防毒入门-认识防毒技术 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/62/2021_2022__E9_98_B2_E6_AF_92_E5_85_A5_E9_c40_62194.htm 病毒代码扫描法 将新发现的病毒加以分析后, 根据其特征, 编成病毒代码, 加入资料库中。以后每当执行杀毒程序时, 便能立刻扫描程序文件, 并作病毒代码比对, 即能检测到是否有病毒。病毒码扫描法又快又有效率(例如趋势科技的PC-cillin及Server Protect, 利用深层扫描技术, 在即时扫描各个或大或小的文件时,平均只需1/20秒的时间), 大多数防毒软件均采用这种方式, 但其缺点是无法检测到未知的新病毒及以变种病毒。 加总比对法(Check-sum) 根据每个程序的文件名称、大小、时间、日期及内容, 加总为一个检查码, 再将检查码附于程序的后面, 或是将所有检查码放在同一个资料库中, 再利用此Check-sum系统, 追踪并记录每个程序的检查码是否遭更改, 以判断是否中毒。一个很简单的例子就是, 当您把车停下来之后, 将里程表的数字写下来。那么下次您再开车时, 只要比对一下里程表的数字, 那么您就可以断定是否有人偷开了您的车子。 这种技术可检测到各式的病毒, 但最大的缺点就是误判断高, 且无法确认是哪种病毒感染的。对于隐形飞机式病毒, 也无法检测到。 人工智慧陷阱(Rule-based) 人工智慧陷阱是一种监测电脑行为的常驻式扫描技术。它将所有病毒所产生的行为归纳起来, 一旦发现内存的程序有任何不当的行为, 系统就会有所警觉, 并告知用户。这种技术的优点是执行速度快、手续简便, 且可以检测到各式病毒；其缺点就是程序设计难, 且不容易考虑周全。不过在这千变万化的病毒世界中, 人工智慧陷阱扫描技术是一个至少具

有安全功能的新观点。目前趋势科技的PC-cillin, 就对病毒的可疑行为设下了将近12道的陷阱, 以达到预防重于治疗的目标。 软件模拟扫描法 软件模拟技术专门用来对付千面人病毒(Polymorphic /Mutation Virus)。千面人病毒在每次传染时, 都以不同的随机乱数加密于每个中毒的文件中, 传统病毒代码比对的方式根本就无法找到这种病毒。软件模拟技术则是成功地模拟CPU执行, 在其设计的DOS虚拟机器(Virtual Machine)下假执行病毒的变体引擎解码程序, 安全并确实地将多型体病毒解开, 使其显露原本的面目, 再加以扫描。 VICE(Virus Instruction Code Emulation)先知扫描法 VICE先知扫描技术是继软件模拟后的一大技术上突破。既然软件模拟可以建立一个保护模式下的DOS虚拟机器, 模拟CPU动作并假执行程序以解开变体引擎病毒, 那么应用类似的技术也可以用来分析一般程序检查可疑的病毒代码。因此VICE将工程师用来判断程式是否有病毒代码存在的方法, 分析归纳成专家系统知识库, 再利用软件工程的模拟技术(Software Emulation)假执行新的病毒, 则可分析出新病毒代码对付以后的病毒。 实时的I/O扫描(Realtime I/O Scan) Realtime I/O Scan的目的在于即时地对资料的输入/输出动作做病毒代码比对的动作, 希望能够在病毒尚未被执行之前, 就能够防堵下来。理论上, 这样的即时扫描程序虽然会影响到整体的资料传输速率, 但是使用Realtime I/O scan, 文件传送进来之后, 就等于扫过了一次毒, 整体来说, 是没有什么差别的。 文件宏病毒陷阱(MacroTrapTM) MacroTrapTM 是结合了病毒代码比对与人工智慧陷阱的技术, 依病毒行为模式(Rule base) 来检测已知及未知的宏病毒。 其中,配合OLE2技术,可将宏与文件分开,使得扫描速度变得飞快,

而且更可有效地将宏病毒彻底清除! 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com