

# Dr.Web vxCube

- A CLOUD-BASED INTERACTIVE ANALYSIS OF UNKNOWN THREATS (ZERO-DAY), INCLUDING THOSE USED IN TARGETED ATTACKS
- AN IMMEDIATELY GENERATED CURING UTILITY BASED ON ANALYSIS RESULTS
- FOR SECURITY RESEARCHERS AND CYBERCRIME INVESTIGATORS



## Dr.Web vxCube

Imagine that despite the fact that your network is protected by an anti-virus, a malicious file has managed to get inside.

Sending a suspicious file to an anti-virus laboratory for examination and waiting for a reply would be the best way to address this issue. However, employing security researchers to undertake a single analysis is expensive and can be time-consuming.

### **But time is of the essence—the threat must be neutralised pronto.**

In situations like this, the cloud-based interactive analyser Dr.Web vxCube is indispensable.

In one minute Dr.Web vxCube will assess how malicious a file is and provide you with a curing utility that will eliminate the effects of its activity.

- No installation required.  
Cloud-based

- Comprehensive malware-behaviour analysis

- Easy-to-understand reports

- An API to automate service usage

## Dr.Web vxCube: An innovative way to combat brand-new, unidentified threats

Today virus making is a well-established, illicit business. New malicious programs, most of which are Trojans, appear in the hundreds of thousands every day. Some programs analysed in the Doctor Web anti-virus laboratory aren't malicious. However, they must all be examined by our security researchers. Analysing a malicious file takes time. And more time is required to build, test, and upload an update to a server. And then users will have to install it on their computers, which also takes time.

**An anti-virus's job is to prevent systems from getting infected.**

It is believed that anti-viruses neutralise all malicious programs as soon as they get into a computer. However, technologically sophisticated and particularly dangerous Trojans, especially those designed for commercial gain, are tested by their makers against all anti-viruses to make sure that they will remain undetected for as long as possible once they are unleashed into the wild. That's why a time gap always exists between the moment when a Trojan is released by attackers and the moment security researchers obtain samples of it for analysis.

**Computers are ALWAYS at risk of getting infected with brand-new, UNKNOWN malicious programs.**

With the Dr.Web vxCube service, you can check a file and determine that it is malicious, identify what local and network resources it has accessed, and get a special Dr.Web CureIt! build.

<b>What harm can a Trojan do on your PC?</b> You will find that out before it actually commences with its activity.	<b>What would the aftermath of a hypothetical attack on your company look like?</b> Find out in advance.	<b>What did the attackers plan to do in your network?</b> Dr.Web vxCube will give you the complete details.
--	---	--

Files are analysed in multiple operating systems. The applications most commonly attacked today by criminals are used:

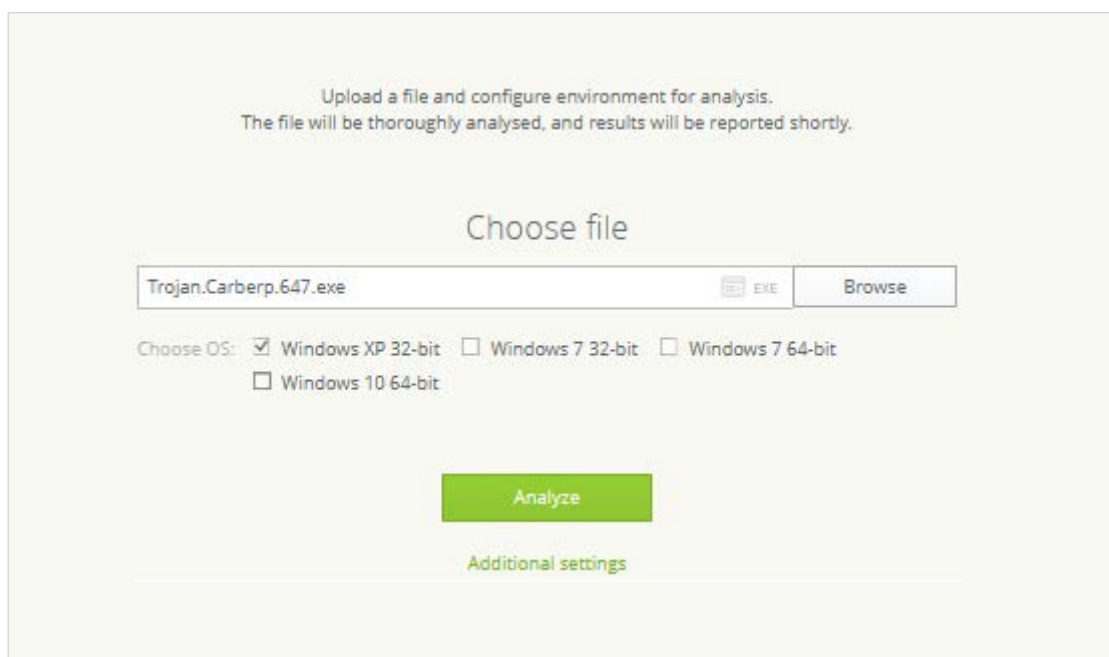
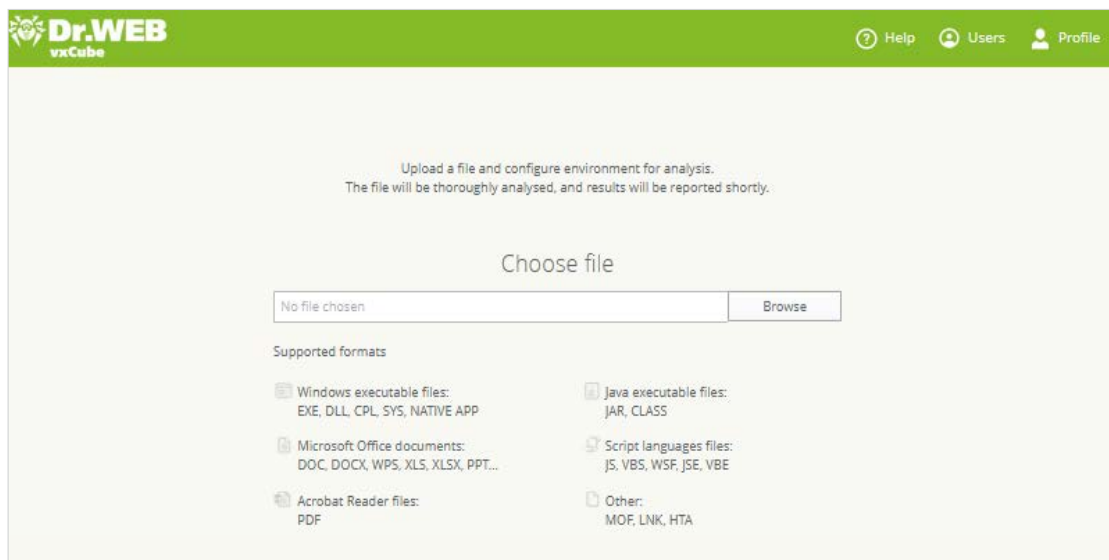
- Windows executable files
- Microsoft Office documents
- Acrobat Reader files
- JAVA executable files
- Scripts

**!** A suspicious file can be examined in both manual and automatic mode. When you integrate Dr.Web vxCube into your IT infrastructure, you can not only examine more files, but also pinpoint with a high degree of accuracy the most advanced and sophisticated malware attacks.

## How does Dr.Web vxCube work?

1. Users get access to the analyser's interface and can upload files to the cloud for examination.

To sign in and use the Dr.Web vxCube service, you only need a browser and an Internet connection.



The Service carefully protects personal and confidential data according to the principles stipulated in the Doctor Web privacy policy: <https://company.drweb.ru/policy>. Files uploaded to Dr.Web vxCube are separated from the other files our anti-virus laboratory receives for analysis.

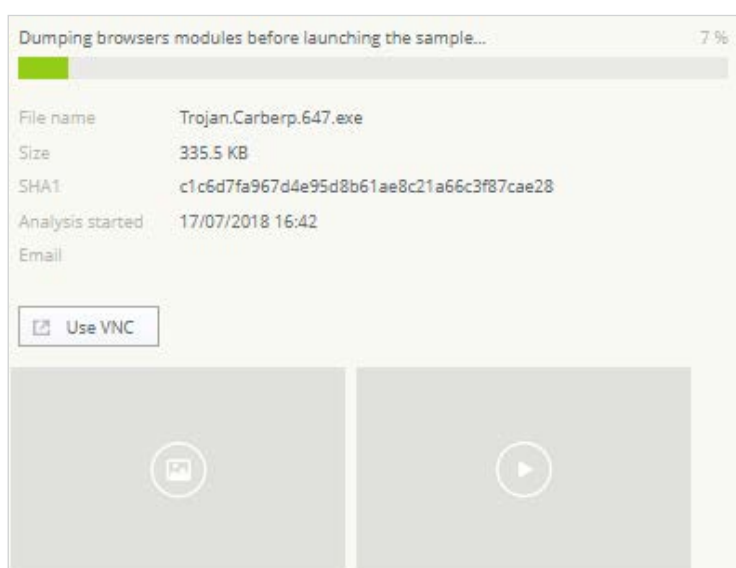
2. The service launches or opens uploaded files in a sandbox and analyses their behaviour. The analysis is conducted automatically, without the involvement of our security researchers.

The examination takes as little as one minute!

The user can:

- Specify the operating systems and application versions that will be used during the examination;
- Specify the duration of the examination (if it is felt that one minute is insufficient to thoroughly examine a suspicious file);
- Remotely monitor the examination's progress via the Dr.Web vxCube interface and even influence its course by connecting to the analyser via VNC (Virtual Network Computing) to participate in the analysis process.

**! To control the examination, the option to display pop-up windows must be enabled in your browser.**



**! Malicious programs are known to detect attempts made to launch them in a sandbox and do what they can to hinder their analysis. Dr.Web vxCube uses a special virtual machine that never exposes itself to malicious programs.**

3. If a file poses a threat, the user is instantaneously provided with a custom Dr.Web CureIt! build\* that will neutralise the malware and undo any harm it has caused to the system.

**This way you can disarm a new threat extremely quickly, without waiting for your anti-virus to eventually receive an update that would address it.**

Thanks to its versatility, Dr.Web CureIt! can operate without being installed in any system where another (non-Dr.Web) anti-virus is in use; this may particularly come in handy for companies that haven't yet chosen Dr.Web to be their primary means of protection.





4. Analysis results are provided in a report. Reports can be viewed in your Dr.Web vxCube account area or downloaded as archives. In your account area, you can also review the results of previous examinations.

\* Si esto forma parte de la licencia.

**!** Because an analysis report contains information about an examined file—including pieces of its code, your anti-virus may detect it as a threat. However, such reports pose no danger to computers.

## Dr.Web vxCube reports

Analysis reports contain the following information:

<p><b>A threat severity assessment</b></p>  <p>The service determines whether the examined file is malicious and how dangerous it may be.</p>		
<p><b>Network activity map</b></p> <p>Learn which servers the malware was trying to contact and where they are located.</p> 	<p><b>Video recording</b></p> <p>Watch how the file was opened and launched and what happened next.</p> 	<p><b>Interaction</b></p> <p>See what files the program has accessed, which registry keys have been modified by the application, which Internet nodes it connected to, etc.</p> 
<p><b>Technical details</b></p> <p>Learn what files should be removed from the system and which system components may require special attention.</p>	<p><b>Created Files</b></p> <p>A list of the files that have been created by the examined sample, including their checksums. This information may help you undo the damage caused by an infection.</p>	<p><b>API log</b></p> <p>Learn how malware hides in a system.</p>

**!** Pursuant to section 6 of the Dr.Web vxCube license agreement, the publication or distribution of Dr.Web vxCube reports for any purpose, including commercial gain, must be approved by Doctor Web in writing.

### Useful links

Trial access: <https://download.drweb.ru/vxcube>

Licensing: <https://www.drweb.com/vxcube/licensing?lng=en>

## Malware analysis by Doctor Web security researchers

No automated routine can ever replace the experience and knowledge of a security researcher. If Dr.Web vxCube returns a “safe” verdict on your analysed file, but you still have your doubts about this result, Doctor Web’s security researchers, who have a wealth of experience analysing malware, are ready to assist you.

**With this service, a malicious file of any complexity can be analysed. The resulting report includes:**

- Information about the malware’s basic principles of operation and that of its modules;
- An object assessment: downright malicious, potentially dangerous (suspicious), etc.;
- An analysis of the malware’s networking features and the location of its command and control servers;
- The impact on the infected system and recommendations on how the threat can be neutralised.

You can submit an anti-virus research request here: <https://support.drweb.ru>.

## Virus-related computer incident (VCI) expert consultations

If malware has wreaked havoc in your corporate infrastructure and you require the expertise of security researchers to investigate the incident, Doctor Web’s information security task force is at your service.

**VCI consultations include:**

- An initial assessment of the incident, the scope of the investigation, and the measures required to remedy the consequences of the incident.
- An examination of the computer and the other related items (hard disks, and text, audio, photo, and video materials) that are presumably related to the VCI.
- **Exclusive!** A psychological evaluation of individuals (company personnel) to identify facts related to the possible accomplices involved in/assisting with/covering up or supporting illegal activities against the customer (a comprehensive risk assessment) as well as facts related to employee inaction or dereliction of duty.
- Recommendations on the deployment of an anti-virus protection system that would prevent VCIs or reduce them to a minimum in the future.

### Useful links

Find out more about VCI consultations: <https://antifraud.drweb.com/expertise?lng=en>

Submit your consultation request here: <https://support.drweb.ru/expertise>

## About Doctor Web

Doctor Web is the Russian developer of Dr.Web anti-virus software. Dr.Web anti-virus software has been developed since 1992. The company is a key player on the Russian market for software that meets the fundamental need of any business — information security.

Doctor Web was the first company on the Russian market to offer an anti-virus as a service and, to this day, is still the undisputed Russian market leader in Internet security services for ISPs.

## Customers trust Dr.Web

Doctor Web's IT security experts possess a wide range of capabilities, which allows the company to thoroughly understand the operational nuances of all kinds of businesses and offer its customers the best selection of quality products at minimal TCO.

The fact that Doctor Web has satisfied customers—home users, major corporations, and small businesses—all over the world is clear evidence that the quality of its products, created by a talented team of Russian programmers, is undisputed.

Here are just some Dr.Web customers: <https://customers.drweb.com>.

## Why Dr.Web?

All rights to Dr.Web technologies are reserved by Doctor Web. The company is one of the few anti-virus vendors in the world to have its **own technologies** for detecting and curing malware. Doctor Web has its own anti-virus laboratory, global virus-monitoring service, and technical support service.



**Doctor Web**  
**2003–2018**

3rd street Yamskogo polya 2-12A, Moscow, Russia, 125040

Tel.: +7 (495) 789–45–87

Fax: +7 (495) 789–45–97

<https://www.drweb.com> | <https://free.drweb.com> | <https://ru.av-desk.com> | <https://curenet.drweb.com>