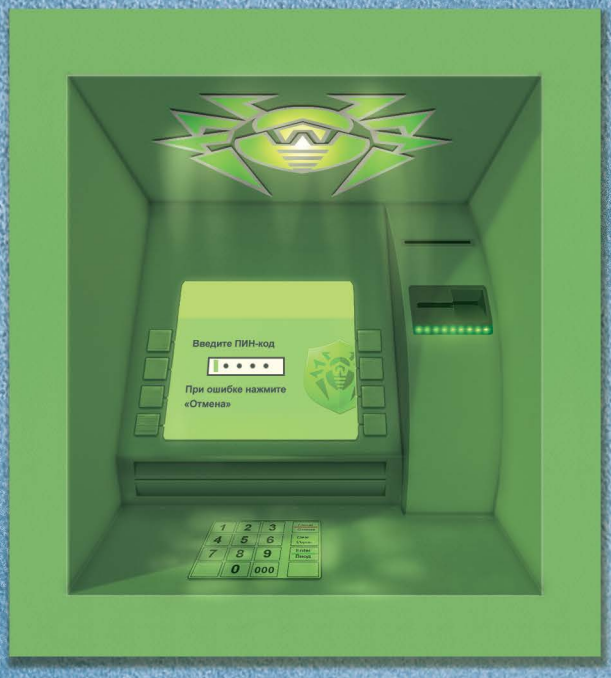
Dr.WEB®
ATM Shield



Centralised protection
for embedded systems
(ATMs, payment terminals, multi-kiosks, cash registers, etc.)

The first malware species targeting ATMs was detected in Russia in March 2009. ATMs infected with Trojan.Skimer were found in Moscow and later in St. Petersburg.

Doctor Web was the first to respond to this threat: the company revealed Trojan.Skimer's existence to the public, and then developed **Dr.Web ATM Shield** – an anti-virus that provides embedded computer systems (ATMs, payment terminals, multi-kiosks and POS networks) with real-time protection against viruses.

Dr.WEB®
ATM Shield

Admit it; you do it, too, right?

- You use USB devices without scanning them with an anti-virus?
- You open emails from unknown senders?
- You work under an administrator account in Windows?
- You don't install security updates for the programs you use?
- You access the Internet from office computers that run programs containing vulnerabilities?
- You use weak passwords that can be easily cracked?

What makes you think that the employees responsible for maintaining ATMs and terminals don't do the same?

Hold on, you say—are there actually viruses for ATMs?

Specialised ATM viruses – malicious programs capable of self-replication – have not yet been found. But the number of Trojans is increasing constantly! In just one month – December 2013 – four new ATM Trojans were discovered: Trojan.Ploutus.1, Trojan.Ploutus.2, Trojan.Skimer.19 and Trojan.PWS.OSMP.21.

These are the specific features of ATM Trojans:

- they are controlled by means of specially designed master cards or from mobile devices;
- they intercept entered PIN codes and decrypt them, **using the software already installed on the ATM**;
- they steal data from bank cards; They save stolen data on plastic cards designed by hackers or print it on cash receipts;
- they disperse cash when the attackers enter a command through the ATM keypad or by means of a special SMS message.

ATMs are maintained by competent personnel — how can anything get into them?

An ATM can get infected via:

- **removable media** intended for routine ATM maintenance but also adopted by personnel for personal use;
- **removable media** plugged in by criminals who access the servicing area with a special key;
- malware from the **infected internal network** of the company, if the embedded system is accessible via the network;
- exploiting **vulnerabilities** in the ATM's software.

Even if an ATM gets infected with an ordinary malicious program that can't compromise ongoing transactions, BSODs and screenshots of ransom demands that have been distributed all over the Internet will damage your business's reputation—something that is not only unpleasant, but also costly as the equipment will have to be made operational again.

Dr.Web ATM Shield is not just an anti-virus!

Dr.Web ATM Shield is packed with features that will minimise the probability of any deliberate or inadvertent infection of ATMs:

- the file monitor makes it impossible to run malicious software on the ATM;
- the anti-rootkit discovers previously unknown threats;
- the Office Control restricts access to local directories and websites, so that malware can't transmit data to criminals or connect to a command and control server;
- by disabling access to removable media, you eliminate the possibility of unknown removable data storage devices infecting your embedded device with malicious programs;
- the HTPP monitor will ensure that only trusted applications will access the Internet via allowed ports.

Dr.WEB®
ATM Shield

Dr.Web ATM Shield has been specifically designed to neutralise common ATM threats

Why use complex solutions when you can simply install an ordinary anti-virus?

The common features of embedded systems include:

- Low RAM and a relatively slow CPU.
- Round the clock uptime.
- Embedded editions of operating systems.

Dr.Web ATM Shield is specifically designed to run on low-end hardware

For **Dr.Web ATM Shield** to operate normally, an embedded device only needs to have 512 MB of RAM.

Small virus databases and updates have traditionally distinguished Dr.Web software; these features allow it to be used to protect remote hosts with low network bandwidth.

Dr.Web ATM Shield can run under embedded editions of operating systems

Dr.Web ATM Shield can not only be used with conventional operating systems, such as Windows® XP Professional, Windows® Vista and Windows® 7 and Windows® 8, but also with Windows® XP Embedded, Windows® 7 Embedded and Windows® 8 Embedded.

Dr.Web ATM Shield is not just an anti-virus! It also incorporates:

- technologies to minimise loading and scanning time (multi-thread and delayed scanning of files that have been read);
- stable operation on low-end machines;
- a state-of-the-art anti-virus engine, which detects and neutralises the latest viruses that have not yet been registered in the virus database, including those hidden under unknown packers;
- powerful self-protection that prevents viruses from disrupting Dr.Web's operation.

Dr.Web ATM Shield is a unique solution, tailored for embedded devices

Attention!

Using malicious software to steal money is a crime

Doctor Web can investigate malware-related incidents and can also perform a psychological evaluation of individuals (company personnel) to identify possible accomplices involved in illegal activities against customers as well as instances of negligence.

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

The Legal Corner of the Doctor Web site at http://legal.drweb.com/ contains samples of statements that can be given to law enforcement and other authorities, as well as recommendations on what action to take after a theft has been detected. Use this information

About Doctor Web

Doctor Web is the Russian developer of Dr.Web anti-virus software.

Dr.Web anti-virus software has been developed since 1992. The company is a key player on the Russian market for software that meets the fundamental need of any business—information security. Doctor Web is one of the few anti-virus vendors in the world to have its own technologies to detect and cure malware. Dr.Web anti-virus software allows IT environments to effectively withstand any threats, even those not yet known.

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

Doctor Web's customers include large, internationally known companies; Russian and international banks; governmental organisations; and educational institutions and research departments with tens of thousands of computers in their networks. Russia's highest bodies of state and executive power, as well as the country's oil and gas companies, trust Doctor Web's anti-virus solutions.

.

125124, Russia, Moscow, 3d street Yamskogo polya 2-12A
Phone: +7 (495) 789-45-87
Fax: +7 (495) 789-45-97
http://www.drweb.com | http://www.av-desk.com | http://freedrweb.com | http://mobi.drweb.com