# 浅析杀毒软件的现状及趋势

曹丽萍
(广州康大职业技术学院，广东 广州 511363)

[摘 要] 随着病毒的破坏力越来越大，杀毒软件成为人们关注的焦点。文章首先从杀毒软件的两个重要产品(单机版和网络版)分析了杀毒软件的发展历程，然后对杀毒软件未来发展趋势提出了本人的观点，认为在杀毒技术上，要变被动为主动；在营销模式上，由收费走向免费。

[关键词] 病毒；单机版；网络版；特征码；主动防御

## 1. 引言

随着网络的发展，杀毒软件的地位发生了巨大的变化。以前电脑出问题的时候，需要拿一个杀毒软件来查杀病毒，那个时候的杀毒软件仅仅是临时的应急处理工具。最近几年来，随着病毒产业利益链的深化，杀毒软件对人们的电脑越来越重要，杀毒软件已经和办公软件、IE 浏览器一样，牢牢地占据着用户的桌面，成为了操作系统必装工具之一。了解杀毒软件的现状及趋势，对我们清除病毒，提高电脑安全防范力度有着重要作用。

谈及杀毒软件，必然离不开病毒。计算机病毒是能够实现自身复制且借助一定的载体存在的具有潜伏性、传染性和破坏性的程序。病毒对电脑具有破坏作用，杀毒软件对电脑具有保护作用，杀毒软件与病毒从诞生之日起，就是一对生死对头。杀毒软件的发展历程，同时也是一部病毒演变史。

## 2. 杀毒软件的发展现状

本文将从杀毒软件的两个最重要的产品 (单机版和网络版) 来分析杀毒软件的发展现状。

### 2.1 单机版杀毒软件

单机版杀毒软件，简称单机版，是指只能在一台电脑上安装的杀毒软件。单机版发展到今天，已衍生出了多个细分产品。包括专业版，服务器版，USB 版等。

病毒越来越猖獗，杀毒软件的技术水平也越来越高。1998 年，CIH 病毒泛滥时，江民杀毒软件在这次的病毒疫情中，大放异彩。从现在的角度来看，当时的江民与其说是一个杀毒软件，还不如说是一个专杀工具。在 2006 年之前，病毒仅处于萌芽期，病毒传染范围，传染速度及目的性皆不是很明确。杀毒厂商升级病毒库也比较慢，那个时候，瑞星大概一个星期升级 2-3 次，诺顿一个星期升级一次，卡巴斯基在中国市场还是一个无名小卒。普通网民对病毒的感觉还不是很强烈，甚至有些网民从不装杀毒软件，电脑处于“裸奔”状态。

真正给中国网民以惨痛教训的是在 2006-2008 年间，这段时间爆发了一系列的重大病毒事件，迄今为止，人们记忆犹新，例如维金病毒、熊猫烧香病毒、AV 终结者病毒，机器狗病毒。这些病毒产生的背景带有鲜明的利益产业链色彩，通过病毒传播达到利益诉求。在这场病毒风暴中，各杀毒软件厂商轮番登场，大显身手。中国大陆的个人版杀毒软件市场也从以前的三足鼎立时代，变成了百花争艳的局面。其中卡巴斯基和 360 安全卫士成了最大的赢家，从以前的名不见经传，变成了现在号称拥有上亿用户的杀毒软件。360 安全卫士并不算是杀毒软件，但它在杀毒软件市场中搅起的滔天巨浪不可忽视。经过病毒的洗礼，中国的网民也经历了一次电脑安全的全面教育。用户越来越重视系统是否稳定，数据是否安全，账号是否被盗。人们的安全意识越来越高，意识到杀毒软件的重要性，杀毒软件此时才真正的占领了用户桌面。中国的正版杀毒软件市场也得以大大提升，越来越多的用户倾向于购买正版杀毒软件，本人曾听到软件店老板亲口说：“这年头，卖什么软件都亏钱，只有卖杀毒软件还有点赚头。”可见购买正版杀毒软件的用户越来越多。

### 2.2 网络版杀毒软件

网络版杀毒软件，也叫企业版杀毒软件，简称网络版，主要针对政企客户开发出来的杀毒软件。它与单机版杀毒软件的显著区别是，它带有安全管理功能。企业安全，只有把管理与技术结合起来才能真正保证安全，单有管理或单有技术并不能保证安全。网络版杀毒软件满足了企业用户的需求。

网络版杀毒软件有着鲜明特色，注重管理与报表功能。安全管理方面，网络版杀毒软件大部分具有统一安装、统一升级、统一杀毒等功能。在企业全网杀毒管理的基础上，有些网络版还具备了其他更为强大的功能，比如说远程消息、远程桌面、分组管理、漏洞补丁管理等。这样大大减轻了企业管理员的负担，同时对企业中的各个客户端的安全也有了提升，杜绝了“木桶理论”中短板的出现。在报表功能方面，网络版杀毒软件同样有着优异的表现。在管理控制台上，管理员可统计所有授权用户的病毒感染情况，可以按时间、按部门、按病毒种类统计企业全网中的病毒情况，并形成各种报表，包括柱状图，曲状图等等。这些数据非常详细，对企业在安全方面的投资提供了权威的参考。网络版杀毒软件同样也提供了本地化升级，即首先服务器端把病毒库全部下载到本

作者简介：曹丽萍，女，湖南郴州人，学士，教师，研究方向：计算机应用技术，多媒体。

地，再由本地的服务器分发到每个客户端上。这样可大大节省网络出口资源，并且对于外部网络攻击也起到了阻隔作用。

网络版杀毒软件对企业确实有着重要作用，同时也是各个厂商角逐的重点。它的普及是我国企业网络安全的重要屏障。

3. 杀毒软件的发展趋势

杀毒软件作为安全领域的一个细分行业，其未来的趋势令人关注。本文将从杀毒技术与运营模式上探讨其未来的发展趋势。

3.1 技术上，探索主动防御的巅峰

主动防御技术是针对特征码杀毒技术而言的，它能防范未知病毒。由于以前的杀毒软件大部分是通过提取病毒特征码，把它写入到病毒库中，从而进行查杀，这种杀毒技术是有很大漏洞，它必须是在病毒出现之后，才能查杀，根据不同厂商的病毒收集能力的不同，杀毒软件的能力有高有低，并且实时性得不到保障。如果杀毒软件一直是用这种方式来查杀病毒的话，那么广大用户就成了新病毒的小白鼠，把用户电脑蹂躏过后，才由杀毒软件登场把病毒清除掉。杀毒是一件很痛苦的事情，杀毒过后，往往具有后遗症，只有防毒才是用户最需要的。而特征码杀毒仅能防住已经收录的病毒，对新病毒一筹莫展。所以，特征码杀毒是被动的。主动防御是未来杀毒软件的方向，因为主动防御是主动的，真正的主动防御是可以防止新病毒、未知病毒的入侵。

主动防御是一个大的概念，也是一项复杂的工程。它需要分析文件的行为，动作及特征，从而判断该进程或文件是否有害，实现主动防御，起码应具备以下几个特点：

⑴ 准确判断

必须要对程序进行准确判断，及时阻止恶意行为的发生。

⑵ 防止误报

误报是指把合法程序报告为病毒的行为，主动防御如果行为规则不够严谨，可能会产生误报，这种情况一定要尽量避免，否则将影响用户正常使用。

⑶ 人工智能参与

病毒程序有其规则，但往往令人琢磨不透，必须对其进行智能判断。程序非法则阻止，程序合法则放行。

3.2 营销模式上，免费＋增值服务

杀毒软件在用户心中地位的变化，让杀毒软件逐步成为了基础型工具，它会成为每个用户必装的软件之一，为了抢占用户，基本功能走向免费是大势所趋。但如果所有功能皆免费，杀毒厂商没有营利点，将会无法生存。笔者认为，基本功能免费，个性化功能收费的模式，将会是以后的趋势。

基本功能包括病毒库升级，查杀病毒，实时监控。这些功能是用户电脑安全最基本的需求，应该要为用户免费提供。那么杀毒软件如何提供增值服务呢？那么必须为用户提供个性化功能，比如针对炒股及网购人士提供账号保护功能，如需账号保护功能，则需付费。再如针对中小学生健康上网的绿网功能，屏蔽一些暴力或黄色信息，进行收费。只有加大功夫把用户市场再进行细分，做到个性化服务，杀毒厂商才能在占有用户桌面的基础上赢利。这里要特别注意一点，那就是免费仅会对个人用户，企业版杀毒软件市场收费模式依旧。

4. 结束语

杀毒软件与人们的日常生活息息相关，电脑“裸奔”时代已经一去不返。最近几年，尽管人们的安全意识已经有了大大提高，但同时人们中毒的机率依然居高不下，杀毒厂商捕获的病毒数有增无减。普及杀毒软件，提高杀毒意识，有利于我们对抗病毒的攻击。为网民提供更为优质的服务，将是杀毒厂商任重道远的事情。

参考文献：

[1] 刘功中. 计算机病毒及其防范技术[M]. 北京：清华大学出版社，2008.

[2] 老虎工作室，赵亮，李卫华. 从零开始——防治电脑病毒[M]. 北京：人民邮电出版社，2005.

[3] 赵树升. 计算机病毒分析与防治简明教程[M]. 北京：清华大学出版社，2007.

## Analysis of the Antivirus Software’Status and Trends

Cao Liping

(Guangzhou Kangda Vocational and Technical College，Guangzhou 511363，Guangdong)

【Abstract】 As computer viruses become more and more destructive，the antivirus software has been the focus of attention. Firstly，this article analyses the development of two important antivirus software products (antivirus for profession and antivirus for enterprise). Then the author puts forward views about the trend of the antivirus software development：it's necessary to change view from passive to active on the antivirus technology；and it's better free for people on the marketing mode.

【Keywords】 virus；antivirus for profession；antivirus for enterprise；condition code；active defense