

Dr.Web Anti-virus Service

for



Introduction

▪ Modern virus threats.....	2
▪ Security is a service.....	11

Dr.Web anti-virus protection system

1. Anti-virus protection components	
▪ Control Center.....	15
▪ System administrators.....	18
▪ Groups. Group management.....	19
▪ Dr.Web as a service subscription packages and protection components.....	20
▪ Subscription Control Center (SCC).....	23
2. Information security policies	
▪ Creation of a solid protection ecosystem.....	28
▪ File server protection.....	29
▪ Regular updates of virus databases and program modules.....	31
▪ Regular scans of workstations.....	32
▪ Removable media access restriction.....	34
▪ Restricting Internet access.....	36
▪ Protecting against malware infections and phishing.....	36
▪ Reducing Internet costs and employee monitoring.....	38
▪ Anti-spam protection.....	39
▪ Protection against virus attacks on devices with e-banking systems installed.....	42
▪ Protection against hacker attacks.....	45
▪ Protection against intrusions via vulnerabilities.....	46
▪ Protection against infections made using social-engineering techniques.....	47
▪ Reduction of downtime caused by viruses.....	48
3. Services	
▪ Alerts.....	50
▪ Instant messaging.....	50
▪ Statistics and reports.....	50
▪ Audit log.....	50

Conclusion

▪ About Doctor Web.....	52
▪ Contacts.....	53

Introduction

Modern virus threats

Viruses are written by lone hackers

Previously, malicious software was actually created by lone programmers. Today's malware is developed by professional virus writers. This is a well-organized criminal business involving qualified system and application developers.

Structural elements of some criminal organizations

In some cases, the roles of attackers inside criminal organizations can be subdivided as follows:

1. Organizers, – persons who organize and guide the process of creating and using malicious software. Malicious software can either be used directly or sold to other criminals or their associations.
2. Participating members:
 - Malware developers.
 - Malware testers (malware is also tested to see whether it can get past known anti-virus programs).
 - Testers of vulnerabilities in operating systems and application software for criminal purposes.
 - «Experts» in using virus packers and encryption.
 - Malware distributors and social engineering experts.
 - System administrators who ensure that the operating environment is safe within the criminal organization and control botnets.

Criminal groups involved in the development and spread of viruses are thoroughly organized, so virus production has become streamlined, thus leading to explosive growth in the quantity of malicious malware. This immediately spawned a host of daily signature records being added to virus databases..

Facts

- The Doctor Web virus monitoring service collects samples of malicious programs all over the Internet.
- The Dr.Web anti-virus lab receives on average about 60,000 malware samples daily.
- A record of sorts was set on November 28, 2012, when the Dr.Web anti-virus lab received over 300,000 samples. And that is not all of the malware that was created that day.

Virus analysts are not magicians and cannot instantly process the thousands and thousands of suspicious files received daily. Therefore, automated systems that can process incoming suspicious files are becoming an essential anti-malware element. The performance of such systems is no less important than the quality of commercial software running on user computers.

An anti-virus should detect 100% of viruses

The prehistory of a misconception

In the anti-virus industry, independent testers have long been conducting so-called comparative testing on virus detection. For these tests, a collection of viruses and malware is assembled, anti-viruses are updated to the latest versions, and the collection is scanned. To win the test, 100% of the viruses in the collection must be detected.

Some features of these tests are as follows:

- None of the testers can guarantee that its own collection contains malware only;
- These tests show only one of an anti-virus' features, i.e., threat detection;
- Such tests allow the performance of only one component among the multiple components incorporated in the anti-virus to be evaluated – the file monitor or the scanner;– in other words, the anti-virus is tested for its ability to combat known threats only;
- Such tests do not show an anti-virus' behaviour under real computer virus infection conditions, how it knows how to cure a certain virus;
- Such tests do not indicate whether an anti-virus can detect unknown threats.

It is namely tests such as these that created this dangerous misconception.

Facts

- Technologically sophisticated and highly dangerous viruses, including rootkits, are created for commercial gain. Virus writers scan them with all known anti-viruses before releasing them into the wild. After all, they need a virus to do its job on an infected machine for as long as possible. From the point of view of virus makers, an easy-to-spot virus is a bad virus. That's why many malware samples are not detected by anti-viruses before they get into an anti-virus lab.
- A virus can reach your computer by exploiting a zero-day vulnerability (a vulnerability that is still only known to virus writers or hasn't been closed by the software vendor), or a user may fall for a social engineering trick and launch a virus file and even disable an anti-virus' self-protection.

Anti-viruses catch viruses using relevant virus signatures (i.e., records in virus databases)

If this were so, an anti-virus would be helpless in the face of unknown threats.

However, an anti-virus remains the best and the only effective protection tool against all types of malicious threats – and, most importantly, – against viruses both **known** and **unknown** to the virus database.

Dr.Web incorporates many effective non-signature technologies for detecting and removing unknown malware. Together, they make it possible to detect the latest (unknown) threats before they are registered in the virus database. We'll describe just a few of them.

- **Fly-Code technology** ensures the high-quality scanning of packed executables and virtualized file execution to unpack any (even non-standard) packers; this makes it possible to detect viruses that are even unknown to Dr.Web anti-virus software.
- **Origins Tracing** treats a scanned executable as a specific sample which it then compares against the database of known malicious programs. The technology makes it highly likely that viruses not yet added to the Dr.Web virus database will be detected.
- **Structural entropy analysis** detects unknown threats by arranging pieces of code in objects protected with encryption compression, interrupting the routines they use, and utilizing some additional parameters. This allows Dr.Web to detect a substantial portion of unknown threats.
- **ScriptHeuristic** prevents any malicious browser scripts and PDF documents from being executed without disabling features provided by legitimate scripts. It protects against infection with unknown viruses that try to get into a system via a web browser. It works independently of the Dr.Web virus databases in any web browser.
- **Traditional heuristic analyser** features routines to detect unknown malware. The heuristic analyser relies upon knowledge (heuristics) about certain properties typical to virus code and, vice versa, those that are extremely rare in viruses. Each of these attributes is characterized by its "weight" – that is to say, by a number whose module refers to the importance and severity of the attribute; and its sign, respectively, indicates whether that attribute confirms or refutes the hypothesis on the possible existence of an unknown virus in the code being analyzed.
- An execution emulator module is used to detect polymorphic and highly encrypted viruses when the search against checksums cannot be applied directly or is very difficult to perform (because secure signatures cannot be built). The method involves simulating the execution of an analyzed code by an emulator – a programming model of the processor (and, in part, PC and OS).

Facts

- Dr.Web anti-viruses use a record low number of virus definitions in their database; one entry can identify dozens, hundreds or even thousands of similar viruses. This is a fundamental difference between the Dr.Web virus database and virus databases of other anti-virus programs. Even with a smaller number of entries, it can detect the same (or an even greater) number of malicious programs.
- Even if no definition of a virus is present in the virus database, Dr.Web will most likely detect it by means of multiple technologies implemented in its anti-virus engine.
- Dr.Web virus databases are devised in such a way that adding new entries doesn't lower the scanning speed.

What are the advantages of a small virus database with fewer entries?

- Saved disk space.
- Lower memory usage.
- Lower updating traffic.
- Rapid virus analysis.
- Detection of future modifications of existing viruses.



Important!

Every day millions of people around the world use the unique product Dr.Web CureIt!, created specifically to cure infected computers that run other anti-viruses.

But viruses haven't existed for ages!

Indeed, over 90% of today's threats cannot be called viruses in the strictest sense of the word, because they do not have mechanisms for self-replication (the ability to replicate itself independently without user interaction). Most contemporary threats are represented by Trojan horses. They belong to a category of malicious programs and can cause serious damage to the owner of an infected computer.

Dangerous Trojans:

1. Are invisible both to the user and some anti-viruses.
2. Are capable of stealing confidential information, including passwords, data for accessing banking and payment systems, and cash from bank accounts.
3. Can download other malware and even render an operating system inoperable.
4. Can completely paralyze a computer under an attacker's command.

When created, such programs usually cannot be detected by anti-virus engines. Moreover, some of them make attempts to remove anti-viruses.



Only an anti-virus can cure a Trojan-infected system.

Facts

- Modern malware often operates invisibly to computer users, and, from the moment of its creation, it cannot even be detected by many anti-virus programs.
- Modern virus writers aim to create malicious software that will remain undetected in a system for as long as possible, – both by users and special programs (anti-viruses).
- For example, Trojan.Carberp was designed to steal money. When launched on an infected machine, it undertakes a series of steps to avoid being detected by control and monitoring systems. Once it has been successfully launched, the Trojan injects itself into running applications while shutting down its primary process. Thus, this Trojan hides its activity part by part inside other processes.

The myth that any virus can easily be noticed has been quashed completely.

Even if a computer is infected, it's cheaper to recover Windows from the backup than it is to buy an anti-virus

Threat

A malicious program can conceal itself in files stored on other hard disk partitions and removable storage media. In this case, it would not work to reinstall Windows: when accessing such a file, the malware file is activated again.



Important!

An anti-virus is the only tool that can cure your computer of a virus.

Even if you don't have a backup copy of each workstation — — no problem! If your system was infected before you installed Dr.Web, Dr.Web will cure it, and the computer will function normally again. To cure an active infection, it's enough to run a quick scan of your computer, and all threats found will be neutralized. It will take less time to cure even several computers on the network than to restore the system from backup! This will:

- Cure infected files;
- Automatically fix the Windows registry;
- Automatically remove malicious services;
- Automatically remove rootkits and bootkits.

E-mail is the main source of viruses

Facts

The main sources of viruses that infect a corporate network (in descending order of infection cases):

- Personal/home PCs / laptops / mobile devices belonging to employees.
- Laptops / mobile device belonging to customers.
- Removable devices, — and these are not only USB flash drives!
- Legitimate websites (i.e., those required for employees to perform their job duties and, therefore, not subject to blocking) infected by attackers.
- Phishing and specially designed malicious websites.
- E-mail.
- Vulnerabilities in operating systems and application software.

Time to «gather stones»

There was a time in the anti-virus industry's history when programmers in various countries decided for some reason that they could create programs pompously referred to as «anti-viruses». In 1994, the wide distribution of a polymorphic virus Phantom-1, which no anti-virus except Dr.Web could detect, put everyone in their places and put a host of useless anti-virus creations on the scrap heap of the industry.

In July 2001, the CodeRed epidemic broke out. It turned out that Dr.Web was the only anti-virus in the world capable of detecting this virus in a computer's memory. Even now, few anti-viruses can cure such threats.

And today, the anti-virus industry seems ready once again to cleanse itself and drop ballast. In the future, only a very few anti-virus programs will remain on the market. They will:

- Identify and neutralize viruses not only by signatures and heuristic technologies, i.e., they will have the functionality to keep a malicious object from entering a system, even if its signature has not yet been added to the virus database;
- Have an impenetrable self-protection system to prevent itself from being brought down by a new unknown virus that somehow penetrated the system;
- Be capable of thoroughly cleaning the system of malware when the program is active, or resisting, or hindering detection and operating to the detriment of the user. In other words, it should be able to cure a system in real conditions and successfully restore its health, because only a real infection allows the quality of anti-virus technologies to be checked;
- Have a data collection system that facilitates the quick transfer of all information needed to the anti-virus lab so that the problem can be solved quickly;
- Have a strong development infrastructure, an internal virus monitoring service, an anti-virus lab and customer support;
- Be able to model new types of threats before virus writers do and use technology to combat them (these will definitely be non-signature based threats).

And today's Dr.Web anti-virus already features all these qualities.

Always alive, always open

<http://live.drweb.com> — is an open site on which you can monitor the anti-virus lab operation in real time. There you will see how malware samples are processed and which viruses are most widely spread.

Dr-Web Virus Analysts Web Site
Dr-Web Services

Top 10 Threats

Trojan.Necurs.97	69,560
Trojan.PWS.Stealer.946	33,758
JS.Redirector.162	27,149
Win32.HLLM.Netsky.18401	8,693
BackDoor.Hermes.442	7,180
JS.Redirector.168	6,487
JS.Redirector.167	5,626
JS.Redirector.148	3,906
JS.Redirector.161	3,813
JS.Redirector.166	3,383

8,350,100,486 objects checked
2.37% infected
Viral danger: average

Infected Objects

Scanned Objects | Virus-Base Records

Add-On Availability

60%

Recent Virus Records

In Process | Queued | Recent Updates

Virus Name	Analyst	Date Analysed
Adware.Downware.696	Alexander Urakov	05 Dec 2012 15:20
Tool.DnsChange	Alexander Urakov	05 Dec 2012 15:20
Adware.Siggen.25114	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48724	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Panda.547	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48746	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.DownLoader7.33969	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48708	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.Hosts.6457	Konstantin Nikolenko	05 Dec 2012 15:20
Trojan.PWS.Siggen.48738	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48735	Ilya Georgievsky	05 Dec 2012 15:20
BackDoor.BlackHole.11976	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.Inject1.13199	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48733	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48709	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48706	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48720	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48719	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48710	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Stealer.1651	Alexey Gashkin	05 Dec 2012 15:20
Trojan.PWS.Siggen.48726	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.DownLoader7.33967	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48714	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48731	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48722	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48742	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48716	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48732	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48707	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48705	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Wsgame.36091	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48713	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Stealer.1652	Alexey Gashkin	05 Dec 2012 15:20
Trojan.PWS.Siggen.48743	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48741	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.Encoder.102	Vladimir Martynov	05 Dec 2012 15:20
Trojan.Inject1.14718	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48745	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48729	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Panda.3163	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48740	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48712	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.SpyBot.324	Ilya Georgievsky	05 Dec 2012 15:20
Exploit.CVE-2012-4681	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48718	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48721	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48715	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48730	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48744	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Stealer.1653	Alexey Gashkin	05 Dec 2012 15:20
Trojan.FakeAlert.35464	Alexey Gashkin	05 Dec 2012 15:20
Trojan.DownLoader7.33968	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48736	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48734	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48728	Ilya Georgievsky	05 Dec 2012 15:20
BackDoor.Slym.1053	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48739	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48747	Ilya Georgievsky	05 Dec 2012 15:20
Java.Downloader.754	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48725	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.SpySweep.1423	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48711	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48717	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48723	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48727	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.Hoax.6458	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Siggen.48737	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.KillFiles.10139	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Turist.1	Ilya Georgievsky	05 Dec 2012 15:20
Trojan.PWS.Wsgame.36092	Ilya Georgievsky	05 Dec 2012 15:20

Summary

E-mail	Today	All
In Process	16	36,021
Processed	73	223,469
Rejected as Spam	0	670
Total	89	261,060

Honeypots	Today	All
In Process	0	1,828,720
Processed	71	220,891
Total	71	2,049,638

Tickets

Virus Hunter	Confirmed	Reported
Pavel Petrov	125,270	213,763
Stefan Dashich	112,061	281,826
Konstantin Zhdanov	85,513	94,638
Mr. Salyan	35,725	71,566
Mikhail Kasimov	8,077	9,001
RomaNNN	4,210	9,017
Aleksandra	4,001	8,625
Dmitry Shutov	3,324	5,087
EzZo	1,938	2,210
Alex Gorgeous	730	1,121
Aleksandra	613	660
Black Angel	369	434
azza	276	394

Virus Analyst	Today	All
Igor Zdobnov	1	838,725 (+226)
Ilya Georgievsky	-	390,609 (+61)
Grigory Lisin	-	331,610 -
Alexey Tkachenko	-	93,984 (+75)
Kirill Prosyakov	-	86,554 (+96)
Edward Moskalchuk	-	42,897 (+17)
Alexey Otendar	-	41,290 (+29)
Vladimir Martynov	17	34,352 (+14)
Denis Akimov	-	10,023 -
Alexey Gashkin	14	6,640 (+3)
Oleg Gubanov	1	4,886 -
Konstantin Nikolenko	-	4,140 -
Alexandr Chizhov	-	3,585 (+1)
Ivan Sorokin	-	3,274 (+6)
Ilya Kuzmin	-	2,923 -
Nikita Grigoriev	-	2,759 (+28)
Kirill Vostrecov	-	2,208 -
Timofey Brunko	-	2,115 -
Oleg Kalandarashvili	-	1,755 (+5)
Leonid Shagiev	-	1,646 -
Yury Serduk	-	1,471 (+15)
Vladimir Dneprovsky	-	720 (+33)
Petr Kamensky	1	275 (+2)
Alexander Urakov	11	225 -
Igor Daniloff	-	123 -
Kuzmin Ilya	-	108 -
Edward Kovalets	-	103 -
Filipp Rezvyl	2	64 -
Sergey Komarov	-	42 (+1)
Konstantin Kokarev	-	26 -
Eugene Vasiliev	-	14 -
Eugene Gladikh	-	9 -
Nikolai Potanin	-	5 -
Alexander Tarasov	-	2 -
CADPS Watcher	-	1 -
Eugeni Vasiliev	-	1 -
Stepan Sirkin	-	1 -

© Doctor Web 2003 — 2012 | About | News | Privacy Statement

Introduction

Security is a service

Anti-virus software is used in all business processes that involve computers from management planning to accounting and production. An effective anti-virus ensures an enterprise's faultless operation and reduces its IT infrastructure total cost of ownership.

As practice shows, for the most part, small and medium-sized companies use only personal products from the full range of those offered by anti-virus companies.

Which anti-virus does a company choose? The market leader? The one that fits the specific corporate network environment? No! The company gets the anti-virus that its system administrator knows how to configure and maintain. Many software functions might not be used simply because users are unaware of their existence or the way they should be used. As a result, company's information security is held hostage to an administrator's subjective evaluation and qualifications.

A major constraint to the effective functioning of a company's IT infrastructure is the lack of system administrators who can competently manage a company's information security system, a role requiring special knowledge that most IT administrators do not have. This threatens a company's information security and, consequently, significantly increases the total cost of ownership of an anti-virus and leads to problems related to information security legislation.

This challenge is especially relevant for small and medium-sized companies. Typically, their system administrators are either outsourced (and serve more than one company) or under qualified. Overcoming such difficulties is an important task for company management.

Software as a service

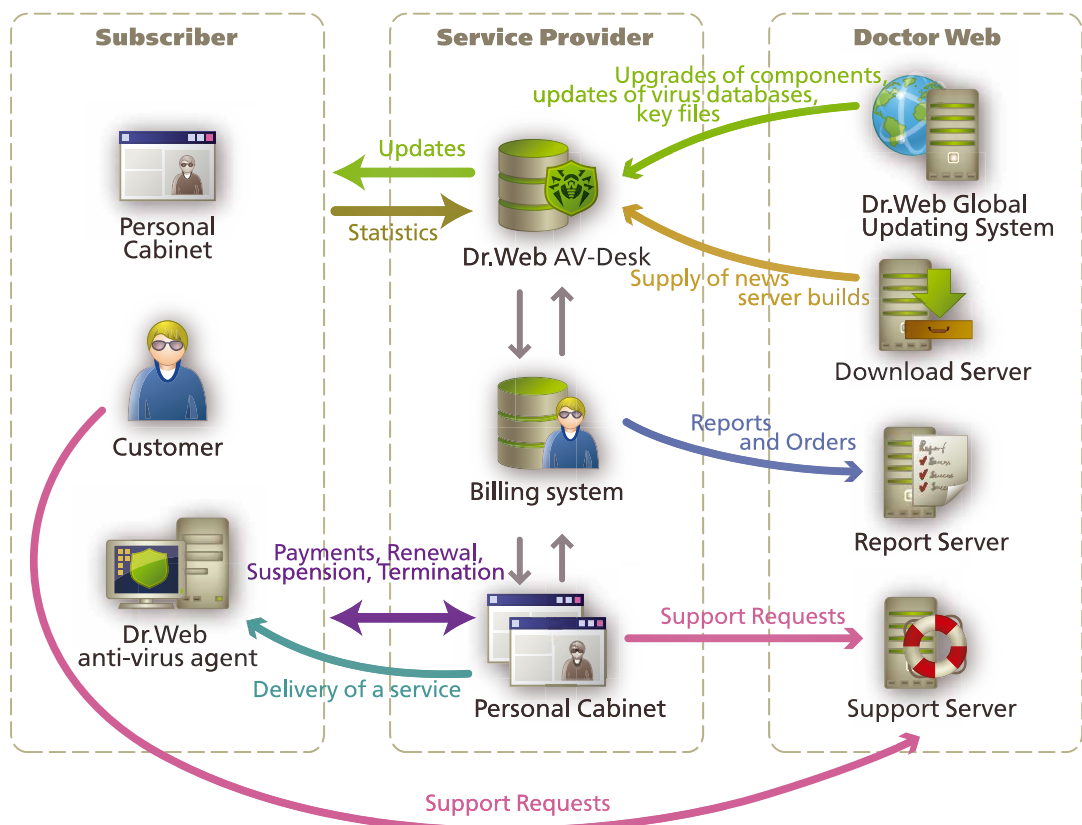
Software as a Service (SaaS), which has long been in wide use outside of Russia, is a business model whereby software is delivered to customers in the form of a service.

In Russia, prior to 2007, use of this model in the anti-virus industry was constrained by the simple lack of domestic solutions of this class. Following Doctor Web's release of the Dr.Web AV-Desk Internet service in May 2007, a new segment emerged on the Russian IT market: – the anti-virus protection service segment.

Such services are rendered by ISPs who install Dr.Web AV-Desk on their hardware to deliver a service offering comprehensive anti-virus and anti-spam protection from Internet threats – Dr.Web Anti-virus as a service.

How it works

1. The provider of Dr.Web Anti-virus as a service installs Dr.Web AV-Desk software on its servers and organizes subscriptions to the Dr.Web Anti-virus as a service.
2. Customers subscribe to the service, install Dr.Web software, and manage subscription parameters themselves.
3. Doctor Web provides service providers with the latest Dr.Web virus database and program module updates, and renders technical support to service providers and subscribers.
4. Providers charge customers a fee for using the service, monitor anti-virus network health, provide subscribers with virus database updates, and collect statistical information about virus infections.



If a company does not have a full-time system administrator

When skilled administrators are in short supply, the anti-virus as a service helps solve the security problem.

- Your company will have qualified personnel to handle your information security processes.
- The provider's IT specialists are professionals trained and certified by Doctor Web. They have comprehensive knowledge of the anti-virus software and how to use it to administer anti-virus protection.
- Restricted personnel access to the software settings ensures full compliance with security policies for all protected computers.
- Thanks to qualified service management, a competent response to virus threats, and the professional actions taken by the provider's specialists to restore network operability after a virus attack, contingencies are minimized. This is also done by eliminating the costs of server hardware and hiring paid professionals in the field of information security.

External administration of the Dr.Web anti-virus service guarantees the reliable operation of an IT infrastructure and an unbiased analysis of network health.

Dr.Web anti-virus protection system

Anti-virus protection
components

Centralized management of the anti-virus protection system

If your company has a full-time or a part-time system administrator, a service provider can convey the anti-virus protection system management duties to that individual through the Control Center. This will ensure that the company has even more control over information protection of the anti-virus network.

Enterprise-class products with a control center are more expensive than single-user versions. They are complicated and require the hiring of an information security specialist to control them

Facts

Supplying Dr.Web enterprise-class server products based on a SaaS model has significantly reduced their cost and made them available to consumers. The Control Center incorporated into the Dr.Web Anti-virus as a service:

1. Is licensed free of charge.
2. Is easy to control by a specialist with any level of qualification.
3. Automates local network protection with minimal maintenance because all stations or groups of stations can be configured in two or three clicks as well as reconfigured just as easily, if necessary.

Using the Dr.Web Anti-virus service Control Center contributes to a company's smooth operation and, as a result, minimizes the costs of business procedures.

The Control Center incorporated in the Dr.Web Anti-virus service allows protection of the following to be controlled:

- Windows and Mac OS X workstations
- Windows file servers
- Android mobile devices.

Convenience and real savings

- The Dr.Web Anti-virus service Control Center makes it possible to view at-a-glance an entire corporate anti-virus network from a single workplace.
- The Control Center minimizes system maintenance time, allows a network security system to be managed quickly at any time, from anywhere in the world, from a computer running any operating system, and just from a browser—with no need to install additional software.
- With the user-friendly, web-based interface of the Control Center, one can centrally install, upgrade and configure anti-virus protection components, and turn on computers in «mobile» mode.
- It reduces the load on local stations by compressing network traffic and data encryption, thus increasing their performance and eliminating personnel complaints of an anti-virus allegedly slowing down the system.

The guarantee of a high level of information security

The Control Center incorporated in the Dr.Web Anti-virus service makes it possible to:

- implement the security policies necessary for a specific company, without having to configure protection components on each workstation;
- ensure that employees cannot disable the anti-virus or its separate components, which would inevitably reduce the level of protection;
- ensure that the anti-virus operates with the settings specified by the network administrator;
- schedule and remotely run regular scans, both under the administrator's command and on a schedule;
- monitor the regularity of updates and ensure they cannot be disabled;
- collect and analyze information on the health of the anti-virus protection system and generate reports for a required period of time;
- notify administrators and users of the health of the protection system;
- timely respond to emerging virus problems that would in turn reduce the risk of network infection and company financial losses caused by personnel downtimes, data losses, Internet connection breakdowns, and viral infections impacting business partners.



Important!

- The inability to capture and substitute traffic ensures the safe administration of any number of workstations — no matter where they are in the world.

Proxy server

The Dr.Web Anti-virus as service can be provided even in the case of a complex network topology, for example, if anti-virus agents do not have direct access to the service's server (i.e., the Dr.Web AV-Desk server), and there is no packet routing between them (internal LAN logically isolated from the Web).

In such a case, a proxy server is provided as an individual component to ensure direct access. A proxy server can also be used to significantly reduce network traffic (traffic optimization) and make updates of anti-viral agents faster because it supports caching the updates and components of anti-virus agents.

Using traffic compression technology (optional on the service's server) is not an obstacle to the use of a proxy server. Information transferred is processed regardless of whether the traffic is compressed.



Important!

An anti-virus network can consist of one or more proxy servers.

Network installation (remote installation)

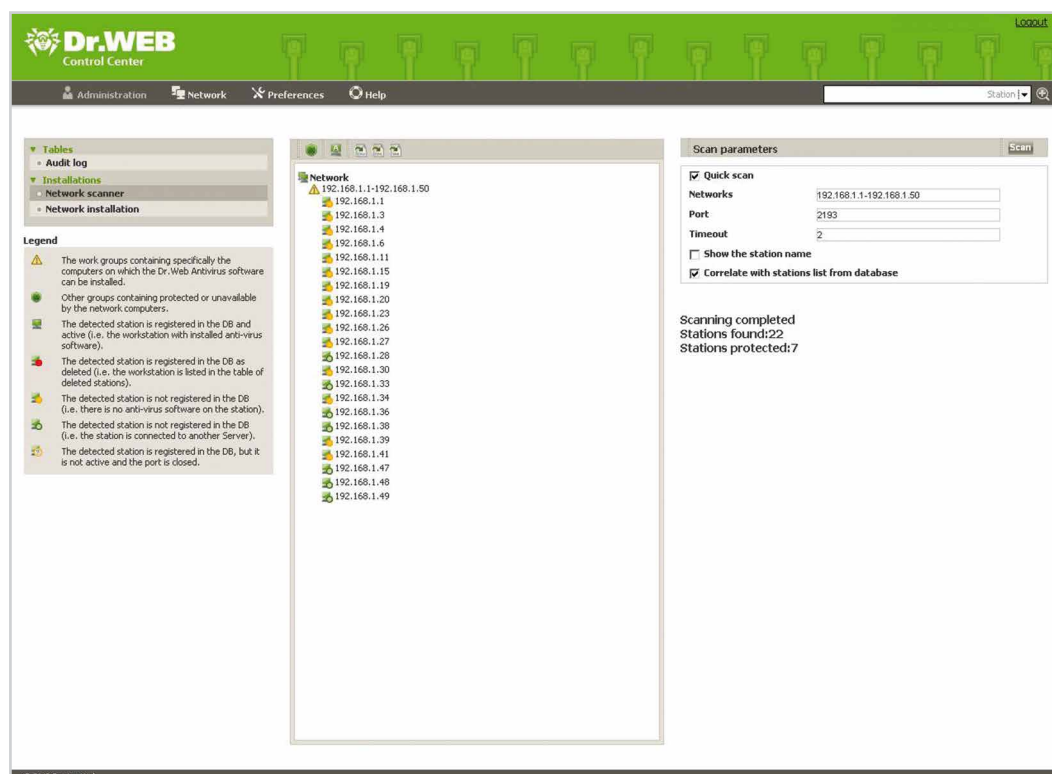
The Dr.Web Anti-virus as a service features all the advantages of enterprise-class products with the centralized management of the anti-virus protection system. Among them is the ability to identify local network computers that have no anti-virus protection installed on them, and enable remote Dr.Web installation on unprotected computers.

Remote installation is available both on a workstation included in a domain under an administrator account, and on a remote station not included in a domain or used under a local account.

Important!

If a remote station is not part of a domain or a local account is used on a remote computer, a number of settings must be made for some MS Windows versions. This is described in the Administrator's Guide.

The Dr.Web Control Center includes the Network Scanner which searches for computers by IP address in the local network and generates a hierarchical list of computers indicating which of them have anti-virus software installed.



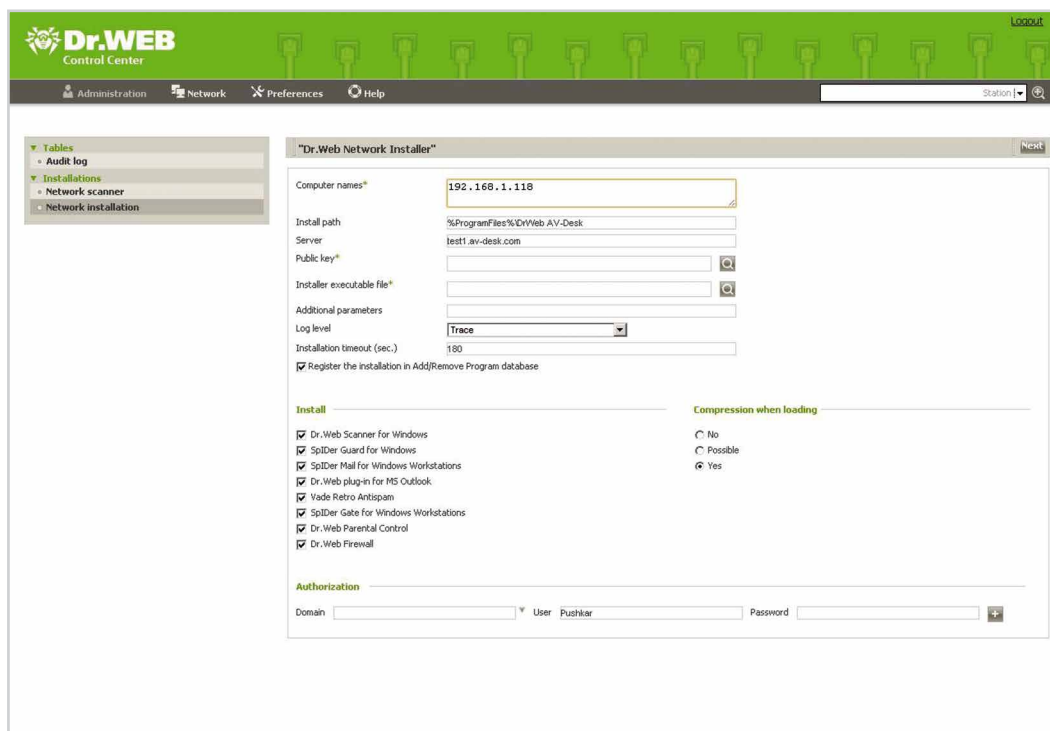
The screenshot displays the Dr.Web Control Center interface. The top navigation bar includes 'Administration', 'Network', 'Preferences', and 'Help'. The main content area is divided into three sections:

- Tables:** A sidebar menu with options for 'Audit log', 'Installations', 'Network scanner', and 'Network installation'.
- Legend:** A list of status icons and their corresponding descriptions:
 - The work groups containing specifically the computers on which the Dr. Web Antivirus software can be installed.
 - Other groups containing protected or unavailable by the network computers.
 - The detected station is registered in the DB and active (i.e. the workstation with installed anti-virus software).
 - The detected station is registered in the DB as deleted (i.e. the workstation is listed in the table of deleted stations).
 - The detected station is not registered in the DB (i.e. there is no anti-virus software on the station).
 - The detected station is not registered in the DB (i.e. the station is connected to another Server).
 - The detected station is registered in the DB, but it is not active and the port is closed.
- Network Scanner:** A central pane showing a list of IP addresses from 192.168.1.1 to 192.168.1.49, each with a status icon.
- Scan parameters:** A panel on the right with a 'Scan' button and settings for 'Quick scan' (checked), 'Networks' (192.168.1.1-192.168.1.50), 'Port' (2193), 'Timeout' (2), 'Show the station name' (unchecked), and 'Correlate with stations list from database' (checked). Below this, it states 'Scanning completed', 'Stations found:22', and 'Stations protected:7'.

The software can be installed on one or more unprotected computers by creating a task in the toolbar.

Important!

Remote installation is ONLY allowed in routed networks.



System administrators

If a company has a full-time system administrator on staff or it employs an outsourced administrator, that individual can manage the Dr.Web Anti-virus protection system through a convenient and user-friendly Control Center, make and implement their own decisions to comply with security policies, and respond to virus incidents; – in other words, they have complete leverage over the company's information security.

Categories of administrators

- **Group administrator with full privileges** – an employee who can access the Control Center and change any system settings. It is recommended that the administrator be the head of the company (in small companies, there is no system administrator, and the head of the company is responsible for the anti-virus protection system) or the individual authorized to administer the anti-virus protection system.

! Important!

A company employing an external administrator must carefully consider whether to delegate the anti-virus protection system control to that individual on such a scale, because this role gives complete control over the system.

- **Group administrator with full privileges (read-only)** – an employee who has access to the Control Center and can get system statistics but cannot change the settings. This role can be assigned to the employee authorized to analyze system statistics and conduct security system audits.
- **Group administrator with limited rights** – an employee who has access to the Control Center and can modify any settings within privileges allowed by a group administrator with full privileges, with the exception of managing subscription control functions (create/suspend/resume/delete). This role can be useful for 1) customers of outsourced Dr.Web Anti-virus service providers, and 2) administrators of access service provider subscribers. In case of multiple groups, each group can have its own administrator.

! Important!

To assign system administrators you must have access to the appropriate functions; – to gain access to them, contact your service provider.

Groups. Group management

To facilitate protection management, medium-sized and large enterprises use a grouping mechanism that ensures exceptional scalability of the Dr.Web Anti-virus service. With grouping you can:

- create groups, consolidate protected stations into groups, add/delete stations from a group;
- apply different security policies for different groups (for example, for the Accounting group you can disable cancellation of updates, while for the Managers group, you can remove all web-surfing restrictions);
- with a single command, assign and initiate jobs for all group members;
- set individual update and scan schedules for different groups which can help distribute the network load;
- generate group reports;
- send notifications – to individual stations, individual groups, or all groups.

If a company has more than 15 Dr.Web Anti-virus service subscriptions, it makes sense to create groups in the anti-virus protection system and to apply different security policies to each of them, using multiple Control Center settings.

A system administrator can expand or limit rights to control agents – for individual users, a user group, or all user groups:

- allow users to change anti-virus settings;
- partially restrict setting modification by users;
- completely restrict changing the settings;
- change the set of Dr.Web software components on customer computers;
- add and remove anti-virus components on user machines;
- start jobs on protected computers;
- force updates of agents that have not been updated for a long time;
- force background scanning on protected computers.

Dr.Web as a service subscription packages and protection components

The service is delivered in subscription packages. Each subscription package includes components for protecting workstations, Windows file servers, and mobile devices.

Choose subscription packages according to your current business needs, information security requirements, and budget limitations.

	Dr.Web Classic Basic anti-virus protection	Dr.Web Premium Comprehensive protection from Internet threats
Protection of workstations		
Windows OS		8/7/Vista/XP
Mac OS X		10.4 and above
Antivirus, anti-spyware and anti-rootkit	✓	✓
Anti-spam		✓
HTTP monitor		✓
Parental Control		✓
Firewall	✓	✓
File server protection		
Windows OS		Windows Server 2003/2008
Protection for mobile devices		
Android OS		2.0/2.1/2.2/2.3/ 3.0/3.1/3.2/4.0/4.1/4.2
Anti-virus	✓	✓
Anti-theft		✓
Anti-spam		✓
Basic technical support		
Virus database updating	✓	✓
Program module updating	✓	✓
Number of requests for support		Unlimited
Other services		
Free upgrades and downgrades	✓	✓
Subscription suspension for 1, 2 or 3 months	✓	✓

Which threats does the Dr.Web Anti-virus service protect against?

	Dr.Web Classic	Dr.Web Premium
Viruses	✓	✓
Trojan horses	✓	✓
Keyloggers	✓	✓
Password stealers	✓	✓
Spyware	✓	✓
Rootkits	✓	✓
Riskware	✓	✓
Polymorphic viruses	✓	✓
Worms	✓	✓
Backdoors	✓	✓
Jokers	✓	✓
Paid dialers	✓	✓
Hack tools	✓	✓
Spam		✓
Phishing		✓
Pharming		✓
Scamming		✓
Bounce messages		✓
Unauthorized access to sensitive information		✓
Internet crimes against children		✓
Unauthorized network access	✓	✓

Today, an anti-virus on its own is no longer a panacea!

Why is just an anti-virus not enough? Indeed, until recently the case was quite the opposite!

Important!

A present-day anti-virus solution is quite different from yesterday's file anti-virus.

A modern anti-virus protection system must include, among other things:

- an effective anti-spam, because spam is one of the main sources of malware;
- HTTP traffic filters to protect against malicious code from web pages;
- tools to restrict access to removable storage devices and internal networking resources (Office Control);
- a personal firewall.

Important!

These features are only included in the Dr.Web Premium subscription package.

When using these components correctly (i.e., in compliance with the guidelines in this booklet), there's no need to purchase additional products with similar features. This makes it possible to deploy an anti-virus protection system on a shoestring.

The best practice

- When customizing user access to components in the Control Center, save the rights to run each of the components but disable the ability to edit the configuration of components and to stop them.
- User opinions about which anti-virus components must be installed on a PC should be IGNORED.

You only pay for what you're using

«Pay only for what you need at the current moment» – is the main principle of the philosophy behind the licensing service. The service can adapt to a company's needs; the company pays only for the amount of services required at the current moment. **A customer pays only for the actual number of connections, the quantity of which can be changed at any time.**

This allows a company to draw up detailed plans for both short- and long-term IT security expenses according to actual business needs, rules out unexpected cost increases, and makes potential future costs of anti-virus and anti-spam protection completely transparent.

The advantages of Dr.Web Anti-virus as a service licensing

- Charging for a month or longer. You pay only for the actual number of connections in a reporting period.
- New agents connect to the server instantly.
- Whenever staff numbers go down, the service ceases to be delivered for the corresponding computers.

Reduce your information security expenses when business permits, and increase them just as much as your business demands.

Discounts

Once you have subscribed to the Dr.Web Anti-virus service, you start saving on information security in the very first month of use.

Sign up for the service and get a discount...

for the number of protected objects...

from 10-40%, – depending on the total number of objects protected by Dr.Web.

PCs	Disc. pct.
1–25	Package basic price
26–50	10
51–100	20
101–200	25
201–300	30
301–400	35
401–500	40

...and for the period of use

from 5-15%, – an additional discount for those who don't interrupt their period of use*

Subscription period	Disc. pct.
1 year	5
3 years	10
5 years	15

* The subscription hasn't been suspended or terminated. Available on month 13, 37, and 61, respectively.

Flexible licensing is the key to real savings on IT.

Subscription Control Center (SCC)





Access to the Subscription Control Center is granted to a customer by the service provider. The SCC lets a customer monitor the subscription and its renewal progress, switch to other subscription packages, receive virus statistics and service operation statistics, receive Doctor Web news in real-time, and contact the helpdesk.

«Dr.Web service» subscription packages

Basic subscription packages | Promotional subscription packages | Discounts

Basic subscription packages

PLEASE NOTE: The fee amount includes protection for one computer for one month.

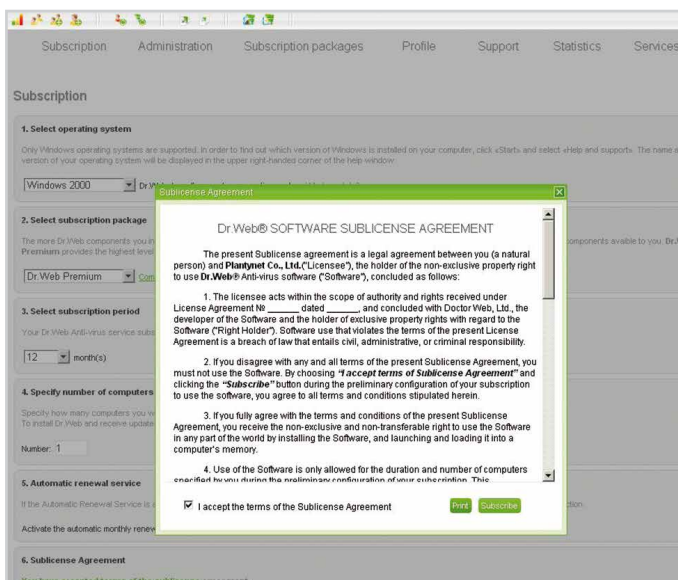
	Supported OS	Components	Free trial period	Free downgrade
 Dr.Web Premium Comprehensive protection from Internet threats 89.00 RUB	Windows 2000 Windows XP Windows Vista Windows Seven	Anti-virus Anti-rootkit Anti-spy Anti-spam HTTP monitor Parental control Firewall	31 days	Dr.Web Classic Dr.Web Standard
 Dr.Web Standard Basic protection enhanced with anti-spam 79.00 RUB	Windows 98 Windows ME Windows NT4 Windows 2000 Windows XP Windows Vista Windows Seven	Anti-virus Anti-rootkit Anti-spy Anti-spam Firewall	31 days	Dr.Web Classic Dr.Web Premium
 Dr.Web Classic Minimum anti-virus protection 69.00 RUB	Windows 98 Windows ME Windows NT4 Windows 2000 Windows XP Windows Vista Windows Seven	Anti-virus Anti-rootkit Anti-spy Firewall	31 days	Dr.Web Premium
 Dr.Web Premium Server Ultimate Windows server protection 390.00 RUB	Windows 2000 Server Windows 2003 Windows 2008	Anti-virus Anti-rootkit Anti-spy Anti-spam HTTP monitor Parental control Firewall	31 days	Dr.Web Classic Dr.Web Standard Dr.Web Premium

Subscription

Whenever you like, you are free to use the Subscription Control Center to increase the number of protected objects (in other words, extend the license) or disable unneeded workstations as business demands require.

To subscribe, please proceed with the following steps:

1. Select the OS you are using.
2. Select a subscription package.
3. Enter the number of PCs.
4. Specify the subscription period (one month or longer).
5. Accept the sublicense agreement terms and conditions.
6. Click «Subscribe».



Subscription Administration Subscription packages Profile Support Statistics Services

Subscription

1. Select operating system

Only Windows operating systems are supported. In order to find out which version of Windows is installed on your computer, click «Start» and select «Help and Support». The name and version of your operating system will be displayed in the upper right-hand corner of the help window.

Windows 2000

2. Select subscription package

The more Dr.Web components you install, the more protection you receive. Dr.Web Premium provides the highest level of protection.

Dr.Web Premium

3. Select subscription period

Your Dr.Web Anti-virus service subscription period is 12 month(s).

12 month(s)

4. Specify number of computers

Specify how many computers you wish to install Dr.Web and receive updates.

Number: 1

5. Automatic renewal service

If the Automatic Renewal Service is activated, you will be automatically renewed every month.

Activate the automatic monthly renewal service

6. Subslicense Agreement

You have accepted terms of the subslicense agreement.

Dr.Web® SOFTWARE SUBLICENSE AGREEMENT

The present Subslicense agreement is a legal agreement between you (a natural person) and **Platynet Co., Ltd.** ("Licensee"), the holder of the non-exclusive property right to use **Dr.Web® Anti-virus software** ("Software"), concluded as follows:

1. The licensee acts within the scope of authority and rights received under License Agreement No. _____ dated _____, and concluded with Doctor Web, Ltd., the developer of the Software and the holder of exclusive property rights with regard to the Software ("Right holder"). Software use that violates the terms of the present License Agreement is a breach of law that entails civil, administrative, or criminal responsibility.
2. If you disagree with any and all terms of the present Subslicense Agreement, you must not use the Software. By choosing "I accept terms of Subslicense Agreement" and clicking the "Subscribe" button during the preliminary configuration of your subscription to use the software, you agree to all terms and conditions stipulated herein.
3. If you fully agree with the terms and conditions of the present Subslicense Agreement, you receive the non-exclusive and non-transferable right to use the Software in any part of the world by installing the Software, and launching and loading it into a computer's memory.
4. Use of the Software is only allowed for the duration and number of computers specified by you during the preliminary configuration of your subscription. This:

I accept the terms of the Subslicense Agreement

Print Subscribe

Important!

If you want your subscription to be renewed automatically each month, check the “Enable automatic renewal” box.

Installation of the service software on an individual station

A link to the Dr.Web installer is available at the SCC immediately after the subscription has been processed. Download and run the installer, then wait for the Dr.Web installation to finish. An icon displaying a spider over a shield will appear in the system tray. A yellow triangle with an exclamatory mark will be flashing over the icon. Reboot the system and wait for the anti-virus to connect to an anti-virus server. You are now successfully subscribed to the service.

Important!

1. Please make sure that no other anti-viruses are installed on your PC before you proceed with installation because the resident modules contained within them may cause software conflicts.
2. The Dr.Web anti-virus protection system starts running after the Dr.Web Anti-virus-as-a-service software is installed.

Renewal

There is no need to be particularly concerned about renewing. A service subscription is renewed automatically as long as the “Enable automatic renewal” box is left checked.

Suspending a subscription

If necessary, a subscription may be suspended at any time for up to 3 months.



In order to suspend a subscription, go to the Administration tab and select Suspend.

Important!

If a subscription is suspended, you are ineligible for a cumulative discount for the continuous use of the service (see the Discounts section).

How suspensions become effective

- If a customer pays for the Service on a daily basis, the change becomes effective on the day of suspension.
- If a customer pays for the Service on a monthly basis, the change becomes effective on the first day of the subsequent calendar month.

Resuming a subscription

- Upon expiry of the suspension period defined by the subscriber. The automatic monthly renewal service is also enabled if it had been activated before the subscription was terminated.

Resuming suspended subscription automatically

A suspended subscription is resumed automatically if the automatic renewal service has been enabled prior to the suspension. The subscription is resumed on the same terms as before.

Subscription termination

You can terminate your subscription at any moment, but:

- If daily charging is in effect, the subscription will be terminated immediately.
- If a customer pays for the service on a monthly basis, the subscription will remain active till the end of the current calendar month. Money paid by a subscriber in advance is not refunded.

Dr.WEB® Anti-virus service

Doctor Web | [Log out](#)

Balance: 1000000000.00 (Russian Ruble)

Subscription Administration Subscription packages Profile Support Statistics Services

Subscription information

Information **Statistics**

Information

Computer name:	A	<input type="checkbox"/> Generate license certificate
Subscription ID:	hoc-b93c28a-eaab-556a-3b72-52d3f64	<input type="checkbox"/> Change subscription package
Subscription date and time:	01/26/2011 16:07:40	<input type="checkbox"/> Disable auto renewal
Subscription status:	Active	<input type="checkbox"/> Suspend subscription
Current subscription package:	Dr.Web Premium	<input checked="" type="checkbox"/> Terminate subscription
Free trial period:	Unavailable	
Subscription period:	31 day(s)	
Automatic renewal:	Enabled	

[Download!](#)
→ 24x

[Back](#)

History

Date and time	Action	Additional information
01/26/2011 16:07:40	Subscription created.	Табличный номер: Dr.Web Premium.

To terminate a subscription, go to the Administration tab and select Unsubscribe.

Manually resuming a subscription after termination

Once the Resume action is selected, your subscription is resumed and the Dr.Web installer download link is available again. This, in fact, is considered a new subscription. The automatic monthly renewal service is also enabled if it had been activated before the subscription was terminated.

Dr.WEB® Anti-virus service

Doctor Web | [Log out](#)

Balance: 1000000000.00 (Russian Ruble)

Subscription Administration Subscription packages Profile Support Statistics Services

Subscription information

Information **Statistics**

Information

Operation successful

Subscription ID:	hoc-86c7f5d-e779-8e06-e96f-09f4c23	<input type="checkbox"/> Generate license certificate
Subscription date and time:	11/26/2012 13:28:06	<input type="checkbox"/> Change subscription package
Subscription status:	Active till 01/31/2013 23:59:59 Subscription suspended from 01/31/2013 00:00:00 till 02/10/2013 23:59:59	<input checked="" type="checkbox"/> Enable auto renewal
Current subscription package:	Dr.Web Premium	<input type="checkbox"/> Unblock subscription
Free trial period:	Unavailable	<input checked="" type="checkbox"/> Terminate subscription
Subscription period:	1095 day(s)	
Automatic renewal:	Disabled	

[Download!](#)
→ 24x

[Back](#)

History

Date and time	Action	Additional information
01/31/2013 11:08:39	Automatic renewal is disabled	
01/31/2013 11:08:26	Suspension of subscription	Suspended from 01/31/2013 00:00:00 till 02/10/2013 23:59:59
11/26/2012 13:28:06	Subscription created.	Табличный номер: Dr.Web Premium.

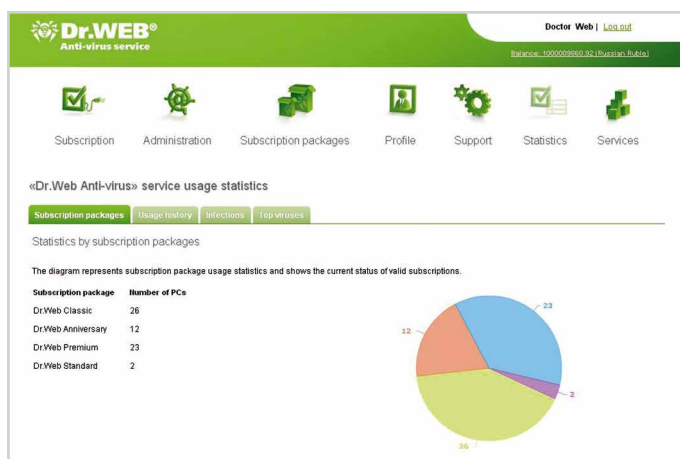
Select Resume subscription in the Administration tab.

Creating a license certificate online

You can generate a Dr.Web license certificate in the Subscription Control Center to prove to inspecting authorities that you are licensed to use Dr.Web software.

Statistics

The Subscription Control Center provides various reports about actions performed by Dr.Web on protected computers. This makes the operation of the software transparent to the user.



You can access information about the parameters of each subscription, its subscription group and overall subscriptions statistics. At any time, you can check your subscription status, view information about each subscription, including subscription history (arranged by group or by package) and overall statistics.

Virus statistics

Easy-to-understand diagrams and ratings showing information about detected malicious programs can be found in the Statistics tab.

You can define a period of time for which you want to view statistics. Infection-information available for each protected computer includes:

- Statistics on malware detected by Dr.Web.
- Top ten viruses detected.

History log

The log contains comprehensive information (history) of user actions in the Subscription Control Center, such as:

- actions performed in the current month with a selected subscription or all subscriptions (subscribe, cancel, suspend, login, etc.);
- user account transactions in the current month (refill, withdraw, and refund).

Date and time	Action
01/01/2013 11:06:39	Automatic renewal is disabled for hoc-81c17bd5-4779-8e0d-4981-0914c22f.
01/01/2013 11:06:26	Subscription for hoc-81c17bd5-4779-8e0d-4981-0914c22f is blocked. Subscription will be suspended from 01/01/2013 00:00:00 till 02/01/2013 23:59:59.
01/01/2013 11:03:31	Subscriptions for computer 'A-PUSHKAR (hoc-893c29ea-eaeb-55da-3b72-52b3c1c4f)' are blocked since 01/01/2013 12:03:31. Subscription package: Dr.Web Premium.
01/01/2013 11:03:19	Automatic renewal is disabled for 'A-PUSHKAR (hoc-893c29ea-eaeb-55da-3b72-52b3c1c4f)'. Subscription for 'A-PUSHKAR (hoc-893c29ea-eaeb-55da-3b72-52b3c1c4f)' is blocked. Subscription will be suspended from 01/01/2013 00:00:00 till 02/01/2013 23:59:59.
01/01/2013 11:00:49	Вход в кабинет управления услугой «Антивирус Dr.Web». IP: 194.85.20.253
01/27/2013 15:28:41	Вход в кабинет управления услугой «Антивирус Dr.Web». IP: 194.85.20.253
12/27/2012 16:51:08	Вход в кабинет управления услугой «Антивирус Dr.Web». IP: 194.85.20.253
12/28/2012 10:06:00	Выход из кабинета управления услугой «Антивирус Dr.Web».

Dr.Web anti-virus
protection system

Information security
policies

Creation of a solid protection ecosystem

As practice shows, workstations, and servers are the most vulnerable LAN spots. That's where viruses and very often spam are disseminated.

Viruses can get into computers using very different methods: from user flash drives, password-protected archives attached to e-mails (and, therefore, not scanned on the server, and compromised websites that users visited after following links from incoming messages).

In accordance with existing standards, each workstation's anti-virus protection system must include effective anti-virus software and a system that restricts access to local resources in order to avoid intentional or unintentional data access, and disrupt system operation.

A common misconception is that there are relatively few malware for Mac, Linux and Unix operating systems, and only Windows workstations and servers need to be protected. As a consequence of such a «security» policy, malicious programs obtain a kind of "asylum" on unprotected computers; – even though they can't infect operating systems and running applications themselves, they can use them as a source of infection, – for example, via shared network resources.



Important!

The Dr.Web Anti-virus Control Center makes it possible to centrally manage an anti-virus protection system for any number of workstations running Windows and Mac OS X.

File server protection

Threat

Normally, companies protect employee computers only, leaving servers, mobile devices, and employee home computers unprotected. Finally, a virus that has gotten into workstations can break free, easily penetrating servers containing critical information.

Why is it important to protect servers?

- A user can infect a server with an unknown virus (bringing it or running from storage). An anti-virus will detect it right away using heuristic mechanisms. Or it will at least cure the virus during the next update.
- The server can be hacked. An anti-virus will prevent this: it will detect and destroy malicious programs. If a server is running under a centralized control system, the administrator will be notified immediately of a change in workstation status (for example, an attempt to stop the protection system).
- Digital technologies are widespread in the modern world. Users work not only in offices but at home; they store data on company and Internet file servers. They use their flash drives and those received from friends and colleagues. These can contain viruses.
- Modern cell phones already have the same features and vulnerabilities as PCs. They run OS and use applications that might also be compromised. And they can disseminate viruses into a corporate network and infiltrate the server.

The best practice

If a company operates a dedicated file server, it must also be protected.

Solution

To protect a file server, Dr.Web Premium, which supports Microsoft Windows 2003/2008, will suffice.

In contrast with standard, costly server-based anti-virus products, protecting your server with the Dr.Web Anti-virus service will cost your company the price of protecting workstations only. And this is another of the service's many benefits.

Important!

The Dr.Web Anti-virus Control Center makes it possible to centrally manage an anti-virus protection system for any number of file servers running Windows.

Protection of employee personal devices

Today, a large portion of the computers found within a company's premises is not company property. Those are employee laptops and smart phones. Enthusiastic employees work not only in the office but also while commuting and when at home. They often sacrifice hours of rest while staying connected. Businesses are happy to take advantage of such an approach. Many companies use outsourced employees, which saves money.

But a coin has two sides. In other words, everything comes at a price. In yesterday's world, such an approach guaranteed the desired level of security — since system administrators controlled every single device at the company's disposal. But now that's impossible.

Threats

- Almost two-thirds of employees (63.3%) remotely access a corporate network from personal devices, including mobile phones.
- Up to 70% of infections infiltrate the corporate environment from personal laptops, netbooks and ultrabooks, mobile devices, and removable media (flash drives)—often brought from home.
- Around 60% of home computers have no anti-virus protection! So outside of their offices, people use devices that are prone to be compromised by hackers; the applications they use may have vulnerabilities, and their computers can be infected with viruses and Trojans. And yet these people regularly access the company's network.
- This greatly increases the risk of data leaks and unauthorized data modification.

Facts

They may be good professionals, but they are not experts on anti-virus protection and are often disconnected from reality.

It is in a company's best interest to ensure that all of the devices used by its staff—wherever they are used and no matter who owns them—are secure.

To do this, companies must ensure:

- that any information on the user devices is secure;
- that they protect themselves against the propagation of viruses and Trojans from user devices;
- that all devices, including mobile phones, are protected; – even a single unprotected device is a backdoor for criminals.

But employees use their personal devices for personal purposes!

And a child can be allowed to use a laptop, spend an evening in the social network infested with viruses, download and install a music file from a suspect site... How can we speak about corporate data security in this case?

With the Dr.Web Anti-virus service, you can virtually do the impossible: – protect any device so that it will be beneficial to – the entire company and its employees.

The best practice

- Obtain a subscription to the Dr.Web Anti-virus service for your employees, – and all of the computers that have access to your company's local network will be protected by the same manufacturer.
- Using the Service Control Center, you can enforce an enterprise information security policy on employee personal devices including making it impossible to disable updates and regular scans and remove certain protection components.
- Employee opinions about which anti-virus should be installed on their personal devices must be IGNORED – until the devices are incorporated into a corporate network. Otherwise, such devices should be declared «untrusted» and should not have access to the network.

This is the only way to ensure that employee personal computers in the network do not get infected.

Benefits for the company

- Employee loyalty. An anti-virus for free is a great bonus!
- It makes protection cheaper.
- It's possible to control any protected computer from one location.
- Employees can work all over the world with the same level of protection.
- Guarantee of data safety (including personal data) at any given time.
- Reduction of downtime due to infection.

Employees moved beyond the protective perimeters of their companies a long time ago, and it's no longer possible to move them back into it. And it's not necessary. It's reasonable to expand the office perimeter including employee spaces within it.

Protection for employee office and personal mobile devices

Now, the most common devices are based on Android OS.

Threats

- The number of threats for Android OS is booming with the increasing number of devices used.
- Banking Trojans for Android already exist.
- Mobile devices may be lost/stolen. Your information (passwords and logins for corporate resources access) can be stolen by hackers.

Solution

The Dr.Web Premium package includes a free subscription to Dr.Web for Android. The system contains the following protection components:

- Anti-virus – to deflect malicious files including those designed to monitor your movements, contacts and communications.

- Anti-theft – a system of protection against the loss of the mobile device. If the device is stolen or lost, you can remotely wipe all data.
- Anti-spam – to protect against unwanted messages and calls, and wallet-busting SMS Trojans.

! Important!

The Dr.Web Anti-virus service Control Center makes it possible to centrally control the anti-virus protection for any number of mobile devices running Android (starting from version 6.2).

Regular updates of virus databases and program modules

Threat

An anti-virus whose updates can be disabled by users or are made on a case-by-case basis cannot properly protect your system.

Facts

- Dr.Web virus databases are updated several times a day.
- Daily, Doctor Web adds about 200 new entries to its virus database, which allows it to detect most threats coming in for analysis.
- Hot updates are released as soon as analyses are completed.
- To avoid false positives, an update is tested over a huge number of uninfected files before it is released.
- As soon as an update is released, users can retrieve it from several servers located at various points of the globe.

The best practice

- To ensure the relevance and integrity of the anti-virus protection, timely installation of all updates made to the virus databases and anti-virus application modules is required.
- User opinions about whether the anti-virus protection system should be rebooted after it has been updated should be IGNORED.
- Only a centralized control tool can ensure regular updates and keep the protection components of the anti-virus protection system up to date.
- Updates should be monitored on a daily basis – because viruses capable of disabling updates or blocking access to the update server can emerge.

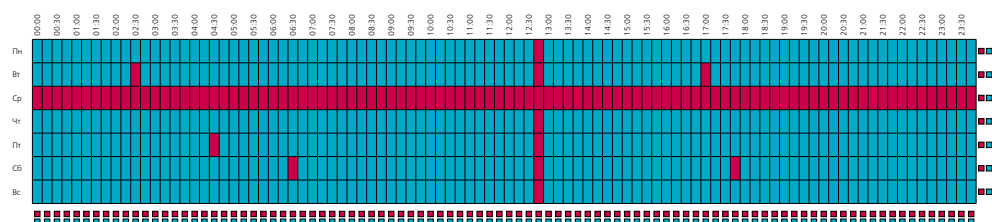
! Important!

No other software requires such frequent updating as an anti-virus. New viruses are being written all the time, and virus databases are updated very frequently. **Never disable automatic updating!**

Solution

With two or three clicks, the Dr.Web Anti-virus service Control Center can the Dr.Web Anti-virus service Control Center can the Dr.Web Anti-virus service Control Center can prevent a workstation from being updated by a user; disconnect an unupdated agent from the network, thus preventing the spread of outbreaks over the local network and beyond; and also:

- configure the Dr.Web component update procedure on protected workstations by distributing the load at different time intervals;



- monitor virus databases and the status of workstations;
- apply the update settings of one station to another station or to a whole group (or groups).

The updating of «mobile agents»

Threat

Though it is protected with a licensed anti-virus but not updated regularly, a single PC can be a potential danger to the entire local network. Moreover, this «travelling» computer might have a Client-Bank system installed.

Solution

If a laptop is not used in a LAN for a long time, set the mobile mode of the agent to communicate with the update server. The Mobile Mode of the Dr.Web Anti-virus service agent makes it possible to receive updates even from outside a corporate local network, which is especially important for employees travelling on business.

Regular scans of workstations

Threats

- An anti-virus is not aware of 100% of viruses at any arbitrary point in time.
- It may take days or even months between a new virus appearing and its signature being added to the virus database.
- Even if a signature added to the database can detect a virus, this does not mean that it can cure the virus, because it may take a long time to invent a way to cure it.

Facts

- After a PC has been scanned and the anti-virus software has been updated, a significant number of threats previously unknown to it may be found.
- The scanner performs a check deeper than that carried out by a background file monitor. That is why sometimes it turns out that the scanner detects viruses not seen by the file monitor.

The best practice

- A system should be scanned at least once a week.
- The Quarantine folder into which suspicious objects are moved should also be regularly scanned because it may contain previously unknown viruses or files moved there as a result of anti-virus false positives.
- Employee opinions about how often regular system scans should be conducted must be IGNORED.

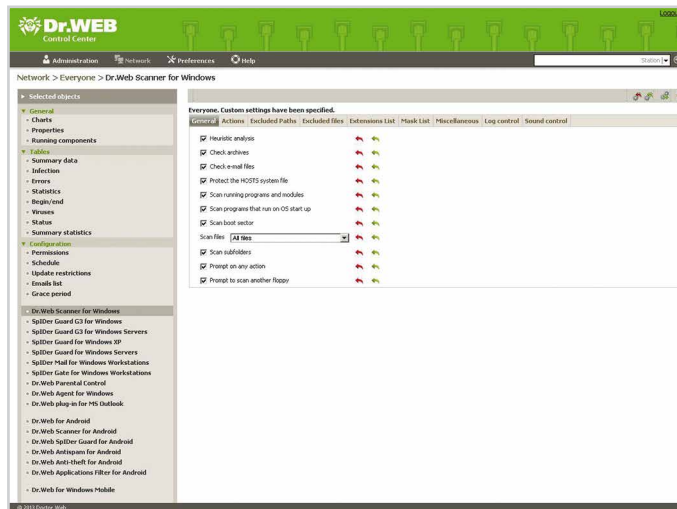
Solution

Regular scans at the individual workstation level are configured in the Scheduler which makes it possible to:

- run an unattended scan of a workstation;
- specify any necessary scan schedules, i.e., scan the system at a time convenient for employees;
- run mandatory scanning upon system booting;
- specify scan paths (locations, disks and folders to be scanned on a compulsory basis) and exceptions;
- specify the sequence of automatic actions to be taken towards detected malware and suspicious objects.

Important!

The default scan settings defined by Dr.Web developers are the most optimal. They don't need to be modified unnecessarily.



Centralized control over regular scanning of workstations

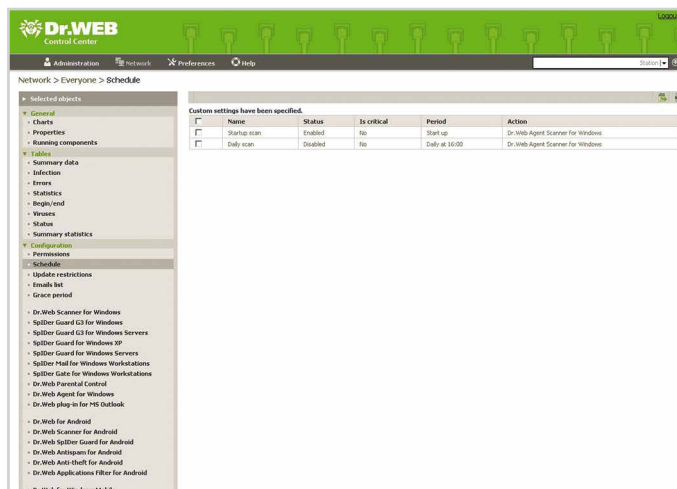
The best practice

- The only way to ensure regular scanning of all local network stations is **to centrally prohibit** the option to disable scanning.

Solution

The Dr.Web Anti-virus service Control Center allows a security policy for regular scanning to be centrally enforced:

- run/stop unattended scans of a workstation;
- specify scan paths;
- specify any necessary group and individual scan schedules, i.e., scan the system at a time convenient for employees.



Additionally, the Control Center allows any agent components (except SpIDer Guard) to be started/stopped.

Removable media access restriction

! Important!

These features are only included in the Dr.Web Premium subscription package.

Threat

- With a great number of new viruses appearing every day, there is no way that an anti-virus can know all of them; – the risk of infection with an unknown virus always persists.
- E-mail is no longer the main source of infection even in highly protected environments. It has been superseded by removable media, particularly, by flash drives.

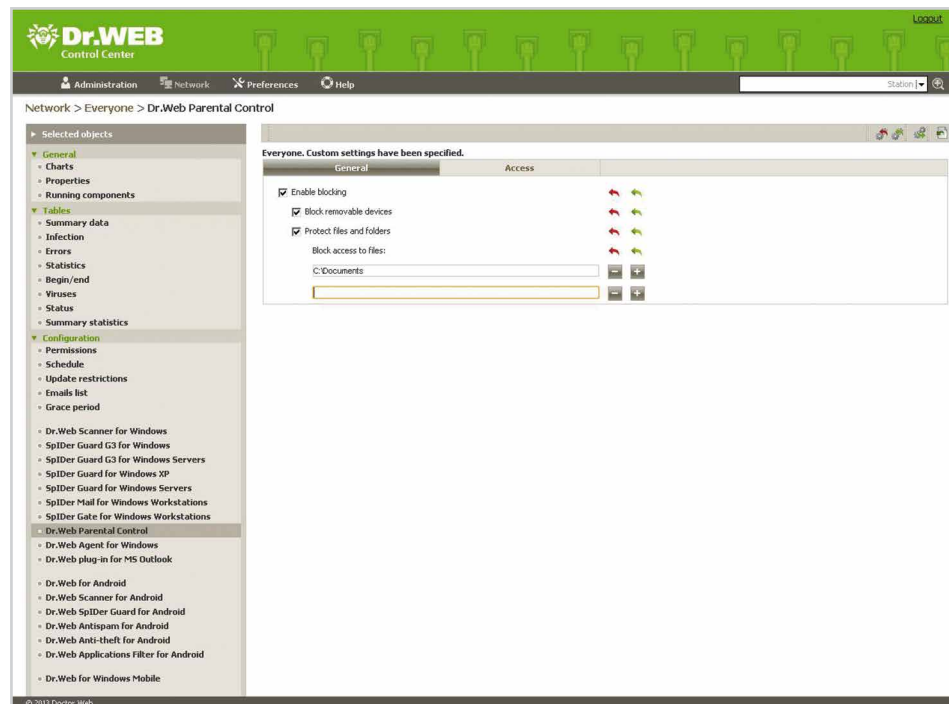
! Important!

Important! Removable media includes not only flash drives but any USB device. A virus can be transmitted from one PC to another even with a camera or a portable media player.

- Trojans are today's most common threats. These are malicious programs incapable of self-replication and unable to spread independently. People spread Trojan horses from one PC to another using flash drives.
- According to various estimates, 7-22% of data-loss incidents are caused by virus activities.
- Viruses can result in sensitive information being leaked, a company being disconnected from the Internet, and employees losing worktime while the health of computers infected with viruses is being restored.
- The constant threat of viruses penetrating the corporate network diverts system administrators from performing other tasks necessary for the development of the company.

Solution

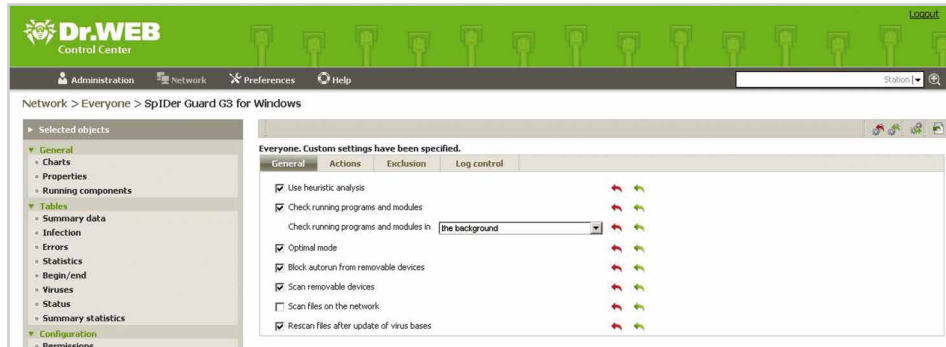
If you want to completely disable removable storage devices from being used on workstations, enable the «Block removable storages» option in Dr.Web Office Control preferences. Using Office Control overrides one of the main sources of viruses: – removable media.



Dr.Web Office Control's access restriction system:

- Defines the files and folders on a local network to which an employee may have access, and prohibits access to those that are off-limits – i.e., this prevents data and sensitive information from being deliberately or intentionally damaged, deleted, or stolen by attackers or insiders (employees seeking access to confidential information);
- restricts or completely prohibits access to Internet resources and removable devices, and, therefore, excludes the possibility of a virus invading via those sources.

An additional mechanism for protecting against viruses that spread through removable media is to bar autorun in the SpIDer Guard file monitor. After enabling the «Block autorun from removable media» option, you can still use flash storages in cases where not using them would be very inconvenient.



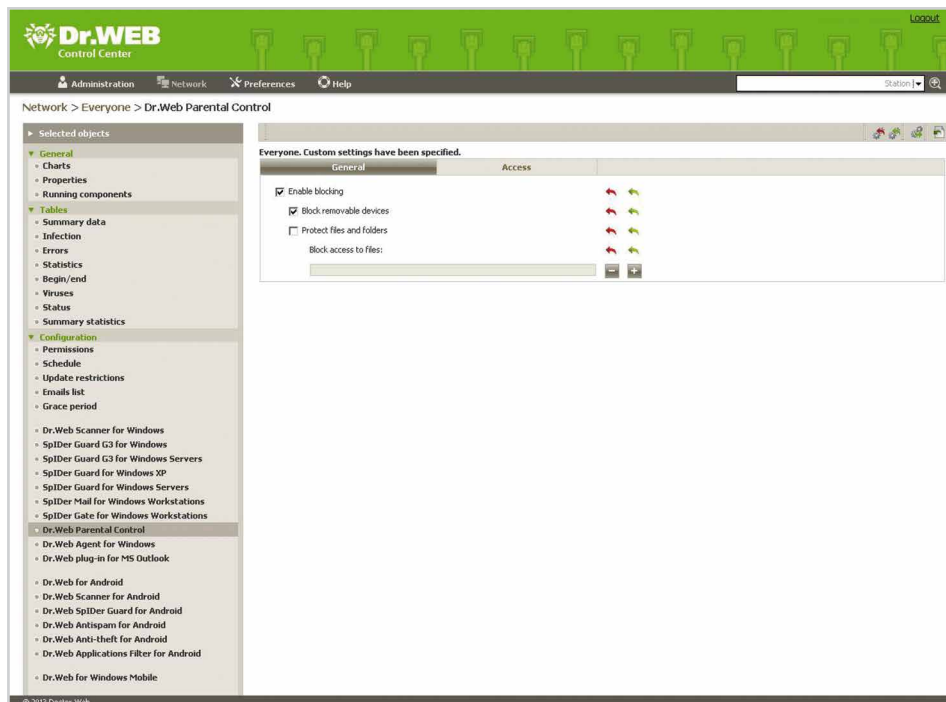
The above steps are effective but still not sufficient, as an employee can find and disable these settings.

The best practice

Users should only have access to the local resources that are required for them to perform their tasks at work. It's no use trying to convince staff that flash drives are dangerous. It is much easier to centrally disable access to such devices.

Solution

Restricting access to removable devices is centrally configured in the Dr.Web Anti-virus service Control Center.



Restricting Internet access

Protecting against malware infections and phishing

Threat

For their work, people need to be able to read news on the Internet and be informed. The danger is that the majority of office staff:

- access the Internet from office computers;
- perform their tasks under an administrator account in Windows;
- use weak passwords that can be easily cracked;
- do not install security updates for programs they use.

Uncontrolled Web surfing increases the risk of data leakage and unauthorized modification of sensitive data

Which websites are most likely to be sources of malware and phishing attacks (in descending order of incident frequency)?

- Sites related to technologies and telecommunications.
- Business websites: business outlets, business news portals, accounting related sites and forums, online courses/lectures, services to improve business efficiency.
- Adult content websites.

The best practice

An anti-virus system should be used to scan all the links that offer to download resources from the network, and all traffic until it enters a computer.

Solution

Composite protection is recommended to protect your system against infection when visiting a malicious website.



Important!

Dr.Web anti-virus features allow you to:

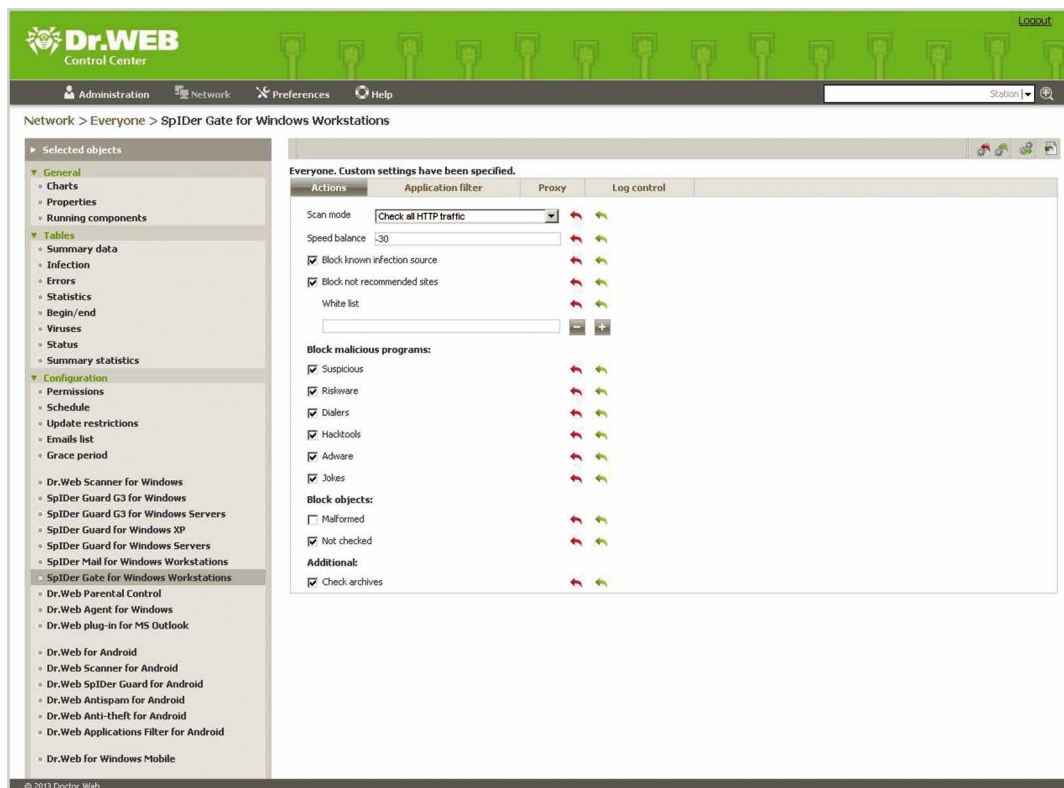
- partially restrict Internet access;
- create and use black and white lists of addresses, so you won't have to block Internet access completely for employees if it is needed to do their jobs;
- block Internet access, where essential (for example, on computers running accounting software);
- Make it impossible for an employee to disable the restrictions locally.

Protection with the Dr.Web Anti-virus engine

- **ScriptHeuristic** prevents any malicious browser scripts and PDF documents from being executed, while not disabling features provided by legitimate scripts.
- **The heuristic analyzer** designed to identify new, previously unknown viruses that have no entries in the virus database.
- **Fly-Code technology** to detect and neutralize viruses disguised with unknown packers.
- **Part of Dr.Web Anti-rootkit (Anti-rootkit API, or arkapi)**, the resident background scan subsystem that searches for active threats among critical Windows areas such as start-up objects, running processes and modules, system object heuristics, RAM, MBR/VBR, and BIOS. When threats are detected, the subsystem cures them and blocks harmful effects.

Software-based protection for individual workstations

- **SpIDer Guard file monitor** ensures protection against active infections in the system.
- **Dr.Web Office Control** scans 10 categories of dangerous and unwanted websites (social networks, gambling, etc.) against an updatable database.
- **SpIDer Gate® HTTP monitor** scans traffic before it enters a PC – against signatures and using heuristic techniques.
- The SpIDer Gate module transparently scans incoming and outgoing HTTP traffic in real time, intercepts all HTTP/HTTPS connections, filters out data, automatically blocks infected web pages in any browser, scans files in archives (such as those downloaded via download managers and other applications that exchange data with web servers), and protects users from phishing sites and other dangerous web resources.
- You can disable the scan of outgoing or incoming traffic and create a blacklist of applications whose HTTP traffic will be scanned no matter what (black list). You can also define applications whose traffic will not be scanned (white list).
- SpIDer Gate operates independently from web browsers.
- Filtering does not affect overall system performance, surfing speed, and traffic.
- No configuration is required in the default mode; Dr.Web SpIDer Gate starts scanning right after installation.



Important!

These components are only included in the Dr.Web Premium subscription package.

Reducing Internet costs and employee monitoring

Threat

- One hour of daily web surfing by every employee can add up to 12.5% of what companies spend on salaries.
- During certain times of day (e.g., lunch hour), employees can monopolise up to 80% of a corporate network bandwidth for their personal needs.

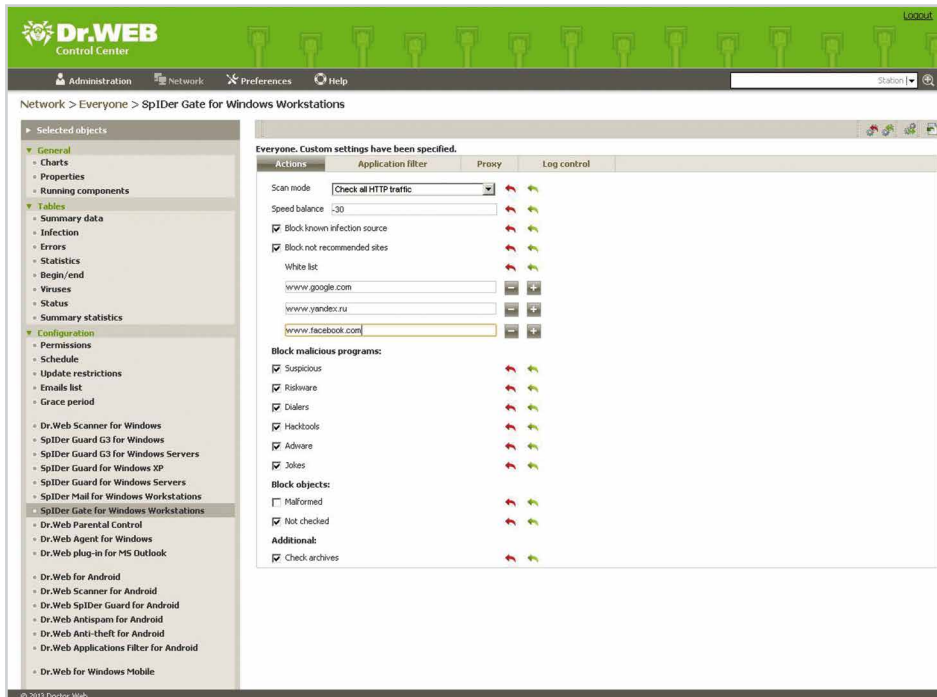
The best practice

- During working hours, staff should have access only to Internet resources required for their work.
- Use the **centralized** control to deny employees access to unwanted Internet resources.
- In this case employee opinions about whether certain websites are malicious should be IGNORED.

Solution

The Dr.Web Anti-virus service Control Center makes it possible to:

- create Internet access policies for single users and user groups;
- prevent employee attempts to visit unwanted pages, such as social networks, online shops, and game sites.



Anti-spam protection



These features are only included in the Dr.Web Premium subscription package.

Reduction of spam traffic and elimination of up to 99% of threats that spread via spam

Threats

1. Mail traffic is the main **transport** for viruses and spam. If malware infects a computer, it can access the employee's address book which, along with contacts of other employees, may contain addresses of customers and partners; – that is, the infection won't be confined to the corporate network but will spread outside.
2. Carelessness, negligence and ignorance of simple basics of computer security are often the reasons why computers become a part of botnets and a source of spam that damages a company's image and can place it on a black list, possibly compelling a provider to disconnect the company from the Internet for sending out spam.

Risks of using a free anti-virus without anti-spam

Virus-related risks	Reputational risks
<ul style="list-style-type: none"> ▪ The possibility of infecting a computer and turning it into a botnet node and a target for hacker attacks – up to a denial of service. ▪ The possibility of compromising a company by entering it on a black list and disconnecting it from the Internet for sending out spam in the event it got into a botnet. ▪ Increasing costs of IT infrastructure (paying for «parasitic» traffic/costs for e-mail storage including spam) and traffic. 	<ul style="list-style-type: none"> ▪ Preventing partners from receiving e-mail by entering the company on black lists. ▪ Worsening reputation in the eyes of consumers and partners. ▪ Perception of the company as being technologically backward. ▪ Loss of customers; – refusal of a company's services.

Misconception

Anti-spam needs to be constantly trained.

Facts

An intelligent Dr.Web anti-spam filtering system does not require configuration and training, – unlike trainable anti-spam systems that require daily work on the part of system administrators.

The best practice

- E-mail traffic should be scanned before messages are downloaded by a mail client to prevent it from being exploited by malicious code.
- Only comprehensive solutions for e-mail that combine an **anti-virus** and an **anti-spam** can ensure its complete protection and reduce non-production costs (i.e., losses arising from organizational and management shortcomings).

Solution

Dr.Web Anti-spam, included in SpIDer Mail monitor, scans messages before they are downloaded by a mail client and prevents malware arriving with spam from exploiting software vulnerabilities. Its operation does not affect overall system performance. The effectiveness of rejecting spam reaches 97–99%.

Advantages of Dr.Web anti-spam

- **No training** – unlike anti-spam solutions that require daily training, the intelligent Dr.Web anti-spam starts working as soon as the first message arrives, without any training or configuration.
- **High spam-detection rate** – different filtering technologies ensure the high probability of detecting spam, phishing, pharming, scamming, and bounce messages.
- **Anti-botnet** – your company will not be disconnected from the Internet by your provider for sending out spam.
- **E-mail will not get lost** – filtered e-mail is not deleted, but is moved into the special folder of a mail program (provided this folder is configured on a local PC) where they can be checked for false positives, if necessary.
- **Less traffic** – a spam analyzer module is absolutely self-contained; no connection to an external server or access to a database is required for its operation.
- **Always up-to-date** – unique spam detection technologies based on thousands of rules allow updates to be made as often as once every 24 hours.
- **Low system load** – the anti-spam does not affect overall system performance and does not delay e-mail delivery.

Increasing employee performance

Today's information surplus makes employee concentration a valuable and almost non-renewable resource. An excessive amount of information and its easy accessibility over the Internet make it extremely easy for office workers to get distracted. Daily spam cleanings, persistent pop-ups, and flashing banners lower concentration and negatively impact an employee's emotional and mental state. It turns out that keeping employees focused costs more than combating distractions.

Threats

1. On average, an office worker spends 6 to 11 minutes of daily working time to view and delete spam.
2. The higher the position of such an employee, the more the company loses on paying for their labour.

Risks

Using anti-virus without anti-spam:

- reduces the performance of all employees who receive mail and have to clean up their mailboxes from spam;
- leads to unproductive losses of working time and delays in job duties, as well as delays in the fulfilment of the company's obligations towards its customers and partners;
- makes employees less attentive and more tired because of distractions;
- causes employees to be irritated and frustrated with the management's inability to cope with the problem (high reputational risk for the management!).

Solution

Using anti-spam as part of Dr.Web Premium is an effective tool against numerous distractions that reduce the loss of working time thanks to:

- stable and secure operation of the computer (free of viruses and spam in the mail traffic);
- the absence of spam in employee mailboxes which may take a lot of time to clean up.

Configuring anti-spam on an individual workstation

The anti-spam can be enabled in the Dr.Web SplDer Mail software component.

Black and white lists

When necessary, it's possible to create lists of trusted and blocked addresses, the mail from which will be filtered as needed by default.

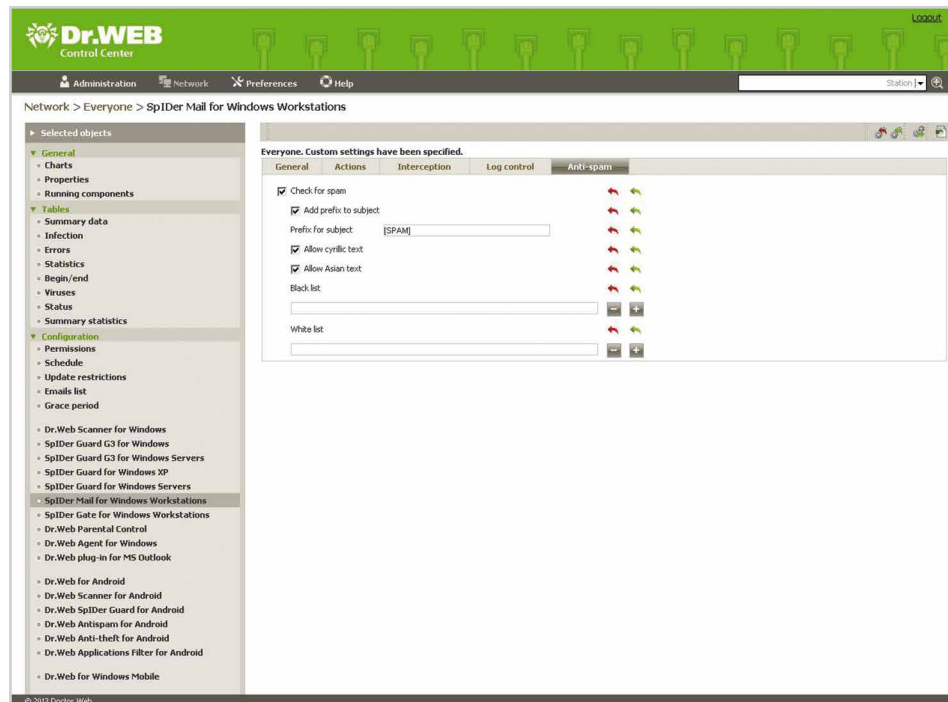
Centralized control making it impossible to disable anti-spam

The best practice

Centralized prohibition of anti-virus setting modification by employees is only one efficient measure to prevent users from disabling an anti-spam or editing black and white lists.

Solution

Centralized anti-spam settings are configured in the Dr.Web Anti-virus service Control Center.



Protection against virus attacks on devices with e-banking systems installed

Note!

1. Modern threats are created by well-organized criminal gangs, not to hone programmer skills, but to rob money from those who know how to earn money.
2. Any software, including e-banking systems, contains vulnerabilities.

Scenarios of modern attacks aimed at stealing money

To penetrate/imbed viruses into a system that is used to work in the Client-Bank system, the following can be used:

- Phishing websites.
- Creating fake websites.
- Hacking Internet websites and resources with high traffic.
- Social engineering techniques.
- Hacking computers.

Types of attacks aimed at stealing money

- A PC can be infected with a WebInject (sometimes with redirection to a phishing site).
- An attack on data links; – HTTP requests are intercepted in order to get login/password or transferred screen forms
- A virus attack on a server in which case their objectives may be to search for e-banking server vulnerabilities or to conceal a theft of funds
- Attacks on a computer over the Internet in order to steal a private, digital signature key and passwords.
- Attacks on a computer over the Internet in order to capture computer resource management remote control.
- Attacks in order to substitute documents when they are submitted for signature.
- Attacks in order to substitute some or all software.
- Implementation of backdoors or Trojans.

Targets of attacks

- office PCs;
- personal employee devices;
- personal devices of a target company.

Objectives of attacks

- to steal and substitute access authentication credentials (login and password) for an e-banking system;
- to post banking transactions using remote access – in an existing or parallel session;
- to penetrate protected corporate networks.

Theft methods

- The criminal creates a remote unauthorized payment directly from a client computer using malicious software.
- The intruder sends payment orders via a client computer to coincide with a client's session in the «Client-Bank» system (with the possibility of signing a document with a key stored on alienated media such as eToken, iKey, etc.).

Outraged customer

«We bought an anti-virus, and our system administrator is earning his keep; the systems are being updated...But money was lost! Who is to blame?»

Facts

1. In most small and medium-sized companies only the CEO is entitled to sign payment orders. But two digital signatures – the CEO's and the accountant's – significantly reduce the risk of virus-related thefts.
2. Users access e-banking systems not only from their office computers. Quite often they use home PCs and mobile devices (usually those running Android OS) that sometimes don't have any anti-virus installed, or operate a free version with restricted functionality.

In Russia, there are no solid statistics on money being stolen via e-banking systems. Very often, victims do not approach law enforcement authorities for help, believing that it is impossible to have the money returned, and this only makes matters worse. They do not know how to act in that situation, how to initiate an investigation; they lose time.

Threats

1. Modern, effective Trojans are aimed at stealing money from companies and individuals.
2. The most effective and dangerous, **Trojan.Carberp** spreads using Black Hole Exploit Kit, a set of vulnerabilities that exploit browsers and operating system bugs and undocumented features.
3. An organized criminal group works on the development and «promotion» of **Trojan.Carberp**: the developers are located in one country, while the servers that disseminate the Trojan are in another, the organizers are in the third, and «partners» who buy a part of a botnet for criminal use are in several countries.
4. The Trojan can also download special plug-ins. At the moment, plug-ins exist for almost all kinds of known e-banking systems. **Trojan.Carberp** can open any file located in a compromised system, establish Remote Desktop session over RDP, or even remove an OS from a compromised system. Thanks to remote control and plug-ins, an attack can be carried out against a specific company from the outside, on demand. The Trojan's actions against your company depend on the «customer».
5. Carberp family viruses merely get into user computers **during visits to hacked websites, including news and accounting sites** which are visited daily by potential victims. No need to take any action to get the system infected. **It occurs automatically.**
6. Just 1 to 3 minutes are enough for a Trojan to steal passwords and cash from a victim's account.
7. Daily, several signatures of this Trojan are added into the Dr.Web virus database; – the program is constantly being improved by its authors. Here is an example of new Trojan entries in one day:

```
Trojan.Carberp.14(2) Trojan.Carberp.15(7) Trojan.Carberp.194 Trojan.Carberp.195
Trojan.Carberp.196 Trojan.Carberp.197 Trojan.Carberp.198 Trojan.Carberp.199 Trojan.Carberp.200
Trojan.Carberp.201 Trojan.Carberp.202 Trojan.Carberp.203 Trojan.Carberp.204 Trojan.Carberp.205
Trojan.Carberp.206 Trojan.Carberp.207 Trojan.Carberp.208(14) Trojan.Carberp.209
Trojan.Carberp.210 Trojan.Carberp.211 Trojan.Carberp.212 Trojan.Carberp.214 Trojan.Carberp.215
Trojan.Carberp.216 Trojan.Carberp.217 Trojan.Carberp.218 Trojan.Carberp.219 Trojan.Carberp.220
Trojan.Carberp.221 Trojan.Carberp.222 Trojan.Carberp.224 Trojan.Carberp.225 Trojan.Carberp.226
Trojan.Carberp.227 Trojan.Carberp.228 Trojan.Carberp.229 Trojan.Carberp.230 Trojan.Carberp.231
Trojan.Carberp.232 Trojan.Carberp.233 Trojan.Carberp.234 Trojan.Carberp.235 Trojan.Carberp.236
Trojan.Carberp.237 Trojan.Carberp.238 Trojan.Carberp.239 Trojan.Carberp.240 Trojan.Carberp.241
Trojan.Carberp.242 Trojan.Carberp.243Trojan.Carberp.244 Trojan.Carberp.245 Trojan.Carberp.246
Trojan.Carberp.247 Trojan.Carberp.248 Trojan.Carberp.249 Trojan.Carberp.250 Trojan.Carberp.251
Trojan.Carberp.252 Trojan.Carberp.253 Trojan.Carberp.254 Trojan.Carberp.255 Trojan.Carberp.256
Trojan.Carberp.257 Trojan.Carberp.258 Trojan.Carberp.259 Trojan.Carberp.260 Trojan.Carberp.261
Trojan.Carberp.262 Trojan.Carberp.263 Trojan.Carberp.264 Trojan.Carberp.265 Trojan.Carberp.266
Trojan.Carberp.267 Trojan.Carberp.29(14) Trojan.Carberp.33(10) Trojan.Carberp.45(4)
Trojan.Carberp.5(3) Trojan.Carberp.60(6) Trojan.Carberp.61 Trojan.Carberp.80
```

Meanwhile, it's only one Trojan modification...

What can a company do to counter this, having at its disposal only a file anti-virus with no comprehensive anti-virus protection suite? – NOTHING.

The best practice

1. An anti-virus on its own is not enough to protect against such attacks. To significantly reduce the risk of infection, an anti-virus protection system should include:
 - A system able to cure active infections, – to «extinguish» the activity of the malware that somehow penetrated the system and clean it up.
 - The best self-protection system is the system that functions normally until an update is released that can cure an infection.
 - Office control has a mechanism to limit access to Internet sites (remember that Trojan horses are distributed through sites).
 - Hyperlink scanner (HTTP monitor).
 - Control Center; – the system should not allow employees to change the settings under the pretext that «everything is slowing down.»

2. Practice shows that payments can be made not only from PCs located in the accounting department, but also from home PCs and mobile devices. Therefore, all machines and mobile devices used by company employees need to be protected.
3. A computer on which an accounting system or a «Bank-Client» system is installed must be completely disconnected from the Internet. The use of removable devices should be CENTRALLY blocked on such a PC*.
4. An accountant's opinion about measures taken to protect such a computer should be IGNORED completely.

* This is performed by using the Office Control in the Dr.Web Premium subscription package.

Facts

The first-ever banking Trojan for Android, Android.SpyEye.1, already exists.

What to do if money gets stolen from an e-banking system

Unfortunately the victim discovers the theft when it's already happened. At this point, the way the victim responds to the incident becomes extremely important. Before you follow our recommendations, make sure that the theft occurred as a direct result of the virus. For this purpose, it's enough to briefly interview employees having access to the e-banking system. If you or they did not perform an operation that you consider suspicious, it's likely the result of a virus or an attacker.



Important!

- Do not attempt to update the anti-virus or run a scan— you may destroy the traces of intruders in the system!
- Do not attempt to reinstall the operating system!
- Do not attempt to remove any files or programs from the disk!
- **Never use the computer** from which e-banking system authentication credentials have allegedly leaked — even if there is an urgent need for it!

Your actions must be swift and decisive:

1. Immediately contact your bank; — it may still be possible to stop payment. Even if the payment has already been transferred, ask for all transactions with a compromised account to be blocked before new access authentication credentials (login and password, etoken etc.) are issued to you.
2. Notify your bank (the bank sending the payment) by fax. Print out the request in TRIPLICATE, and submit them to the bank. Ask for the registration numbers to be included on two copies: — one will remain with you, and the other will be attached to your statement to the police. Your application should contain the date and serial reference number of the document accepted by the secretary.
3. Fax a notification to the beneficiary, the bank that receives funds from your account. Similarly, make THREE copies and register them.
4. Submit a statement to the police and attach the notifications to the two banks to it (recipient and sender of the payment). To do this, visit the nearest police department.
5. Notify your provider in writing, asking them to provide logs of network connections for the period when the theft occurred.



Important!

ISPs keep logs of network connections no longer than two days, — so you have little time!

All the above must be completed within 1–2 days after the theft has been discovered!

Protection against hacker attacks

Types of hacker attacks

There are many types of network attacks. As a rule, to carry out attacks, criminals take advantage of vulnerabilities of the operating system or other installed software; they also limit the victim's processing power. Network attacks can be subdivided as follows:

- **DoS or DDoS attacks** (attacks that cause denial of service) are directed towards temporarily disrupting a targeted system.
- **Password attacks** aimed at identifying used passwords, – through brute force or by means of social engineering.
- **Spoofing** inserts false information or malicious commands into the normal data flow; traffic redirection to a false IP address and/or its substitution.
- **Sniffing** – the capture of traffic (for example, all of a victim's e-mail messages) for subsequent analysis.
- **TCP Session Hijacking.**
- **Man-in-the-Middle.** The attacker is located between two network hosts, and, in fact, acts as a proxy server, viewing the transmitted information and being able to modify it for his own purposes. The purpose of these attacks is to steal information, intercept the current session and obtain access to private network resources, analyze traffic, obtain information about the network and its users, perform DoS attacks, distort transmitted data and input unauthorized information into network sessions.

And that's not all. Network attacks also include all methods of intelligence carried out on network channels, breach of trust and unauthorized access. For example, port scanning; – this type of threat is not an attack but usually precedes one, as it is one of the main ways to get information about a remote computer. Information obtained by a scanner (a «snapshot» of the system) allows an attacker to get an idea about the type of operating system on the remote computer, and thus about the OS-specific vulnerabilities.

New types of attacks are constantly emerging. In particular, the transition of companies to «clouds» has caused attacks on communication channels to intensify, and the introduction of IPv6 has led to the creation of new types of attacks related to vulnerabilities of this protocol whose implementation is still undergoing refinement.

Consequences of attacks

- Damage or destruction of information resources rendering them impossible to use, and downtimes.
- Leaks of confidential data, including passwords, email, and generally any information that can be stolen.
- Reputational risks – delays or failures to fulfill obligations to customers and partners.

Important!

Attacks aimed at the introduction of malicious software usually remain unnoticed by victims, and their computers get controlled by attackers.

Objectives of attacks

- Political motives.
- Orders of competitors (including industrial intelligence, revenge).
- Hooliganism.

Solution

Firewall included in the Dr.Web Anti-virus service:

- protects from insiders by preventing the network from being scanned or connections to a remote desktop from being made;
- prevents hacker infiltration through unsecured ports;
- protects against unauthorized access;
- reduces the risk of hacking through a vulnerability;
- prevents data leaks over the network;
- blocks suspicious connections on package and application layers;
- application layer connection control makes it possible to monitor the interaction of applications and processes with network resources and to register all access attempts in the applications log;

- packet-layer filtering makes it possible to control the connection to the Internet regardless of what application is using it. The packet-filter log stores information about packets sent over network interfaces.

Important!

By default, the Dr.Web firewall is not installed. To install this component, you need to uncheck the box next to its name during installation.

Protection against intrusions via vulnerabilities

Threat

- A vulnerability is a flaw in the software that can be exploited to compromise its integrity or render it non-operational.
- There are vulnerabilities in every piece of software. There are no invulnerable programs.
- Modern virus writers exploit vulnerabilities to penetrate a computer's operating systems and applications (browsers, office products, such as Adobe Acrobat Reader, and plug-ins for browsers to display flash).

Important!

No software other than an anti-virus can clean a system from malicious software that has penetrated it by exploiting a vulnerability.

The best practice

Keeping installed software up to date is as important as updating your OS. Theoretically any error in the program code can be used to cause harm to the system. In this case it does not matter whether it is a short-term failure or serious data damage. To avoid this, it is important to monitor the condition of your software and promptly download updates or new versions.

Solution

Using SpIDer Gate HTTP monitor and SpIDer MailD mailbox monitor makes it possible to keep malicious objects from penetrating program vulnerabilities (such as browsers, Adobe Flash and Adobe Acrobat software, e-mail clients), since all the traffic, including encrypted traffic, is scanned before it gets into an appropriate program.

Protection against infections made using social-engineering techniques

The most terrible virus is a user.

Folk wisdom

Most modern malware found in the wild cannot spread on its own and is meant to be distributed by users.

It is users, ignorant of computer security basics or simply tired or careless, who unintentionally help malware penetrate a network (by using USB devices, automatically opening e-mails from unknown senders, uncontrollably surfing the web during business hours, etc.).

To distribute Trojan horses, virus writers resort to social engineering techniques to take advantage of users and trick them into launching malicious files. The tricks are many: phishing links, fake e-mails from banks or social-networking website administrators, and much more. The aim of all social engineering techniques is to acquire personal information ranging from passwords to access various web services to confidential and bank account information.

The best practice

One does not need much to cope with scammers who use this method of attack. Adhering to some simple rules helps to significantly reduce the risk of data loss:

1. If you have received a letter containing a request to report or confirm your password for any resource, – delete it, no matter what horrible threats it may contain (account deletion, account reset, etc.). Administrations of network resources, especially banks, will never ask a user for credentials.
2. If you have received a letter or a strange message allegedly from your friend that, among other things, contains hyperlinks to certain resources, – then contact this person some other way (for example, by telephone) and make clarify what they sent to you and why. It is possible that this person's account was compromised and is being used by hackers.
3. If any third-party resources invite you to visit a page where you will have to enter your personal data (for example, the link to vkontakte.ru), – please spend some time manually entering the text of the link into the browser address bar; – this will completely exclude the risk of getting into a phishing site (there are many methods of masking the true paths of links). Before entering the link in your browser, check whether the domain name of the site corresponds to the original domain name (to trap you, a malicious link, for example, may contain vkontakte.ru instead of vk.ru).
4. After reading online about a «fried» fact – e.g., about a new way of reading other people's SMS; – it's best not to test it in action. Hackers never unveil which vulnerabilities they have found. In this case, they are exploiting user curiosity to make them move to the infected sites they need.
5. Do not disable the HTTP monitor in the anti-virus; – this will protect you even more when surfing the network.

Important!

Do not disable the SplDer Guard file monitor. It must reside in the computer's memory and prevent infection by scanning files before they are launched as well as all system processes—every time the anti-virus is updated. SplDer Guard is effective against all known and many unknown threats, because it utilizes heuristic-analysis techniques. Even if a new virus is not detected by SplDer Guard, it will still not be able to perform a malicious action.

Reduction of downtime caused by viruses

Viruses and spam are the main threats to the security of a company of any size. Analysis of corporate network security, preventive measures and overcoming consequences of virus attacks are daily tasks of IT personnel. Reducing downtimes caused by malware is a key task for system administrators. The efficiency of an entire company's business routines and its positive image of a reliable partner depend upon the successful accomplishment of this task.

Threat

- Downtimes per user average 2 hours per month.
- The higher an employee's position – the more costly the downtime.

Time spent waiting for a problem to be resolved, resolving the issue, and searching for a solution on one's own may have unpredictable consequences including data losses.

Solution

If you use the anti-virus as a service:

- software is upgraded and updated centrally in an automatic mode under the control of the service provider or a company's system administrator;
- downtimes caused by untrained users' inappropriate responses to virus infections, resulting in disrupted daily business routines, are a complete non-issue (the anti-virus software is maintained by the provider).

The Dr.Web Anti-virus service is a powerful tool for reducing outages caused by viruses and malware.

Dr.Web anti-virus protection system

Services

Alerts

A system administrator receives alert messages about problems in the anti-virus network, for example, reports on virus attacks, system alerts, and notifications about the results of scans performed by users. Alerts are sent out by e-mail or over Windows standard wideband broadcast channels. Message bodies can be customized.

Instant messaging

The messenger interface allows an administrator to send informational messages to selected users or to entire user groups. This feature can be used, for example, to send messages on virus outbreaks and on what to do in case of infection by malware, as well as to report network technical problems, or send season's greetings.

Statistics and reports

The system allows administrators to receive the following detailed information on the anti-virus network's status:

- Detected viruses (list of infected objects, virus, anti-virus actions, etc.).
- Information about detected viruses arranged by virus type.
- Information about installed virus databases: the name of the file containing the specific virus database Virus database version Total signatures in the virus database Virus database creation date.
- A list of scanning errors that occurred on user computers in a defined period.
- A list of components launched on the computer.
- Information about an abnormal status (possibly requiring intervention) registered in a defined period.
- A list of jobs assigned for the computer in a specified period.
- Detailed information about all the of Dr.Web anti-virus modules: module description – its functional name A file that corresponds to a certain product module The full version of the module, etc.
- The list of software installations on the target machine.
- Summary statistics.

Network security information can be presented in graphs. A system administrator can collect and analyse virus event data from every protected computer on a regular basis and provide easy-to-read statistical reports on the results of the monitoring.

Audit log

The audit log allows all of the system administrator's steps, when installing and configuring the system, to be tracked. In case questions arise regarding the chronology of or justification for an administrator's actions, it can always submit a complete report on the work done. This guarantees that its actions are highly transparency.



Important!

When investigating computer incidents, the audit log is used as part of the evidence base.

Conclusion

About Doctor Web

Doctor Web – Russian developer of Dr.Web anti-virus software. Our products have been developed since 1992. Doctor Web is a key player on the Russian market of software that provide the information security, the basic businesses needs.

Doctor Web is one of the few anti-virus vendors in the world that have their own technologies to detect and cure malware, an anti-virus laboratory, a global virus monitoring service and technical support.

The development of technologies to protect systems from both known and unknown threats is among top priority of our programmers. Our anti-virus protection system allows information systems of our customers to be protected from any even unknown threats. Dr.Web solutions that fully satisfy businesses' needs in anti-virus protection.

Doctor Web creates innovative business models based on its developments. In 2007 we become the first company to offer an innovative anti-virus as a service model. From this point on, the Software-as-a-Service (SaaS) era in Russia's anti-virus industry is underway and to this day, Doctor Web is still the undisputed leader in this segment of the market.

Doctor Web's annual sales growth rate is above the industry average. Home users from all over the world, small companies, large enterprises and backbone corporations are the loyal users of Dr.Web products for many years. Doctor Web has received state certificates and awards; our satisfied customers spanning the globe are clear evidence of the high quality of the products created by our talented Russian programmers.

Contacts

Russia

Doctor Web

3d street Yamskogo polya 2-12A, Moscow, Russia, 125124

Tel: +7 (495) 789-45-87

Fax: +7 (495) 789-45-97

www.drweb.com | www.av-desk.com | www.freedrweb.com |
mobi.drweb.com

China

Doctor Web Software Company (Tianjin), Ltd.

112, North software tower, № 80, 4th Avenue, TEDA, Tianjin, China

天津市经济技术开发区第四大街80号软件大厦北楼112

Tel: +86-022-59823480

Fax: +86-022-59823480

E-mail: D.Liu@drweb.com

www.drweb.com

France

Doctor Web France

333 b Avenue de Colmar, 67100 STRASBOURG

Tel: +33 (0) 3-90-40-40-20

Fax: +33 (0) 3-90-40-40-21

www.drweb.fr

Germany

Doctor Web Deutschland GmbH

Rodenbacher Chaussee 6, D-63457 Hanau

Tel: +49 (6039) 939-5414

Fax: +49 (6039) 939-5415

www.drweb-av.de

Japan

Doctor Web Pacific, Inc.

NKF Kawasaki building 2F, 1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi,
Kanagawa-ken
210-0005, Japan

Tel: +81 (0) 44-201-7711

www.drweb.co.jp

Republic of
Kazakhstan

Doctor Web – Central Asia

Republic of Kazakhstan, 050009, Almaty, Shevchenko, 165b office 910

Tel: +7 (727) 323-62-30, 323-62-31, 323-62-32

www.drweb.kz

Ukraine

Doctor Web Technical Support Centre

Office 3, 4 Kostelnaya str., Kiyev 01001, Ukraine

Tel./fax: +38 (044) 238-24-35, 279-77-70

www.drweb.ua



© Doctor Web,
2003–2013