

# Dr.Web vxCube

- ANALIZADOR INTERACTIVO DE AMENAZAS DESCONOCIDAS EN LA NUBE (0-DAY), ASÍ MISMO, USADO PARA ATAQUES OBJETIVO
- GENERACIÓN INMEDIATA DE LA UTILIDAD DE DESINFECCIÓN SEGÚN LOS RESULTADOS DEL ANÁLISIS
- PARA EXPERTOS EN SEGURIDAD INFORMÁTICA Y CIBERCRIMINALISTAS



## Dr.Web vxCube

Imagine que, a pesar de la protección de su red con un antivirus, un archivo nocivo logró penetrar en el perímetro. O Vd. sospecha que haya algo nocivo en la red.

Lo correcto será enviar el archivo sospechoso para el análisis al laboratorio antivirus y esperar la solución. Pero el trabajo de cada analista es caro y requiere mucho tiempo.

**Y no se puede esperar:** la amenaza debe ser eliminada enseguida.

Un medio seguro en estos casos es el analizador activo en la nube Dr.Web vxCube.

Dr.Web vxCube en **un minuto** detectará si el archivo es nocivo y preparará una utilidad de desinfección para corregir las consecuencias de su funcionamiento.

<ul style="list-style-type: none"><li>▪ No requiere instalación. Funciona en la nube</li></ul>	<ul style="list-style-type: none"><li>▪ Análisis completo de comportamiento del software nocivo</li></ul>	<ul style="list-style-type: none"><li>▪ Informes claros</li></ul>	<ul style="list-style-type: none"><li>▪ API para automatizar el trabajo con el servicio</li></ul>
--	---	---	---

## Dr.Web vxCube — es un medio innovador para afrontar las amenazas desconocidas más nuevas

Hoy día la creación de virus es **un negocio criminal bien gestionado**. Centenares de miles de nuevos programas nocivos, en su mayoría, troyanos, aparecen todos los días. No todo lo que se recibe para el análisis al laboratorio antivirus de Doctor Web son programas nocivos. Pero todos deben ser procesados por nuestros expertos. El análisis de archivos nocivos requiere tiempo, así mismo, la compilación y las pruebas de actualizaciones, su carga en los servidores de actualizaciones y la instalación de actualizaciones por los usuarios lleva mucho tiempo.

### La tarea del antivirus es impedir la infección.

Así mismo, se considera que un antivirus debe detectar todos los programas nocivos en el momento de su penetración. Pero los troyanos tecnológicamente sofisticados y peligrosos, especialmente los creados para fines comerciales, los creadores de virus los comprueban en todos los antivirus para ver si pueden ser detectados, antes de lanzar su obra, para que el virus exista lo más tiempo posible sin ser detectado por los antivirus. Por lo tanto, siempre hay un periodo entre el lanzamiento del troyano por los malintencionados, la llegada de su muestra al laboratorio de virus para el análisis y la preparación del «antídoto».

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

El servicio Dr.Web vxCube permite comprobar y asegurarse de que un archivo es nocivo, revelar sus solicitudes a recursos locales y de red, así como recibir una compilación especial de la utilidad de desinfección Dr.Web CureIt!.

<b>¿Qué puede hacer un troyano en su PC?</b> Vd. lo verá antes de que el mismo empiece a funcionar.	<b>¿Cómo pueden ser las consecuencias de un ataque hipotético a su empresa?</b> Averígüelo de antemano.	<b>¿Qué tenían previsto hacer los malintencionados en su red?</b> Dr.Web vxCube lo analizará con detalle.
--	--	--

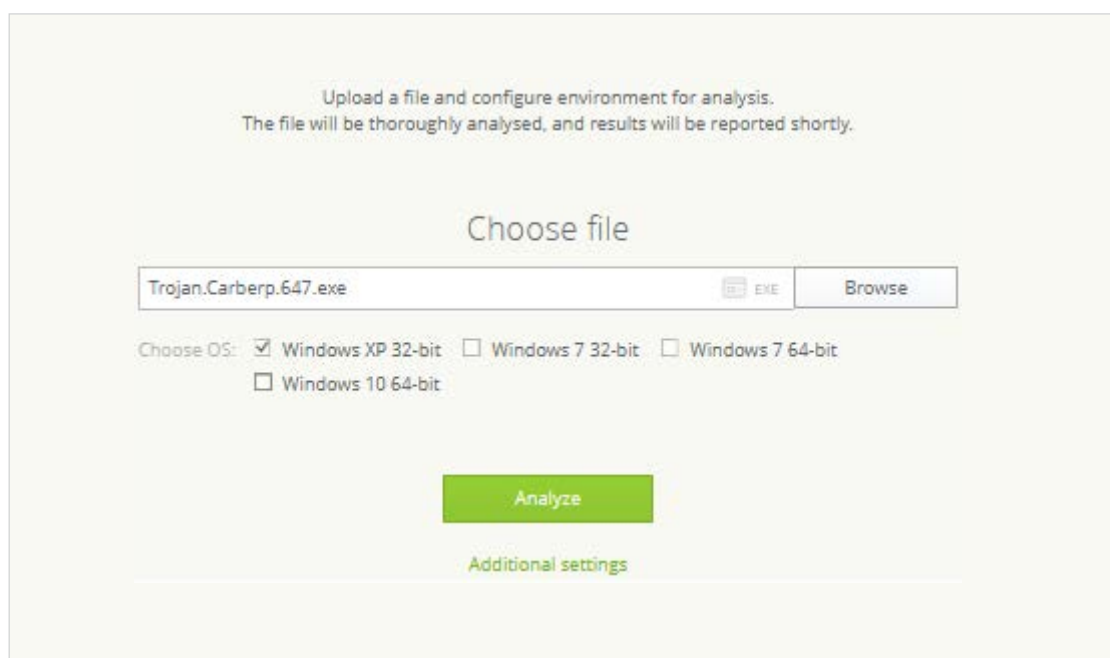
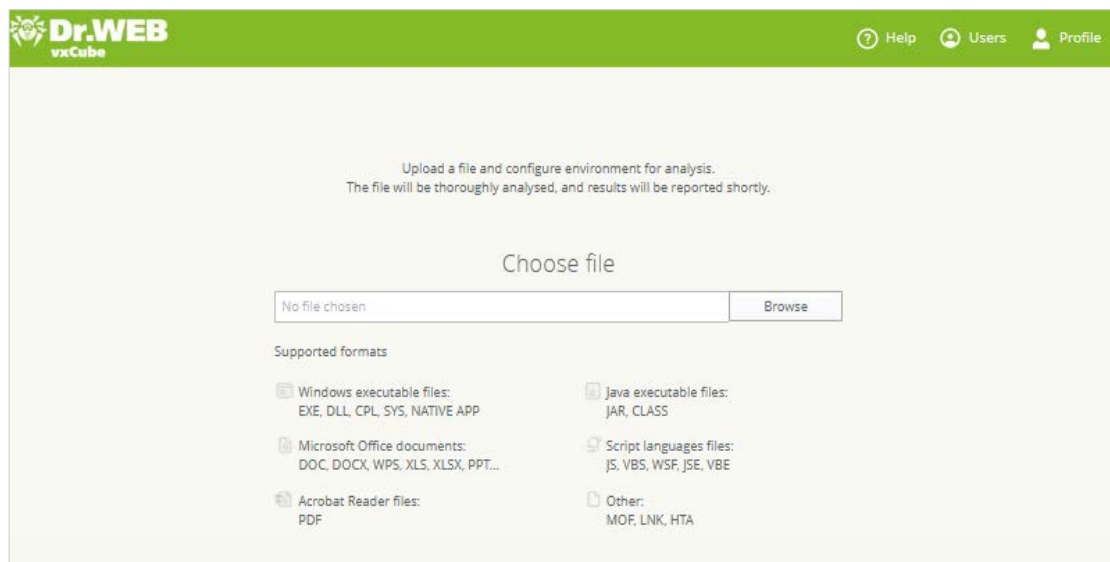
El análisis se realiza en varios sistemas operativos, se usan aplicaciones típicas más atacadas por los malintencionados hoy día:

- Archivos ejecutables de Windows
- Documentos de Microsoft Office
- Archivos de Microsoft Office
- Archivos ejecutables JAVA
- Archivos script

**!** Es posible escanear un archivo sospechoso tanto manualmente como en modo automático. La integración de Dr.Web vxCube en los servicios de la empresa permite no solamente aumentar el número de los archivos escaneados, sino también con mucha precisión detectar los ataques más nuevos, así mismo, los ataques objetivo.

## Cómo funciona Dr.Web vxCube

1. El usuario recibe acceso al analizador para enviar archivos sospechosos para el análisis en la nube. Para entrar en Dr.Web vxCube y trabajar en el mismo, basta con disponer de un navegador y la conexión a Internet.



El servicio respeta los datos personales y privados según los principios de política de privacidad de Doctor Web»: <https://company.drweb.ru/policy>. Los archivos que llegan para el análisis a través de Dr.Web vxCube, se separan de los archivos que llegan de otra forma.

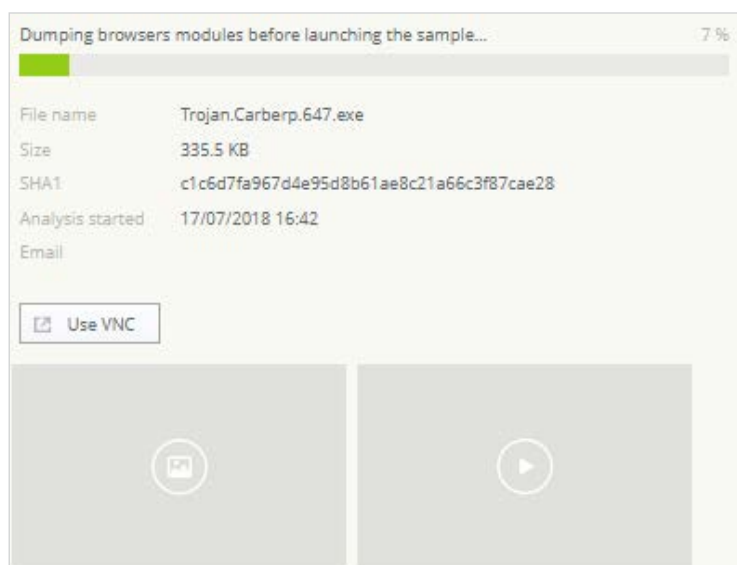
2. El analizador inicia el objeto enviado por el investigador en el entorno aislado e investiga su comportamiento. El análisis se realiza de forma automática, sin participación de los analistas de virus de Doctor Web.

El análisis lleva a partir de un minuto!

El investigador puede:

- indicar en qué sistemas operativos y con qué versiones de aplicaciones debe realizarse el escaneo;
- Indicar el periodo deseado de comprobación en configuración, si considera que un minuto no es suficiente para el análisis completo del comportamiento del archivo sospechoso;
- de forma remota — a través de la interfaz Dr.Web vxCube — supervisar el análisis y hasta influir en el mismo, al conectarse al analizador a través de VNC (Virtual Network Computing) para participar en el proceso de investigación

**! Para administrar el proceso de análisis en modo interactivo, deben permitirse las ventanas emergentes en el navegador.**



**! Como sabemos, los programas nocivos supervisan los intentos de ser iniciados en un entorno de pruebas especial e impiden este análisis. Durante el desarrollo del servicio Dr.Web vxCube fue creada una máquina virtual protegida del análisis por los programas nocivos.**

3. Si el objeto analizado sin duda es de amenaza, el usuario enseguida recibe una compilación especial de la utilidad de desinfección Dr.Web CureIt!\* para limpiar el sistema de las acciones realizadas por el archivo analizado.

**Esto permite desinfectar la amenaza más nueva lo más rápido posible, sin esperar las actualizaciones del antivirus usado.**

Gracias a la utilidad universal Dr.Web CureIt!, capaz de funcionar sin instalar en cualquier otro sistema donde se usa otro antivirus (no Dr.Web ), esto sobre todo será útil para las empresas que aún no usan Dr.Web como medio básico de protección.





4. Se ofrece un informe de los resultados del análisis. El informe puede ser consultado en la cuenta personal o descargado como archivo archivado. Así mismo, el usuario puede consultar los resultados de escaneos anteriores en su cuenta personal.

\* Si esto forma parte de la licencia.

**!** El informe sobre los resultados de pruebas contiene los datos sobre el programa analizado, en particular, las partes de su código, y por lo tanto puede ser detectado como un programa nocivo, pero no supone ningún peligro para el equipo.

## Informes del servicio Dr.Web vxCube

En el informe resultante al usuario del servicio se le ofrecen los datos siguientes.

<p><b>Valoración de nocividad</b></p>  <p>El servicio valora si el programa analizado es nocivo, y si puede ser peligroso.</p>		
<p><b>Mapa de la actividad de red</b></p> <p>Informará qué servicios y en qué países del mundo consultaba el programa nocivo.</p> 	<p><b>Grabación de vídeo</b></p> <p>Visualizará el proceso de inicio y funcionamiento del archivo.</p> 	<p><b>Conexiones</b></p> <p>Informará qué archivos solicitó el programa, en que ramas del registro se guardaba la información, qué recursos de Internet han sido usados etc.</p> 
<p><b>Información técnica</b></p> <p>Informará qué hay que eliminar del sistema, a la protección de qué partes del mismo hay que prestar más atención.</p>	<p><b>Archivos creados</b></p> <p>Se visualiza un listado de archivos creados por la muestra analizada y sus sumas de comprobación. El conocimiento sobre estos archivos permitirá eliminar las consecuencias de la infección.</p>	<p><b>Registro API</b></p> <p>Informará cómo el programa nocivo se oculta en el sistema.</p>

**!** Según la cláusula 6 del Acuerdo de licencia para Dr.Web vxCube, la publicación u otra difusión de informes, así mismo, con ánimo de lucro, debe ser acordada por escrito con Doctor Web.

### Enlaces de interés

Acceso demo: <https://download.drweb.ru/vxcube>

Licencias: <https://www.drweb.ru/vxcube/licensing>

## Análisis de archivos nocivos por los expertos del laboratorio antivirus de Doctor Web

Ningún servicio automatizado nunca sustituirá la experiencia y el conocimiento de un analista de virus. Si la resolución de Dr.Web vxCube sobre el archivo analizado dice que el mismo no es: nocivo sin duda, pero Vd. tiene sospechas sobre la misma, ofrecemos usar los servicios de los expertos del laboratorio antivirus de Doctor Web que tienen experiencia de análisis de virus de muchos años.

**Los servicios incluyen el análisis de archivos nocivos de cualquier grado de dificultad, y según los resultados del mismo, se ofrece un informe que contiene:**

- la descripción del algoritmo de funcionamiento del software nocivo y sus módulos;
- categorización de objetos: nocivo sin duda, potencialmente nocivo (sospechoso) etc.;
- descripción de algoritmos de funcionamiento del software nocivo y sus módulos;
- análisis del protocolo de red y detección de los servidores de comandos;
- influencia en el sistema infectado y recomendaciones para eliminar la infección.

Las solicitudes de análisis antivirus se reciben en la dirección siguiente: <https://support.drweb.ru>

## Peritaje de incidentes informáticos vinculados con virus (IIV)

Si su empresa ha sido víctima de un software nocivo y se requiere peritaje cualificado de los analistas de virus, use los servicios del departamento especial de la empresa Doctor Web.

**El peritaje IIV 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 vídeo) 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 en relación al 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.

### Enlaces de interés

Sobre el peritaje de IIV: <https://antifraud.drweb.ru/expertise>

Solicitudes de peritaje: <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  
2003–2018

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](http://www.drweb-av.es) | [www.av-desk.com](http://www.av-desk.com) | [curenet.drweb.com](http://curenet.drweb.com) | [www.drweb.com](http://www.drweb.com)