

传统的病毒检测技术依靠数据库中的病毒签名来工作，通过扫描文件内容，与病毒签名进行比对。为了降低误报率并提高扫描速度，签名的长度不能太长，也不能太短。这种方法只能用于检测已知病毒。

启发式，或启发式扫描定义了一种新的病毒检测技术，通过分析程序的结构和它的行为来发现病毒，不依赖病毒签名。通过这种新技术，病毒扫描程序可以检测出大约70%到80%的未知病毒。但是启发式扫描的误报率可能较高，如果不能很好地解决这一问题，用户不会喜欢这一检测手段。

检测过程通常分为两个阶段，**第一阶段是发现程序的行为**，主要检测程序前段和后段部分，大约几K的代码。发现方法分静态扫描和动态扫描两种，区别主要在于是否利用CPU模拟器来检测程序的行为。

静态启发式扫描检测方法：字节序列（签名）比对法：通过匹配字节序列来发现程序中的某些行为。静态检测方法开销小，但是可能会漏掉一些经过精心设计的病毒。

动态启动式扫描检测方法：在隔离的仿真环境里运行可疑文件，扫描程序监视可疑文件的系统调用。动态检测方法开销大，效率低。对于只有在特定条件下才感染新文件的病毒，可能无法检测出（如果在检测时没有满足病毒的活动条件），这种情况下，静态检测方法更有效。

Bloodhound综合使用上述两种方法进行可疑行为检测。

**第二阶段是分析发现的可疑行为**，这一部分必须精心设计，因为通常的情况下，在前一阶段并不能发现病毒的所有可疑行为，所以必须根据发现的部分可疑行为做出判断，且必须保证较低的漏报和误报率。Bloodhound和Bloodhound-Macro都是不错的专家系统，前者可以检测出80%的未知病毒，后者可以检测出90%的未知宏病毒。

启发式：简化虚拟机和简化行为判断引擎的结合

Heuristic(启发式技术=启发式扫描+启发式监控)

重点在于特征值识别技术上的更新、解决单一特征码比对的缺陷。目的不在于检测所有的[未知病毒](http://baike.baidu.com/client/view/477361.htm?app=1&font=2&statwiki=1)，只是对[特征值扫描](http://baike.baidu.com/client/view/463956.htm?app=1&font=2&statwiki=1)技术的补充。

主要针对：木马、间谍、[后门](http://baike.baidu.com/client/view/20922.htm?app=1&font=2&statwiki=1)、[下载者](http://baike.baidu.com/client/view/1147199.htm?app=1&font=2&statwiki=1)、已知病毒(PE病毒)的变种。

启发式技术是基于[特征值扫描](http://baike.baidu.com/client/view/463956.htm?app=1&font=2&statwiki=1)技术上的升级，与传统反病毒特征值扫描技术相比，优点在于对[未知病毒](http://baike.baidu.com/client/view/477361.htm?app=1&font=2&statwiki=1)的防御。是特征值识别技术质的飞跃。

传统反病毒[特征值扫描](http://baike.baidu.com/client/view/463956.htm?app=1&font=2&statwiki=1)技术，由反病毒样本分析专家通过逆向反编译技术，使用反编译器（ollydbg、ida、trw等）来检查可疑样本文件是否存在[恶意代码](http://baike.baidu.com/client/view/16443.htm?app=1&font=2&statwiki=1)，从而判定[程序文件](http://baike.baidu.com/client/view/600314.htm?app=1&font=2&statwiki=1)是否属于正常程序或病毒、恶意软件。在确认程序为病毒、恶意软件后，不同的安全厂商根据自己的标准对此可疑程序样本进行特征提取和样本命名（不同安全厂商有自己规定的特征提取点和样本命名规则）。最后经过测试部门测试通过后，更新到服务器，提供用户的本地[病毒库](http://baike.baidu.com/client/view/176772.htm?app=1&font=2&statwiki=1)更新。在用户操作系统正常监控或用户[手动扫描](http://baike.baidu.com/client/view/647412.htm?app=1&font=2&statwiki=1)后，利用[杀毒引擎](http://baike.baidu.com/client/view/792968.htm?app=1&font=2&statwiki=1)对系统上的文件自动进行特征值提取并与[病毒库](http://baike.baidu.com/client/view/176772.htm?app=1&font=2&statwiki=1)中已存特征值比对，条件符合即比对结果为真时，即判断此文件为病毒库中记录的特征值对应的病毒名称的病毒（[恶意软件](http://baike.baidu.com/client/view/362867.htm?app=1&font=2&statwiki=1)）。

病毒、恶意软件通常最初的指令是直接读写磁盘操作、解码指令，或获取系统目录(GetSystemDirctory)、获取磁盘类型(GetDriveType)、打开服务管理器([OpenSCManager](http://baike.baidu.com/client/view/4579843.htm?app=1&font=2&statwiki=1))等相关操作指令序列。这些都是病毒样本分析专家分析中得到的经验。

启发式技术，在原有的特征值识别技术基础上，根据反病毒样本分析专家总结的分析可疑程序样本经验（移植入反病毒程序），在没有符合特征值比对时，根据反编译后程序代码所调用的win32 API函数情况（特征组合、出现频率等）判断程序的具体目的是否为病毒、恶意软件，符合判断条件即报警提示用户发现可疑程序，达到防御[未知病毒](http://baike.baidu.com/client/view/477361.htm?app=1&font=2&statwiki=1)、恶意软件的目的。解决了单一通过特征值比对存在的缺陷。

例如：一个可疑程序通过反病毒[杀毒引擎](http://baike.baidu.com/client/view/792968.htm?app=1&font=2&statwiki=1)反编译后，发现代码中自动释放[可执行文件](http://baike.baidu.com/client/view/159830.htm?app=1&font=2&statwiki=1)驻留系统目录、[伪装系统文件](http://baike.baidu.com/client/view/4169457.htm?app=1&font=2&statwiki=1)、注册win32服务获取系统管理权限、通过命令行删除自身文件，调用系统组件svchost.exe来开启后门服务，隐藏自身进程并尝试通过[OpenSCManagerA](http://baike.baidu.com/client/view/2314068.htm?app=1&font=2&statwiki=1)、OpenServiceA、ControlService等函数来开启系统自身的终端服务，以便进一步控制计算机。通过这些条件即可判断为[恶意软件](http://baike.baidu.com/client/view/362867.htm?app=1&font=2&statwiki=1)（[后门程序](http://baike.baidu.com/client/view/1352.htm?app=1&font=2&statwiki=1)）。

写得较为全面，推荐给大家  
  
病毒和正常程序的区别可以体现在许多方面，比较常见的如：通常一个应用程序在最初的指令，是检查命令行输入有无参数项、清屏和保存原来屏幕显示等，而病毒程序则没有会这样做的，通常它最初的指令是直接写盘操作、解码指令，或搜索某路径下的可执行程序等相关操作指令序列。这些显著的不同之处，一个熟练的程序员在调试状态下只需一瞥便可一目了然。启发式代码扫描技术实际上就是把这种经验和知识移植到一个查病毒软件中的具体程序体现  
  
启发式指的“自我发现的能力”或“运用某种方式或方法去判定事物的知识和技能。”一个运用启发式扫描技术的病毒检测软件，实际上就是以特定方式实现的动态高度器或反编译器，通过对有关指令序列的反编译逐步理解和确定其蕴藏的真正动机。例如，如果一段程序以如下序列开始：MOV AH ,5/INT,13h，即调用格式化盘操作的BIOS指令功能，那么这段程序就高度可疑值得引起警觉，尤其是假如这段指令之前不存在取得命令行关于执行的参数选项，又没有要求用户交互性输入继续进行的操作指令时，就可以有把握地认为这是一个病毒或恶意破坏的程序。  
  
启发式杀毒代表着未来反病毒技术发展的必然趋势，是具备某种人工智能特点的反毒技术。因此它和HIPS（主机入侵防护技术）一样，都是主动防毒的有效方式之一。相比较而言,它更注重行为分析。  
  
正因为具备如此多的优点，国外流行的杀毒软件，大部分都有自己开发的独特启发式引擎和特色技术。下面就让笔者用拙笔一一来简介下各大国外厂商的杀软产品的启发式引擎和专业技术吧。  
  
  
**王者风范之Dr.Web**  
  
  
Dr.Web有个很犀利的中国名字：大蜘蛛。大蜘蛛反病毒是在国际上享有盛誉的、以独一无二的非特征风险程序运算法则而著称的顶级安全软件，更是唯一获得俄罗斯联邦国防部许可证的安全品牌。1992年至今，大蜘蛛反病毒软件一直受到俄罗斯国会、总统办公室以及全球数以万计的消费者及商业用户、企业用户的亲睐及认可，曾多次获得英国知名杂志 Virus Bulletin100%的奖项。蜘蛛于08年进入中国开拓市场，到目前已经推出了最新的6.0版本。  
  
**Dr.Web启发式引擎**  
蜘蛛使用Dr.Web启发式引擎，该引擎是蜘蛛自己开发的，在侦测未知威胁方面卓有成效。它的启发式引擎，加入了俄罗斯人一贯擅长的一系列复杂的脱壳运算算法。因此可以轻而易举地对目前将近4000多种壳进行脱壳，并且在脱壳的时候，不卡系统，内存和CPU占用水平都维持在低水准中。蜘蛛能够高精度侦探加壳对象，将其分解为组成部分并进行逐一检查，判断是否存在隐藏的危险。即便是有害程序使用的是新加壳方式，也不会逃过它的检查。  
  
实际上，目前流行的加壳方式分为加密保护和压缩保护。蜘蛛的启发式引擎，主要负责对加密保护这类壳（ASProtect、tElock、Armadillo、SVK Protector、Xtreme-Protector、Obsidium、PElock等）进行脱壳。而对于压缩保护的壳（UPX、ASpack、Petite、PECompact、PE-PACK等），蜘蛛还有自己的特色技术（Origins.Tracing TM）来额外处理，以便分担启发式分析仪单方面脱壳的压力。  
  
**Dr.Web AV-Desk版中的云安全技术**  
蜘蛛在自己的福云版AV-Desk加入了云安全技术，为提高对未知病毒的反映处理时间做出了贡献。  
  
**独特的非特征性分析技术Origin.Tracing**  
FLY-CODE 是独一无二的全能解包器，设于Dr.Web 5.0及6.0版的搜索模块。利用这一解包器Dr.Web可解未知的打包器。利用Dr.Web病毒库中的专门记录，搜索模块能够对存在于打包压缩文件中的有害对象作出启发式判断，这时在被侦测出的对象名称后添加《可能是 Trojan.Packed》。Packed就是捆绑打包之意。即该技术有利于侦测任何含压缩保护的文件中内含有的恶意捆绑内容（广告程序、后门、木马等）。此技术是对传统特征分析（常规病毒特征码对比）和Dr.Web启发式分析仪（启发式引擎）的补充，大大分担启发式分析仪脱壳的压力。该技术同时有利于降低启发式分析仪的误报及缩短侦测时间。   
因此，当我们下载的一些程序包内含有广告插件时，蜘蛛就能很敏锐地侦测到，非常强悍。致使很多人误以为其误报正常安装程序。不过，蜘蛛也是有缺点的，那就是它的本地化控制得不好，对部分国内软件（即使没有捆绑插件）误报。  
  
Tips：以卡饭论坛的4月测试样本扫描测试报告来显示蜘蛛的启发报警率，去掉最低时为0%，并去掉最高时为18.5%，初步统计后为6.69%。  
  
  
**高才卓识之NOD32**  
  
  
说到NOD32，许多人都会误以为它是Norton。其实，只要稍稍对比下厂商名和软件主色调就容易区分了。深绿色的ESET NOD32和太极黄的Symantec Norton，完全不是一个产物。NOD32在国际上是鼎鼎大名的启发式强悍杀软，同时兼顾高侦测未知威胁率和极低误报率。它所讲究的轻、快、准、狠，已经深入人心，因此拥有一大票拥趸者。NOD32的公司是ESET，成立于1992年。其研发总部在斯洛伐克，销售总部在美国的黄金西海岸圣地亚哥。ESET NOD32连续10年In the wild病毒无一遗漏，连续2年获得AV-Comparatives评测连年度总冠军。更恐怖的是，它还是截止到2010年4月份时全球首款61次通过VB100%权威认证的防病毒软件。ICSA、Checkmark等认证更是悉数拥有。NOD32于2006年4月通过Version LTD代理进入中国市场，其目前最新的英文版是4.2.40.0，中文版是4.0.474.10。  
  
**ThreatSense启发式引擎**  
NOD32之所以能斩获如此多的奖项，其终究还是要归功于它所使用的高效综合性防护架构引擎——ThreatSense启发式引擎。利用单一的ThreatSense启发式引擎，来处理不同的威胁（病毒、蠕虫、木马、间谍软件、广告软件、后门程序、网络钓鱼）。以此来简化工序，提高执行效能。  
  
除了常规病毒特征码检测外，NOD32基于TS启发式引擎的检测技术还有2种。1、静态启发。静态启发这一块含有2种技术。第一种是基于病毒库中已有的特征码对比，并在静止状态下通过简单的反编译，核对病毒头静态指令来识别病毒。第二种就是基因码检测（国外的叫法），类似于国产杀软的广谱查杀技术。主要是从各病毒变种中找到一些相同的非连续的程序代码，制作出通用的家族启发规则，内置于NOD32中。一旦在对比中发现可疑文件含有的部分代码符合或接近此家族启发规则，就进行报毒。这对NOD32来说，还算是小儿科的。真正厉害的是它的动态启发。2、动态启发  动态启发远比静态启发要先进和复杂很多。它辨别病毒的方法并非依靠任何特征数据库，而是在档案扫描时主动地拆解与分析档案的执行码，并使用虚拟机技术，给可疑文件构建一个虚拟仿真的运行环境，诱使它在杀软的模拟缓冲区中运行，如运行过程中检测到可疑的动作，则判定为危险程序并进行拦截。这种方法对加壳病毒依然有效，但如果控制得不好，会出现较多误报的情况。动态启发因为考虑资源占用的问题，因此目前只能使用比较保守的虚拟机技术。  
  
我们常见的NOD32静态启发报毒，就是那些有“变种(variant)”、“可能（probably）”或带“Gen（Generic——基因启发）”字样的报法。而动态高启发报毒，则是以“未知的NewHeur\_PE病毒”（probably unknown NewHeur\_PE virus [7]）来标示的。  
  
**ThreatSense.Net全球病毒预警系统**  
ThreatSense.Net类似于ESET的云安全，它可以将客户端的启发式引擎报警为未知NewHeur\_PE病毒的样本，从后台遣送至ESET的病毒实验室，从而进一步深入指纹对比，并最终确认威胁的具体种类、名称和危害度等级。它是从NOD32 2.5就延续下来的功能，那时候很多厂商都没有云安全这个概念呢。可见ESET的技术和理念都是很有前瞻性的。通过TS.Net，用户可以将威胁的应对时间，从以往的数天降低至几小时甚至于几分钟以内，从而得到接近于零时差的保护。  
  
ESET NOD32的优点如上述般多，但缺点也是并存的。它在开了高启发之后，对于某些加壳的文件进行模拟运行分析时，会不稳定。这样导致的结果是偶尔CPU会瞬时飙升很高，直观上就是电脑卡几下。不过，瑕不掩瑜，NOD32的启发侦测病毒率占全部侦测率的大部分，同时误报控制得极低，所以说，它终究高启发低误报的典范代表杀软之一。  
Tips：以卡饭论坛的4月测试样本扫描测试报告来显示NOD32的启发报警率，去掉最低时为11.4%，并去掉最高时为34.2%，初步统计后为19.3%。  
  
  
**稳中求胜之McAfee**  
  
  
McAfee是一家从事于防毒和电脑安全的美国公司，成立于1989年，总部坐落于加州的圣塔克拉拉市。因其在1998年和2003年分别收购欧洲第一大反病毒厂商Dr.Solomon和专注于反垃圾邮件的Deersoft 公司而名噪一时。它目前在75个国家设有服务据点，并于1998年进入中国大陆，注册中文名“迈克菲”（昵称是麦咖啡）。随后在2001年时，在中国大陆正式注册成立了独资公司，进一步拓展市场。McAfee公司拥有世界权威的反病毒紧急事务响应小组（AVERT）和Mcafee实验室（Mcafee LAB），提供7/24的研发和支持服务。咖啡的防病毒产品在美国拥有50,000+家组织机构用户，97%的《财富》1000家组织机构选用了咖啡的产品。据IDC统计，McAfee公司已经连续六年占据企业级防病毒市场的第一名，并且占据硬件网关防病毒市场第一名。咖啡全面保护全球300万美国国防部用户,已经被美国国防部主机安全系统选作标准系统。美国国防部采用咖啡的工具为网络提供深层防护的同时，为主机安全系统提供管理，并且提高主机设备的标准配置。  
  
**McAfee启发式引擎&Artemis云技术**  
咖啡的启发式引擎也是自家独创的，拥有基因启发和模拟行为分析的能力。它使用了启发式杀软普遍使用到的基因码侦测技术，能非常有效地对付种类繁多的病毒和木马的变种。同时也有着很好针对未知威胁的前摄性侦测能力。  
  
Artemis月神技术是McAfee为了即时防御在线的恶意威胁，而开发出的一种云技术应用，最早见于企业版的咖啡产品中。不过从09年开始，咖啡的家庭版产品，也加入了此技术，并更名为“Active Protection”。Artemis会查找可疑的 PE 文件，并当侦测到时，把某类的总和检查码（不会包含个人／敏感的数据）传送到由McAfee AVERT Labs架设的中央数据库服务器。该中央数据库服务器会不断地更新新发现的恶意软件，而且 McAfee 的恶意软件队列到目前为止并未建立官方 DATs. 如果符合中央数据库内的数据，扫描仪会报告并处理侦测到的恶意软件。在 McAfee 的队列中的文件并未经历过任何分析，但会由 McAfee 的巨大白名单交叉检查以避免误判。根据由远程维护的黑名单，可以提供较每日多次发布特征码更新来对付每小时大量出现新的恶意软件的厂商快速的保护，以防止新的恶意软件的入侵，达到所谓的零时差防护！  
Artemis在企业版咖啡产品中，其等级是可调的。而在家庭版产品中，无法调节相应等级。  
  
**System Guard主机防护技术**  
会监视用户计算机上疑似病毒、间谍软件或黑客活动的可疑行为，并进行阻挡、警告与记录。其实它就是迈克菲的HIPS模块。可以对系统的注册表、关键文件以及应用程序来加以保护。值得注意的是，这个在家庭版McAfee 2009软件上也是有的，但更多的是使用内置的规则来记录行为，而不能对其进行操作。企业版的8.7.0i就不同了，可以自建规则，来保护想要保护的任何关键部位，例如禁止某些敏感注册表键值处的写入，或者限制某些系统路径文件写入等。我们常说咖啡的规则厉害，实际上讲的就是咖啡企业版的System Guard这个HIPS模块的自定义规则防御功能很厉害。  
  
关于咖啡的缺点，企业版的就在于它的规则对于新手来说有些复杂，同时资源消耗有点大。至于家庭版的缺点，就在于它没有自定义排除文件的选项，很伤脑筋。另外其清除率也有待提高。  
Tips：不知道是不是受McAfee近期误报XP SP3下svchost.exe的影响，卡饭上并没有它4月的测试样本扫描报告。唯一有的一个5月样本测试报告帖子，还没有开始进行测试。所以就无从计算McAfee的启发报警率了。  
  
  
**后发制人之Norton**  
  
  
Norton,诺顿。它属于大名鼎鼎的赛门铁克公司旗下的家庭版杀软子品牌。赛门铁克（Symantec Corporation），总部设于美国加利福尼亚州库笔底诺的一家互联网安全技术厂商，在全球40个国家设有分公司。该公司的Ghost软件闻名于世界。在美国，赛门铁克所有软件的市场占有份额是超越迈克菲的，目前是美国的第一。另外值得一提的是，赛门铁克的诺顿系列杀毒软件，其通过VB100%的次数仅次于ESET NOD32，居第二位。赛门铁克成立于1982年，拥有悠久的历史。其杀软技术从早期靠学习效仿到今天的自主创新。虽然06年时曾经低潮过一段时间，但随着SONAR 等创新革命性技术的研发成功并加入，赛门铁克又重新焕发了活力，成为安全业界的执牛耳者。  
  
**BloodHound启发式引擎**  
BloodHound是赛门铁克独家的启发式侦测技术。和众多启发式引擎无异，它会借由可疑的行为来侦测病毒。BloodHound会制造一个虚拟的安全环境，使病毒展现出他的不良企图，而不会影响到本身计算机运作的稳定性。  
  
**综合性SONAR行为侦测/防御技术**  
启发只运行于虚拟主机当中，倘若病毒木马不幸进入实体主机，就得利用“行为防御技术”了；行为防御会分析可疑程序的行为，并事先阻拦，诺顿著名的SONAR无疑是当中最成熟的。直观来说，SONAR是一种行为侦测/防御的技术，其可以在建立病毒定义档及间谍软件侦测定义档前，阻止恶意程序码侵入。这些新兴且未知的恶意程序码会透过木马程序、蠕虫、大众邮件病毒、间谍软件或者下载软件病毒的形式进行攻击与破坏。当许多产品仅使用一组有限的启发式法则时，SONAR可以透过广泛且异质的应用行为数据，大幅提升其防护能力，且明显地将误判率降至最低。  
  
具体来说，SONAR技术与卡巴单纯的主动防御技术不同，它更注重途径防御（诺顿注重的"途径防御",主要通过过各种不依赖病毒库的防御技术,封锁各种病毒感染途径,如漏洞防御,浏览器防御）。SONAR更多的是根据产品中一系列的引擎例如防火墙，防毒引擎，入侵防护引擎（IPS）、浏览器防护引擎（Browser Defender）等等来收集和整合信息的。然后所有这些信息会被分类器所使用来提高效能。这和其他厂商的技术有很大的区别。很多其他安全厂商没有如此庞大的信息来制作好的分类器。  
  
**全球智能云防护技术**  
和众多主流杀软一样，诺顿也拥有自己的全球智能云防护技术。除已知威胁病毒定义以外，“诺顿全球智能云防护”还可以通过“诺顿社区防卫”的安全和数据来确定新威胁及其来源，从而为用户提供额外的安全防护。另，SONAR技术拦截到的未知可疑文件，也会自动上传至“诺顿社区防卫”来进行分析。  
  
**Norton Insight**  
诺顿2009年增加的新技术Norton Insight，简单来说是一种白名单(但名单规则并不内存于软件当中，而是通过赛门铁克另有的平台随时更新)，其原理为只扫描不被信任的文件或网站扫描，并略过知名又或者安全的文件及网站，该项技术可让扫描速度大幅提快，并降低误判率。  
经由这些前摄性革新技术的加入，诺顿似乎更符合防毒软件而不是杀毒软件的定义。即使诺顿本身的手动扫描侦测率并不高，但有了这些技术，一样可以将病毒拒之门外，而不是中毒后的消极杀毒。  
  
Tips：以卡饭论坛的4月测试样本扫描测试报告来显示诺顿的启发报警率，去掉最低时为11.1%，并去掉最高时为66.7%，初步统计后为28.7%。  
  
  
**全面发展之Kaspersky**  
  
  
Kaspersky，卡巴，我想每一个中国人闻之都如雷震耳的神话型杀软。卡巴的创始人Eugene Kaspersky于1989年第一次遇到了有关计算机病毒问题，随后开发了Kaspersky反病毒产品的第一个版本。1991年，尤金和KAMI公司及其助手一起，研发出了AVP（AntiViral Toolkit Pro）。1994年，多家国外安全公司（芬兰F-Secure、德国G-Data、日本Vintage Solutions、中国的Kingsoft）购买了AVP内核的使用权。1997年6月卡巴斯基实验室有限股份公司（Kaspersky Lab）成立，总部在俄罗斯首都莫斯科，目前在英国、法国、德国、荷兰、波兰、日本、美国和中国都有子公司，在全球的销售代理公司超过500家。从1997年6月Kaspersky Lab公司正式成立以来。Natalya Kaspersky一直担任总经理，Eugene Kaspersky主要负责反病毒研究的工作。卡巴斯基斩获的奖项不计其数，其全球用户甚广。目前卡巴通过VB100%的次数是第三位的。仅次于NOD32和诺顿。  
  
**加入了启发式技术的AVP引擎**  
从卡巴7开始，卡巴顺应潮流，也对自己的软件加入了启发式扫描的技术。卡巴和众多启发式杀软一样，也是基于虚拟机模拟运行分析病毒行为的。它的启发率似乎并不是很高，但对某些特定壳，启发侦测就稍微多一些。它的启发强度是可调的，有低、中、高三个等级。总的来说，启发只是卡巴的一种辅助侦测手段，其主要的侦测手段还是靠病毒特征库和主动防御模块。  
  
**卡巴的“云”——“卡巴斯基安全网络”**  
在强大的后台技术分析能力和在线透明交互模式的支持下，卡巴斯基2009可以在用户“知情并同意(Awareness & Approval)”的情况下在线收集、分析(Online Realtime Collecting & Analysing)用户计算机中可疑的病毒和木马等恶意程序样本，并且通过平均每小时更新1次的全球反病毒数据库进行用户分发(Instant Solution Distribution)。从而实现病毒及木马等恶意程序的在线收集、即时分析及解决方案在线分发的“卡巴斯基安全网络”，即“云安全”技术。卡巴斯基2009通过“卡巴斯基安全网络”，将“云安全”技术透明地应用于广大计算机用户，使得全球的卡巴斯基用户组成了一个具有超高智能的安全防御网，能够在第一时间对新的威胁产生免疫力，杜绝安全威胁的侵害。"卡巴斯基安全网络"经过了卡巴斯基实验室长期的研发和测试，具有极高的稳定性和成熟度。  
  
**Proactive Defense 主动防御技术**  
这项主动防御技术，是在卡巴6的时候加入的。当然，那时候这个还不能算是合格的HIPS模块。因为它只提供了部分的RD，少量的AD。可是这在2009版中得到了完善，卡巴全功能安全套装2009，提供了完整的HIPS组件。并且与原有的防火墙结合，形成了4D防护（AD、FD、RD、ND）。卡巴的主动防御，在2009版中加入了自动模式和交互模式，旨在让用户自行选择适合自己的模式。非常人性化。  
  
**iChecker技术&iSwift技术**  
使用iChecker技术能够经由跳过从上次扫描后没有被修改的物件来增加扫描的速度，倘若那些扫描的设定(威胁的特征与设定)没有被改变。关于这些信息会被储存于一个特别的资料库（包括：EXE，COM，LNK，TTF，ELF，INF，SYS，CHM，ZIP这些格式）之中。iChecker于档案系统下独立运作(FAT，NTFS)。根据档案的种类与校验总和(混杂)；资料被储存于sfdb.dat之中。它的优点是： 辨识的同样档案储存于记录之中。当档案第一次被检查过后，任何此档案的复本同样迅速地被鉴定，即使假如它位于其他的路径、在资料夹之中或在邮件的附件里。  
使用iSwift技术能够增加扫描的速度，经由只有扫描新的和变更过的档案。iSwift只能于NTFS分区下运作。它是由NTFS内部的描述符号来识别档案的。每个档案的「痕迹」会被储存于专用的资料库，被称为FIDBOX。它的优点是：因为没有效验总和被计算，运算法则是快速的，比iChecker技术速度还快。此运作与档案的格式与大小无关。  
  
卡巴的优点在于全面，既有主动防御、启发式侦测，又有云技术。不过哦，缺点也在于其主动防御的SSDT钩子经常容易被一些病毒刻意去掉，另外因为树大招风，病毒作者常以卡巴作为首要免杀对象。最后，卡巴还是有点卡机。  
Tips：以卡饭论坛的4月测试样本扫描测试报告来显示卡巴的启发报警率，去掉最低时为0%，并去掉最高时为37.8%，初步统计后为14.1%。  
  
  
**老骥伏枥之BitDefender**  
  
  
BitDefender成立于2001年，是SOFTWIN的子公司，总部位于罗马尼亚首都布加勒斯特，同时在德国，西班牙，英国，加拿大等地设有相应的分公司。SOFTWIN公司成立于1990年，提供高端软件解决方案及相关服务，客户主要面向于大型银行业、国家服务部门、公共事业、物流及通信行业。BitDefender用户遍及80多个国家和地区，包括超过300万个企业用户License和4100万个人用户；同时，BitDefender领先的安全技术也得到了众多同业公司的认可和应用，包括Data Becker GmbH，G-Data，GFI，Ipswitch，Laplink)，Software602 and Hauri。甚至还有我们国内的奇虎360。  
  
　　BitDefender的中文译名为比特梵德，简称“BD”，有超过453万超大病毒库，可实时更新，具有反病毒引擎功能以及互联网过滤技术。BitDefender可以在家庭或商业上提供全面的网络安全保护。包括：病毒、黑客、间谍软件、垃圾软件、钓鱼邮件、安全备份和保护儿童访问不适当的网站等，该软件在Toptenreviews的综合测评中连续9年列世界第一。  
  
**含有B-HAVE启发式技术的BD引擎**  
（B-HAVE, Behavioral Heuristic Analyzer in Virtual Environments）- 在计算机内生成虚拟环境，模拟软件运行并识别是否存在恶意插件，将病毒与您的操作系统完全隔离。此技术已在实际应用得到检验：MemScan: Adware.Nail.A（BitDefender检测）在BitDefender用户系统已发现的恶意文件中排名前列。和众多启发式杀软一样，这种启发虚拟分析的技术也在BD的引擎中得到使用。  
  
**Active Virus Control（活动病毒控制）**  
BD 2010加入了AVC技术，结合B-HAVE应用环境，精确判断可疑行为，清除潜伏恶意程序，最大限度保护计算机安全。  
  
**Active Virus Control技术新特点：**  
十项认定为可疑进程活动迹象的行为：请求任何类型的用户交互后没有等待、终止执行程序时没有显示任何类型用户界面、复制或移动文件到系统文件夹、没有相关链接类型的图标、对其他进程执行代码、运行由本身创建的二进制文件中已存储代码、在一个磁盘中不同文件里复制本身代码、在操作系统启动项里添加自己、隐藏在已知应用程序、卸载系统文件夹中的驱动并重新注册、虚拟环境中行为启发式分析。  
  
BD有不少优点（基因启发、动态启发、病毒库大，清除能力强等），但缺点也是有的。它的产品体积很臃肿，并很难卸载干净，另外就是不能够检测一些新兴的恶意软件，检测能力有些滞后。  
  
Tips：由于卡饭论坛的4月测试样本扫描测试报告中没有BD的，所以只好提供3月的报告，作为小小参考而已，不做对比评论。去掉最低时为2.33%，并去掉最高时为73.7%，初步统计后为16.7%。  
  
  
**锋芒毕露之Panda**  
  
  
熊猫安全科技是全球第4大反病毒销售商（仅此于赛门铁克、迈克菲和趋势），市场占有率达3.2%。同时也是欧洲发展最快的500个公司之一，更是西班牙软件销售行业的领头羊。成为欧洲的顶级防毒软件开发者。特别是在2003年，熊猫软件曾在全球创造了高达101000%的收入增长。熊猫安全科技成立于1990年，至今已走过20个年头。99年之初进入中国，后其股东之一的方正科技代理销售。当前，熊猫软件用户遍布230个国家和50个分公司遍布全球，国家包括扩乌拉圭，美国，加拿大，德国，中国，英国，法国等。为全球计算机用户提供全方位的安全保障和相关服务。  
  
**Panda遗传性启发式引擎和SmartClean 2清除技术**  
毫无疑问，熊猫启发式引擎，也是自己开发的。能够进行基因静态启发和高级启发虚拟环境运行分析确认病毒。该遗传性启发式技术有利于检测出未知病毒或潜在的危险病毒，也就是病毒代码库中还没有的病毒。同时与最新的SmartClean II技术结合，在清除了蠕虫或者木马后，恢复受损的系统设置和关键部分。  
  
**Collective Intelligence云计算技术**  
熊猫安全2010系列采用其自主研发的综合云计算智能技术（Collective Intelligence），基于"云"技术的强大在线分析系统，实时保持样本更新和数据库升级。可智能分析病毒属性和行为，通过快速判断和分析进行清除或隔离。同时其拥有1500万恶意软件样本库，是业内最多的安全厂商之一，每天新增2.5万个样本，也是当前自动收集和处理化程度最高的病毒实验室。  
  
**TruePrevent行为分析技术**  
TruPrevent技术通过分析中计算机中正在运行的程序的行为，检测未知病毒和入侵。  
TruPrevent技术与其他技术有很大的不同，如，启发式技术（它能扫描存储在硬盘中的所有文件和程序，按照一种通用的规则来判断哪些是潜在的危险）。TruPrevent技术扫描每一个程序的具体行为或正在运行的文件。通过此种方式，TruPrevent技术能准确识别未知病毒并阻断它们在本机中的危险操作，在他们转变成威胁之前，阻止在网络中传播。基于事件关联性或运行中的程序执行的操作，分析进程行为来判断哪些是真正的威胁。 此特点提供了高可靠性 ，防止误报，并将网络管理员从手动监控任务中解放出来。  
最后，如果一个程序的行为超过了一定的危险程度，Truprevent技术将阻断它的行为，并通过Internet自动发送该程序的样品到熊猫实验室，熊猫实验室将立即研制疫苗，抵御这种新病毒，以后这种病毒都自动被清除。  
  
这个活动模型赋予了Truprevent技术智能属性，与目前的响应式技术相比，是一个巨大的飞跃。  
  
基于这些技术，熊猫可谓是锋芒毕露。熊猫的检测率一向不错，这是它的优点。它缺点是进程多，有些耗费系统资源，另外扫描速度有待提高。  
Tips：以卡饭论坛的4月测试样本扫描测试报告来显示熊猫的启发报警率，去掉最低时为29.6%，并去掉最高时为76.0%，初步统计后为43.4%。  
  
写在最后  
  
以上就是国外启发式杀软所使用的自家引擎和一些独创技术的概况。在这些启发式杀软中，有些是自带有HIPS模块的，所以笔者也顺带提了下。另外还有Avira、AVG、AVAST等3A启发式杀软，由于其在卡饭4月26日前的样本扫描测试中的启发报警率均低于5%，所以这里就不捎带提了。  
  
关于启发报警率，是基于卡饭论坛4月初一直到本文截止时的4月26日的样本扫描测试报告统计得出的。需要注意的是这些比率并不代表这些启发杀软的总体侦测率。比如Avira，在4月份的样本扫描测试中的总体检测率就相当可观。启发报警率低，不代表这些杀软的总体检测率也低（因为某些如卡巴、红伞、熊猫、诺顿，还有HIPS模块以及常规特征码检测这些额外的固有强项检测方式）。另外，至于蜘蛛的启发报警率在4月份的卡饭测试中偏低，我想说，它在卡饭3月份的测试中，还是高一些的。不过它似乎并没有像NOD32的启发报警率那样，维持在一个很稳定的中高水平中。