# 软键盘安全性

物理键盘的内部有一块微处理器，它控制着键盘的全部工作，比如主机加电时键盘的自检、扫描，扫描码的缓冲以及与主机的通讯等等。当一个键被按下时，微处理器便根据其位置，将字符信号转换成二进制码，传给主机和显示器。如果操作人员的输入速度很快或CPU正在进行其它的工作，就先将键入的内容送往内存中的键盘缓冲区，等CPU空闲时再从缓冲区中取出暂存的指令分析并执行。

而一般键盘记录间谍软件有三个模块组成：主模块，钩子过程模块以及FTP模块。

按键记录木马是Trojans木马的变种之一。是功能比较单一的特洛伊木马。攻击者会力图使它保持较小的体积，通常是10 KB 到30 KB，以便快速激活而不引起注意。该木马由3个模块组成：主模块，钩子过程和ftp模块。主模块负责安装一个全局钩子过 程。该钩子的任务是把每次按键事件向主模块汇报，由主模块把所有的击键保存到一个文件中。当记录文件达到预定的大小时，主模块命令ftp模块把记录文件上载给一个n甲服务器。三个模块问的通讯是通过Windows消息机制实现的。

一旦用户的电脑感染了按键记录木马病毒。系统就被种下了“钩子”，黑客通过“钩子”程序监听和记录用户的击键动作，然后通过自身的邮件发送模块把记录下的密码发送到黑客的指定邮箱。

比较典型的案例如“密码大盗”。“密码大盗”病毒运行后。在被感染的计算机上释放下列四个文件：用来记录病毒原始目录的文 件mmdat．dat、病毒主程序intrenat．exe、钩子模块ntdll32．dll和记录用户输入数据的文件wdata32．dU。病毒运行后安装钩子模块，子类

化IE服务器窗口(Iutemet Explorer\_Server)，当发现网贞上有“Password”、“密码”、“Submit”等字符时开始记录用户输入信息．并将记录的用户信息发往指定邮箱。

为对付按键记录木马，密码输入中目前普遍采用的方法就是软键盘输入。软键盘输人可反击基于钩子技术的键盘监视程序。该 技术方便易用．兼容性强，因此受到了广大用户的欢迎。

软键盘技术的工作原理是利用一个软件程序模拟实现硬键盘所具备的功能。在软键盘内部有一个编辑控件。用此编辑控件将 针对每次用户击键譬成一个模拟的随机键击串。木马的监视程序将截获用户的击键和伪击键，这样一来木马的键击记录器就无法 提取记录随机产生的相对应按键，使它很难或者不可能检索实际的输入文本。因此只要不直接通过键盘输入，而用软键盘输入，木 马软件就无法获得每个按键的ID，也就起到了动态隐藏密码的效果，随机键击串麻该是一个乱数，也就会有效地阻止键击记录器获 取信息的途径。而用户输入的数据被存储于～个成员变量中。应用程序就可以很容易地通过编辑控件存取该变量的值，从而能够防止木马窃取密码的事情发生。

软键盘输入技术使得用按键记录技术的木马失去了作用，但“屏幕快照”窃密木马却可以通过屏幕快照的方法来破解软键盘输入技术。“屏幕快照”窃密木马一般会伪装成后缀名为rar的压缩艾件，诱骗用户上当点击运行。“屏幕快照”窃密木马运行后，会将其中部分网页链接改造成可偷偷打开黑客事先设定的恶意网页的“陷阱”链接，然后自行利用各种IE浏览器的MHT漏洞尝试对点击者的计算机进行木马种植．2004年江民反病毒中心截获的“证券大盗”病毒、2008年1月14日围家计算机病毒应急处理中心发布通告的一个以盗取网上银行和“支付宝”账号密码的“网银木马”，都是使用“屏幕快照”窃密技术的木马案例。

“证券大盗”木马病毒运行时，会自动查找包括IE、Maxthon、Trraveler、MYIE、TouchNet、Opera、SmartExplore、k—meleon、GreenBrowser在内的多种浏览器，或寻找一些包含著名券商名称的窗口标题．一旦发现用户使用其中任一种浏览器臀录个人网上银行等界面．就开始启动键盘钩子对用户瞀录信息进行记录，包括用户名和密码。同时在后台以复制的方式将屏幕分为黑、白两种图片。其中软键盘界面为黑色图片，是固定不动，其后通过屏幕快照的方式在一段时间内进行连续截屏．记录每一次鼠标点击的位置．将用户的登录界面保存为多张白色图片，一般存放于：“c：、Screenl．bmp”和“C：＼-Screen2．bmp”下。当记录达到指定次数后．木马病毒会将存档中记录的信息和图片通过电子邮件发送到黑客自己的邮箱中。发送成功后，木马病毒还会实施自杀，将自身删除。黑客通过对照图片中鼠标的点击位置．就很有可能破译出用户的登录账号和密码，从而突破软键盘密码保护技术。（何太星 "证券大盗"木马病毒原理及防范[期刊论文]-计算机安全 2005(3)）

软键盘改进：将原始的“静态”软键盘模型改进成“动态”的软键盘模型，每当用户利用软键盘点击输入一个数据的同时．键盘上所有按键的显示内容自动隐藏，随后出现的软键盘上所有的按键是随机出现的新的顺序，这种变换过程本身完全随机、无规律町寻，这就可以有效防止密码的失窃。

具体实现选用VB来编写设计软键盘程序。弯用户鼠标指向软键盘上某个键位时，则所有按钮上的内容不显示：当用户击点键位后松开鼠标时，则更换所有按钮上的内容。采用这样的软键盘设计的好处有：一是软键盘的键位随着每次的按键而改变．可有效防止采用黑白片方案的窃密手段：二是软键盘在指向按键的同时隐藏键位的内容，可有效阻止按键截屏的窃密手段。运用动态软键盘设计的不足之处：键位更换应当采用完全点击时软键盘状态随机形式，以增强安全性。但如果每按一个键位后．布局就进行一次完全变换，则可能造成用户的使用不便。（ 顾海艳， 顾刚， 薛斌，软键盘技术研究和改进，2008,4（35））