Dr.WEB®
desde 1992

Dr.Web KATANA

Kills **A**ctive **T**hreats **A**nd **N**ew **A**ttacks*

* Elimina amenazas activas y nuevos ataques

Doctor Web S.L., 2021

Dr.Web KATANA

Kills **A**ctive **T**hreats **A**nd **N**ew **A**ttacks

Un antivirus no basado en firmas de nueva generación para mejorar la protección del PC junto con su antivirus tradicional

Para cualquier empresa son críticos los daños de procesos de negocios, el acceso no autorizado a dispositivos, el uso de vulnerabilidades, la averiguación de contraseñas, phishing y otras acciones no autorizadas, realizadas, así miso, durante los incidentes informáticos vinculados con virus (IVV) a través de software nocivo.

Lamentablemente, hoy día, por varias razones, uno no puede confiar en la protección antivirus de solo un vendedor.

Los creadores de virus hacen pruebas de sus virus sofisticados desde el punto de vista tecnológico y de los más peligrosos para ver si los mismos se detectan por las bases de virus de todos los antivirus antes de lanzar los mismos.

Por lo tanto, si uno confía en la protección basada solo en las bases de virus de antivirus, por muy eficaces que fueran, los malintencionados siempre tendrán una ventaja temporal: el código nocivo puede ya ser conocido para el vendedor de antivirus, pero aún no recibido por el antivirus en el dispositivo del usuario.

SIEMPRE hay amenaza de infección por un virus más nuevo y DESCONOCIDO.

¿Cuándo se necesitan dos antivirus?

- Cuando el antivirus básico omite las amenazas.
- Cuando no se puede actualizar frecuentemente el antivirus básico.
- Cuando el PC lleva mucho tiempo desconectado de Internet.
- Cuando el PC está en una red aislada donde las actualizaciones no llegan con mucha frecuencia.

El antivirus no basado en firmas es necesario siempre: Vd. no puede saber si su antivirus ya dejó pasar un programa nocivo.

Le ofrecemos usar el antivirus no basado en firmas **Dr.Web KATANA**, además de Su antivirus basado en firmas tradicional (no Dr.Web) para mejorar la protección de Su red local, así como los equipos por separado contra las amenazas nocivas más peligrosas — entre ellas, los troyanos cifradores.

Hoy día ningún antivirus conoce el 100% de los programas nocivos en el momento de penetración. Lamentablemente, los programas nocivos más peligrosos, tales como los cifradores, pueden esquivar los métodos tradicionales de protección antivirus.

Hasta si un antivirus ha ganado muchas veces en varias pruebas, conviene recordar que en el momento de realizar las pruebas todos los programas nocivos de prueba ya eran conocidos para los analistas y organizadores de pruebas. Lo cual significa que el premio obtenido por las pruebas de este tipo no significa la posibilidad de atacar las amenazas activas desconocidas en el momento del ataque.

¿Por qué muchas empresas protegidas por los productos que ganaron en estas pruebas fueron víctimas de WannaCry? Sus antivirus no tenían firmas del nuevo troyano, y los analizadores heurísticos no podían proteger correctamente.

Y los clientes de Dr.Web no han sido víctimas de WannaCry.

La protección extra contra las amenazas modernas más nuevas que pueden ser desconocidas para Su antivirus puede ser realizada a base de las tecnologías **Dr.Web KATANA** al analizar el comportamiento de programas — la búsqueda de indicios de comportamiento nocivo en procesos iniciados. El producto protege contra las amenazas no detectadas por los métodos de detección tradicionales (firmas).

Todos los troyanos o hacen

Funcionan usando los mismos algoritmos	**Cometen el mismo error:**
y usan los mismos sitios críticos en sistemas operativos para penetrar, tienen conjuntos similares de funciones nocivas.	Empiezan a actuar primeros (atacan al sistema).

Dr.Web KATANA es capaz de detectar y desinfectar un troyano cuando el mismo solo empieza a funcionar.

Dr.Web KATANA es capaz de detectar y desinfectar un troyano cuando el mismo solo empieza a funcionar:

- detecta los procesos nocivos,
- afronta los ataques de programas nocivos,
- previene los intentos de penetración en el sistema,—pero lo hace de forma más... fina.

Dr.Web KATANA detectará la actividad nociva en cuanto el troyano intente actuar.

- Muchos troyanos funcionan usando los mismos algoritmos y los mismos sitios críticos en sistemas operativos para penetra tos similares de funciones malintencionadas.
- Todos los troyanos cometen el mismo error: empiezan a funcionar primeros (atacan al sistema).
- La actividad de un troyano es suficiente para Dr.Web KATANA,
- para detectar al enemigo y afrontarlo.
- Dr.Web KATANA analiza al vuelo el comportamiento de amenazas y bloquea enseguida los scripts y los procesos nocivos que no pudo detectar (=ÓMITIÓ) su antivirus.

Y no hace falta ninguna firma, lo cual convierte Dr.Web KATANA en un arma muy ligera.

Los analizadores heurísticos tradicionales funcionan según las reglas de comportamiento de programas ilegítimos conocidos indicados en la base de conocimiento.

Los malintencionados también conocen estas reglas!

Las vulnerabilidades y la posibilidad de implementar exploits permiten esquivar esta protección.

Dr.Web KATANA funciona «al vuelo»	**El análisis lleva menos de un segundo**	**No es necesario consultar las bases de virus de mucho volumen**

Qué controla Dr.Web KATANA

- Procesos de aplicaciones legítimas.
- Partes críticas del sistema y servicios del sistema — sectores de arranque del disco, claves del registro, así mismo, los responsables de controladores de dispositivos virtuales.
- Reglas de inicio de programas.
- Desactivación del modo seguro Windows.
- Posibilidades de añadir a la lógica del funcionamiento del sistema operativo las nuevas tareas necesarias para los malintencionados.
- Carga de controladores, nuevos o desconocidos para el usuario.
- Comunicaciones entre los componentes del software espía y el servidor de control.
- Procesos de creación estándar de copias de seguridad de archivos.
- Todos los navegadores de Internet populares (Internet Explorer, Mozilla Firefox, Yandex.Browser, Google Chrome, Vivaldi Browser).
- Aplicaciones de MS Office (Word/Excel/InfoPath/Lync/Access/Outlook/Visio/WordPad), Windows Media Player.
- Aplicaciones del sistema
- Aplicaciones que usan las tecnologías java (Java 1.8/6/7), flash- y pdf (Acrobat Reader).

Posibilidades funcionales de Dr.Web KATANA

- Protege las partes críticas del sistema contra la modificación por los programas nocivos.
- Detecta y detiene los scripts y procesos nocivos, sospechosos o no seguros.
- Detecta los cambios de archivos no deseados, supervisando el funcionamiento de todos los procesos en el sistema en busca de acciones características para los programas nocivos (por ejemplo, de troyanos extorsionistas) impidiendo que los objetos nocivos se implementen en los procesos de otros programas.
- Detecta y neutraliza las amenazas más recientes: los troyanos extorsionistas (cifradores), los inyectores, los objetos nocivos administrados de forma remota (difundidos para organizar botnets y espionaje), así como los empaquetadores de virus.
- Protege contra los exploits — objetos nocivos que para penetrar en el sistema intentan usar las vulnerabilidades, así mismo, aún desconocidas para todos excepto los creadores de virus (las así llamadas vulnerabilidades del «día cero»).
- Supervisa el funcionamiento no solo de los navegadores más populares, sino de cualquier complemento para los mismos; protege contra los bloqueadores de navegadores.
- Bloquea la posibilidad de cambio de secciones de carga de la unidad por los programas nocivos para impedir el inicio (por ejemplo, de troyanos) en un equipo.
- Previene la desactivación del modo seguro de Windows bloqueando los cambios del registro.
- Impide que los programas nocivos añadan a la lógica del funcionamiento del sistema operativo la

realización de las nuevas tareas necesarias para los malintencionados. Bloquea algunas opciones en el registro de Windows, lo que impide, por ejemplo, que los virus cambien la visualización correcta del Escritorio u oculten la presencia del troyano en el sistema por un rootkit.

- No permite que el software malintencionado modifique las reglas de inicio de programas.
- Impide la carga de controladores nuevos o desconocidos sin que el usuario lo sepa.
- Bloquea el autoinicio de programas nocivos, así como de aplicaciones determinadas, por ejemplo, de anti antivirus, impidiendo que los mismos se registren en el registro para el inicio posterior.
- Bloquea las ramas del registro responsables de controladores de dispositivos virtuales, lo que imposibilita la instalación del nuevo dispositivo virtual.
- Bloquea las comunicaciones entre los componentes del software espía y el servidor que los controla.
- Impide que el software malintencionado afecte al funcionamiento correcto de servicios del sistema, por ejemplo, afectar a la creación ordinaria de copias de seguridad de archivos.

Algoritmo de funcionamiento de Dr.Web Katana

- Al detectar un intento de uso de la vulnerabilidad, Dr.Web de forma emergente finaliza el proceso del programa atacado. El antivirus realiza ninguna acción con archivos de la aplicación, incluida la de mover a cuarentena.
- Como notificación, el usuario ve un aviso sobre la prevención del intento de una acción nociva, que no requiere respuesta.
- En el registro de eventos Dr.Web se crea una entrada sobre la prevención del ataque.
- La base de conocimiento en la nube del sistema recibe una notificación inmediata sobre el incidente. En caso necesario, los expertos de Doctor Web dan una respuesta inmediata al mismo, por ejemplo, mejorando el algoritmo de control.

Cómo la Nube Dr.Web ayuda a la protección

La Nube Dr.Web contiene:

- los datos sobre algoritmos de programas con intenciones nocivas;
- la información sobre los archivos deliberadamente "limpios";
- la información sobre las firmas digitales comprometidas de los desarrolladores de software conocidos;
- la información sobre las firmas digitales del software de publicidad/potencialmente peligroso;
- los algoritmos de protección de aplicaciones

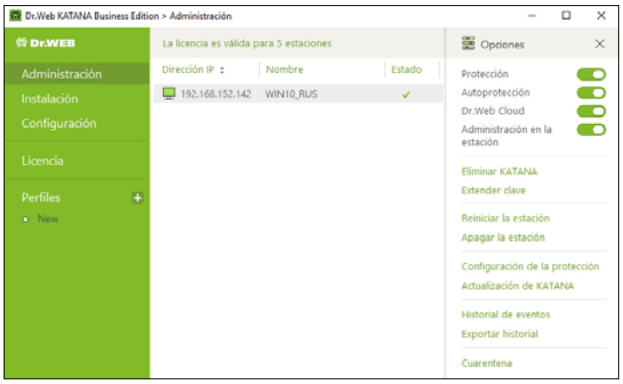
El sistema de la nube obtiene la información sobre el funcionamiento de Dr.Web en el PC protegido, así mismo, sobre las amenazas más nuevas detectadas, lo que permite dar respuesta operativa a los errores de funcionamiento del sistema detectados y actualizar las reglas almacenadas en el equipo de forma local.

No se transfiere ningún archivo de usuario del sistema protegido a los servidores de Doctor Web!

Prevención máxima	Extrema resistencia	Posibilidad de funcionamiento autónomo
▪ Dr.Web KATANA ofrece la seguridad casi a partir del inicio del sistema operativo. ▪ Empieza a proteger antes de iniciar un antivirus tradicional basado en firmas, su otro antivirus.	▪ Dr.Web KATANA contiene un módulo de autoprotección Dr.Web SelfPROtect que no tiene análogos en el mercado. ▪ Si un troyano «mata» el proceso de otro antivirus, luego tendrá que dañar Dr.Web KATANA, pero afrontará un módulo de autoprotección. ▪ Gracias a la autoprotección, Dr.Web KATANA resistirá, y el proceso nocivo será detenido.	▪ Los troyanos no pueden difundirse de forma autónoma. ▪ Los empleados los difunden en dispositivos USB y otros dispositivos. ▪ Donde no es posible un antivirus basado en firmas de mucho volumen, ayudará el antivirus no basado en firmas Dr.Web KATANA que tiene requisitos mínimos al sistema y la posibilidad de funcionamiento sin acceso a Internet.

Control

▪ Instalación centralizada en las estaciones de red protegidas, configuración y supervisión de los eventos de virus, así como del estado de Dr.Web KATANA en las estaciones protegidas.	▪ Escenarios de protección predeterminados (óptimo, medio, paranoico) — el producto funciona directamente «out of the box», listo para usar.	▪ Posibilidad de crear las reglas flexibles para las aplicaciones de confianza y evitar conflictos de software en caso de funcionamiento de Dr.Web KATANA.	▪ Posibilidad de configurar las opciones de control de protección para una aplicación en concreto, asegurar el acceso solo a los determinados recursos para el mismo.

Centro de Control	Agentes
	

Compatibilidad

Durante el desarrollo de Dr.Web KATANA, fue confirmada la compatibilidad con los productos TrendMicro, Symantec, Kaspersky, Mcaffee, ESET etc.

¡Novedad! Dr.Web vxCube

Analizador inteligente interactivo de objetos sospechosos en la nube para expertos en seguridad informática y cibercriminalistas

Dr.Web vxCube:

- Analiza un objeto de forma remota en un entorno que corresponde a Su situación
- Permite observar el procedimiento de análisis
- Reproduce cualquier acción del objeto sospechoso para la investigación del mismo
- Ofrece un informe sobre el análisis realizado

Al detectar una amenaza, se creará una compilación especial de la utilidad Dr.Web CureIt! para desinfectar Su sistema, antes de que los medios de protección instalados resuelvan el problema. Dr.Web CureIt! puede funcionar sin instalación hasta si hay otro antivirus.

Más información sobre Dr.Web vxCube

Peritaje de incidencias de equipo vinculados con virus (IEVV)

El peritaje incluye:

- Valoración previa del incidente, volumen de peritaje y medidas necesarias para corregir las consecuencias.
- Investigaciones de peritaje de artefactos informáticos y otros (unidades de discos duros, materiales de texto, audio, foto y video) que supuestamente tienen que ver con IIV.
- ¡No tiene análogos! Peritaje psicológico de personas (personal) para detectar los hechos de realizar / ser cómplice / ocultar / estimular las acciones ilegales para el cliente (valoración integral de riesgos), así como los hechos de inactividad o negligencia.
- Recomendaciones para crear un sistema de protección antivirus para evitar IIV o reducir su número en el futuro.

Más información sobre el peritaje de Doctor Web

Las solicitudes de peritaje se reciben en la dirección siguiente:

https://support.drweb.ru/expertise

Sobre la empresa Doctor Web

Doctor Web es un productor ruso de los medios antivirus de protección de la información bajo la marca Dr.Web. Los productos Dr. Web. se desarrollan a partir del año 1992. Es una empresa clave en el mercado ruso del software para asegurar la necesidad básica del negocio - la seguridad de información.

Doctor Web fue la primera empresa que ofreció un modelo de innovación de uso de antivirus como servicio en el mercado ruso y hoy día sigue siendo líder del mercado ruso de los servicios Internet de seguridad para proveedores de servicios de IT.

Los clientes confían en Dr.Web

La plantilla de Doctor Web la componen los expertos de varios ámbitos de seguridad informática, lo que permite a la empresa tomar en cuenta lo máximo posible las peculiaridades del funcionamiento de empresas de varios tamaños y perfil de actividad y ofrecer a los clientes los productos de calidad óptimos por precio total mínimo.

Entre los clientes de los productos de la empresa hay usuarios de hogar de todas las regiones del mundo y grandes empresas rusas, pequeñas empresas y corporaciones estratégicas. La geografía de los usuarios Dr.Web confirma la gran confianza en el producto desarrollado por los informáticos rusos de gran talento.

Véase un listado de solo algunos clientes de Dr.Web: https://customers.drweb.com.

¿Por qué Dr.Web?

Todos los derechos de las tecnologías Dr.Web pertenecen a la empresa Doctor Web. La empresa es uno de los pocos vendedores antivirus en el mundo que tiene sus propias tecnologías únicas para detectar y desinfectar los programas malintencionados, cuenta con su propio laboratorio antivirus, el servicio global de supervisión de virus y el servicio de soporte técnico.

© Doctor Web 2003–2021

125124, Rusia, Moscú, c/3 Yamskogo Polya, ed.2-12A
Teléfono: +7 (495) 789-45-87
Fax: +7 (495) 789-45-97

www.drweb-av.es | www.av-desk.com | curenet.drweb.com | www.drweb.com