Dr.WEB®
desde 1992

El correo es la fuente principal de difusión de troyanos y spam

El correo es la fuente principal de difusión de troyanos y spam

Los troyanos suelen penetrar en los equipos como resultado de alguna acción de usuarios — en dispositivos extraíbles o en el correo.

Ejemplos de solicitudes de usuarios, víctimas del troyano de la familia Encoder, al soporte técnico de Doctor Web, cuyos equipos estaban protegidos con otro antivirus (no Dr.Web):

Descargué un archivo recibido por correo — un archivo archivado, y se cifraron todos los archivos de Word y Excel, así como las imágenes. La extensión era 1TXT.

Los archivos han sido cifrados en formato 1txt. Abrimos un mensaje sospechoso del correo correo y se inició el cifrado.

10/10 a eso de las 11 11 recibí un mensaje a mi correo, abrí el mensaje y empezó el cifrado.

Hoy, una vez abierto un archivo del correo, todos los archivos de formato DOC, XLS se convirtieron en archivos de formato VAULT.

Buenos días: un empleado recibió un mensaje de una empresa con un archivo archivado con la nota «urgente», lo abrió, contenía un archivo .js, luego se produjo la infección por el virus VAULT que cifró todos los archivos. Ayuden a desinfectar y descifrar los datos.

¿Es suficiente la protección de las estaciones de trabajo para impedir estas infecciones?

No.

Buenos días. Hemos recibido un mensaje por correo con un adjunto «18.06.18.Gz». Lo hemos abierto. Resultó ser un virus. En el equipo el disco está dividido en dos discos lógicos. En el disco «C» muchos archivos y carpetas están en azul. En el disco «D» no.

Solicitud al soporte técnico de Doctor Web.

El análisis del informe del antivirus (un archivo que puede ser localizado en la dirección %userprofile%\desktop\drweb.log) confirmó lo siguiente:

1. El antivirus instalado en el equipo conocía el cifrador.
2. Lo más interesante es lo siguiente: cómo se inició este troyano.

threat: DPH:Trojan.Encoder.9 ==> send user blocked alert	Inicio por el usuario, el antivirus identifica el troyano y visualiza una notificación.
threat: DPH:Trojan.Encoder.9 ==> send user blocked alert	Otro inicio.

Luego hubo más intentos, hasta que el usuario decidió que si el antivirus molesta, es más fácil desactivarlo.

Y no son todas las causas de organizar el filtrado del correo en el servidor.

Los flujos de correo que pasan a través de la estación de trabajo y el servidor, no coinciden.

- El usuario (o los programas que permitió instalar sin enterarse de sus posibilidades) puede enviar y recibir mensajes:
  - directamente a los servidores de correo de la red Internet (por protocolo SMTP) si en la red está abierto el puerto 25;
  - a los servicios de correo de tipo mail.ru/gmail.com — por protocolos pop3/imap4.
- El usuario (o los programas que permitió instalar sin enterarse de sus posibilidades) puede enviar mensajes por canales privados, y el servidor no podrá analizarlos.
- El servidor (o los programas instalados en el mismo) puede crear los envíos de correo y notificar a los usuarios y remitentes automáticamente sobre varios eventos.

Todo lo que entra en la empresa y sale de la empresa a través del correo debe ser escaneado — ANTES DE PENETRAR en los equipos y dispositivos de usuarios.

En los casos descritos más arriba el usuario simplemente no debía recibir el mensaje infectado.

Solo el antivirus de servidor Dr.Web para servidores de correo es capaz de:

- filtrar en el servidor tanto el correo externo (saliente y entrante) como el correo interno en busca de virus y spam — tanto en el servidor controlado por la empresa como en el alquilado;
- filtrar el correo en la Gateway, e.d. al aislar el servidor de la red Internet;
- escanear los mensajes de correo almacenados en el servidor en busca de las amenazas anteriormente no detectadas;
- mover el correo filtrado a la cuarentena y/o al archivo por si surgen dudas sobre el filtrado incorrecto;
- proteger todas las vías de recepción y envío del correo entre los servidores de correo de sucursales de la empresa y con los servicios de correo externos (Mail.ru, Gmail etc.);
- recuperar mensajes borrados accidentalmente por los usuarios en sus buzones de correo, así como realizar investigaciones relacionadas con la filtración de información.

El antivirus para el filtrado del correo ahorra el tráfico

La presencia de virus y de spam en el tráfico de correo provoca los siguientes problemas:

- reducción del rendimiento del servidor de correo dedicado a procesamiento del tráfico parásito;
- aumento de la carga de la red interna, reduciendo el rendimiento de recursos de red y el ancho de banda de canales;
- fallo del servidor por causa de recibir "una bomba de correo";
- tiempo muerto del equipamiento

Los virus y el spam en el tráfico de correo causan más requerimientos a la parte hardware de servidores de correo, y, por lo tanto, la necesidad de actualizar o comprar nuevos equipos.

El antivirus para filtrar el correo ahorra el tráfico de Internet

gracias a la posibilidad de recepción de varios adjuntos y la posibilidad de análisis de mensajes en caso de su recepción parcial.

El correo debe ser filtrado de forma integral

El uso del antivirus sin antispam:

- permite a los hackers realizar los ataques spam de phishing a los servidores de correo de la empresa y los clientes de correo de su personal; en algunos casos basta con recibir un mensaje para infectar el equipo o dañar su funcionamiento;
- causa el aumento de pago de tráfico;
- causa el aumento de la carga parásita no productiva de servidores de correo;
- baja el rendimiento de todo el personal de la empresa que recibe el correo y está obligado a limpiar sus cuentas de correo de spam.

El Antispam Dr.Web funciona a base de reglas y borra de los mensajes, de forma eficaz, hasta los programas nocivos desconocidos para el antivirus.

El Antispam Dr.Web:

- se entrega como solución conjunta (y no como un producto autónomo);
- se instala en el mismo servidor que el producto para filtrar virus

Esto simplifica la administración y asegura un precio total más bajo que las soluciones de empresas competidoras.

Ventajas del antispam Dr.Web:

- No requiere formación y empieza a funcionar de forma eficaz a partir de la instalación — a diferencia de los antispam de competidores basados en el uso del algoritmo bayesiano.
- La decisión si es spam/no es spam no depende del idioma del mensaje.
- Permite establecer varias acciones para varias categorías de spam.
- Usa sus propias listas blancas y negras, por lo tanto, no es posible comprometer las empresas por medio de añadirlas de forma malintencionada a los listados de direcciones no deseadas.
- Permite pocos falsos positivos.
- Necesita actualización no más de una vez al día, y, por lo tanto, ahorra el tráfico - las tecnologías únicas para detectar el correo no deseado a base de varios miles de reglas permiten evitar las descargas frecuentes de actualizaciones que pesan mucho.

Productos Dr.Web para el filtrado del correo

Dr.Web Mail Security Suite

Unix: ▪ Sendmail ▪ Postfix ▪ Exim ▪ QMail ▪ Communigate Pro ▪ Courier ▪ ZMailer	MS Exchange	IBM Lotus Domino	Kerio (Windows, Linux, macOS)

Posibilidades de administración:

- Administración a través de a interfaz web.
- **Administración a través de la consola Dr.Web Enterprise Suite.** La integración en el sistema Dr.Web Enterprise Suite permite asegurar la administración del sistema de la protección antivirus «desde un solo punto» con máxima comodidad para el administrador de sistemas.
- Administración a través de las utilidades de la línea de comandos.

UNA CLAVE para cualquier producto deDr.Web Mail Security Suite.

Licencias

Por el número de direcciones	Licencia por servidores (hasta 3000 direcciones)	Licencia ilimitada, para cualquier número de servidores

Tipos de licencias

- Antivirus
- Antivirus + Antispam
- Antivirus + Antispam + SMTP Proxy
- Antivirus + SMTP Proxy
- Antispam + SMTP Proxy

! La mejor calidad de filtrado es posible en caso de usar la Gateway de correo Dr.Web SMTP proxy — un filtro que procesa los mensajes antes de que los mismos llegan al servidor de correo.
Vd. no necesita recibir ningún mensaje nocivo si su servidor está conectado a Internet, el atacante le encontrará (por ejemplo, al averiguar la dirección).

El uso de **Dr.Web SMTP proxy:**

- mejora significativamente la seguridad global de la red;
- mejora significativamente la calidad de la filtración debido a la ausencia de las restricciones establecidas por los servidores de correo;
- reduce la carga de los servidores de correo internos y estaciones de trabajo;
- mejora la estabilidad de funcionamiento del sistema de escaneo de correo en total.

El uso de la zona desmilitarizada y los medios de escaneo del tráfico de correo a nivel de la Gateway SMTP aumenta el nivel de protección.

El servidor también debe ser protegido

Igual que un servidor de correo, una puerta de enlace es un servicio ordinario ubicado en un servidor ordinario. Por lo tanto, además de la protección del servicio de correo, es necesario usar la protección del servidor y de los canales de comunicación con el mismo.

- Un servidor de correo puede ser infectado tanto desde dentro como desde fuera.
- Solo la protección del servidor y los canales de comunicación con el mismo (tanto internos como externos) le podrá proteger para que el mismo no se convierta en una fuente de difusión de infecciones si un virus desconocido penetra en la red.
- Cualquier servidor necesita protección, tanto un servidor ubicado en la empresa como un servidor externo alquilado

Consecuencias técnicas de infección del servidor	Consecuencias comerciales de la infección del servidor
▪ Reducción del rendimiento del servidor o el fallo completo del mismo (tiempo muerto). ▪ Aumento de la carga de la red interna, reduciendo el rendimiento de recursos de red y el ancho de banda de canales. ▪ Rechazo de servicio — la empresa puede ser desconectada de la red Internet o ser introducida en las listas negras por enviar spam en caso de formar parte de una botnet. ▪ Más gastos en la infraestructura IT (pago del tráfico parásito / aumento del número de servidores / gastos para almacenar el correo, así mismo, spam).	▪ Errores de la continuidad de los procesos de negocios: – Los empleados tardan más en cumplir con sus tareas laborales; – Retrasos de cumplimiento de obligaciones para los clientes; – Bloqueo de la recepción del correo por los socios porque la empresa forma parte de las listas negras; ▪ peor imagen para consumidores y socios; ▪ opinión sobre la empresa como tecnológicamente atrasada; ▪ pérdida de clientes, renuncia a los servicios de la empresa.

El antivirus para la protección del servidor ahorra el tráfico

- El correo se filtrará una vez en el servidor, y no varias veces en cada estación, lo que mejorará la velocidad de funcionamiento de las mismas, y el personal se quejará mucho menos de "demoras" en sus equipos de trabajo.
- Gracias al uso del antispam en Dr.Web Mail Security Suite, la carga parásita no productiva del servidor de correo se reducirá (el volumen de spam en el tráfico de correo es de hasta 98%, y el filtrado del mismo mejorará el funcionamiento del servidor de correo). Las demoras de la entrega del correo y los mensajes perdidos serán muy poco frecuentes.

Solución correcta Dr.Web Server Security Suite + Dr.Web Mail Security Suite

- Las tecnologías de protección preventiva de Dr.Web Server Security Suite para Windows protegerán hasta contra las amenazas aún desconocidas y exploits, los intentos de comunicación de objetos nocivos administrados de forma remota con el servidor de los malintencionados (para administrar las botnets y espionaje). Sin depender de las bases de virus y la frecuencia de sus actualizaciones.
- El módulo de autoprotección Dr.Web SelfPROtect que no tiene análogos en el mercado no permitirá dañar Dr.Web para controlar el servidor — la filtración del correo no será detenida, y la copia de seguridad del servidor será protegida contra los intentos de cifrado o vandalismo.
- **Inicio antes de finalizar el inicio del SO** Funcionamiento a nivel mínimo posible del sistema operativo

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.

125040, 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