**教你打造免查杀Teamviewer内网木马**

2009-03-10 17:09 小地瓜 IT168.com [我要评论(0)](http://netsecurity.51cto.com/art/200903/113824.htm#commment) 字号：[**T**](javascript:setfont(12);) | [**T**](javascript:setfont(16);)

如今网上的木马，已经多到了数不胜数的地步，但是真正好用能够逃脱杀软查杀，且不受网络环境限制的木马确很少。其实我们完全可以自己将Teamviewer木马，打造成一个免杀且不受环境限制的超强木马。

AD：

如今网上的木马，已经多到了数不胜数的地步，但是真正好用能够逃脱杀软查杀，且不受网络环境限制的木马确很少。即使你碰到也是所谓的VIP版木马，难道真的非要花钱才能买到“好马”?答案当然是否定的，其实我们完全可以自己将Teamviewer木马，打造成一个免杀且不受环境限制的超强木马。

**一、了解Teamviewer远程控制**

Teamviewer是一款功能强大的远程管理软件，由于软件建立的初哀，是为了方便网络管理员们的远程管理，所以有些杀毒软件没有将它列入到木马的行列，并且它还是至今唯一的一款能穿透内网，及各种防火墙的远程控制软件。

Teamviewer不同于其他同类软件，它的服务端配置需要在被控制主机上操作，例如这里将下载下来的“Teamviewer”压缩包程序，上传并释放到被控制主机上，然后运行里面的Teamviewer.exe程序，此时就会弹出“Teamviewer”对话框，并且自动连接服务器进入VPN网络，获得分配的ID、密码(图1)。

|  |
| --- |
| <http://new.51cto.com/files/uploadimg/20090310/1722450.jpg> |
| 图1 |

如果此时你要想控制这台主机，只要在自己的电脑里，同样运行“Teamviewer”程序，然后在右边ID框内，将它分配的ID输入，并选择“远程支持”选项，就可遥控其受控主机了。

**二、让Teamviewer远程控制软件“摇身变”木马**

之前我们说到Teamviewer是一款远程控制软件，所以如果按照以上不加“修饰”的去安装服务并连接，那很容易被网管们所发现。所以下面笔者要做的就是将Teamviewer远程控制软件，打造成一个隐蔽性极强并具杀伤力的木马。

大家知道文件的体积越大，就越容易被管理员所关注，而Teamviewer的大小为3.89MB，其主程序Teamviewer.exe就有3.04MB，所以要想为其“减肥”只能从其它文件上着手了。

将下载的Teamviewer文件解压后，你会发现里面有三个文件夹，分别是W2K、X64、X86，如果在Windows 2000/2003中则需要用到W2K，在64位系统中就是X64，Windows Xp则是X86，这里你可以根据被控主机的系统，来确定保留的文件，无用的文件删除即可(图2)。

|  |
| --- |
| <http://new.51cto.com/files/uploadimg/20090310/1722451.jpg> |
| 图2 |

除了三个文件夹外，主目录里的uninstall.exe反安装程序、License.txe软件协议、Unicows.ddl库文件也都删除掉。而Intall64.exe、install.exe、install.reg文件都是安装程序用的，如果现在用不上可以将它们移出，等到用的时候在恢复，这样Teamviewer才会在原来的基础上减下很多“脂肪”。

接下来为了保证自己能够与被控制主机连接上，我们需要对Teamviewer的连接密码进行设置，以避免连接密码因不固定而连接不上。

这里打开“Teamviewer程序”对话框，在其上方依次单击“额外”→“选项”标签，此时就会弹出的“Teamviewer选项”对话框内，我们在密码和确认密码文本内，输入想要设定的连接密码后，单击“确定”按钮，这样每次启动电脑，就可自动打开Teamviewe连接专用网络，从而可以保证控制端的正常连接(图3)。

|  |
| --- |
| <http://new.51cto.com/files/uploadimg/20090310/1722452.jpg> |
| 图3 |

除此之外，为了防止被控端上的Teamviewe关闭，我们需要在被控制主机上的Teamviewe，依次单击“额外”→“选项”标签，在弹出的“Teamviewe选项”对话框内，切入至上方“安全”标签，然后分别勾选上里面“更改要求本电脑上的管理员权限”和“禁止Teamviewe关闭”复选框(图4)。

|  |
| --- |
| <http://new.51cto.com/files/uploadimg/20090310/1722453.jpg> |
| 图4 |

最后别忘了将“入站访问控制”里的滑块拖到最上方，使其变为“完全访问”状态，来保证我们以后能够完全控制使用其各项功能。

如果以上的操作，你是在自己主机里进行配置的，你可以在“Teamviewe选项”对话框内，切入至“高级”选项，在“导入/导出选项”栏内，单击“导出”按钮指定保存路径后，即可将当前Teamviewe配置信息导出生成。

接下来我们只要将Teamviewe缩小的体积和生成的配置信息，上传到肉鸡主机，然后运行Teamviewe.exe程序，并导入刚才生成配置文件，此时就可以完全，且非常安全的控制这台主机了。

## 

AFX windows rootkit 2005