Dr.WEB®
desde 1992

Cómo seleccionar un antivirus

Metodología de selección de los medios de protección antivirus

Para autónomos, directivos de departamentos de IT de empresas y entidades, así como para expertos en sistemas antivirus de protección de empresas

Dr.WEB®
desde 1992

CONTENIDO

Introducción

Actualmente en el mercado hay bastantes ofertas de software antivirus. Al parecer, es fácil seleccionar lo mejor es fácil — los mejores serán los ganadores de las pruebas antivirus, sobre todo porque los líderes de pruebas muchas veces son soluciones gratuitas, lo cual ofrece maravillosas posibilidades de ahorrar. Pero si todo fuera tan fácil...

- Buenos días, el equipo fue infectado por un cifrador, el antivirus ... no ayudó.
- Buenos días, estimado equipo de Dr.Web, necesito ayuda para descifrar los datos, mi equipo fue infectado por el virus WannaCry. Se infectó al abrir un sitio web (no recuerdo cuál, porque no enseguida me di cuenta de la infección), tenía activado un antivirus ...

Los tres puntos en las citas se usan en vez de los nombres de antivirus cuyos usuarios solicitaron ayuda a la empresa Doctor Web, para descifrar los datos por causa de una infección por el troyano Wanna Cry — una epidemia que afectó hasta las grandes empresas.

Además, las descripciones de las tecnologías usadas por el antivirus para detectar los programas nocivos no siempre son muy claras, por lo tanto, no siempre es muy fácil seleccionar una solución que protege de verdad.

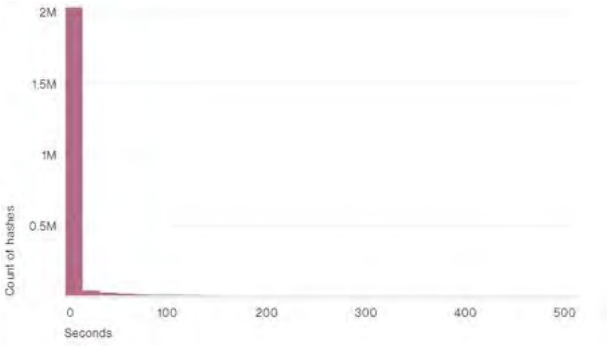
I. Causas básicas de infección y medidas para afrontarla

Casi todos los días en los medios de comunicación se informa de infecciones de varias empresas y entidades. A veces se informa de pérdidas importantes. La mayoría de estas empresas usaban un antivirus en el momento de infección. ¿Por qué pasa eso?

1. Los malintencionados pueden automatizar el desarrollo de los programas nocivos, por lo cual, el número de muestras de programas nocivos que llegan a la empresa Doctor Web para el análisis en un solo día alcanza un millón.

- Como es necesario añadir las nuevas reglas a las bases antivirus, las bases de reglas del Firewall y la protección preventiva, se acumula mucha «basura» en estas bases, por lo tanto, la empresa Doctor Web las limpia estas quitando las entradas duplicadas sin perder la calidad de detección.
- La característica única de las bases antivirus Dr.Web es un algoritmo de búsqueda de firmas en las bases antivirus, las bases de reglas del Firewall y del analizador heurístico que no aumenta el periodo de búsqueda si aumenta el número de entradas.

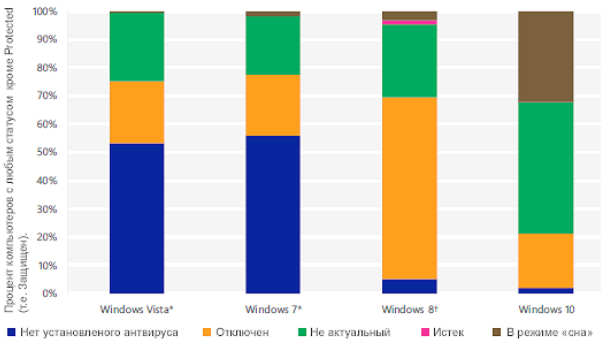
El antivirus no debe funcionar lentamente.



Más de 99% muestras de programas nocivos (hashes) existen solo 58 segundos o menos.

2. Los usuarios de los medios de protección antivirus no los actualizan o los desactivan completamente una vez instalados.

- Las estadísticas de escaneo del equipo por la utilidad de escaneo emergente Dr.Web CureIt! demuestran que hasta un 60% de los equipos no están protegidos lo suficiente.
- Casi un 30% de los usuarios de la versión gratuita de la utilidad Dr.Web CureIt! son los usuarios del antivirus Microsoft Windows Defender incrustado en el SO Windows 7 y 10.



Рейтинг угроз

Период: неделя ; 10 строк

Название	Класс	%
DFH:HOSTS.corrupted	virus	6.73
Program.MediaGet.142	riskware	2.54
Program.Unwanted.1183	riskware	2.21
Trojan.InstallCore.2896	virus	1.24
Program.Unwanted.276	riskware	1.17
Adware.Zaxar.62	adware	1.08
Program.Unwanted.2	riskware	1.02
Program.Unwanted.1678	riskware	0.86
Program.Zona.86	riskware	0.75
Adware.Elemental.1	adware	0.69

Всего: 524508

Estadísticas de escaneo de equipos con la utilidad Dr.Web CureIt!

Dr.Web encuentra amenazas

3. Los usuarios de los medios de protección antivirus ignoran las advertencias del sistema de protección y lo configuran de tal forma que los archivos nocivos al llegar al sistema no se escanean por el antivirus. ▪ Una de las causas básicas de infección es cuando los usuarios excluyen del escaneo antivirus los programas que se conectan a Internet y los discos enteros de equipos. ▪ Otro modo de reducir el nivel de la protección del antivirus es reducir el nivel de protección del componente la Protección preventiva.	**! Muchas infecciones se producen por causa de las acciones del personal de la empresa, sus clientes o socios.**
4. En las redes locales no se instalan las actualizaciones durante mucho tiempo y están permitidos los servicios vulnerables. ▪ Los exploits usados para penetrar en el sistema atacado son válidos para vulnerabilidades localizadas hace tres años y antes. En realidad, el periodo de disponibilidad de la vulnerabilidad coincide con el periodo de funcionamiento del sistema operativo. ▪ El cifrador WannaCry fue difundido con un exploit para una vulnerabilidad de Microsoft ya cerrada.	

II. Requisitos a los medios de protección usados

El sistema de protección antivirus debe:

1. **ser capaz de detectar los programas nocivos anteriormente desconocidos.** Los creadores de virus hacen pruebas de sus «obras» en los servicios especializados, y, como resultado, si el antivirus dispone solo de mecanismos heurísticos, eso no le permite garantizar la detección de los programas nocivos más nuevos. Un medio frecuente de ocultar las firmas ya conocidas es volver a comprimir los programas nocivos creados anteriormente, así mismo, usando los formatos de comprimidores desconocidos para el sistema de protección. Para afrontar este método, en las soluciones Dr.Web se usan las tecnologías capaces de buscar los programas nocivos existentes recomprimidos (**Dr.Web Fly-Code**), así como los medios de protección proactivos que detectan los modelos de comportamiento típicos de programas nocivos que no requieren sus firmas (**la Protección preventiva Dr.Web**).

2. **tener un sistema de autoprotección seguro** que no permite que los programas nocivos más nuevos ni el personal que desea esquivar las normas de seguridad de la empresa lo desactiven. En caso de disponer de este sistema, las soluciones antivirus pueden afrontar los ataques de programas nocivos antes de recibir las actualizaciones que bloquean el origen del ataque.

3. **disponer de bloqueo de desactivación de la protección antivirus.** Para ello, debe usarse la protección centralizada con la posibilidad de restringir los permisos de usuarios en función de sus actividades laborales, así como la protección con la contraseña del acceso a la configuración del sistema de protección en as estaciones que no disponen de administración centralizada.

4. **instalar las últimas actualizaciones.** El sistema de actualizaciones Dr.Web usa los servidores ubicados en todo el mundo. Las tecnologías de actualización permiten actualizar todas las estaciones del sistema protegido a la vez, sin cargar la red local. El uso de la protección centralizada permite actualizar las estaciones de la red según la programación y reiniciar las estaciones, y la protección con la contraseña del acceso a la configuración del sistema de protección en las estaciones que no disponen de administración centralizada permite evitar el rechazo de las actualizaciones.

5. **actualizar la licencia.** En los productos Dr.Web funciona un sistema de renovación automática de la licencia por su proveedor de los medios de protección antivirus.

III. Seleccionar las medidas de protección

El sistema de protección antivirus debe no solamente bloquear los programas nocivos conocidos, sino también impedir la difusión de los programas nocivos desconocidos por la red y fuera de la misma.

1. Deben estar protegidos los nodos de la red local donde es posible instalar el antivirus - así mismo, Linux y Mac, las Gateways de Internet, los dispositivos móviles. Si el personal usa los dispositivos móviles y los equipos de hogar, los mismos también deben estar protegidos. En caso de rechazar la protección de dispositivos móviles y equipos personales, se requiere la protección de servidores de correo y Gateways Internet usados por el personal para acceder a los servicios de la empresa.
2. Los sistemas donde pueden penetrar los programas nocivos (así mismo, las impresoras) y donde no es posible instalar los sistemas antivirus, debe estar aislados al máximo del resto de la red local.

El medio de protección antivirus de estaciones de trabajo usado debe:

1) Saber desinfectar no solo en el momento de penetración de programas nocivos en el sistema, sino también en caso de programas nocivos anteriormente desconocidos ya iniciados;
2) detectar las muestras conocidas de programas nocivos comprimidos en archivos de formato desconocido;
3) tener posibilidad de aplicar los mecanismos extra (además de los de firmas y heurísticos) para detectar los programas nocivos desconocidos — así mismo, la protección preventiva y los componentes de la nube;
4) Para la protección contra la penetración de programas desconocidos en el momento de infección, disponer de:

- Firewall personal que impide el escaneo de la red local, así como la protección contra los ataques intranet;
- un sistema de restricción de acceso a dispositivos extraíbles y recursos intranet, así mismo, los discos extraíbles, los catálogos y los sitios Internet;
- un sistema centralizado de escaneo periódico en busca de programas nocivos no activos y vulnerabilidades conocidas;

5) escanear todos los archivos que se reciben a través de la red local hasta el momento de recepción de los mismos por las aplicaciones usadas, lo que evita el uso de vulnerabilidades desconocidas de estas aplicaciones por las aplicaciones nocivas;
6) tener un sistema sólido de autoprotección que no permitirá al programa nocivo desconocido dañar el funcionamiento correcto del antivirus — la solución antivirus debe funcionar correctamente hasta recibir la actualización que permita desinfectarlo;

7) disponer de un sistema para recabar la información que permite transmitir lo más rápido posible toda la información necesaria para resolver el problema al laboratorio antivirus. Evitar las situaciones cuando para cada caso de infección es necesario recabar la información necesaria manualmente;
8) alojar todas las bases antivirus usadas en la memoria operativa para evitar la carga de las mismas (así mismo, el montaje) desde el disco duro que ralentiza las operaciones de operaciones de escaneo antivirus;
9) asegurar el escaneo multiflujo que evita las colas de archivos escaneados;
10) funcionar en sistema operativos ya no soportados por su productor;
11) para la protección contra los programas nocivos desconocidos transferidos en mensajes de correo usar antispam (antipishing) que no requiere formación continua;
12) evitar la necesidad de configuración manual de opciones de carga del procesador usando el sistema de análisis automático de su carga.

El sistema de administración centralizada de la protección antivirus debe:
1) al igual que el sistema de actualización de la solución antivirus: ser independiente de los mecanismos correspondientes usados en sistemas operativos; estar incluido en el sistema de autoprotección del antivirus, lo que permite evitar la posibilidad de intercepción del sistema de actualizaciones por un programa nocivo. No está permitido que el antivirus use los componentes de sistema no protegidos por el sistema de autorotección del antivirus;
2) usar en todas las estaciones de trabajo y servidores un antivirus que incluye el analizador heurístico proactivo y el Firewall personal;
3) asegurar la recepción más rápida de las actualizaciones de las bases de virus por las estaciones de trabajo y servidores protegidos - así mismo, por decisión del administrador, hasta si eso reduce el rendimiento de la red local protegida. La reducción del periodo de recepción de actualizaciones debe asegurarse por la reducción del tamaño de estas actualizaciones, así como por la conexión continua de las estaciones de trabajo protegidas y servidores al servidor de actualizaciones;
4) tener posibilidad de aplicar configuración individual para grupos y usuarios por separado;
5) tener posibilidad de realizar escaneo antivirus completo o personalizado del nodo de red en busca de amenazas de virus tanto por comando del usuario o administrador, como por programación;
6) tener posibilidad de instalación centralizada, actualización y configuración de los medios informáticos de la protección antivirus, así mismo, en los nodos de red no disponibles desde el servidor;
7) tener posibilidad de funcionamiento en las redes separadas en segmentos.

Además de usar el antivirus, se recomienda:
1. Restringir los permisos de usuarios. Así mismo:
   1) Rechazar el uso de permisos de administrador en las estaciones de trabajo;
   2) Restringir los permisos de acceso a recursos locales y de red;
   3) Restringir el acceso de dispositivos extraíbles. En este caso hay que tener en cuenta que las listas blancas de dispositivos no suelen ser eficaces porque los ID de todos los dispositivos del conjunto coinciden.

2. Dividir la red local en segmentos aislados instalando el sistema de filtrado de tráfico entre los mismos.
3. Eliminar los productos, servicios y componentes no usados.
4. Usar un sistema de reserva alojado en un servidor separado.
5. Alojar las bases de datos en servidores separador evitando el acceso a los mismos y versionar los archivos y documentos guardados.
6. Prohibir el acceso a Internet y a la red local para todos los programas excepto los permitidos.
7. Prohibir el uso de las contraseñas de dominio de administradores en las estaciones de trabajo.
8. Usar la instalación centralizada de todas las actualizaciones de seguridad para todos los productos usados. Actualizar con regularidad todo el software instalado en las estaciones.

Para el escaneo emergente de las estaciones potencialmente infectadas debe usarse un escáner antivirus de red, así como el disco antivirus / el dispositivo extraíble de arranque.

IV. Dr.Web Enterprise Security Suite — un conjunto de productos para el negocio

Para sus clientes corporativos, la empresa Doctor Web ofrece su producto insignia – el conjunto Dr.Web Enterprise Security Suite que dispone de muchas posibilidades únicas:

- protección centralizada de todos los nodos de la red – estaciones de trabajo, servidores de archivos y servidores de aplicaciones, entre ellos, de terminales, puertas de enlace y dispositivos móviles;
- protección integral de estaciones de trabajo contra la mayoría de las amenazas existentes gracias al antivirus incorporado, antispam, web antivirus, Firewall y control de oficina;
- precio mínimo total de implementación comparado con los programas de competencia gracias a la posibilidad de implementar servidores tanto para Windows como para Unix, base de datos incorporada, facilidad de instalación y seguridad de la protección. Usando Dr.Web Enterprise Security Suite, la empresa no tendrá que adquirir equipamiento caro;
- posibilidad de instalar la parte agente en un equipo ya infectado y alta probabilidad de desinfección;
- uso mínimo de recursos de equipos y de servidores gracias al tamaño reducido del núcleo antivirus y uso de las nuevas tecnologías en el mismo;
- detección de amenazas muy eficaz; asimismo, de los virus aún desconocidos;
- administración de toda la infraestructura de protección de red desde un solo sitio de trabajo (a través del administrador web) dondequiera que esté el mismo;
- realización de las directivas de seguridad necesarias para una empresa en concreto y los grupos de empleados;
- asignación de varios administradores para varios grupos, lo que permite usar Dr.Web Enterprise Security Suite tanto en las empresas con altos requisitos de seguridad como en empresas multi-filial;
- configuración de las directivas de seguridad para cualquier tipo de usuarios, entre ellos, los móviles, y para cualquier estación – incluso las que no están en la red en el momento – permite asegurar la protección actual en cualquier momento;
- protección de cualquier red, incluyendo las que no tienen acceso a Internet;
- posibilidad de usar la mayoría de las bases de datos existentes. Asimismo, como bases de datos externas pueden servir Oracle, PostgreSQL, Microsoft SQL Server o cualquier sistema de administración de bases de datos con soporte de SQL-92 a través de ODBC;
- posibilidad de crear sin ayuda los procesadores de eventos lo que ofrece el acceso

directo a las interfaces internas del Centro de Control;
- claridad del sistema de control del estado de protección, búsqueda de estaciones de red muy eficaz y cómoda;
- posibilidad de seleccionar un listado de componentes del productos actualizados y control de posibilidades de pasar a las nuevas versiones permiten a los administradores instalar solo las actualizaciones necesarias y comprobadas en su red.

El conjunto Dr.Web Enterprise Security Suite contiene los productos siguientes:

Dr.Web Desktop Security Suite – protección de estaciones de trabajo, clientes de servidores terminales, clientes de servidores virtuales y clientes de sistemas incorporados.

Dr.Web Server Security Suite – protección de servidores de archivos y servidores de aplicaciones (entre ellos, servidores de terminales y virtuales)

Dr.Web Mail Security Suite – protección del correo

Dr.Web Gateway Security Suite – protección de puertas de enlace

Dr.Web Mobile Security Suite – protección de dispositivos móviles

Dr.Web Enterprise Security Suite forma parte del Registro de software nacional y cumple con todos los requisitos de la legislación de protección antivirus actual.

Todos los productos de Dr.Web Enterprise Security Suite pueden ser usados gratis durante 30 días. Invitamos a empresas a solicitar la licencia demo para valorar la seguridad de la protección y la calidad de detección y desinfección Dr.Web.

Descripción: https://products.drweb-av.es/enterprise_security_suite?lng=es

Solicitar la demo: https://download.drweb-av.es/demoreq/biz/v2?lng=es

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 es uno de los pocos vendedores antivirus en el mundo que tiene sus propias tecnologías únicas para detectar y desinfectar los programas malintencionados. La protección antivirus Dr.Web permite a los sistemas de información de los clientes afrontar cualquier amenaza, hasta la desconocida.

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 certificados y los premios estatales, así como la geografía de los usuarios Dr.Web confirman la alta calidad de los productos creados por los informáticos rusos altamente competentes.

125040, Rusia, Moscú, c/3 Yamskogo Polya, 2, edif. 12a

Tel.: +7 (495) 789-45-87 (multicanal)

Fax: +7 (495) 789-45-97