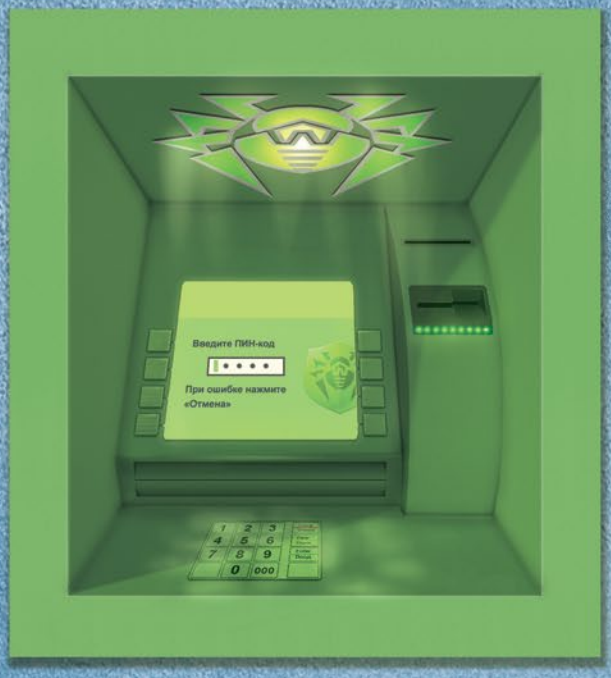
Dr.WEB®
ATM Shield



2009年在俄罗斯侦测到第一例能够感染自动取款机的恶意软件。被木马**Trojan.Skimer**感染的自动取款机先是在莫斯科，之后在圣彼得堡被发现。

Doctor Web 公司第一个对**Trojan.Skimer**作出反应并公布预警信息，之后研发了专门的反病毒软件，用于实时保护内置电脑系统（自动取款机、支付终端、多功能终端、结账设备），并将其命名为**Dr.Web ATM Shield**。

统一保护

内置电脑系统

（自动取款机、支付终端、多功能终端、结账设备等）

Dr.WEB®
ATM Shield

说老实话，您有时也会这样做，不是吗？

- 使用USB设备之前并不检查是否上面是否有病毒。
- 打开未知发件人发来的邮件。
- 在 Windows系统下使用管理员权限。
- 不对安装在电脑上的所有软件进行安全更新。
- 从所安装软件存在漏洞的办公电脑上互联网。
- 使用很容易被破解的简单密码。

既然您会这样做，为什么会认为自动取款机和支付终端的维护人员绝对不会这样做？

是否存在针对ATM机的病毒？

专门为自动取款机设计的病毒，也就是有自我传播能力的恶意软件，目前还没有发现，但木马的数量却在迅速增加！仅2013年12月一个月的时间就出现了4例自动取款机新木马：Trojan.Ploutus.1, Trojan.Ploutus.2, Trojan.Skimer.19 и Trojan.PWS.OSMP.21.

自动取款机木马的一些特征：

- 可利用专门制作的MasterCard或从移动设备对恶意软件进行控制；
- **利用ATM机自带的软件**在持卡人输入PIN密码后进行拦截并破解密码！
- 盗取银行卡数据；将被盗数据保存在不法分子专门制作的塑卡上或将其打印到交易收据；
- 木马根据不法分子从自动取款机键盘输入的指令或专门的短信指令从自动取款机出现金；

自动取款机由专业人员维护，恶意软件怎么会入侵呢？

可能的感染途径：

- **从移动载体**，移动载体专门用于专业人员对自动取款机进行维护，但也被用于其他目的；
- **从不法分子的移动载体**，这种方法需要使用专门的钥匙打开ATM机设备外壳
- **从被感染的公司内网**，如果从内网可以访问内置设备，恶意软件就有可能通过这一途径进入内置设备；
- 利用自动取款机软件**漏洞**。

甚至不涉及盗取资金和转账的“普通”恶意软件，也可能引起蓝屏、信息加密现象，在屏幕上出现赎金要求。结果是此类照片传遍互联网使相关机构名誉受损，这不仅是令人不快的事件，而且要付出代价才能恢复正常运行。

Dr.Web ATM Shield提供的不仅是反病毒保护！

Dr.Web ATM Shield所包含的组件能够大大降低有意或无意感染自动取款机的可能性：

- 文件监视器确保已知恶意软件无法运行；
- 反rookit侦测之前未知的威胁；
- 办公控制限制对本地目录和网络资源的使用，不允许恶意软件向不法分子发送数据或连接其管理中心；
- 禁止使用可移动载体的功能防止设备被未知可移动设备感染；
- 网络流量监控系统保证只有被允许的软件通过被允许端口连接互联网。

Dr.WEB®
ATM Shield

Dr.Web ATM Shield 专门为抵御内置设备典型威胁而研发

为什么不安装一般的反病毒软件，而一定要使用专门的解决方案？

内置系统的特征是：

- ✓ 内存小，处理器性能较低；
- ✓ 必须全天候24小时连续运行，不能重启；
- ✓ 除了普通的操作系统，还使用专门用于内置设备的系统。

Dr.Web ATM Shield专为在低配置设备上使用而研发

内置设备只需要512MB内存就足以保证**Dr.Web ATM Shield**正常运行。

所有Dr.Web产品，包括Dr.Web ATM Shield，与其他产品相比，历来以病毒库小和更新占用少而著称，能够保护连接互联网或公司内网带宽“窄”的远程设备。

Dr.Web ATM Shield支持的内置设备操作系统

Dr.Web ATM Shield不仅支持普通的操作系统（如Windows® XP Professional、Windows® Vista以及Windows® 7和Windows® 8），还可用于Windows® XP Embedded、Windows® 7 Embedded、Windows® 8 Embedded。

Dr.Web ATM Shield提供的不仅是反病毒保护：

- 是先进的技术，能够最大程度的缩短扫描和加载时间（包括利用多线程扫描和对“只读”文件的延时扫描）；
- 是稳定运行的系统，在配置过时的电脑系统中也能够确保稳定运行；
- 是文件预扫描，即在其进入相应应用前进行扫描，不给黑客利用软件漏洞的机会；
- 是卓越的反病毒引擎，能够侦测到并清除还未添加到病毒数据库中的最新病毒；包括隐藏在未知打包器下的病毒；
- 是强大的自保系统，不允许病毒破坏保护系统的运行。

Dr.Web ATM Shield——唯一一种在考量内置设备特点的基础上研发的解决方案。

注意！

利用恶意软件盗取资金署犯罪行为。

Doctor Web公司提供电脑病毒性事件鉴定服务，对人员（员工）进行心理鉴定，确定是否有实施犯罪/ 协助犯罪/ 隐匿事实/ 纵容犯罪的行为，以及确定是否没有及时采取措施或没有认真执行岗位职责。

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

在公司官网上的“法制角”http://legal.drweb.cn/ 可以了解到发现失窃后应该采取的行动，欢迎利用这些信息来保护您的权益！

Doctor Web公司简介

DoctorWeb公司是俄罗斯信息安全产品厂商，产品商标为Dr.Web。产品研发始于1992年。公司是信息安全软件市场的重要一员。DoctorWeb是世界上为数不多的拥有独创的恶意软件侦测和清除技术的反病毒厂商之一。Dr.Web反病毒保护能够使用户信息系统有效应对包括未知威胁在内的任何威胁。

DoctorWeb公司率先在俄罗斯市场上推出将反病毒软件作为服务的新销售模式，直到今天仍然雄踞俄罗斯IT服务供应商网络安全服务市场的领先地位。多项国家证书和荣誉，以及Dr.Web用户分布之广是对俄罗斯天才软件人员所研发产品优异品质的有力证明。

DoctorWeb公司的客户中有局域网规模为几万台电脑的世界知名企业、俄罗斯银行和跨国银行、政府机关、教育和科研机构。俄罗斯国家最高权力机关、最高执行机构以及能源行业的大企业同样信任Doctor Web公司的解决方案。

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