瑞星发布报告指正规公司成网络安全幕后黑手 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/61/2021_2022__E7_91_9E_E6_98_9F_E5_8F_91_E5_c40_61482.htm 1月10日，瑞星公司发布《中国大陆地区2005年度计算机病毒疫情&amp.网络安全报告》，该报告显示，瑞星公司在2005年共截获的72836个病毒，其中90%以上带有利益驱动的特征，而正规商业公司正日趋成为黑客和流氓软件的主要推动力。瑞星副总裁毛一丁指出，贪婪是目前病毒和黑客的最大特征，而一些正规商业公司和互联网企业，则正在成为网络威胁的最大的幕后黑手。《瑞星安全报告》指出，2005年整个网络威胁的发展呈现出一个明显的特征，那就是病毒、黑客和流氓软件紧密结合，拥有明确的利益目的，并且已经形成了清晰的“ 产业链条 ”。他们的手段可以总结为“ 一偷二骗三劫持四流氓 ”，有的是自己盗窃有价虚拟财产牟利，有的是为幕后的买家服务，而这些买家往往是正规的商业公司和一些互联网企业。以“ 偷 ”为目的黑客们的典型案例有：2005年3月，金华警方破获一个专门盗取“ 传奇 ”游戏账号的黑客团伙，其中某一个黑客窃取的账号就价值百万元；2005年11月，“ QQ被盗第一案 ”被深圳警方破获，两名黑客出卖窃取的QQ号获利至少6万5千元。所谓“ 骗 ”，就是黑客会先设立一个“ 钓鱼网站 ”，然后大量发送垃圾邮件、手机短信等，以“ 免费软件、手机彩铃 ”为诱饵欺骗用户登陆，用户“ 上钩 ”之后就会中毒，或被欺骗进行网络购物。2005年国庆黄金周，全国各地爆发大规模银行卡短信诈骗，其中某用户一次被骗走31万元。
自2005年年初以来，公安部、北京市公安局等相继发布警示

，网络钓鱼欺诈、网络木马等犯罪行为正在成为新型高科技犯罪热点。“ 劫持 ”是指黑客利用病毒控制用户的电脑，并将这些电脑变成自己胡作非为的工具。根据《瑞星报告》的统计，2005年“ 波特 ”（BOT）类病毒有23844个，占到总病毒数的32.7%。该类病毒感染计算机后，会在这些机器上开置后门，接受黑客的远程控制。被安装了后门的计算机被称为“ 肉鸡 ”，由许多“ 肉鸡 ”组成的计算机网络被称为“ 僵尸网络（Botnet）。黑客控制的“ 僵尸网络 ”，可以帮某个的网站带来巨大的点击量，也可以替“ 雇主 ”攻击竞争对手，前提是“ 你得付得起价钱 ”。 2005年1月10日，唐山警方抓获黑客徐某，他操纵6万多台中毒电脑（僵尸网络）攻击一个音乐网站；有国外黑客利用类似的攻击来敲诈商业网站，每次敲诈的金额在1万到10万美元之间；而国内某黑客团伙则自称控制着数十万台电脑，可以在24小时之内为雇主网站带来上百万点击，或者让竞争对手的网站瘫痪。“ 流氓软件（注） ”是指具有一定的实用价值，但具备电脑病毒和黑客的部分行为特征的软件，他们以“ 强制、隐瞒、欺骗 ”用户为最基本特征，帮助商业公司特别是互联网企业抢夺用户资源，或者加载广告软件等，以牟取暴利。 据《瑞星安全报告》透露，某国内网站借助流氓软件偷换用户的首页，在短短两个半月里全球排名从零上升到前500位。而浏览器被劫持、乱弹广告等常见的流氓软件，已成为网民司空见惯的事情。在利益驱使和生存压力下，很多共享软件作者也在软件里强行捆绑“ 流氓软件 ”，这些捆绑“ 流氓软件 ”的共享软件，已经成为“ 流氓软件 ”的主要传播渠道。 根据统计和分析，《瑞星安全报告》显示出，以某些网络企业为主的商业公司已经成为

上述网络威胁的“第一驱动力”，而病毒制造者、黑客和部分共享软件作者则成为帮凶，并且两者之间已经形成完整的“产业链条”。《瑞星安全报告》最后指出，随着网络深入到社会的方方面面，“流氓软件”等网络威胁牵涉到各种不同群体的利益，因此彻底解决这些问题，需要全社会各个方面的共同努力。譬如，某些共享软件作者加入“流氓软件”的行业，和我国软件盗版率居高不下是分不开的，他们无法通过正常渠道获取应得的报酬，只能沦为商业公司的帮凶。