SiC

Revista
seguridad en informática y comunicaciones

www.revistasic.com

Nº 98

Febrero 2012 - Año XXI

ENTREVISTAS

Joaquín Álvarez Pérez
Subdirector de Seguridad de la Información
ENDESA

Barmak Meftah
Presidente y CEO
ALIENVAULT

Laboratorio SiC
- Kaspersky BSS
- Faronics ALSB

PROYECTOS
- CAJA DE INGENIEROS
- CLOUD CERT INTECO
- ENDESA

QUÉ PREOCUPA
Cómo ser un pulpo con solo dos brazos

EN CONSTRUCCIÓN
Smartgrids: ¿privacidad asegurada?

ESCENARIOS DE NUBE
Clarity in the Cloud

EVOLUCIÓN
Cómo ser CISO hoy y no morir en el intento

SGEE Y ANÁLISIS FORENSE
Confiabilidad y evidencias-e por la vía de la normalización

ESTRATEGIA
Huawei Enterprise: un aliado en la protección de entornos TIC

El avance imparable del pago por móvil

Estrategias para una Seguridad Completa de las Estaciones de Trabajo

El número promedio de días para solucionar un ciberataque es de

14 días

Las empresas en el estudio experimentaron un ataque exitoso por empresa, por semana

—Instituto Ponemon

Un ordenador de escritorio protegido y bien gestionado puede ser un

42%

más barato

de mantener que uno no administrado

La estrategia de seguridad por capas se centra en cada nivel de amenazas potenciales, proporcionándole la tranquilidad y la seguridad necesarias para llevar a cabo sus labores diarias.

Protege Contra los ataques originados desde los equipos de los usuarios

Los días en los que una solución informática podía combatir todas las amenazas quedaron atrás. Faronics proporciona una protección a toda la empresa, sin comprometer el rendimiento del sistema. Ya sea a través de nuestra protección de restauración del sistema, o mediante la capacidad de permitir únicamente la ejecución de aplicaciones autorizadas, nosotros le tenemos cubierto.

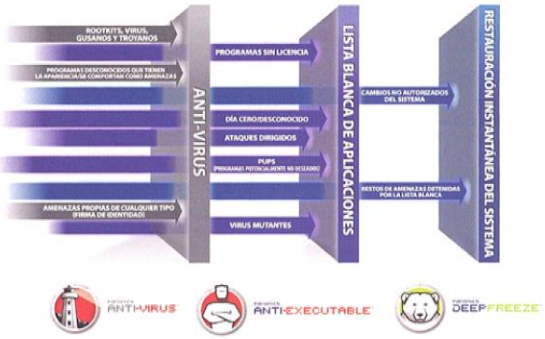
Acelera la Productividad Informática

¿Qué podría hacer su personal de TI si tuviera más tiempo? Al reducir las solicitudes de soporte informático, nuestras soluciones ayudan al departamento técnico a centrarse en los objetivos estratégicos en lugar de concentrarse en cuestiones triviales de soporte técnico que consumen tiempo. Nuestro software ayuda a reducir la degradación del sistema y mantiene los ordenadores en funcionamiento en todo momento.

Cumple con las Regulaciones

Al garantizar que únicamente las aplicaciones y los programas aprobados se ejecuten, podemos ayudarle a cumplir con las regulaciones de licencias y de cumplimiento. En caso de que sus equipos estén expuestos al acceso accidental o intencional de terceros, nuestra tecnología de restauración del sistema garantiza que los datos sensibles sean suprimidos al reiniciar, ayudándole a cumplir con los requisitos de cumplimiento normativo.

Para saber cómo proteger su negocio visite
www.esfaronics.com



FARONICS ANTI-VIRUS · FARONICS ANTI-EXECUTABLE · FARONICS DEEP FREEZE

La solución integral de tres capas de seguridad

Productos Destacados:

FARONICS DEEP FREEZE

FARONICS ANTI-EXECUTABLE

FARONICS ANTI-VIRUS

Usted puede encontrar Faronics en:

FARONICS
Intelligent Solutions for ABSOLUTE Control

Descargue gratis software de evaluación totalmente funcional en
www.esfaronics.com

España
Rosselló 255, 2n 4a 08008 • Barcelona (España)

Telf: + 34 93 415 31 15 • **Fax:** + 34 93 415 38 18

esfaronics@qualiteasy.com • www.esfaronics.com

© 1999 - 2011 Faronics Corporation. Todos los derechos reservados. Faronics Anti-Executable, Deep Freeze, Faronics Anti-Virus, Faronics Insight, Faronics Power Save, Faronics System Profiler, y WINSelect son marcas comerciales o marcas registradas de Faronics Corporation. El resto de compañías y nombres de productos son marcas registradas de sus respectivos propietarios.

Faronics ALSB *(Absolute Layered Security Bundle)*

En el presente laboratorio se identifica, examina, analiza, valora y evalúa ALSB de Faronics, una herramienta de seguridad de naturaleza software escalable, del tipo paquete de protección multi-funcional para estaciones de trabajo contra posibles ataques. Integra anti-*malware* (antivirus, anti-*spyware*, etc.), bloqueo de ejecución de ficheros ejecutables y de aplicaciones no permitidas o dañinas, y prevención de cambios de configuración no autorizados. Opera bajo la pila de protocolos TCP/IP con plataforma de sistema operativo Windows 32/64 bits y base de datos SQL. Se gestiona globalmente de forma centralizada utilizando el enfoque cliente-servidor en base a Faronics Core con filosofía multi-servidor. Soporta LDAP y Active Directory, utiliza particiones NTFS y posibilita generar informes en base al uso de componentes Loadin.

IDENTIFICACIÓN DE LA HERRAMIENTA

La herramienta de seguridad de naturaleza software ALSB *(Absolute Layered Security Bundle)* de Faronics puede catalogarse como un sistema de protección de estaciones de trabajo y sus aplicaciones. Integra las siguientes funcionalidades:
(i) Control de aplicaciones. (ii) Controlador anti-ejecución; explora posibles cambios no autorizados en el sistema. (iii) Antivirus/anti-*spyware*.

Actúa protegiendo contra diferentes tipos de *malware*. (iv) Aplicación de restauración del sistema basado en *Deep Freeze*. (v) Se gestiona de forma centralizada utilizando la *consola Faronics Core*, que permite controlar, configurar y administrar el despliegue, las actualizaciones, el mantenimiento y el estado de *Deep Freeze*.

CARACTERÍSTICAS PRINCIPALES

Las principales características constatadas son:
(1) Bloquea las aplicaciones no autorizadas o dañinas que se intentan ejecutar-instalar en las estaciones de trabajo y las elimina al reiniciar el sistema.
(2) Las actualizaciones de antivirus se guardan de forma centralizada en el *Servidor Faronics Core* y se aplican a todos los computadores en estado *Frozen* sin *Trawed*.
(3) Rastrea las aplicaciones bloqueadas, el estado de *Deep-Freeze* en tiempo real y recibe informes detallados acerca de todas las estaciones de trabajo.
(4) Utilización de una arquitectura escalable.
(5) Realiza y programa tareas-acciones sobre cualquier número de estaciones de trabajo. (6) Administración-gestión centralizada unificada basada en la plataforma *Faronics Core*.

Faronics ALSB es una herramienta software escalable de seguridad de red de buen rendimiento y con administración centralizada, catalogada como sistema multi-nivel de protección de estaciones de trabajo bajo plataforma Windows y pila de protocolos *TCP/IP*, que integra funcionalidades anti-*malware* (incluso de día cero), de prevención de ejecución de ficheros-aplicaciones no autorizados o maliciosos y protege de intentos de cambios no autorizados permanentes en la configuración.

FUNCIONALIDAD ANTIVIRUS. MODALIDADES

La *funcionalidad* antivirus (*Faronics AV*) de la herramienta aquí evaluada proporciona protección de las amenazas de seguridad sin hacer que las máquinas de computación funcionen con lentitud debido a los tiempos de análisis lentos y espacios de utilización grandes. Protege las estaciones de trabajo de amenazas como gusanos, caballos de Troya, *spyware*, *adware*, programas de seguridad de uso no honesto y *rootkits*. Se puede implantar en múltiples estaciones de trabajo a través de *Faronics Core*. Cuando se instala con *Deep Freeze*, las definiciones antivirus se pueden actualizar en las estaciones de trabajo administradas sin que sea necesario reiniciar en modo *Trawed* o en modo mantenimiento.
Se ha constatado que la *funcionalidad* antivirus se puede utilizar de los dos siguientes *modos*:
(1) *Administración de Faronics AV a través de la consola Faronics Core*. En este caso: (i) Se instala *Anti-virus Loadin*. (ii) Se implementa el cliente Anti-virus en las estaciones de trabajo. (iii) Se crean, editan, eliminan y aplica las políticas antivirus por defecto o personalizadas. (iv) Se analiza las estaciones de trabajo a través de la *consola Faronics Core*. (v) Se revisan y toman medidas acerca de los ficheros en cuarentena. (vi) Se actualizan las definiciones antivirus a través de la *consola Faronics Core*. (vii) Se generan informes.
(2) *Utilización de Faronics AV en la estación de trabajo*. En este caso: (i) Se inicia la funcionalidad *Faronics Anti-virus* en la estación de trabajo. (ii) Se realiza el análisis de la estación de trabajo. (iii) Se procede a realizar la actualización de las definiciones AV en la estación de trabajo.

FUNCIONALIDAD ANTI-EJECUTABLE

La funcionalidad *Anti-ejecutable* permite proteger las estaciones de trabajo impidiendo la ejecución de ficheros ejecutables no autorizados. Se ha constatado la imposibilidad de ejecutar ficheros ejecutables que no sean parte de la lista de ficheros denominada ***lista** blanca* que se encuentra bajo el control de los usuarios autorizados, los cuales pueden realizar operaciones como editar, modificar, eliminar, etc. Posibilita el bloqueo aunque se renombren los ficheros ejecutables o se traten de ejecutar desde dispositivos de almacenamiento extraíbles o incluso desde la red. Permite la protección de equipos locales y remotos. El acceso a la funcionalidad *Anti-ejecutable* puede ser desde la *consola Faronics Core* mediante la selección de una o más estaciones, desde la lista de estacio-

nes, o directamente desde la estación de trabajo en donde se implementó. Se ha constatado que la funcionalidad *Anti-ejecutable* puede ejecutarse en: (i) *Modo invisible*. Para evitar su detección. (ii) *Modo mantenimiento*. Si los nuevos ficheros ejecutables agregados o modificados se añaden automáticamente a la lista blanca. (iii) *Modo de ejecución* temporal. Se puede iniciar cualquier ejecutable en la estación de trabajo. Permite habilitar o deshabilitar el ratón y el teclado de una o varias estaciones de trabajo; así mismo, permite activar o desactivar la opción de registrar en el visualizador de eventos. Se posibilita activar listas blancas y negras tanto en una como en varias estaciones.

Se ha constatado que *Anti-ejecutable* puede *acceder a las siguientes fichas*: (1) Estado. Permite ver la versión instalada, así como si existen nuevas versiones disponibles; igualmente hace posible que el usuario importe y exporte configuraciones y posibilita establecer la protección *Anti-ejecutable* en los modos habilitar, deshabilitar y mantenimiento. (2) Listas blancas. Permite integrar los ficheros permitidos. Posibilita crearlas, editarlas y aplicarlas. (3) Listas negras. Incluye los ficheros no permitidos. Permite crearlas, editarlas y aplicarlas. (4) Usuarios. Permite agregar administradores, usuarios de confianza y sus contraseñas. (5) Modo ejecución temporal. Permite iniciar cualquier ejecutable en la estación de trabajo. (6) Configuración. Posibilita configurar el modo invisible, administrar el inicio de sesión, los mensajes de alerta y habilitar la compatibilidad de *Anti-ejecutable* con *Deep Freeze*.

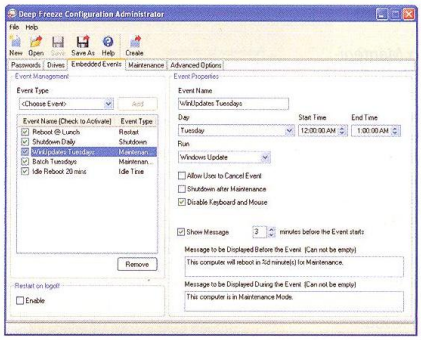


Fig. 1.- Pantalla de eventos de DF de ALSB de Faronics.

FUNCIONALIDADES DEEP FREEZE. DEEP FREEZE LOADIN. DATA IGLOO. DESPLIEGUES DF.

La funcionalidad *Deep Freeze (DF)* protege las estaciones de trabajo, restaurando a su estado original al reiniciarse. Permite eliminar los posibles daños y el tiempo de inactividad en las estaciones de trabajo, haciendo que la configuración sea resistente a la posible destrucción. Una vez instalada esta funcionalidad evita que sea permanente cualquier cambio que se haga, independientemente de si es accidental o intencionado. *Deep Freeze* protege contra cambios inevitables de configuración, configuraciones erróneas accidentales en el sistema, actividades de software malicioso y degradación debida a incidentes. Se ha constatado que *Deep Freeze* protege a los equipos que se encuentran configurados para arrancar desde el disco duro, configura el *CMOS* para arrancar solamente desde el disco duro, de modo que el *CMOS* se protege por contraseña robusta para evitar cambios no autorizados. La funcionalidad *Deep Freeze Loadin* extiende la funcionalidad de *Deep Freeze Enterprise* a *Faronics Core* y proporciona la funcionalidad de reiniciar las estaciones de trabajo en estado *Frozen* o *Trawed*. *Deep Freeze Loadin* se instala a través de la *consola Faronics Core* (un componente de *Faronics Core*). *Deep Freeze Loadin* posibilita la instalación remota del fichero de instalación de *Deep Freeze Enterprise Workstation* a través de la *consola Faronics Core* en las estaciones de trabajo.

La utilidad *Data Igloo* creada para operar con *Deep Freeze*, aunque también puede usarse independientemente sin instalar *Deep Freeze*, permite redirigir perfiles de usuario, carpetas específicas y claves de registro a una ubicación diferente de las máquinas de computación (*denominada ThawSpace*) y mantener los datos incluso después de reiniciar cuando la máquina esta protegida con *Deep Freeze*. Se ha constatado que se debe crear un *ThawSpace* en *Deep Freeze* antes de guardar los datos. También puede guardarse los datos en Unidades *Thawed* si se está utilizando *Deep Freeze* estándar. *Deep Freeze* le permite crear *ThawSpace* ocultos.

La función de redirección del perfil de usuario redirige todo el perfil de usuario a cualquier volumen *NTFS* o partición de la máquina de computación, lo cual es útil si *Deep Freeze* está instalado con objeto de retener los datos del usuario nuevos o modificados como *Favoritos de Internet*, *Mis documentos* e información del *Escritorio* incluso después de reiniciar. Se ha constatado que no es posible redirigir el perfil del usuario cuya sesión está iniciada actualmente; así mismo, todas las unidades de origen como de destino deben ser particiones *NTFS*.

Se ha constatado que *Deep Freeze* puede pasar por los *siguientes estados*:

(1) *Estado Frozen*. Los cambios realizados a la estación de trabajo se perderán cuando se reinicie dicha máquina.

(2) *Estado Thawed*. Los cambios realizados a la estación de trabajo se retendrán, incluso después de que se reinicie dicha máquina.

(3) *Estado No instalado*. *Deep Freeze* no se encuentra instalado en esa estación de trabajo. (4) *Estado Deep Freeze Seed instalado*. *Deep Freeze Seed* se encuentra instalado en esa máquina de computación.

(5) *Estado Deep Freeze está Thawed y Locked*. *Deep Freeze* se encuentra en

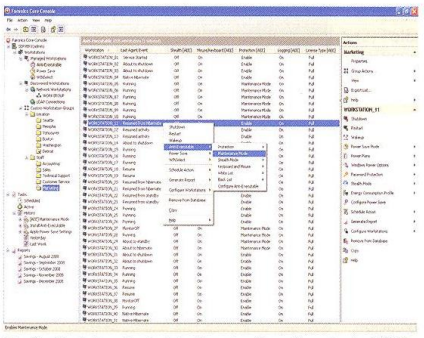


Fig. 2.- Pantalla principal de Faronics Core Console de ALSB de Faronics.

EQUIPOS UTILIZADOS EN LA EVALUACIÓN

- Equipamiento de PCs con Windows (7, XP, Vista, 2000, 2003, Server 2000/2003/2008, 2000 a 32/64 bits), con procesador Intel Core i7 a 3 GHz., con 4Gb de memoria, disco duro de 160 Gb, unidad DVD/CD-ROM, tarjeta gráfica WXGA, tarjeta NIC de red 10/100/1000/10000Base T compatible NE2000/NDIS. Navegadores Internet Explorer 7/8/9, Mozilla Firefox y Google Chrome. Servidores Directorio Activo-MS, LDAP. Microsoft .NET 2.0. Base de datos con Microsoft SQL Server 2008E/R2E.
- Nueve redes locales, Ethernet 10/100/1000/10000 BaseT con IEEE 802.2-LLC, como soporte físico de las comunicaciones con Protocolo de Control de Acceso al Medio o MAC CSMA/CD. Acceso a Internet.
- *Hubs/Switches* de 16 puertos Ethernet 10/100/1000/10000. Módems analógicos para RTB/RTC V.90/ITU-TSS (a 56 Kbps) y tarjetas digitales RDSI-BE 2B+D/Acceso Básico-BRA como acceso conmutado al exterior y conexiones ADSL/cable módem. Acceso GSM/GPRS/UMTS/HSDPA/LTE/GPS. *Routers*. Cortafuegos. IPSs, *Proxies Web*, AV, Analizadores de vulnerabilidades, VPN. Puntos de acceso Wi-Fi, IEEE 802.11g/b/a/n. Impresoras.
- Analizador de protocolos para monitorizar las comunicaciones intercambiadas en todos los niveles de la arquitectura. Módulos de valoración de mecanismos de autenticación y control de acceso. Módulos de valoración de criptoanálisis/esteganoanálisis y pruebas forenses/antiforenses para *malware*.
- Módulo de pruebas para medidas de seguridad con diferentes cargas de tráfico en la red. Baterías de ataques tipo *malware* y contra el control de acceso. Ataques a las configuraciones bajo control gestionable de cargas de tráfico. Módulos de amenazas a la gestión de la herramienta y mecanismos criptográficos utilizados. Generación de ataques al software y aplicaciones con caballos de Troya y a la implementación del software con motores de ingeniería inversa.

estado *Thawed* y el teclado y ratón se encuentran deshabilitados.
(6) *Estado Deep Freeze está en Mantenimiento*. El mantenimiento de *Deep Freeze* se encuentra en progreso.
ThawSpace, una función de *Deep Freeze*, es una partición virtual que puede utilizarse para almacenar programas, guardar ficheros o realizar cambios permanentes. Todos los ficheros almacenados en el *ThawSpace* se retienen después de un reinicio aunque la máquina de computación se encuentre en estado *Frozen*.
Se han constatado y evaluado diferentes posibles despliegues del entorno *Deep Freeze*:
(1) **Subred simple**. Todos los equipos cliente se colocan en la misma subred que el equipo de la consola. Este entorno no requiere consola remota, aunque podría utilizarse. En este caso, los clientes utilizan un mismo puerto y la consola configura una conexión de servicio local para el mismo puerto.

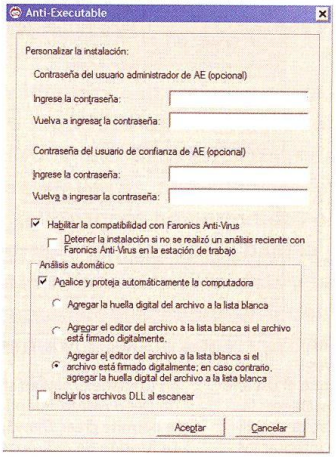


Fig. 3.- Pantalla de AE en una estación de trabajo con ALSB de Faronics.

(2) **Múltiples subredes y un servicio local**. En este entorno, los clientes se ubican en más de una subred. Sólo se utiliza una consola, no requiere consola remota aunque podría utilizarse. Tanto los clientes como la conexión que alberga la consola utilizan el mismo puerto que se configura en la ficha de opciones avanzadas. Para que los clientes estén visibles, necesitan estar configurados para utilizar una *conexión LAN/WAN*. Al seleccionar la *opción LAN/WAN* aparece el campo IP de la consola.
(3) **Utilización de múltiples puertos y acceso remoto a consola**. En este entorno, los clientes se localizan en distintos puertos. Se utiliza más de una consola. Se accede a múltiples consolas utilizando un servicio local cuyo administrador ha dado a conocer la información de conexión. El administrador ha configurado una conexión utilizando el servicio local. Si existen N puertos podremos tener (N + 1) consolas; desde una consola se podrán ver todas las estaciones de todas las subredes y habrá N consolas, cada una sólo permitirá monitorizar las estaciones de trabajo de cada subred.
(4) **Utilización de múltiples subredes y múltiples servicios locales**. En este entorno hay más de una ubicación separada (cada una usando un puerto diferente y varias subredes). Las ubicaciones se separan y sólo tienen un mínimo de conexión entre sí. Cada ubicación tiene un administrador de red que es responsable de la protección de *Deep Freeze* en esa ubicación. Las consolas remotas se configuran en cada ubicación y se utiliza un servicio local. Este entorno permite que todos los paquetes enviados desde los clientes de una ubicación se incluyan en dicha ubicación. Todas las ubicaciones se pueden administrar desde una ubicación separada-externa con única consola y permite acceder a todas las ubicaciones en base a las contraseñas de cada servicio local de cada ubicación, así como interaccionar con todos los clientes desplegados de forma distribuida.

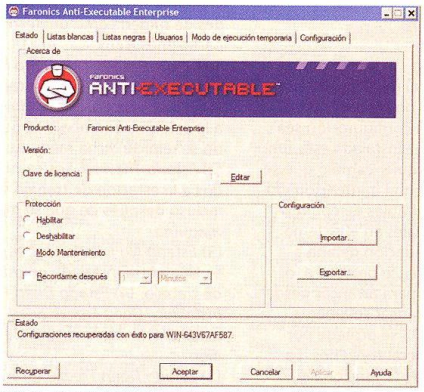


Fig. 4.- Recuperación del estado con AE de ALSB de Faronics.

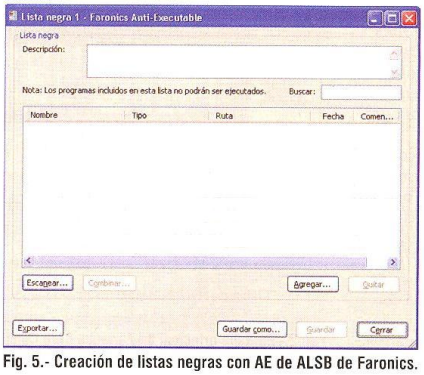


Fig. 5.- Creación de listas negras con AE de ALSB de Faronics.

COMPONENTES DE LA GESTIÓN CENTRALIZADA: FARONICS CORE. LOADINS.

La *consola Faronics Core* permite de forma centralizada y unificada la administración, monitorización, supervisión, instalación, configuración, actualización y protección de múltiples estaciones de trabajo desde un único punto de control. Permite mostrar el estado actual de las estaciones de trabajo administradas y posibilita la ejecución de comandos en una o más de esas estaciones de trabajo. Es posible ampliar la funcionalidad de *Faronics Core* instalando diferentes clases de *Product Loadins (o simplemente Loadins)*. Se trata de cargas que agregan estados, acciones e informes específicos a la funcionalidad de *Faronics Core*. Posibilita configurar y administrar diversos tipos de usuarios que pueden asignarse a diferentes grupos de acuerdo con diferentes funciones.
Con respecto a las ***funciones de usuario*** se han constatado las siguientes: (i) *Administrador*. Tiene como permisos: administrar usuarios, activar y desactivar usuarios, administrar la conexión con la base de datos, exportar la clave privada en el servidor. (ii) *Usuarios con poder*. Tienen como permisos: programar acciones, instalar-actualizar-desinstalar agentes. (iii) *Usuarios*. Tienen como permisos: apagar-reiniciar, programar acciones que ellos crearon, activar la estación de trabajo, generar informes. (iv) *Invitado*. Tiene como permisos: ver todas las estaciones de trabajo, generar informes para los *Loadins* si los hay.
Faronics Core presenta una arquitectura con los siguientes componentes:
(1) Consola Faronics Core. Constituye el nivel de interfaz de usuario; se utiliza para administrar y monitorizar los servidores centrales (*Core Servers*) y las estaciones de trabajo. Se puede conectar una instancia única de la consola *Faronics Core* a varios servidores centrales.
(2) Servidor Faronics Core. Constituye el nivel lógico que se encarga de la administración de las estaciones de trabajo, el procesamiento de tareas y la comunicación entre la consola *Faronics Core* y las estaciones de trabajo. Dentro del servidor *Faronics Core* se almacenan: (i) Credenciales *LDAP*. (ii) Configuración, incluida la conexión de la base de datos. (iii) Tareas programadas para las estaciones de trabajo. (iv) Grupos de estaciones de trabajo personalizadas a medida. (v) Comportamiento frente a acciones.
(3) Base de datos Faronics Core. Constituye el nivel de datos; almacena la lista de estaciones de trabajo y la información acerca de las estaciones de trabajo existentes. Dentro de la base de datos *Faronics Core* se almacena: (i) Usuarios y funciones. (ii) Sistema operativo de cada estación de trabajo. (iii) Dirección *IP-L3*, direc-

ción MAC-L2, dominio y subred con la máscara. (iv) Estado de la estación de trabajo e historial de eventos. (v) Lista de estaciones de trabajo.
(4) Agente Faronics Core. Se instala en la estación de trabajo; permite la comunicación entre la estación de trabajo y la base de datos.
Los niveles de *Faronics Core* son rutas de comunicación desde la consola hasta la base de datos y desde la base de datos hasta los agentes implantados en las estaciones de trabajo. *Faronics Core* implementa una funcionalidad de administración de base. Su rol principal consiste en actuar como una plataforma común para la administración de otros productos; esto se consigue instalando diferentes *Loadins*. Cada *Loadin* o carga es una biblioteca de software que agrega una nueva función específica de un determinado producto o funcionalidad *Faronics Core*. Se ha constatado que los productos-funcionalidades que utilizan *Faronics Core* constan de dos componentes principales, *Loadin* y el *Cliente* de la estación de trabajo. El *Cliente* de la estación de trabajo integra las funciones específicas existentes de un producto, instaladas en la estación de trabajo. El *Loadin* sólo se instala en el servidor *Faronics Core* y le permite administrar el *Cliente de la estación de trabajo* instalado en las distintas estaciones de trabajo.
Se han observado cuatro maneras de ampliar la funcionalidad básica de *Faronics Core* al integrar un *Loadin*:
(1) Los componentes *Loadin* agregan nuevas columnas de estado en el panel principal de la estación de trabajo. Las estaciones de trabajo que tienen ese *Loadin* instalado completan con datos específicos los valores correspondientes a esas columnas.
(2) La ventana Propiedades se invoca al hacer clic derecho en el nodo Servidor *Faronics Core* principal y seguidamente seleccionar *Propiedades*. Se ha constatado que los componentes *Loadin* pueden agregar nuevas fichas a esa ventana para la configuración general del producto.
(3) Los componentes *Loadin* agregan nuevas acciones específicas del producto, que pueden ejecutarse en las estaciones de trabajo seleccionadas.
(4) Los componentes *Loadin* agregan la capacidad de generar informes compilados de los datos informados a la base de datos por las estaciones de trabajo. Los informes generados se muestran en el nodo *Informes* en el panel *Árbol de la Consola*.
Faronics Core permite albergar múltiples componentes *Loadin* de forma simultánea y puede administrar todos los productos al mismo tiempo.

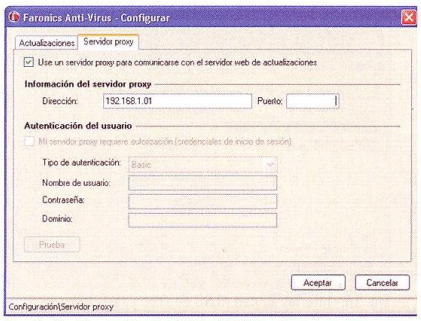


Fig. 6.- Configuración del AV de ALSB de Faronics.

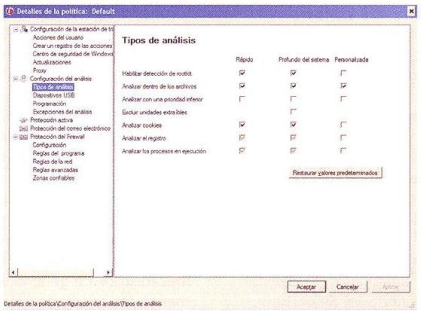


Fig. 7.- Pantalla de detalles de la política AV de ALSB de Faronics.

Fig. 8.- Interfaz AV en la estación de trabajo con ALSB de Faronics.

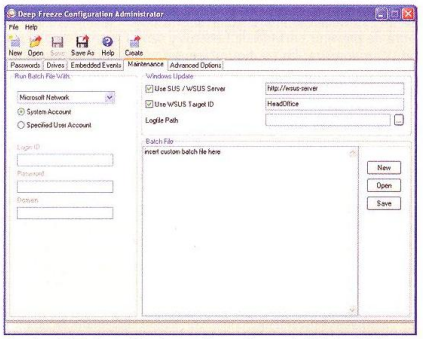


Fig. 9.- Administración de configuraciones de DF de ALSB de Faronics.

INTERFAZ DE USUARIO

Se ha constatado que los principales componentes de la interfaz del usuario de la *consola Faronics Core* son:
(1) **Panel árbol de la consola**. El nodo de consola *Faronics Core* puede tener varios nodos de servidor *Faronics Core*. El nodo de servidor *Faronics Core* contiene tres nodos principales: estaciones de trabajo, tareas e informes. Al hacer clic en uno de estos nodos se visualiza la información en el panel de resultados. El *panel árbol de la consola* tiene los siguientes *nodos*: (i) Consola *Faronics Core*. Es el nodo raíz. (ii) Servidor *Faronics Core*. Puede haber varios nodos servidor. La administración de las estaciones de trabajo, el procesamiento de tareas y la comunicación entre la consola y las estaciones de trabajo está a cargo del servidor. Existe un nodo servidor por cada conexión entre la consola y un servidor. (iii) Estaciones de trabajo. Una para cada servidor. Bajo el nodo *estaciones de trabajo* existen tres *sub-nodos*: estaciones administrativas, estaciones de trabajo detectadas y el nodo grupo personalizado de estaciones de trabajo. En este último se pueden crear e insertar grupos personalizados de estaciones de trabajo. (iv) Tareas. Una para cada servidor. El nodo tareas muestra el estado actual de todas las tareas del servidor. Una tarea se define como una acción aplicada a una o más estaciones de trabajo. Al expandir el nodo tareas se muestran tres *sub-nodos* con los posibles estados de una tarea. El nodo *Programadas* muestra las tareas planificadas que se ejecutarán en el futuro. El nodo *Activas* muestra las tareas que se están procesando. El nodo *Historial* muestra las tareas que ya se han completado. Las tareas últimas a una fecha determinada se eliminan automáticamente. Esto se puede configurar a través de la ficha servidor del cuadro de diálogo *Propiedades*. (v) Informes. Es el nodo raíz. La consola muestra los informes creados por los componentes *Loadin*.
(2) **Panel acciones**. Las acciones se aplican a las estaciones de trabajo seleccionadas y sólo se muestran si se han seleccionado una o más estaciones de trabajo. Este panel es un duplicado del menú contextual que aparece al hacer clic con el botón derecho del ratón. Se ha constatado que las principales tareas posibles desde la consola son: (i) Apagar una o varias estaciones de trabajo. (ii) Reiniciar una o varias estaciones de trabajo, de forma inmediata o posteriormente. (iii) Reactivar una o varias estaciones de trabajo. (iv) Enviar mensaje a una o varias estaciones de trabajo. (v) Desde *Faronics Core* instalar agen-

te/actualizar agente/desinstalar agente. (vi) Generar informe de una o varias estaciones de trabajo. (vii) Eliminar de la base de datos una o varias estaciones de trabajo de la lista. (viii) Exportar la lista de estaciones de trabajo en formatos *.csv* o *.txt*. (ix) Copiar una estación de trabajo para pegarla en un grupo o subgrupo de estaciones personalizadas.

(3) **Cuadro de diálogo de propiedades de la consola *Faronics Core***. Para acceder a él debe hacerse clic con el botón derecho en el icono del panel *console tree* y seleccionar *Propiedades*.

(4) **Cuadro de diálogo de propiedades del servidor *Faronics Core***. Para acceder a él se debe hacer clic con el botón derecho en el icono de *conexión del servidor* en el panel *console tree* y se selecciona *Propiedades*.

(5) **Verificación de actualizaciones**. Para verificar si hay actualizaciones se hace clic en el nodo consola *Faronics Core* y se selecciona conexión con la *URL* de *Faronics*.

(6) **Grupos LDAP**. Es posible utilizar grupos de estaciones de trabajo que ya hayan sido definidos en un servidor de directorios. Una vez instalado el agente en las estaciones de trabajo detectadas mediante *LDAP*, dichas estaciones de trabajo pueden administrarse directamente a través del nodo *Grupos LDAP*. Estas estaciones de trabajo también pueden agregarse a grupos personalizados.

(7) **Grupos de estaciones de trabajo personalizados**. Es posible agregar estaciones de trabajo a un grupo personalizado por medio de la función del *Portapapeles* de Windows. Se corta, copia o pega una estación de trabajo a un *grupo*. Para crear un grupo se hace clic con el botón derecho del ratón en el icono *Grupos personalizados* de estaciones de trabajo y se selecciona *Crear subgrupo*. Es posible agregar o editar *filtros dinámicos* a través del menú contextual o el *panel Acciones*.

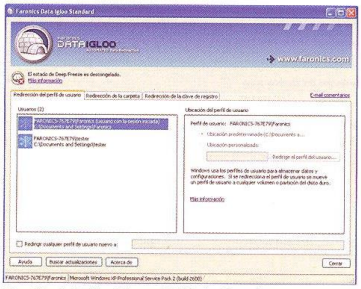


Fig. 10.- Interfaz DI con ALSB de Faronics.

CONSIDERACIONES FINALES

Se ha sometido la presente herramienta durante veinte días a un continuado y exhaustivo conjunto de pruebas y diferentes baterías de *test*, evaluándose la herramienta software con resultados globales en efectividad de protección, gestión y potencial de las funcionalidades en torno al 95,4%. Los resultados a las pruebas contra amenazas *malware* de síntesis no convencional y del día cero con tecnologías de *ocultación esteganográfica* han sido del 93,2%; los resultados de efectividad de la protección AV a las pruebas con las baterías de virus convencionales, excelentes, y los de las pruebas de los test contra cambios de configuración no deseados o no autorizados en situación de cargas de trabajo, tráfico elevado con ataques de virus han sido del 95%.

Por su parte, la valoración de los mecanismos de actualización ha sido muy satisfactoria (96,7%), al igual que los resultados de las pruebas de efectividad de los diversos mecanismos de bloqueo *anti-ejecución* (96,2%). La valoración en el nivel de gestión centralizada ha sido muy satisfactoria, destacando la flexibilidad de programación de tareas y la operativa de paneles.

Los resultados de las pruebas de rendimiento frente a cargas de trabajo y tráfico pesado han sido del 95,2%, y la valoración de los mecanismos de generación de informes ha sido del 96,2%. Finalmente, los resultados globales de protección contra las baterías de ataque frente a los diferentes despliegues *DF* (*Deep Freeze*) han sido satisfactorios (94,1%), y muy satisfactoria la valoración de las pruebas de redirección, flexibilidad e impacto (95,1%). ■

CONCLUSIONES

- **Objetivo**: herramienta de seguridad de red de naturaleza software catalogada como paquete de protección multi-funcional para estaciones de trabajo bajo plataforma de sistema operativo Windows y pila de protocolos *TCP/IP*. Integra funcionalidades *anti-malware* (incluso de día cero), de prevención de ejecución de ficheros-aplicaciones no autorizadas o maliciosas utilizando listas blancas y negras, y protege de intentos de cambios no autorizados permanentes en la configuración. Se gestiona de forma centralizada utilizando la plataforma *Faronics Core*.
- **Puntualizaciones/limitaciones**: si se desactiva un usuario las tareas programadas creadas por dicho usuario no se ejecutarán. Sólo los usuarios con derechos de administrador tienen permiso de utilizar *Data Igloo*. Si ocurre un error durante el proceso de redirección, Data Igloo volverá al estado original sin ningún cambio a los datos o la configuración. Sólo se pueden redirigir las claves del registro *hkey_local_machine* utilizando *Data Igloo*. La lista y las tareas de las estaciones de trabajo se guardan en el servidor *Faronics Core*, en cambio los informes se guardan localmente en la máquina de computación donde esta instalada la consola *Faronics Core*. Si no se ha instalado ningún *Loadin*, no es posible generar informes. Las acciones disponibles se basan en los privilegios del usuario conectado a la consola. El control de línea de comandos *Faronics Antivirus y Anti-ejecución* permite a los administradores de red una mayor flexibilidad de administración de las estaciones de trabajo al posibilitar el control a través de herramientas de administración de terceros. Los *Loadins* se deben instalar a través de la *Consola Faronics Core*. Sólo puede haber una *lista blanca* activa a la vez. No es posible agregar a la lista blanca activa los ficheros ejecutables instalados en una estación de trabajo remota, a no ser que dicha estación sea visible a través del navegador de ficheros en el diálogo *scan* de la funcionalidad *Anti-ejecución*.
- **Impacto de su utilización**: el nivel de ralentización y de utilización de la *RAM* en el proceso antivirus es muy bajo. Es posible detener los programa no autorizados y no deseados (con listas negras), que intenten ejecutarse en el sistema, al igual que el software malicioso y virus incluso polimórficos, mutantes y con ocultación atípica. Así mismo impide la instalación de dichos códigos. Proporciona escalabilidad y es simple de gestionar. Proporciona una buena celeridad en las operaciones de *escaneo* y actualizaciones. Permite encender estaciones de trabajo que incluyan placa de red con capacidades *Wake-on-LAN*.
- **Prestaciones/ventajas específicas**: permite seleccionar qué aplicaciones aparecen en la lista blanca ayudando a los procesos de cumplimiento de licencias, regulaciones y reglamentación. Es de gran ayuda a la hora de prevenir borrado de ficheros y cambios en la configuración. Herramienta con gran flexibilidad y buen rendimiento. Permite, a través de la funcionalidad *DF*, memorizar las configuraciones devolviendo al sistema al estado original con cada reinicio. El impacto en la *CPU* de la funcionalidad antivirus es poco significativo. Las capacidades de programación de tareas desde la consola son significativas y presentan un nivel de granularidad satisfactorio. Incorpora mecanismos para generar contraseñas de única vez (*OTP*).
- **Documentación**: suficiente. Utilización de ficheros *.pdf*.
- **Estructuración de la herramienta**: los principales componentes son: (i) *Anti-Virus* (Loadin/Client). (ii) *Deep Freeze (DF)* (Loadin/Client) y *Data Igloo*. (iii) *Anti-Executable* (Loadin/Client) con listas blancas/negras. (iv) Sistema de gestión centralizado *Faronics Core* (Server/Client/base de datos/Console). El destino de la herramienta son las *estaciones de trabajo* desplegadas integrando agentes *Faronics Core*.
- **Calificación final**: herramienta de seguridad escalable, de buen rendimiento, de naturaleza software, del tipo sistema multi-nivel de protección para estaciones de trabajo contra ataques y procesos indebidos. Integra múltiples funcionalidades: de antivirus (incluso del tipo tecnología *rootkit* y *spyware*), de prevención de ejecución de aplicaciones no deseadas y de protección contra posibles intentos de cambio de configuración permanente. Se administra de forma centralizada a través de la plataforma *Faronics Core* que permite gestionar la protección multi-funcional a nivel de toda la empresa. Incluye un cuidado proceso de actualización antivirus en combinación con *Deep Freeze*. Posibilita generación de informes grupales y selectivos a medida por nivel de defensa. El *proceso de actualización* de *firmas de virus* es de al menos dos veces al día. Incluye un proceso de escaneo de *dispositivos USB* automático a su conexión. Posibilita un proceso de planificación de escaneo y configuración utilizando políticas que se aplican a las estaciones de trabajo de forma centralizada. *Deep Freeze* incluye contraseñas de única vez como mecanismo que impide el uso no autorizado de la consola. Permite desplegar *Deep Freeze* de forma flexible dependiendo de las particularidades de la organización, incluso en múltiples ubicaciones, cada una con varias subredes, así como con múltiples servicios locales.

EQUIPO DE EVALUACIÓN

Prof. Dr. Javier Areitio Bertolín
Catedrático de la Facultad de Ingeniería.
Director del Grupo de Investigación Redes y Sistemas.
UNIVERSIDAD DE DEUSTO