Dr.WEB®
since 1992

Filtering email with Dr.Web anti-viruses

Email is the main source of the spread of Trojans and spam

As a rule, Trojans get into computers when users act carelessly with removable media or email.

Here are some Dr.Web support requests received from users whose systems were compromised by Encoder programs:

I downloaded an archive file from an email. As a result, all of my Word and Excel documents and images are encrypted; the extension was 1TXT.

The encrypted files have the extension 1txt. I opened a dubious email and everything started getting encrypted.

On 10/10 at around 11:00 AM, I received an email in my Yandex mailbox, opened it, and the encryption happened.

Today, I opened an attachment, and all of my DOC and XLS files got the extension VAULT.
Good afternoon! An employee received an email with an attached archive file. The message was marked as urgent. The archive contained a .js file. After that the malware VAULT infected the system, encrypting all the files. Help us cure and decrypt our data.

Is workstation protection enough to prevent those infections?

No.

Hello; We received an email with the file "18.06.18.Gz" attached to it. We opened it. It turned out to be a Trojan. The hard drive is split into two partitions. On the C drive, many files and folders are highlighted in blue, but nothing like that happened to the data on the D partition.

From a request submitted to the Doctor Web support service

An analysis of the anti-virus log (the log file can be found in %userprofile%\desktop\drweb.log) revealed the following picture:

1. The installed anti-virus had the definition of the encryption ransomware in question.
2. But the most unusual thing is how the Trojan managed to launch itself:

threat: DPH:Trojan.Encoder.9 ==> send user blocked alert	The user is trying to launch the program; and the anti-virus is detecting the Trojan and displaying the corresponding notification.
threat: DPH:Trojan.Encoder.9 ==> send user blocked alert	Another launch attempt!

A few more attempts to launch the Trojan followed until the user decided that since the anti-virus wouldn't let them start the program, they would be better off disabling it.

And this is not a complete list of reasons to establish email filtering on a server.
The mail flows passing through a workstation and a server are not the same.

- Users (or programs installed by uninformed users) can send and receive messages:
  - directly to Internet mail servers (via SMTP), if port 25 is open in the network;
  - to mail services like mail.ru/gmail.com — via POP3/IMAP4 protocols.
- Users (or the programs they agreed to install without knowing their functionality) can send messages over secure channels, and the server will not be able to check them.
- A server (or the programs installed on it) can create its own mailing lists and notify senders and recipients of various events independently.

Everything that a company receives or sends via email must be scanned BEFORE it reaches user computers and devices.

In the cases we described above, the user simply must not have received an infected email.

Only Dr.Web for Mail Servers can:

- filter both the external (incoming and outgoing) and the internal mail for viruses and spam—on both company-controlled servers and company-leased servers;
- filter email at the gateway, i.e., by isolating a server from the Internet;
- scan emails stored on a server for the presence of previously undetected threats;
- move filtered email to the quarantine and/or archive to address any complaints about filtering errors;
- protect all the channels that send and receive email between the mail servers of a company's branches and with external mail services (Mail.ru, Gmail, and so on);
- recover messages accidentally deleted from employee mailboxes, and also pursue investigations related to data leaks.

An email-filtering anti-virus saves traffic

Viruses and spam in mail traffic cause the following issues:

- the mail server used for processing spurious traffic performs poorly;
- an increase in the internal network load and a decrease in the performance of network resources and channel bandwidth;
- server failure after a "mail bomb" is received;
- hardware downtime.

Viruses and spam in mail traffic lead to an increase in the requirements related to mail server hardware and, therefore, to the need to upgrade or purchase new workstations.

An email-traffic-filtering anti-virus saves Internet traffic by restricting the receipt of attachments and analysing emails once they have been partially received.

Email should be filtered in its entirety

Using an anti-virus that has no anti-spam:

- lets hackers carry out attacks on a company's mail servers and the email clients used by its employees; sometimes the fact of receiving an email may be sufficient to infect a machine or disrupt its operation;
- leads to increased traffic costs;
- increases unproductive, spurious loads on mail servers;
- reduces the productivity of all email-receiving employees, who have to spend time deleting spam from their mailboxes.

Dr.Web Anti-spam operates on the basis of rules and even effectively removes malware that is unknown to the anti-virus.

Dr.Web Anti-spam:

- is delivered as part of a single solution (not as a separate product);
- is installed with a virus-filtering product on the same server.

This simplifies administration and ensures a lower total cost than would have been the case had our competitors' solutions been purchased instead.

Advantages of Dr.Web anti-spam:

- The anti-spam doesn't require training. Unlike competitive anti-spam solutions based on Bayesian filtering, it starts working as soon as it is installed;
- It detects spam messages regardless of their language;
- Actions can be customised for different categories of spam;
- It uses its own whitelists and blacklists, which makes it impossible to discredit companies by deliberately adding them to lists of unwanted addresses;
- Low number of false positives;
- Requires updating only once a day, thus saving bandwidth. Unique spam-detection technologies based on several thousands of rules eliminate the need for downloads of frequent and bulky updates.

Dr.Web products for email filtering

Dr.Web Mail Security Suite

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

Ways the products can be administered:

- Via the web interface
- Via the Dr.Web Enterprise Suite console. Because the console is integrated into the Dr.Web Enterprise Suite system, the anti-virus protection system can be administered from a single point, offering system administrators maximum convenience.
- Via command-line utilities.

ONE KEY for any Dr.Web Mail Security Suite product.

Licensing

Per number of addresses	Per server license (up to 3,000 addresses)	Unlimited license for any number of servers

Types of licenses

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

! For maximum filtration quality, use Dr.Web SMTP proxy—a filter that processes email messages before they reach your mail server.
You don't even have to get a malicious email; if your server is on the Internet, an attacker will find you (e.g., via a brute-force attack).

Dr.Web SMTP proxy:

- substantially increases network security;
- significantly improves the filtering quality due to the absence of any mail-server restrictions;
- decreases the workload for local mail servers and workstations;
- improves a mail-filtering system's stability.

Using a demilitarised zone and solutions that check email traffic at the SMTP-gateway level increases the level of security.

The mail server must also be protected

A mail server is a service located on a standard file server. Therefore, in addition to protecting your email service, you need to protect the server itself and the channels that communicate with it.

- A mail server can be infected both internally and externally.
- Only by protecting the server itself and the channels that communicate with it (both internal and external) can you protect the server from becoming a source of infection when an unknown virus penetrates the network.
- Any server needs protection — both one that is located within a company's premises and a leased external server.

Technical consequences of a server infection	Commercial consequences of a server infection
▪ Server performance slows down or crashes. ▪ An increase in the internal network load and a decrease in the performance of network resources and channel bandwidth. ▪ Denial of service – a company is disconnected from the Internet or placed on blacklists for sending out spam if it has become part of a botnet. ▪ An increase in IT infrastructure costs (paying for "spurious" traffic/more servers/mail storage costs, including those for spam).	▪ A breach in continuity of business processes: – delays in staff being able to carry out their duties; – delays in the fulfilment of the company's obligations towards its customers and partners; – Partners are prevented from receiving email because the company has been placed on blacklists; ▪ Consumers and partners feel less confident in the company's abilities; ▪ The perception that the company is technologically backward; ▪ Customers lost because they don't want to use the company's services.

An anti-virus for server protection saves traffic

- Email will be filtered on the server once, rather than several times on each PC—this will improve performance, and employees will be much less likely to complain about low PC performance.
- The encryption and compression employed by Dr.Web products will help decrease local traffic; no other developer provides this feature in products for PCs.
- Thanks to the anti-spam incorporated into Dr.Web Mail Security Suite, the mail server won't be involved in processing large volumes of spam (the amount of spam in email traffic reaches up to 98%, and filtering it out will improve the mail server's performance). Delivery delays and lost emails will be rare events!

The right decision: Dr.Web Server Security Suite + Dr.Web Mail Security Suite

- The preventive protection technologies available in Dr.Web Server Security Suite for Windows will protect against even unknown threats and exploits as well as communication attempts between remotely managed malicious objects and a malicious server (to control botnets and for espionage)—without any dependency on virus databases and the frequency with which they are updated.
- Dr.Web SelfPROtect is a unique anti-virus component that neutralises any attempts by malicious programs to disrupt the Dr.Web anti-virus's operation—email filtering won't be stopped and the server backup will be protected from encryption attempts and vandalism
- **Launches before the OS boots up!** Operates on the lowest possible system level!

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.

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