“ 也许新的‘ 毒王 ’就在你的电脑里，但你并没有发觉。 ”反病毒工程师称。自从6月份以来，“ 帕虫 ”成为新的毒王，在电脑感染数量和破坏力方面都超过了“ 熊猫烧香 ”。 病毒制造模块化、批量化“ 帕虫(金山称为AV终结者；江民称为U盘寄生虫) ”的出现，代表了“ 病毒工业 ”发展的新趋势。黑客和病毒制造者正在大量采用“ 模块化编写 ”的方法来批量制造新病毒。 所谓“ 模块化编写 ”，就是黑客们把功能齐全的病毒，拆分为不同的功能模块，每个模块都成为单独的病毒。“ 帕虫是一个先头部队，传播到用户端后，先把防毒设施破坏掉，然后再从黑客指定的其他网站下载病毒，只要用户被一个帕虫攻击了，就会感染上很多病毒。 ”史说。“ 熊猫烧香 ”闹得满城风雨，最后引起公安部门注意，将病毒制造者捉拿归案，而新毒王却并没有掀起更大的风波，这是为什么呢？因为“ 熊猫烧香 ”的特征非常明显，会直接造成机器瘫痪。而“ 帕虫 ”以窃取账号获利益为目的，所以一般不会导致机器瘫痪，用户也很难感觉到病毒的存在。 据瑞星《上半年病毒疫情分析报告》显示，中国内地每天有数百甚至上千种病毒被制造出来，其中大部分是木马和后门病毒，占到全球该类病毒的三分之一左右。 奇虎360安全小组负责人傅盛告诉记者，现在，互联网上有很多工具，那些没有多高技术造诣的人也能很容易地制造病毒。“ 几乎能达到傻瓜化应用的程度了。 ”“ 加壳 ”、“ 免杀 ”等技术在网上流行，是另一个可以说明“

病毒工业”精细化程度的例子。“加壳”就像给病毒文件穿了“马甲”，使杀毒软件不容易识别；而“免杀”是指通过特殊技术处理，修改病毒文件，使已知病毒逃过杀毒软件的查杀。“以前病毒的变种都是重新写代码，现在是在网上随便加个壳就是一个变种。”傅盛说。网上著名的“免疫007”，就是一种商业化的自动加壳机，它向它的用户承诺：升级频率超过杀毒软件。“我们每天拿到他们的新版本，然后再编写解壳程序。”史告诉记者，安全厂商就是这样每天与他们玩着猫捉老鼠的游戏。黑客直接攻击杀毒厂商“我们的网站每天都要受到上万次的攻击，我们有一个专门的团队24小时值班，才能看得住。”瑞星市场部马刚告诉记者，从2006年以来，黑客团伙与网络安全厂商的直接对抗越来越多。以前，黑客与安全厂商之间的较量是在用户那里体现。而现在，黑客们为了达到目的，干脆直接对“互联网的警察”下手了。“他们常用的一种手段是在客户端把我们的官方网站屏蔽掉，用户输入我们的网站是登不上去的。还有一种，只要程序当中有‘360’字样的窗口都会自动关闭，任何360的程序都无法运行。还有的黑客，组织一批它能控制的机器，同时向我们网站发送比较大的数据包，造成我们网站的速度缓慢。”傅盛向记者描述了最近受到攻击的景象。史总结目前黑客攻击安全软件的主要手段有：修改杀毒软件设置，默认“忽略(不查杀)”查出的病毒；修改系统时间，让杀毒软件过期；破坏该IM软件自带的木马查杀模块；损坏杀毒软件的完整性，使软件打不开；甚至，只要用户在搜索中带有病毒字样，浏览器都自动关闭，无法找到杀毒软件。“真实”财产成为新灾区 自2006年下半年以来，针对网络银行和证券的

木马、后门程序增加很快，与此相对，大量新股民连基本的杀毒软件都未安装。 根据趋势科技发布的信息来看，上半年所侦测到的木马间谍，窃取在线游戏信息的占了37%，窃取银行账户信息的占17%，试图窃取IM账户信息的占5%。 史介绍了几种常见的偷窃形式。 对于网络银行，最常见的是网络钓鱼：比如，黑客建一个跟正式网站很像的网站，用户无意中进入这个网站，把卡号和密码输进去，这些信息就被黑客窃取了。这类网站存在的时间非常短，往往连一周都不到。还有一种是利用钓鱼软件，在用户进入银行的正式网站后，会弹出一个对话框，跟银行业务相关，要求用户填写卡号和密码。这种情况用户很难分辩。还有一种常见的方式是盗取密码，比如键盘钓子，可以把用户在键盘上输入的信息都记录下来，然后通过一个文件传给黑客，黑客就能分析出账号和密码。在盗取账号和密码后，黑客就会把钱直接转出。 而对于网络证券的窃取形式略有不同。“ 如果能既窃取到炒股的账号也窃取到相应的银行卡号，黑客就会把股票卖掉，把资金转入银行卡里，然后再转到自己的账户里。如果只窃取到炒股的账号，他们就会用高买低卖的形式，自己借机获利。 ”傅盛告诉记者。 傅盛认为，目前盗取真实财产的黑客产业链尚未完全形成。“ 一是网上业务还比较新；二是技术难度比盗取虚拟财产难一些；三是盗取真实财产面临的法律风险比较大。 ”但他认为目前必须重视这个问题了，同时他告诉记者，奇虎已经开始与各大银行就这个问题进行沟通。 从另一方面看，由于网络管理资金账户还是比较新的业务，很多问题也是自身的疏忽给黑客留下空子。许多用户的电脑上根本没有安装杀毒软件，或者安装之后，不会设置，或者长

久不升级。此外，有的用户为了方便，开户之后不修改初始密码，或使用生日、电话号码当做密码，并且股票账户、资金账户使用同一个密码，这样很容易被黑客窃取。另一方面，在券商提供的专用炒股软件中，通常都包含了专用的安全模块，但这些模块很可能很长时间不升级，比如某大券商的股票下单软件，安全模块病毒库的最新日期居然是2006年9月，这样极其容易被黑客利用。