毒霸陈睿:08年新增木马数量将突破100万 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/474/2021_2022__E6_AF_92_E9_9C_B8_E9_99_88_E7_c67_474944.htm 近日，在“ 2008反病毒技术发展趋势研讨会 ”上，金山毒霸技术总监陈睿向记者表示，“ 2008年，新增木马数量将突破100万，木马仍是广大网民电脑安全的主要威胁。而到2010年新增木马的数量更有可能曾几何级增长，达到千万。 自2006年起，偷、骗、抢就已成为信息网络安全的三大威胁。而木马、黑客后门病毒已经成为大多数职业病毒作者的生财工具，互联网也逐步步入了木马、病毒经济时代。据金山发布2007年上半年安全报告显示：2007年上半年，木马新增数占总病毒新增数的68.71%，高达76593种。 而另据近段时间金山毒霸官方网站对用户感染病毒情况的统计结果显示，毒霸大百科.net">http://vi.duba.net 网站是供客户感染病毒后查询病毒详细资料的网站，分析被查询最多的病毒资料的TOP10排名中，有9个是木马，1个是集黑客、蠕虫、木马后门于一身的混合型病毒，其目的也是为盗网络游戏帐号。由此可见，木马已经取代了传统病毒成为当今网络安全的主要威胁。 金山毒霸技术总监陈睿表示，木马之所以如此泛滥主要有三大原因：1、经济利益是木马猖獗的推动者。一个木马传播一次收回来十几万，再传播一次就二十万，所以木马的更新非常快；2、木马传播是手工投放，它可以改程序，今天投放完了，明天可以把程序改一改再投放，而杀毒软件传统的特征码作为一种静态识别技术对于改程序适应面很窄；3、“ 木马技术 ”具有不可判定性，木马是伪装成正常程序进入用户电

脑，进行破坏或者盗取用户信息。比如说蠕虫是利用网络进行复制和传播的程序，你很容易对它进行技术界定，但是对于木马如何用技术界定伪装，这是一个很大的难题。伴随着网民反木马呼声的日益高涨，各大杀毒厂商均推出了各自的解决方案。基于上述木马的三个特性，防御未知木马成为了各大厂商关注的焦点。以金山毒霸为例，金山毒霸2008在原有数据流杀毒的基础上，提出了全新的“病毒库 主动防御 互联网可信认证技术”为一体的“三维互联网防御体系”，即在病毒库和主动防御的基础上，采用了全新的“互联网可信认证”技术，近而大大提高了抵御未知木马病毒的能力。陈睿指出，在现有技术水平下要提升木马的防御能力只能提高两个关键点，第一个是特征码的识别率，第二个是如何减少恶意识别对用户的骚扰，尽可能做到自动判定。金山毒霸2008提出的“三维互联网防御体系”即在“病毒库 主动防御”的基础上，增加了“可信认证技术”，当用户的系统遇到无法准确判断其性质的可疑行为时，即链接金山毒霸的服务器，通过“毒霸互联网可信认证中心”瞬间即可完成后续的处理工作，因而既避免了对普通用户的困扰、又可有效地堵塞安全漏洞，从而大大增强了对木马的查杀能力，也提升了对新病毒的响应速度。而作为金山毒霸的“互联网可信认证中心”，首先通过“网络蜘蛛”的技术，将互联网上每秒钟内刚生成的可执行文件全部“抓”回来，然后通过自动以及人工的分析，以秒为单位对服务端的可信认证中心及病毒库进行刷新；一旦在客户端遇到可疑行为，依据特征码不能够判定的，马上链接至服务端进行判定。这样一来不但提升了杀毒软件对新病毒的响应速度，而且也增强了杀毒软件的

查杀病毒的能力，可以说是一举两得。 据了解，金山毒霸2008自11月15日起联合民间十大反病毒专业论坛一同进行公开测试，测试过程中，金山毒霸2008对病毒的查杀能力以及扫描速度等方面均获得了不少好评。一些业内人士评论指出，金山毒霸2008的“ 三维互联网防御体系 ”弥补了特征码识别技术的滞后性，也解决了目前主动防御给用户带来的困扰。“ 三维互联网防御体系 ”代表了杀毒厂商的一种杀毒理念，也代表了当下主流的声音，同时也希望在这种新的病毒防御理念的指导下，我们的杀毒厂商能够研发出更多、更实用、更管用的杀毒软件。 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