## 冰河木马8.4简介

冰河木马8.4是一款专业的远程控制软件，使用该软件可以实时出卡安电脑当前状态，在线操作控制电脑，提供完整的远程操控功能，支持点对点通讯服务，功能非常强大，欢迎来绿色资源网下载！

冰河木马开发于1999年，跟灰鸽子类似，在设计之初，开发者的本意是编写一个功能强大的远程控制软件。但一经推出，就依靠其强大的功能成为了黑客们发动入侵的工具，并结束了国外木马一统天下的局面，跟后来的灰鸽子等等成为国产木马的标志和代名词。HK联盟Mask曾利用它入侵过数千台电脑，其中包括国外电脑。

## 冰河木马功能

1．获取系统信息：包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率、物理及逻辑磁盘信息等多项系统数据；

2．记录各种口令信息：包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息；

3．远程文件操作：包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件、远程打开文件（提供了四中不同的打开方式--正常方式、最大化、最小化和隐藏方式）等多项文件操作功能；

4．限制系统功能：包括远程关机、远程重启计算机、锁定鼠标、锁定系统热键及锁定注册表等多项功能限制；

5．发送信息：以四种常用图标向被控端发送简短信息；

6．注册表操作：包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能；

7．自动跟踪目标机屏幕变化：同时可以完全模拟键盘及鼠标输入,即在同步被控端屏幕变化的同时，监控端的一切键盘及鼠标操作将反映在被控端屏幕（局域网适用）；

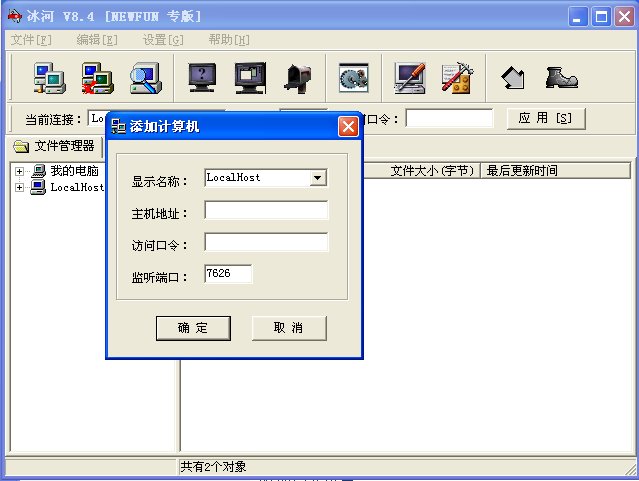
8．点对点通讯：以聊天室形式同被控端进行在线交谈。

## 服务端介绍

1. 进入冰河木马的界面这里就是控制区域，中间有很多图标，点击可以添加主机。



1. 这里就是添加主机的窗口，编辑主机的地址和参数可以自动连接。



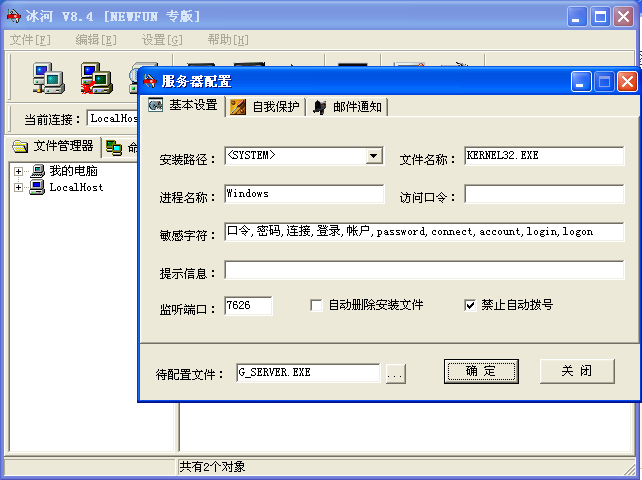
1. 主菜单的功能还是非常多的，捕获屏幕、屏幕控制、冰河信使、升级1.2版本、修改远程配置。



1. 搜索计算机。搜索计算机的范围还是非常大的，可以设置搜索的端口、延迟时间、起始域名、起始地址。



1. 配置服务器参数：支持安装的路径、进程的名称、访问的口令、提示信息、监听端口。



连接到另一台计算机后，可以控制对方计算机。



## 清除方法

1、删除C:\Windows\system32下的Kernel32.exe和Sysexplr.exe文件。（删不掉的话先结束进程）

2、冰河会在注册表HKEY\_LOCAL\_MACHINE/software/microsoft/windows/ CurrentVersion

Run下扎根，键值为C:/windows/system/Kernel32.exe，删除它。

3、在注册表的HKEY\_LOCAL\_MACHINE/software/microsoft/windows/ CurrentVersion/Runservices下，还有键值为C:/windows/system/Kernel32.exe的，也要删除。

4、最后，改注册表HKEY\_CLASSES\_ROOT/txtfile/shell/open/command下的默认值，由中木马后的C: /windows/system32/Sysexplr.exe %1改为正常情况下的C:/windows/notepad.exe %1，即可恢复TXT文件关联功能。

