VENOM, UN FALLO DE SEGURIDAD MÁS PELIGROSO QUE HEARTBLEED QUE COMPROMETE MILLONES DE SERVIDORES

Fuente: http://www.redeszone.net/
Artículo complementado de acuerdo a investigaciones realizadas por Itech SAS
NOTICIA POSTEADA EL 14 de MAYO de 2015

Cada vez es más habitual utilizar servidores alquilados para realizar ciertas tareas, por ejemplo, almacenamiento de datos en la nube o computación. Esto se debe al bajo precio que supone alquilar un servidor en un centro de datos respecto a lo que costaría alquilarlo y mantenerlo personalmente, sin embargo un aspecto que no debemos olvidar es la seguridad de la información que procesamos ya que al igual que podemos acceder al servidor de forma remota otros usuarios no autorizados también podrán.

Esto es habitual con clientes que por el precio toman servidores virtualizados en empresas colombianas y del exterior de hosting económico pero no saben que su página está compartiendo disco virtual con 700 o 800 o hasta 1.000 dominio más.

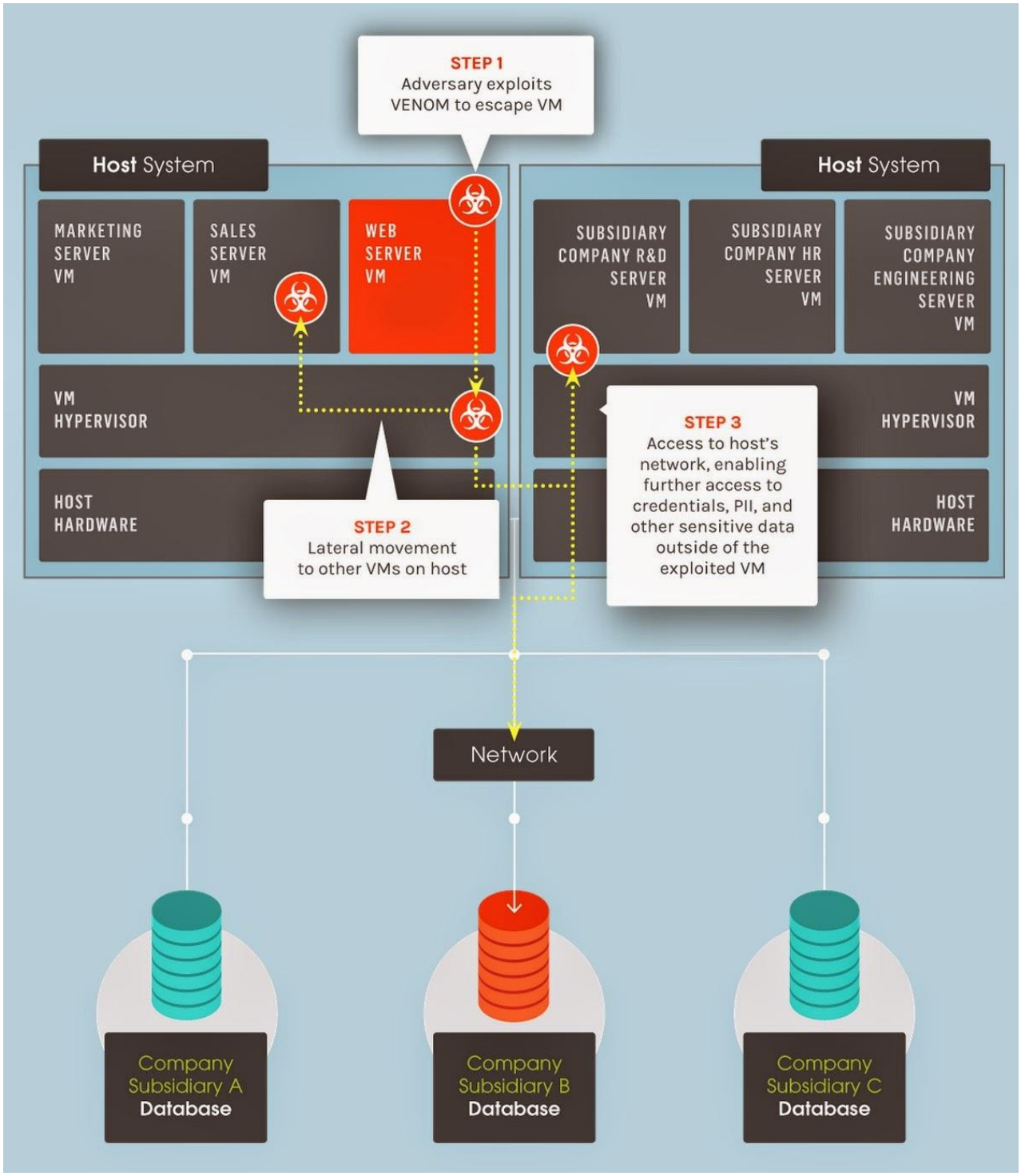
Heartbleed ha sido una de las peores vulnerabilidades a las que se han visto expuestos la mayor parte de los servidores de Internet. Este fallo de seguridad en el módulo OpenSSL permitía recuperar información de la memoria del servidor de forma remota, incluso sin tener permiso de acceso al mismo.

Millones de servidores de todo el mundo se han visto expuestos a esta vulnerabilidad hace ya varios meses, sin embargo, hace algunas horas ha aparecido en la red un nuevo fallo de seguridad que probablemente suponga un peligro aún mayor para los servidores de todo el mundo: VENOM.

QUÉ ES Y CÓMO FUNCIONA VENOM

VENOM es un acrónimo de **Virtual Environment Neglected Operations Manipulation**. Este fallo de seguridad lleva presente en los servidores más de 11 años y permite a un usuario que lo explote correctamente y salir de los límites de una máquina virtual (en un centro de servidores, por ejemplo) y llegar a ejecutar código en la máquina real, acceder a otras máquinas virtuales del mismo servidor e incluso acceder a otras zonas de la red de datos.

A continuación dejamos un gráfico donde se explica cómo funciona la vulnerabilidad y un ejemplo de lo que podría pasar si se explotase en una red de servidores de una gran empresa.


STEP 1
Adversary exploits VENOM to escape VM
Host System
MARKETING SERVER VM
SALES SERVER VM
WEB SERVER VM
VM HYPERVISOR
HOST HARDWARE
Host System
SUBSIDIARY COMPANY R&D SERVER VM
SUBSIDIARY COMPANY HR SERVER VM
SUBSIDIARY COMPANY ENGINEERING SERVER VM
VM HYPERVISOR
HOST HARDWARE
STEP 2
Lateral movement to other VMs on host
STEP 3
Access to host's network, enabling further access to credentials, PII, and other sensitive data outside of the exploited VM
Network
Company Subsidiary A Database
Company Subsidiary B Database
Company Subsidiary C Database

El responsable directo de este fallo de seguridad es el controlador de "floppy" o "disquetes" que permite utilizar estos obsoletos dispositivos de almacenamiento en las máquinas virtuales. Una vez más, un software obsoleto que no debería estar presente en los servidores actuales ha sido el responsable de comprometer la seguridad de más del 95% de los servidores de todo el mundo.

CÓMO PROTEGERSE DE VENOM

Los principales sistemas operativos que se han visto afectados por este fallo de seguridad son:

RHEL (Red Hat Enterprise Linux) 5.x/6.x/7.x

CentOS Linux 5.x/6.x/7.x

OpenStack 4 y 5 para RHEL 6

OpenStack 5 y 6 para RHEL 7

Red Hat Enterprise Virtualization 3

Debian y distribuciones basadas en ella.

SUSE Linux Enterprise Server 5, 6, 7, 10, 11, 12 (con sus respectivos Service Pack)

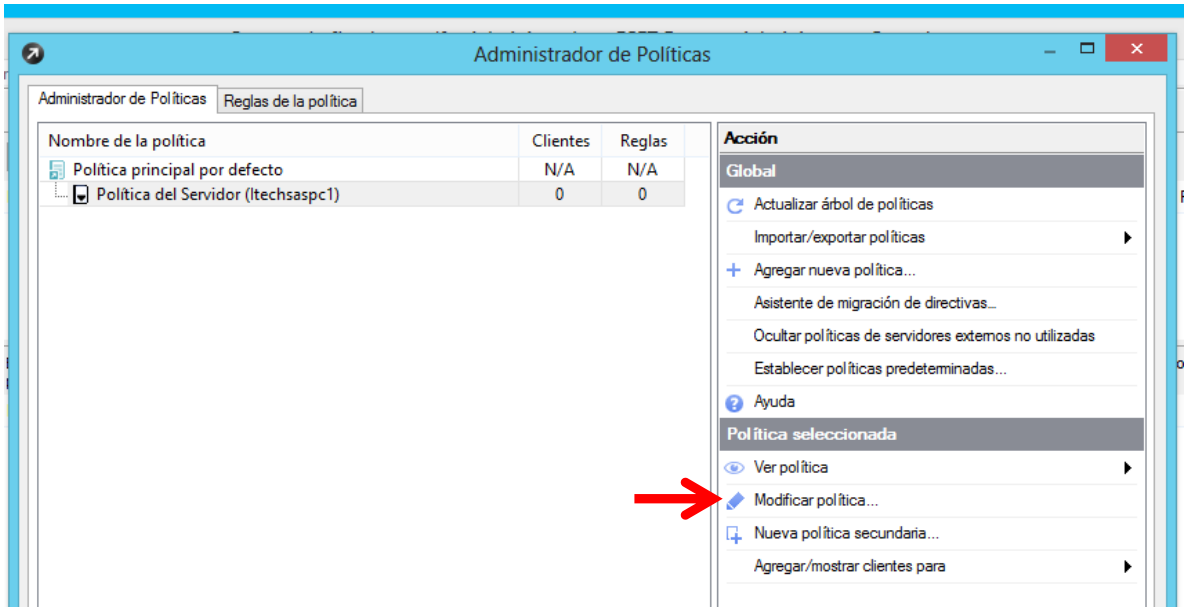
Ubuntu 12.04, 14.04, 14.10 y 15.04

Para solucionar este fallo de seguridad simplemente debemos instalar los parches de seguridad más recientes de nuestro sistema operativo tecleando el correspondiente comando (por ejemplo "sudo apt-get clean && sudo apt-get update && sudo apt-get upgrade" en el caso de Debian y Ubuntu) y actualizar si usamos VirtualBox a la última versión disponible (4.3). Cabe destacar que no es necesario reiniciar el servidor para solucionar este fallo de seguridad aunque sí habrá que reiniciar las máquinas virtuales en uso.

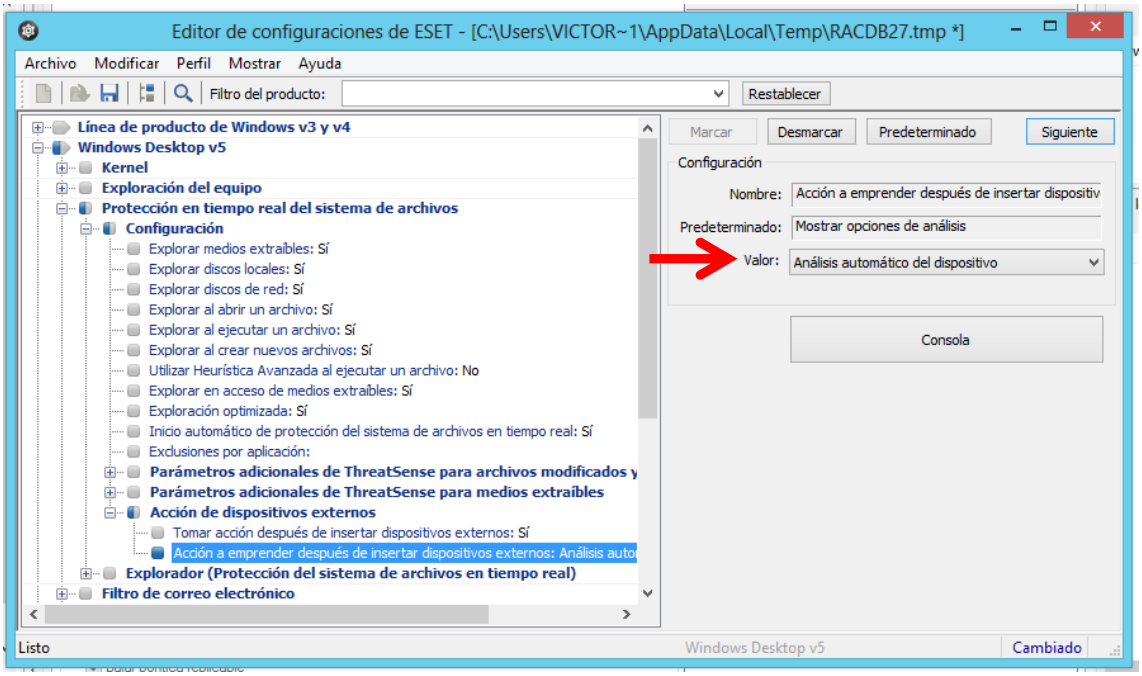
Este fallo de seguridad ha recibido el nombre de CVE-2015-3456. La vulnerabilidad sólo afecta a las máquinas virtuales creadas con QEMU, XEN, KVM y Citrix. Ni la virtualización de Microsoft Hyper-V ni la de VMWare ni BOCHS se han visto afectadas por VENOM.

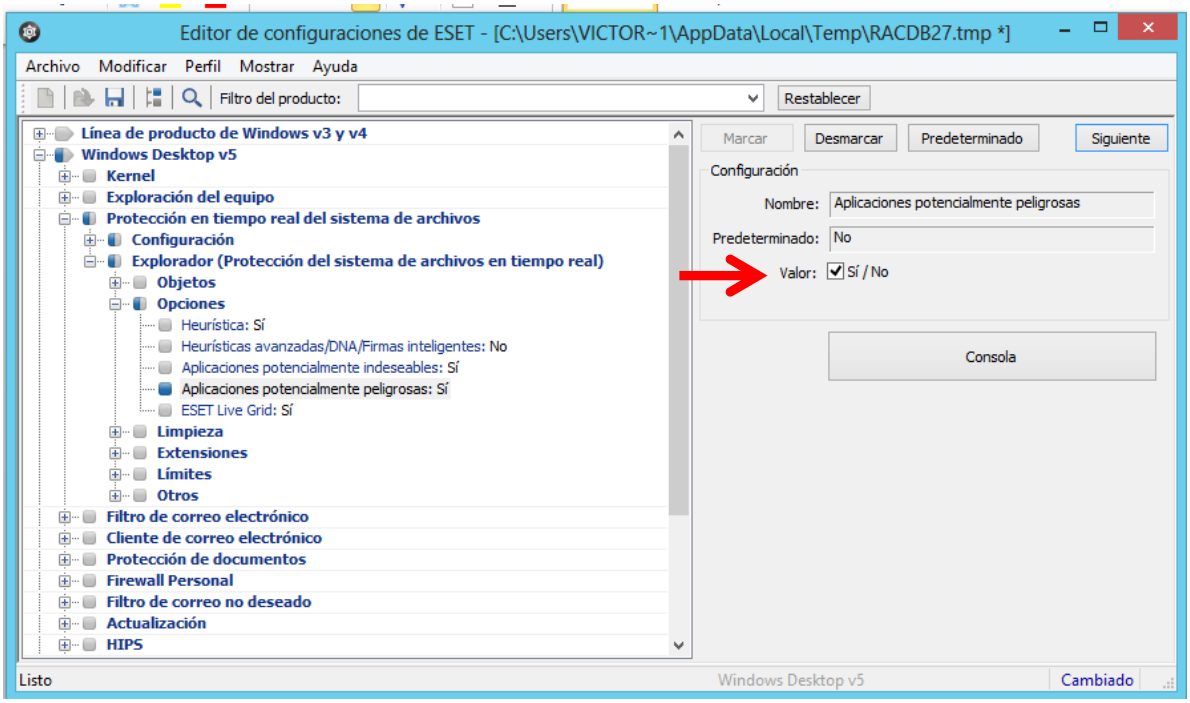
Para la protección con las aplicaciones de ESET END POINT, a nuestros clientes recomendamos que en sus consolas centrales tengan configurados todos los parámetros de detección base y de scaneo de malware en línea en los parámetros más altos. Se mostrara pantallazos que deben estar configurados en sus políticas del servidor ERAS.

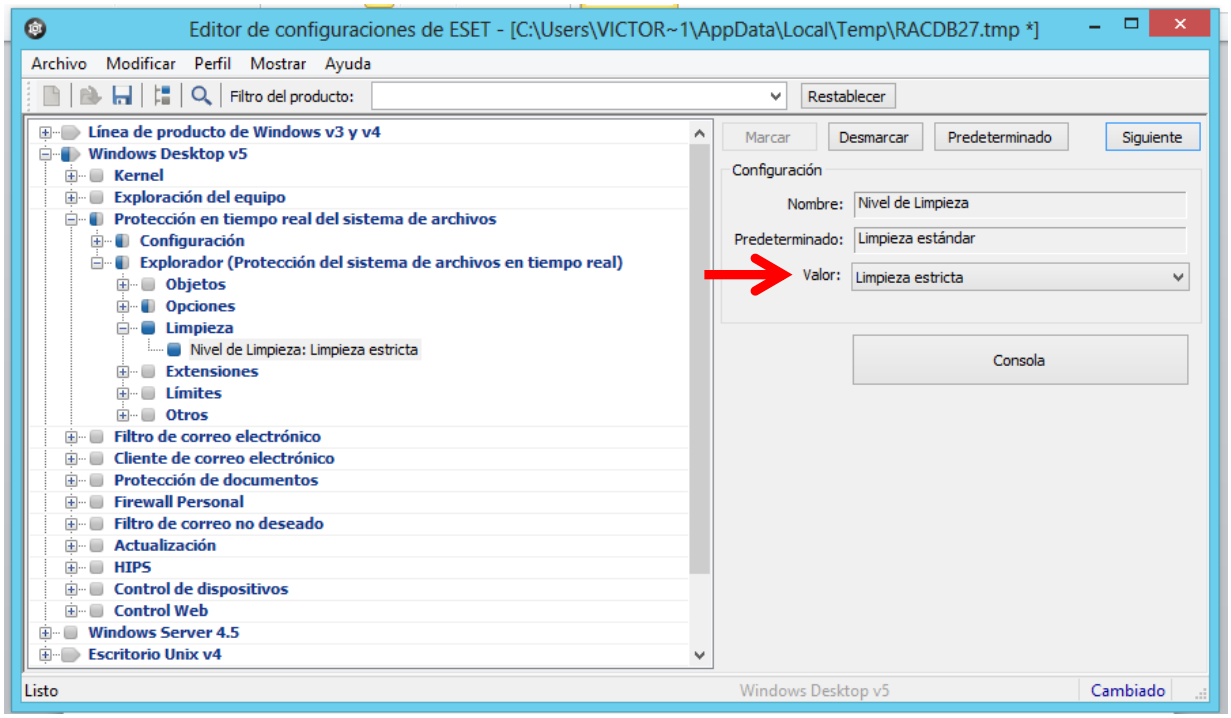
En el panel de políticas del servidor se ingresa y se da click en el árbol de opciones del lado derecho en la opción MODIFICAR POLITICA.

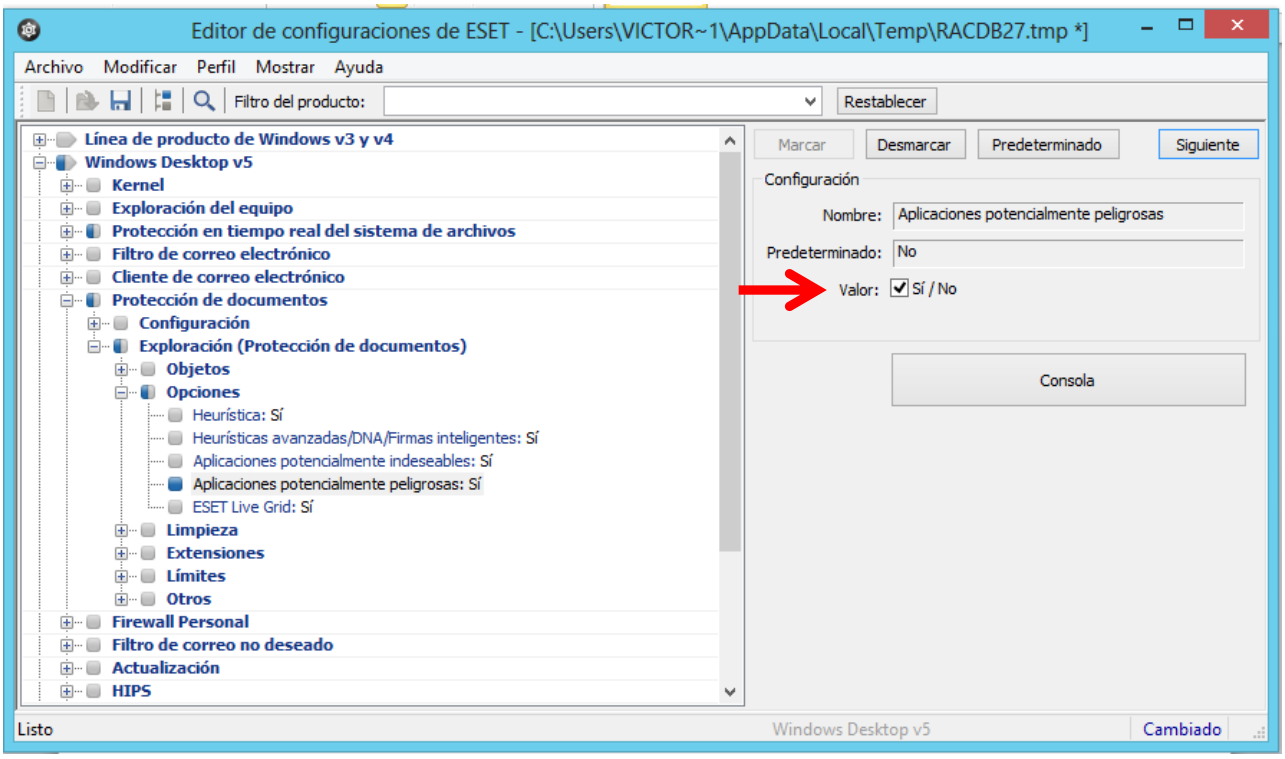


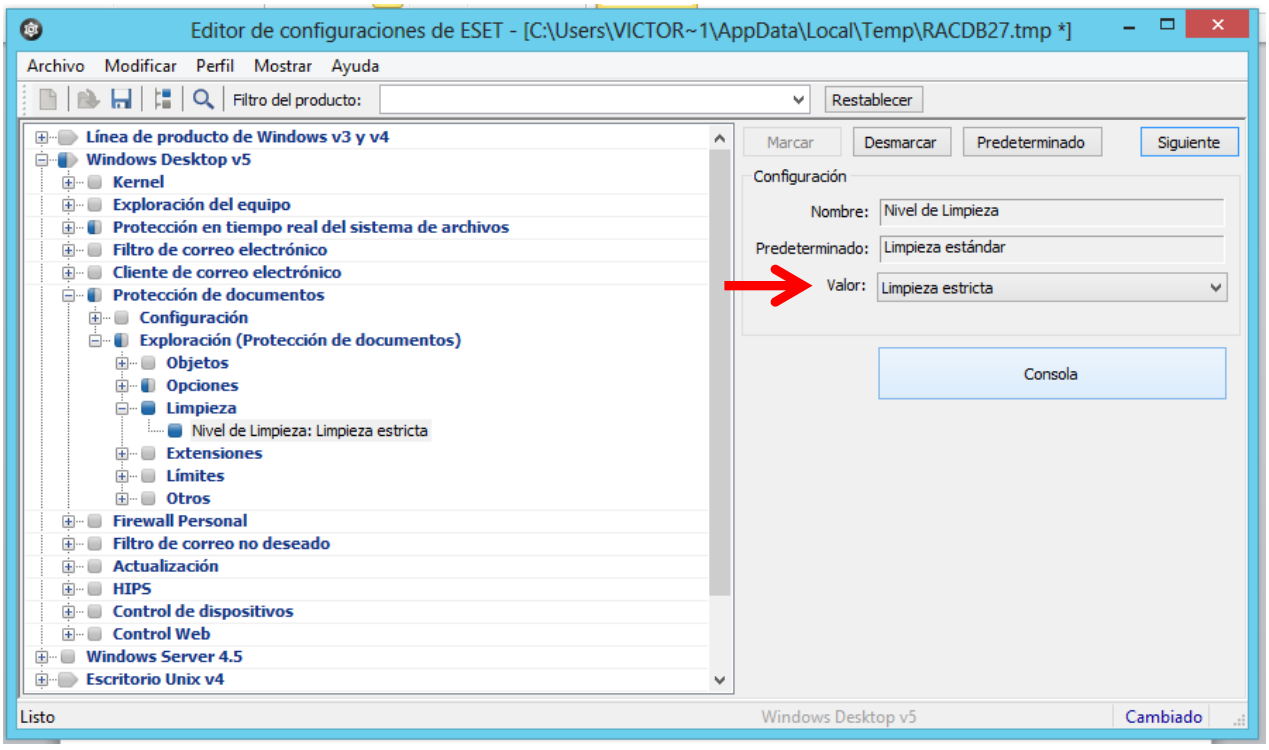
Configure las siguientes opciones en el panel de políticas del Windows Workstation y en las políticas de los servidores también, es importantísimo que este en los dos frentes.



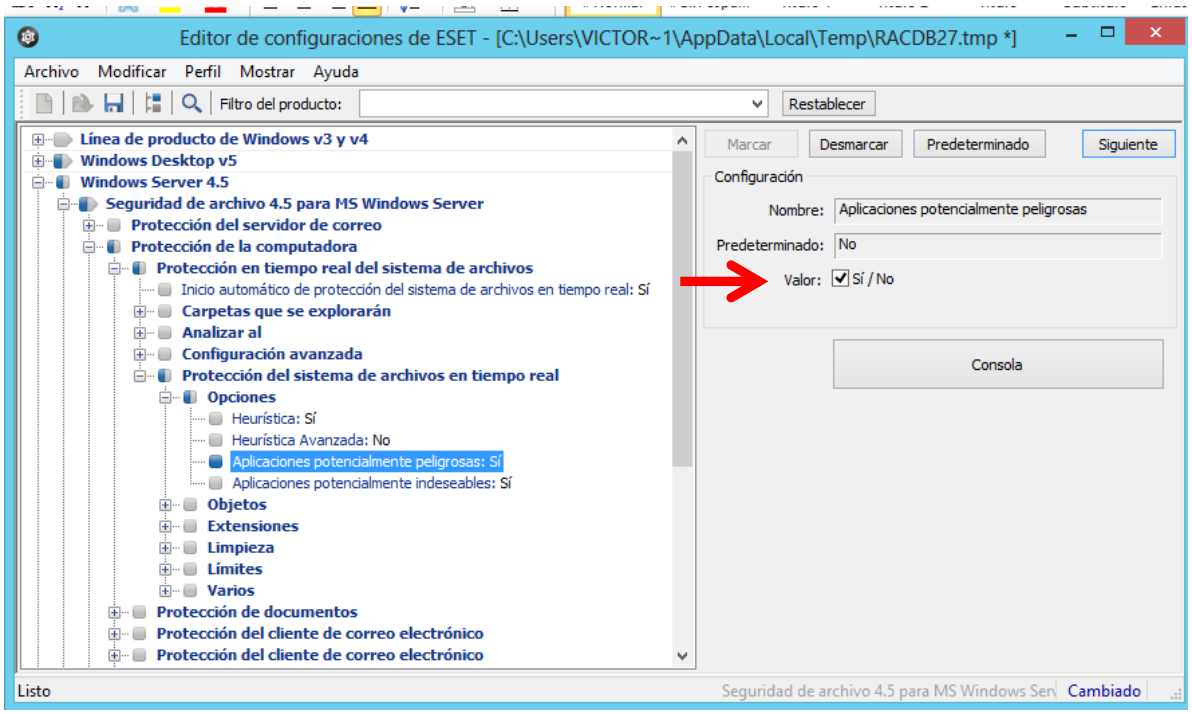

Editor de configuraciones de ESET - [C:\Users\VICTOR~1\AppData\Local\Temp\RACDB27.tmp *]
Archivo Modificar Perfil Mostrar Ayuda
Filtro del producto:
Restablecer
Línea de producto de Windows v3 y v4
Windows Desktop v5
Kernel
Exploración del equipo
Protección en tiempo real del sistema de archivos
Configuración
Explorador (Protección del sistema de archivos en tiempo real)
Objetos
Opciones
Heurística: Sí
Heurísticas avanzadas/DNA/Firmas inteligentes: No
Aplicaciones potencialmente indeseables: Sí
Aplicaciones potencialmente peligrosas: Sí
ESET Live Grid: Sí
Limpieza
Extensiones
Límites
Otros
Filtro de correo electrónico
Cliente de correo electrónico
Protección de documentos
Firewall Personal
Filtro de correo no deseado
Actualización
HIPS
Marcar
Desmarcar
Predeterminado
Siguiente
Configuración
Nombre: Aplicaciones potencialmente peligrosas
Predeterminado: No
Valor: Sí / No
Consola
Listo
Windows Desktop v5
Cambiado

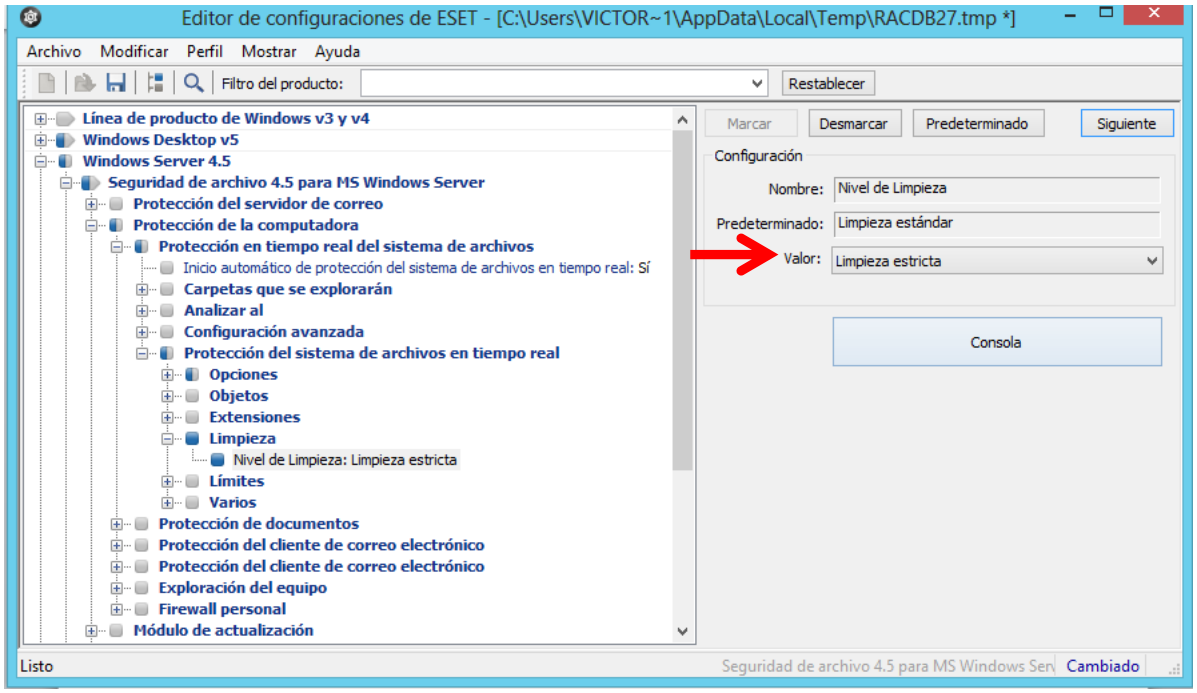

Editor de configuraciones de ESET - [C:\Users\VICTOR~1\AppData\Local\Temp\RACDB27.tmp *]
Archivo Modificar Perfil Mostrar Ayuda
Filtro del producto:
Restablecer
Línea de producto de Windows v3 y v4
Windows Desktop v5
Kernel
Exploración del equipo
Protección en tiempo real del sistema de archivos
Configuración
Explorador (Protección del sistema de archivos en tiempo real)
Objetos
Opciones
Limpieza
Nivel de Limpieza: Limpieza estricta
Extensiones
Límites
Otros
Filtro de correo electrónico
Cliente de correo electrónico
Protección de documentos
Firewall Personal
Filtro de correo no deseado
Actualización
HIPS
Control de dispositivos
Control Web
Windows Server 4.5
Escritorio Unix v4
Marcar
Desmarcar
Predeterminado
Siguiente
Configuración
Nombre: Nivel de Limpieza
Predeterminado: Limpieza estándar
Valor: Limpieza estricta
Consola
Listo
Windows Desktop v5
Cambiado

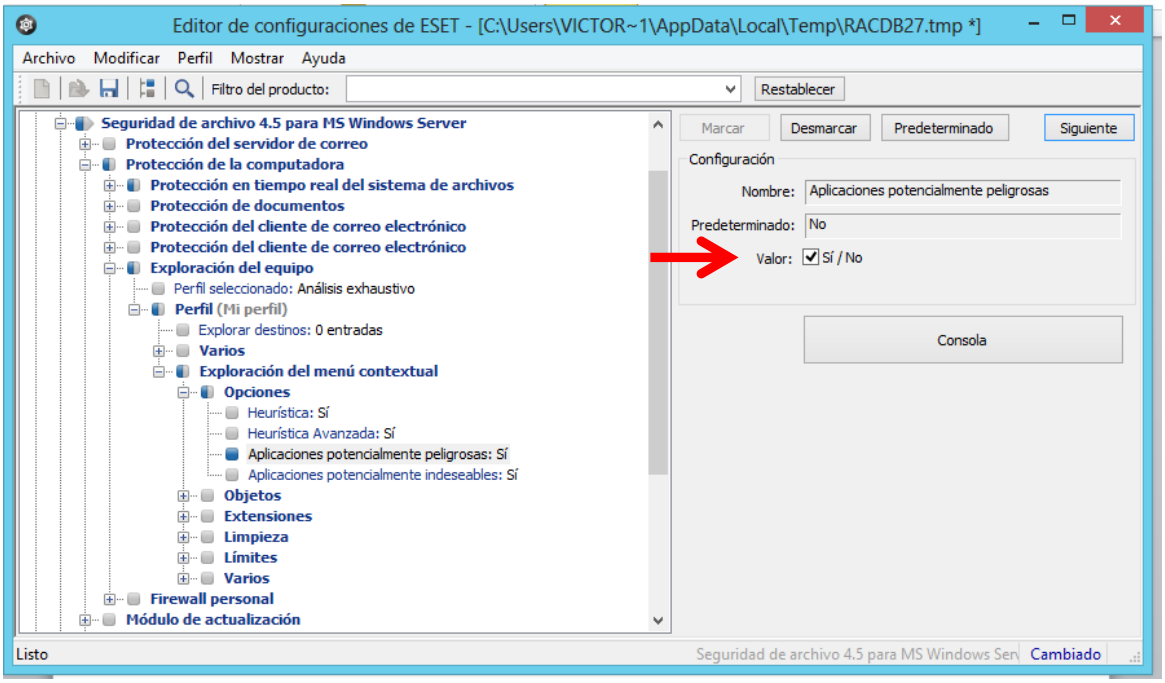

Editor de configuraciones de ESET - [C:\Users\VICTOR~1\AppData\Local\Temp\RACDB27.tmp *]
Archivo Modificar Perfil Mostrar Ayuda
Filtro del producto:
Restablecer
Línea de producto de Windows v3 y v4
Windows Desktop v5
Kernel
Exploración del equipo
Protección en tiempo real del sistema de archivos
Filtro de correo electrónico
Cliente de correo electrónico
Protección de documentos
Configuración
Exploración (Protección de documentos)
Objetos
Opciones
Heurística: Sí
Heurísticas avanzadas/DNA/Firmas inteligentes: Sí
Aplicaciones potencialmente indeseables: Sí
Aplicaciones potencialmente peligrosas: Sí
ESET Live Grid: Sí
Limpieza
Extensiones
Límites
Otros
Firewall Personal
Filtro de correo no deseado
Actualización
HIPS
Marcar
Desmarcar
Predeterminado
Siguiente
Configuración
Nombre: Aplicaciones potencialmente peligrosas
Predeterminado: No
Valor: Sí / No
Consola
Listo
Windows Desktop v5
Cambiado

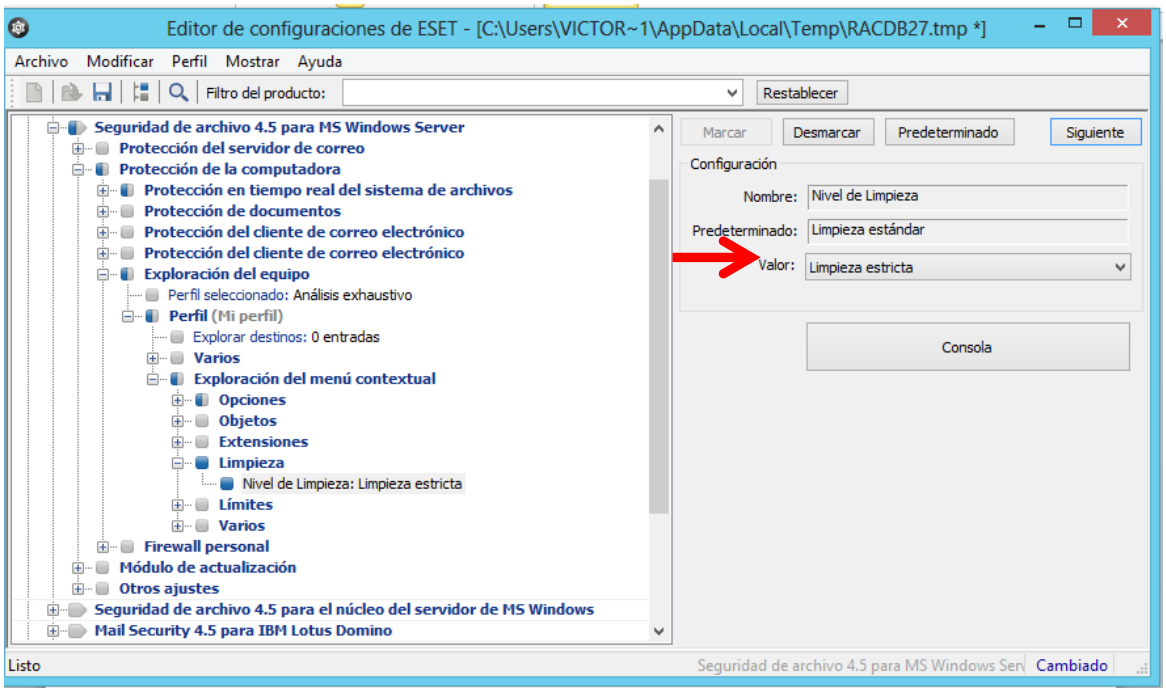

Editor de configuraciones de ESET - [C:\Users\VICTOR~1\AppData\Local\Temp\RACDB27.tmp *]
Archivo Modificar Perfil Mostrar Ayuda
Filtro del producto:
Restablecer
Línea de producto de Windows v3 y v4
Windows Desktop v5
Kernel
Exploración del equipo
Protección en tiempo real del sistema de archivos
Filtro de correo electrónico
Cliente de correo electrónico
Protección de documentos
Configuración
Exploración (Protección de documentos)
Objetos
Opciones
Limpieza
Nivel de Limpieza: Limpieza estricta
Extensiones
Límites
Otros
Firewall Personal
Filtro de correo no deseado
Actualización
HIPS
Control de dispositivos
Control Web
Windows Server 4.5
Escritorio Unix v4
Marcar
Desmarcar
Predeterminado
Siguiente
Configuración
Nombre: Nivel de Limpieza
Predeterminado: Limpieza estándar
Valor: Limpieza estricta
Consola
Listo
Windows Desktop v5
Cambiado

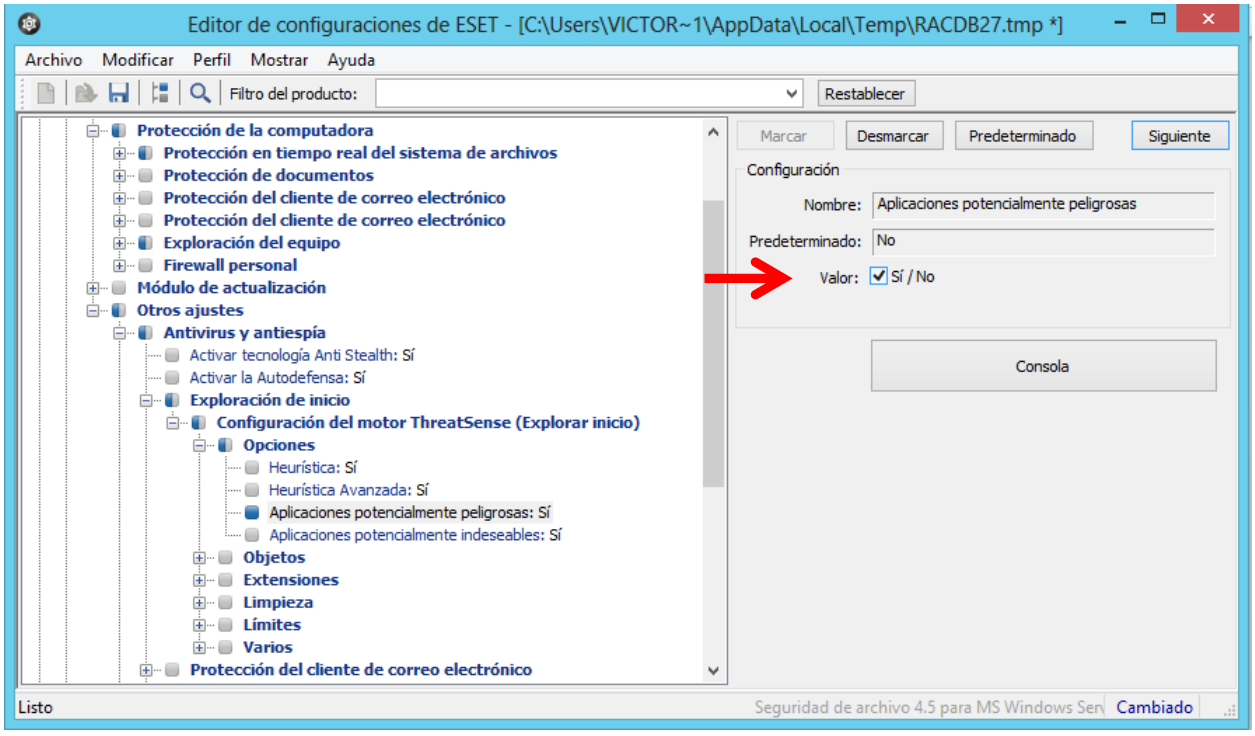
Para los servidores se configuraría estos parámetros.

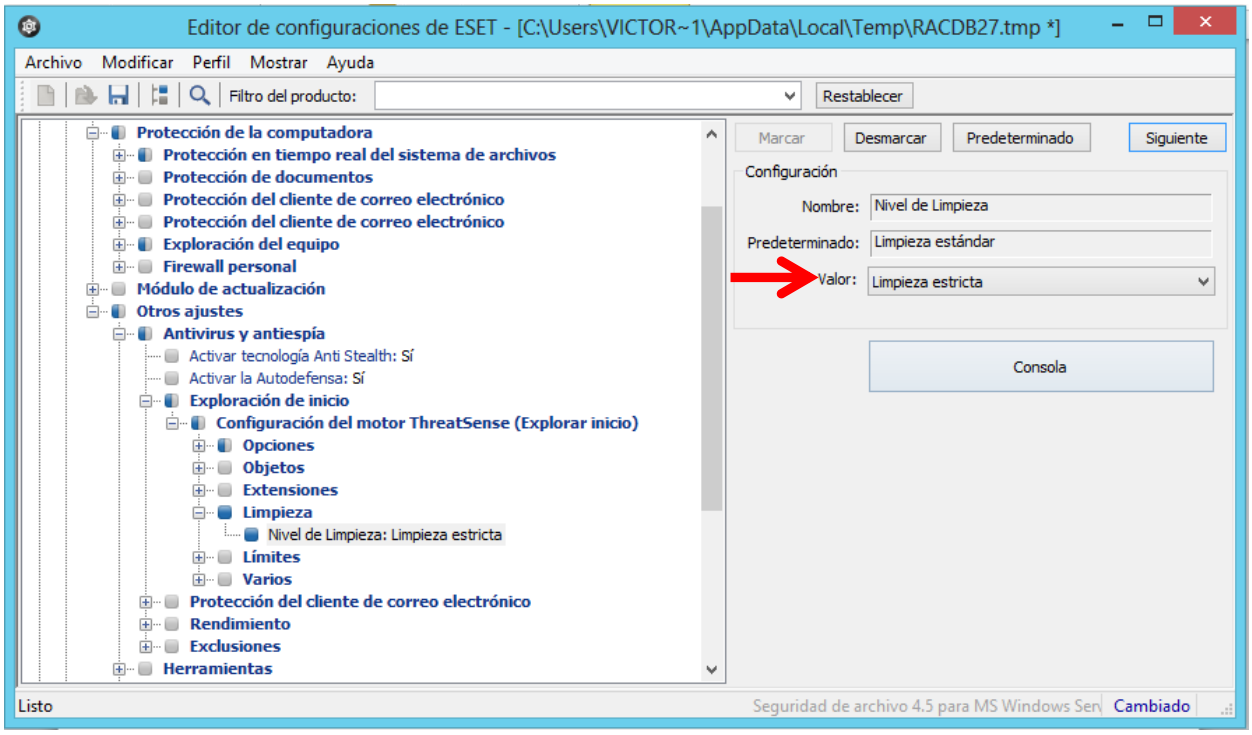


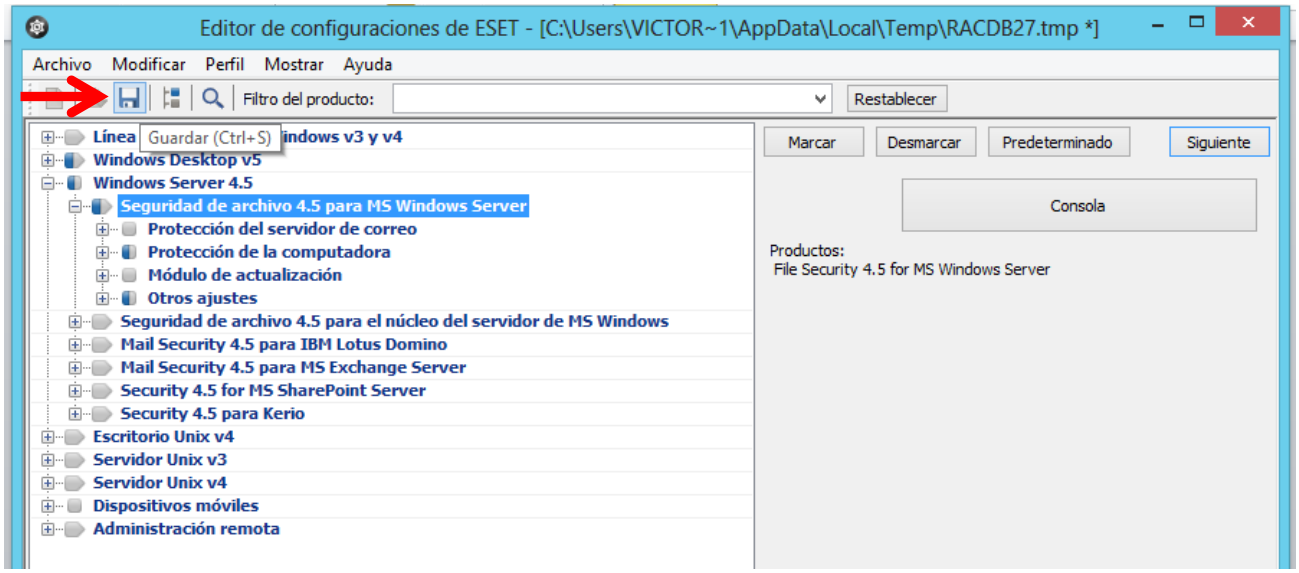



Editor de configuraciones de ESET - [C:\Users\VICTOR~1\AppData\Local\Temp\RACDB27.tmp *]
Archivo Modificar Perfil Mostrar Ayuda
Filtro del producto:
Restablecer
Seguridad de archivo 4.5 para MS Windows Server
Protección del servidor de correo
Protección de la computadora
Protección en tiempo real del sistema de archivos
Protección de documentos
Protección del cliente de correo electrónico
Protección del cliente de correo electrónico
Exploración del equipo
Perfil seleccionado: Análisis exhaustivo
Perfil (Mi perfil)
Explorar destinos: 0 entradas
Varios
Exploración del menú contextual
Opciones
Heurística: Sí
Heurística Avanzada: Sí
Aplicaciones potencialmente peligrosas: Sí
Aplicaciones potencialmente indeseables: Sí
Objetos
Extensiones
Limpieza
Límites
Varios
Firewall personal
Módulo de actualización
Marcar
Desmarcar
Predeterminado
Siguiente
Configuración
Nombre: Aplicaciones potencialmente peligrosas
Predeterminado: No
Valor: Sí / No
Consola
Listo
Seguridad de archivo 4.5 para MS Windows Ser
Cambiado


Editor de configuraciones de ESET - [C:\Users\VICTOR~1\AppData\Local\Temp\RACDB27.tmp *]
Archivo Modificar Perfil Mostrar Ayuda
Filtro del producto:
Restablecer
Seguridad de archivo 4.5 para MS Windows Server
Protección del servidor de correo
Protección de la computadora
Protección en tiempo real del sistema de archivos
Protección de documentos
Protección del cliente de correo electrónico
Protección del cliente de correo electrónico
Exploración del equipo
Perfil seleccionado: Análisis exhaustivo
Perfil (Mi perfil)
Explorar destinos: 0 entradas
Varios
Exploración del menú contextual
Opciones
Objetos
Extensiones
Limpieza
Nivel de Limpieza: Limpieza estricta
Límites
Varios
Firewall personal
Módulo de actualización
Otros ajustes
Seguridad de archivo 4.5 para el núcleo del servidor de MS Windows
Mail Security 4.5 para IBM Lotus Domino
Marcar
Desmarcar
Predeterminado
Siguiente
Configuración
Nombre: Nivel de Limpieza
Predeterminado: Limpieza estándar
Valor: Limpieza estricta
Consola
Listo
Seguridad de archivo 4.5 para MS Windows Ser
Cambiado


Editor de configuraciones de ESET - [C:\Users\VICTOR~1\AppData\Local\Temp\RACDB27.tmp *]
Archivo Modificar Perfil Mostrar Ayuda
Filtro del producto:
Restablecer
Protección de la computadora
Protección en tiempo real del sistema de archivos
Protección de documentos
Protección del cliente de correo electrónico
Protección del cliente de correo electrónico
Exploración del equipo
Firewall personal
Módulo de actualización
Otros ajustes
Antivirus y antiespía
Activar tecnología Anti Stealth: Sí
Activar la Autodefensa: Sí
Exploración de inicio
Configuración del motor ThreatSense (Explorar inicio)
Opciones
Heurística: Sí
Heurística Avanzada: Sí
Aplicaciones potencialmente peligrosas: Sí
Aplicaciones potencialmente indeseables: Sí
Objetos
Extensiones
Limpieza
Límites
Varios
Protección del cliente de correo electrónico
Marcar
Desmarcar
Predeterminado
Siguiente
Configuración
Nombre: Aplicaciones potencialmente peligrosas
Predeterminado: No
Valor: Sí / No
Consola
Listo
Seguridad de archivo 4.5 para MS Windows Ser
Cambiado


Editor de configuraciones de ESET - [C:\Users\VICTOR~1\AppData\Local\Temp\RACDB27.tmp *]
Archivo Modificar Perfil Mostrar Ayuda
Filtro del producto:
Restablecer
Protección de la computadora
Protección en tiempo real del sistema de archivos
Protección de documentos
Protección del cliente de correo electrónico
Protección del cliente de correo electrónico
Exploración del equipo
Firewall personal
Módulo de actualización
Otros ajustes
Antivirus y antiespía
Activar tecnología Anti Stealth: Sí
Activar la Autodefensa: Sí
Exploración de inicio
Configuración del motor ThreatSense (Explorar inicio)
Opciones
Objetos
Extensiones
Limpieza
Nivel de Limpieza: Limpieza estricta
Límites
Varios
Protección del cliente de correo electrónico
Rendimiento
Exclusiones
Herramientas
Marcar
Desmarcar
Predeterminado
Siguiente
Configuración
Nombre: Nivel de Limpieza
Predeterminado: Limpieza estándar
Valor: Limpieza estricta
Consola
Listo
Seguridad de archivo 4.5 para MS Windows Ser
Cambiado



Después de la configuración de la política y realizar los ajustes respectivos en todos los momentos de intervenciones de código malicioso en los servidores que puedan tener virtualización estarán protegidos ya que el threat sense de ESET y en combinación con su tratamiento heurístico del código desconocido le darán mucha fortaleza a los proceso de descubrimiento de malware o código malicioso en el momento que se necesite.

Espero que este documento sirva para la prevención del código malicioso que se está gestando últimamente en internet, lo más importante frente a VEMON es que ya está firmado por la marca y será descubierto en cuanto trate de infectar los servidores o maquinas que tengan virtualización, por encima de los demás.

FIN DEL DOCUMENTO

Víctor Hugo Rico Macías
Laboratorio Antimalware ITECH DEFENSI.
soporte@itechsas.com
vhrico@itechsas.com
Documento realizado en mayo 17 de 2015