Dr.WEB®
ATM Shield

Protección centralizada
de sistemas informáticos incorporados
(cajeros automáticos, terminales de pago, multiquioscos, redes de cajas etc.)

En marzo del año 2009 en Rusia fue detectado el primer programa malintencionado que infectaba cajeros automáticos. Los cajeros automáticos infectados por Trojan.Skimer se detectaron en Moscú, y luego en San Petersburgo. La primera en reaccionar a esta amenaza fue la empresa **Doctor Web** que informó sobre Trojan.Skimer y luego creó un antivirus especializado que protege los sistemas informáticos incorporados de los virus en tiempo real (cajeros automáticos, terminales de pago, multiquioscos, redes de cajas) – **Dr.Web ATM Shield**.

Dr.WEB®
ATM Shield

¿Es verdad que Vd. también lo hace?

- Usa las unidades USB sin escanearlas para ver si hay virus?
- Abre el correo de remitentes desconocidos?
- Trabaja en Windows con derechos de administrador?
- No realiza las actualizaciones de seguridad de todo el software instalado en el equipo?
- Navega en Internet desde su equipo de oficina que tiene software con vulnerabilidades?
- Usa contraseñas no complicadas, fáciles de crackear?

¿Por qué piensa que el personal de servicio de cajeros automáticos y terminales no hace lo mismo?

¿Hay virus de cajeros automáticos?

Todavía no han sido localizados los virus especializados de cajeros automáticos – programas malintencionados capaces de autopropagarse. ¡Pero el número de programas troyanos sigue creciendo! Solo en un mes – diciembre del año 2013 – aparecieron 4 nuevos troyanos de cajeros automáticos: Trojan.Ploutus.1, Trojan.Ploutus.2, Trojan.Skimer.19 y Trojan.PWS.OSMP.21.

Algunas peculiaridades de troyanos de cajeros automáticos:

- administración del programa malintencionado por medio de tarjetas maestras especialmente preparadas, desde un dispositivo móvil;
- intercepción y descifrado del PIN una vez introducido el mismo por el titular ¡usando el software del cajero automático mismo!;
- robo de datos de tarjetas bancarias; almacenamiento de los datos robados en una tarjeta de plástico de malhechores o impresión de los mismos en un ticket de caja;
- entrega de dinero de cajero automático por comando de malhechores transmitido al troyano a través del teclado del cajero automático o por un mensaje SMS especialmente creado.

Los cajeros automáticos se mantienen por personal cualificado —¿cómo algo malintencionado puede penetrar en los mismos?

Las infecciones son posibles:

- desde dispositivos extraíbles que sirven para realizar trabajos planificados en un cajero automático por el personal de servicio que también los usa para sus fines personales;
- desde dispositivos extraíbles de delincuentes, para lo que la parte de hardware del cajero automático se abre usando una clave especial;
- por penetrar los programas malintencionados desde la red interna infectada de la empresa – si hay acceso a los sistemas incorporados desde la misma;
- si hay vulnerabilidades en el software del cajero automático.

Incluso si un programa ordinario malintencionado que no sabe trabajar con dinero y tarjetas bancarias penetra en un cajero automático, — «pantalla azul», cifrado de información visualizando en la pantalla requerimientos de rescate y, como resultado, fotos en todo Internet y la pérdida de buena fama — todo esto no solamente es desagradable, sino también requiere gastos para restaurar el funcionamiento del equipamiento.

¡Dr.Web ATM Shield – no es solamente un antivirus!

Dr.Web ATM Shield incluye los medios que restringen considerablemente las posibilidades de infección voluntaria o involuntaria de cajeros automáticos:

- monitor de archivos asegura la imposibilidad de inicio de programas malintencionados conocidos;
- antirootkit asegura la detección de amenazas anteriormente desconocidas;
- control de oficina restringe posibilidades de trabajo con catálogos locales y recursos en Internet, lo que impide que un programa malintencionado transmita los datos a su "titular" o se conecte al centro de administración;
- prohibición de uso de dispositivos extraíbles permite evitar la posibilidad de incorporación de programas malintencionados desde dispositivos extraíbles desconocidos;
- sistema de control de tráfico de Internet asegura la conexión a Internet solo para programas permitidos y por puertos permitidos.

Dr.WEB®
ATM Shield

Dr.Web ATM Shield ha sido desarrollado especialmente para afrontar las amenazas típicas para dispositivos incorporados

¿Por qué usar una solución especializada si es posible instalar un anvitirus ordinario?

Las peculiaridades de dispositivos incorporados son:

- poca memoria operativa y un procesador relativamente flojo;
- necesidad de trabajar sin reinicio 24 horas;
- uso de SO para dispositivos incorporados además de sistemas operativos ordinarios.

Dr.Web ATM Shield ha sido desarrollado especialmente para funcionar en configuraciones flojas de hardware

Para el buen funcionamiento de **Dr.Web ATM Shield** basta con tener 512 MB de memoria operativa en un dispositivo extraíble.

Una peculiaridad de productos Dr.Web, entre ellos, de **Dr.Web ATM Shield**, son las bases de virus compactas y el pequeño tamaño de actualizaciones, lo que permite proteger los dispositivos remotos que tienen un canal «estrecho» de conexión a Internet o a la red de la empresa.

Dr.Web ATM Shield soporta los sistemas operativos para dispositivos incorporados

Dr.Web ATM Shield puede usarse no solamente en sistemas operativos ordinarios – tales como Windows® XP Professional, Windows® Vista y Windows® 7 y Windows® 8, sino también en Windows® XP Embedded, Windows® 7 Embedded, Windows® 8 Embedded.

¡Dr.Web ATM Shield – no es solamente un antivirus!

También es:

- tecnologías que permiten minimizar el periodo de escaneo y descarga (asimismo, usando el escaneo multiflujo y escaneo de archivos que se abren "para lectura" aplazado);
- funcionamiento estable del sistema incluso en los equipos con la configuración antigua;
- núcleo antivirus moderno que permite localizar y neutralizar los virus más nuevos que todavía no forman parte de las bases de virus, entre ellos, los ocultos por empaquetadores desconocidos;
- sistema de autoprotección potente que no permite que los virus dañen el funcionamiento del sistema.

Dr.Web ATM Shield es la única solución que toma en cuenta las peculiaridades de dispositivos incorporados

Atención!

El robo de dinero usando el software malintencionado es un delito.

La empresa Doctor Web ofrece los servicios de peritaje de incidentes vinculados con los virus, así como el examen psicológico de personas (del personal) para detectar los hechos de estar vinculado con la realización / ayuda / encubierta / promoción de acciones ilegales hacia el cliente, los hechos de inactividad o de cumplimiento irresponsable de las responsabilidades laborales.

http://antifraud.drweb.com/expertise/

En el sitio web Doctor Web, en el apartado «Ámbito lega» http://legal.drweb.com/ pueden consultarse las plantillas de solicitudes a policía y a otras entidades, así como recomendaciones sobre cómo actuar una vez detectado el robo. ¡Use esta información!

Sobre la empresa Doctor Web

Doctor Web es un productor ruso de los medios de protección de la información antivirus bajo la marca Dr.Web.

Los productos Dr.Web se desarrollan a partir del año 1992. Es una de las empresas más importantes en el mercado ruso de software para asegurar la necesidad básica del negocio — la seguridad de la 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 clientes afrontar de manera eficaz a cualquier tipo de amenaza, asimismo, desconocida.

Doctor Web fue la primera empresa que ofreció en el mercado ruso un modelo de innovación para usar antivirus como servicio, y hoy día sigue siendo un líder del mercado ruso de servicios Internet de seguridad para proveedores de servicios de TI. Los certificados estatales y los premios, así como la geografía de los usuarios Dr.Web confirman la alta calidad de los productos creados por los informáticos rusos capacitados.

Entre los clientes de Doctor Web hay empresas importantes en el mercado mundial, bancos rusos e internacionales, entidades públicas, entidades de formación e institutos de ciencia e investigación cuyas redes cuentan con docenas de miles de equipos. Los organismos superiores del poder estatal y ejecutivo de Rusia así como las empresas de sector de combustible y energía confían en las soluciones antivirus de Doctor Web.

Rusia, 125124, Moscu, 3-ra calle Yamskogo campo, edif.2, vivienda 12A
Numero de tel fono: +7 (495) 789-45-87 (multicanal)
Fax: +7 (495) 789-45-97
https://www.drweb.com | https://ru.av-desk.com | https://free.drweb.com