar la fecha y hora del equipo. NOTA: “En realidad solo es necesario asignar el privilegio Windows pero se muestra aquí la pertenencia a grupos para ilustrar la capacidad de BestSafe™ de configurar el contexto de seguridad de los procesos”.

9) Para evitar la suplantación y el *tampering*, BestSafe permite que la regla solo se aplique a aquellos ficheros debidamente firmados digitalmente y/o cuyo nombre no haya sido modificado. Por defecto son de confianza los ficheros del sistema operativo, los firmados por Simarks o los firmados por una entidad certificadora en la que el equipo confíe, por ejemplo la de la propia organización.

10) Las reglas pueden ser aplicadas a un equipo directamente, a los equipos que pertenezcan a un determinado grupo de Directorio Activo, a los equipos ubicados bajo una unidad organizativa o contenedor o bien a todos los equipos de un dominio, subred o *site*.

    No obstante, es posible interrumpir la herencia de reglas marcando cualquiera de estas casillas.

Al pulsar con el botón izquierdo sobre el icono de la regla en su parte izquierda se muestra la pantalla de la Figura A3 donde es posible configurar el resto de opciones.

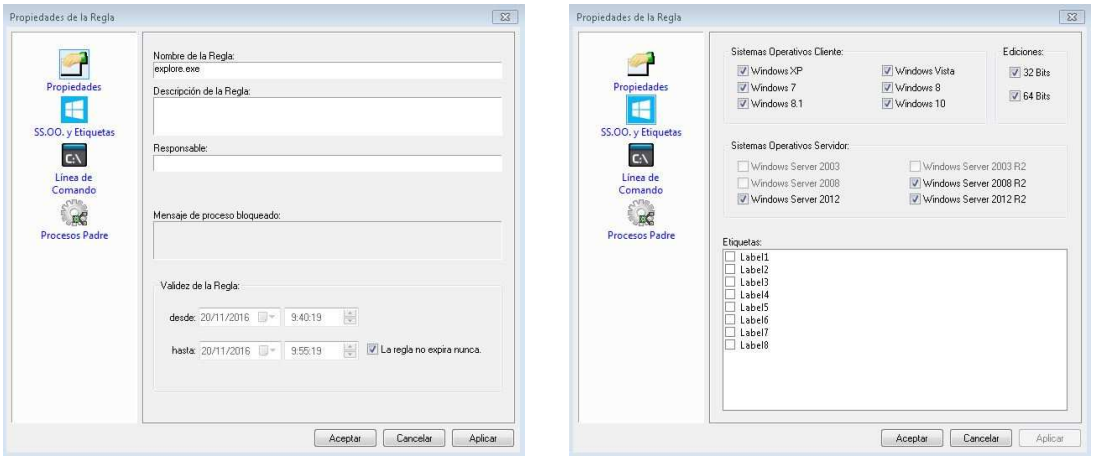


Figura A3

Además de la plataforma y la versión del Sistema Operativo para los que esta regla estará activa, se puede añadir la descripción, las etiquetas a las que pertenece la regla y, si es necesario, el periodo de validez de la regla.

La pestaña “Reglas Activas” de la figura A4 muestra el conjunto de reglas activas para un determinado equipo. Se muestran en orden jerárquico y prioridad de aplicación comenzando por las propias del equipo, los grupos a los que pertenece el equipo y seguidamente las reglas heredadas de los objetos de directorio activo superiores.

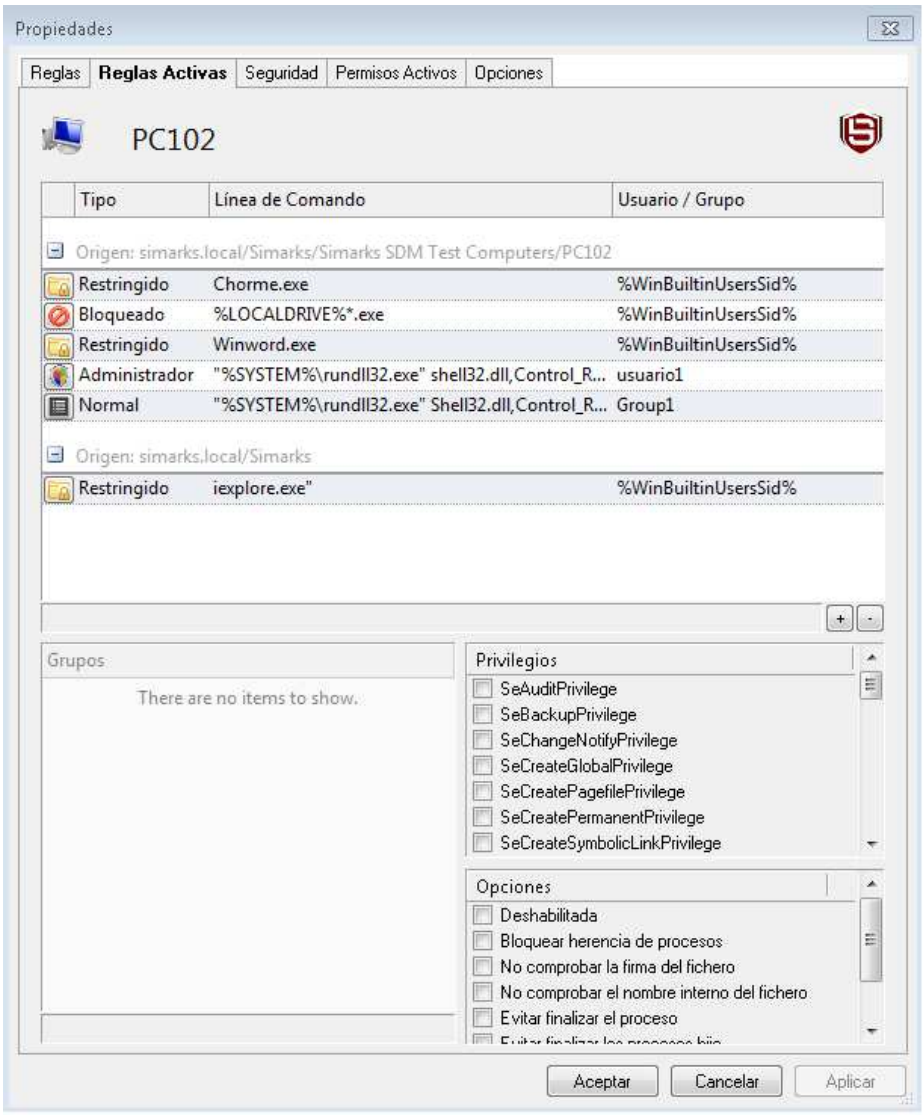


Figura A4

Simarks Software

Simarks™ Software es una compañía española especializada en el desarrollo de software de ciberseguridad y enfocada en la protección ante amenazas de tipo *ZeroDay*, amenazas avanzadas y brechas de seguridad de cualquier tipo, y en especial las que hacen uso de los privilegios de administrador.

BestSafe™ es parte de la Suite BestSafe que incluye el producto Simarks Deployment Manager (SDM™), una solución de Gestión de Aplicaciones que, a partir del núcleo de control del contexto de seguridad de BestSafe, ofrece la posibilidad de construir un "Catálogo Corporativo de Aplicaciones" dónde el usuario final, sin necesidad de otorgarle permisos de administrados, puede gestionar las aplicaciones corporativas que el administrador le haya autorizado.

Con SDM incluso es posible la construcción de un "Portal del Administrador" donde el usuario final puede realizar tareas administrativas delegadas sin necesidad de otorgarle permisos de administrador.

Simarks Software es la única compañía que, gracias a su tecnología patentada de control del contexto de seguridad, ofrece la solución integral en gestión de privilegios y aplicaciones más completa del mercado.

Oficinas Centrales
Centro de Negocios Al Andalus
C/ Copenhague 6
28232 Las Rozas de Madrid
Madrid – Spain
+34 810 526 675
www.simarks.com
info@simarks.com