网络技术:解析木马攻击与防御发展简史计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/584/2021_2022__E7_BD_91_E7_BB_9C_E6_8A_80_E6_c98_584939.htm 2009年下半年全国计算机三级考试时间是2009年9月19日至23日。更多优质资料尽在百考试题论坛 百考试题在线题库 计算机世界中的特洛伊木马的名字来自著名的特洛伊战记。故事说的是在古希腊时代，希腊人和特洛伊人发生了战争，在围困特洛伊城长达整整十年后仍不能攻陷。后来希腊人把一批勇士藏匿于巨大无比的木马后退兵，当特洛伊人将木马作为战利品拖入城内时，高大的木马正好卡在城门间，进退两难，夜晚木马内的勇士们爬出来，与城外的部队里应外合而攻下了特洛伊城。而计算机世界的特洛伊木马(Trojan)是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和拒绝服务攻击等特殊功能的后门程序。 世界上第一个计算机木马是出现在1986年的PC-Write木马。它伪装成共享软件PC-Write的2.72版本(事实上， 编写PC-Write的Quicksoft公司从未发行过2.72版本)，一旦用户信以为真运行该木马程序，那么他的下场就是硬盘被格式化。此时的第一代木马还不具备传染特征。 1989年出现了AIDS木马。由于当 时很少有人使用电子邮件，所以AIDS的作者就利用现实生活中的邮件进行散播：给其他人寄去一封封含有木马程序软盘的邮件。之所以叫这个名称是因为软盘中 包含有AIDS和HIV疾病的药品，价格，预防措施等相关信息。软盘中的木马程序在运行后，虽然不会破坏数据，但是他将硬盘加密锁死，然后提示受感染用户 花钱消灾。可以说第二代木马已

具备了传播特征(尽管通过传统的邮递方式)。 但随着Internet的普及，新一代的木马出现了，它兼备伪装和传播两种特征并结合TCP/IP网络技术四处泛滥。木马的主要目标也不再是进行文件和系统的的破坏，而是带有收集密码，远程控制等功能， 这段时期比较有名的有国外的BO2000(BackOrifice)和国内的冰河木马。它们有如下共同特点：基于网络的客户端/服务器应用程序。具有搜集信息、 执行系统命令、重新设置机器、重新定向等功能。当木马程序攻击得手后，计算机就完全成为黑客控制的傀儡主机，黑客成了超级用户，用户的所有计算机操作不但没有任何秘密而言，而且黑客可以远程控制傀儡主机对别的主机发动攻击，这时候被俘获的傀儡主机成了黑客进行进一步攻击的挡箭牌和跳板。 这时期的木马比较显著的特点是以单独的程序形势存在，带来的问题是木马的网络行为很容易被一些个人防火墙所阻断，为了解决这个问题，一个新的技术被广泛应用，这就是进程注入技术。进程注入技术是将代码注入到另一个进程，并以其上下文运行的一种技术，木马经常注入自己到IE浏览器中，由于IE浏览器经常需要访问网络，因此在防火墙弹出是否允许IE浏览器访问网络时，用户经常会点击允许，殊不知自己机器中的木马已经偷偷地去连接网络了。 但对于杀毒软件来说，使用成熟的特征码杀毒技术仍然可以通过和对病毒同样的处理手段对此时的木马进行查杀。但从04年开始，一切变得不一样了。2004年，在黑客圈子内部，有人公开提出免杀技术，这种技术是针对杀毒软件的特征码直接修改木马的二进制代码，由于当时还没有强有力的工具出现，所以一般都使用WinHEX工具逐字节更改，需要相当的技术能力，这种手

工方式只在少数黑客内部流传。2005年，著名的免杀工具CCL-一个自动化的特征码定位工具被公布，这使得免杀技术在很短的时间内开始公开化，一批黑客站点有意或无意的宣传使得越来越多的人开始讨论免杀技术，各大杀毒软件面临严重的信任危机，一个懂一点基本的PE文件知识与免杀工具的使用的初学者就可以轻易编辑一个木马，修改其特征码使其躲过杀毒软件的检测，据统计，著名木马灰鸽子曾在短短一年之内出现超过6万个变种，绝大部分都源于免杀技术的普及。同样也是在这一年，一些杀毒厂商提出“主动防御”的概念，这门听起来显得很专业的技术是用来增强已经对木马不再构成杀伤力的特征码识别技术，通过对病毒行为规律分析、归纳、总结，并结合反病毒专家判定病毒的经验，提炼成病毒识别规则知识库。模拟专家发现新病毒的机理，通过对各种程序动作的自动监视，自动分析程序动作之间的逻辑关系，综合应用病毒识别规则知识，实现自动判定新病毒，达到主动防御的目的。通过这种技术，在木马访问网络，注入进程等行为发生时杀毒软件会及时通告给用户，虽然还不完善，但至少还是可以对未知的木马做出一定的预警。道高一尺，魔高一丈，为了抵御主动防御技术，木马的开发者们又把目光转向了一门新的技术-“ROOTKIT”技术,这种技术最早应用于UNIX系统，也被称为“系统级后门”，就是在操作系统中通过嵌入代码或模块的方式掌握系统控制权，方便以后随时登陆进系统。木马主要通过ROOTKIT技术来隐藏自己，使杀毒软件无法察觉木马的存在或者干脆从系统级上禁用杀毒软件的某些功能，这样一来，木马和杀毒软件的争夺主要就集中在系统控制权的争夺上了，谁能拿到系统控制

权就可以反制另一方，从2006年开始，双方的争夺开始进入白热化，新的突破点和防护点不断被研究出来，但总体上说，杀毒软件处于被动状态，毕竟操作系统涉及的方方面面太广了，只要无法进行系统级的全面防护，那么一旦单点被突破就前功尽弃。 未知木马样本的收集对于杀毒软件来说也是个新的挑战，现代高级木马可以做到让用户毫无差觉，没有进程，启动后没有文件，这样就很难收集样本的方式来进行分析，而在没有样本的条件下进行木马分析简直是太难了。例如2007年7月，一个新的不可检测 的ROOTKIT - Rustock.c发布，但在接近一年后，Dr.Web(一个俄罗斯反病毒公司)的研究人员才对外宣称他们已经发现了Rustock.c的样本并确认在当时的系统保护手段下这个木马是不可检测的，毫无疑问，Rootkit在这个对抗中明显占据上风。 当时间来到2008，两个新的进展给了我们摆脱这种尴尬局面的希望，第一个是芯片厂商推出的芯片安全和虚拟化技术，这使得安全软件有希望得到系统的彻底控制权，随着技术的发展，基于这种技术的安全软件有望在不远的未来出现，另一方面，基于虚拟化芯片技术的rootkit也将揭开神秘的面纱，两者的对抗仍将继续。 另一个有变革性意义的技术是安全厂商推出的云安全技术，这项技术将从过去由用户受到攻击之后再杀毒到现在的侧重于防毒，实现一个根本意义上的转变。 当前已经出现的云安全实现原理大概可以分为两种：一种是由趋势科技提出的“ Secure Cloud ”，以Web信誉服务(WRS) 、邮件信誉服务(ERS)和文件信誉服务(FRS)为基础架构的云客户端安全架构，把病毒特征码文件保存到互联网云数据库中，令其在端点处保持最低数量用 于验证。其核心在于两点：(1)对复合式

攻击的拦截。通过对疑似病毒组件各部分外延属性进行检查，判断威胁程度.(2)瘦客户端。大量的病毒特征码保存在 云数据库中。简言之，趋势科技云安全技术基于其拥有庞大的服务器群和并行处理能力，构架了一个庞大的黑白名单服务器群，用于客户端查询，在Web威胁到达 最终用户或公司网络之前即对其予以拦截。 国内安全厂商瑞星也提出了云安全的概念，与趋势科技服务器群“ 云 ”不同，瑞星的“ 云 ”则建立在广大的互联网用户上。通过在用户客户端安装软件监控网络中软件行 为的异常，将发现的疑似木马、恶意程序最新信息推送到瑞星的服务器进行自动分析和处理，然后再把病毒和木马的解决方案分发到每一个客户端。 以上两种云安全概念采用的是两种完全不同的模式。趋势科技强调的是阻止外来威胁，基础是庞大的服务器群.瑞星强调的则是对用户计算机上业已存在的未知威胁 进行感知，基础是必须拥有大量的客户端用户。这两种模式都有一定的缺陷，趋势科技忽略了对本机威胁的收集，而瑞星的云安全则只能被动防守，不能在未知威胁进入到电脑前进行拦截。但另一方面，无论哪种云安全概念，都可以缩短杀毒软件的响应时间，从整个互联网的层面上最大程度地确保客户系统的安全。 对于木马而言，云安全缩短了样本的发现时间和响应时间，同时架构了一个基于整个互联网的安全体系，对于未知木马的防护开辟了新的思路，具体效果如何，还要我们拭目以待。 特别推荐： 2009年9月全国计算机等级考试时间及科目预告 2009年上半年全国计算机等级考试参考答案请进入计算机考试论坛 2009年全国计算机等级考试报名信息汇总 2009年NCRE考试有新变化 2009年全国计算机等级考试大纲 2009年上半年全国计