调戏突破 SecureRDP 对远程桌面连接的限制

作者：闪电小子
来自：PKAV
网址：www.2cto.com

缘起自某群某孩纸遇到的一案例
连接远程桌面的时候服务器出现如下提示：
You are not allowed to access to this Terminal Server. Please contact your administrator for more information. Secured by SecureRDP.
仔细一看不是远程管理组的问题，而是 SecureRDP 这个软件搞的鬼，网上一搜，
好家伙，这个软件的功能如下：
secureRDP 是一款用户登录服务器管理软件。防止非法用户试图暴力破解用户密码；可以过滤 IP/MAC 地址、计算机名等。具体有以下功能：
1.连接限制允许按照登陆时间，IP 地址，主机名，MAC 地址，Client 版本等信息作连接

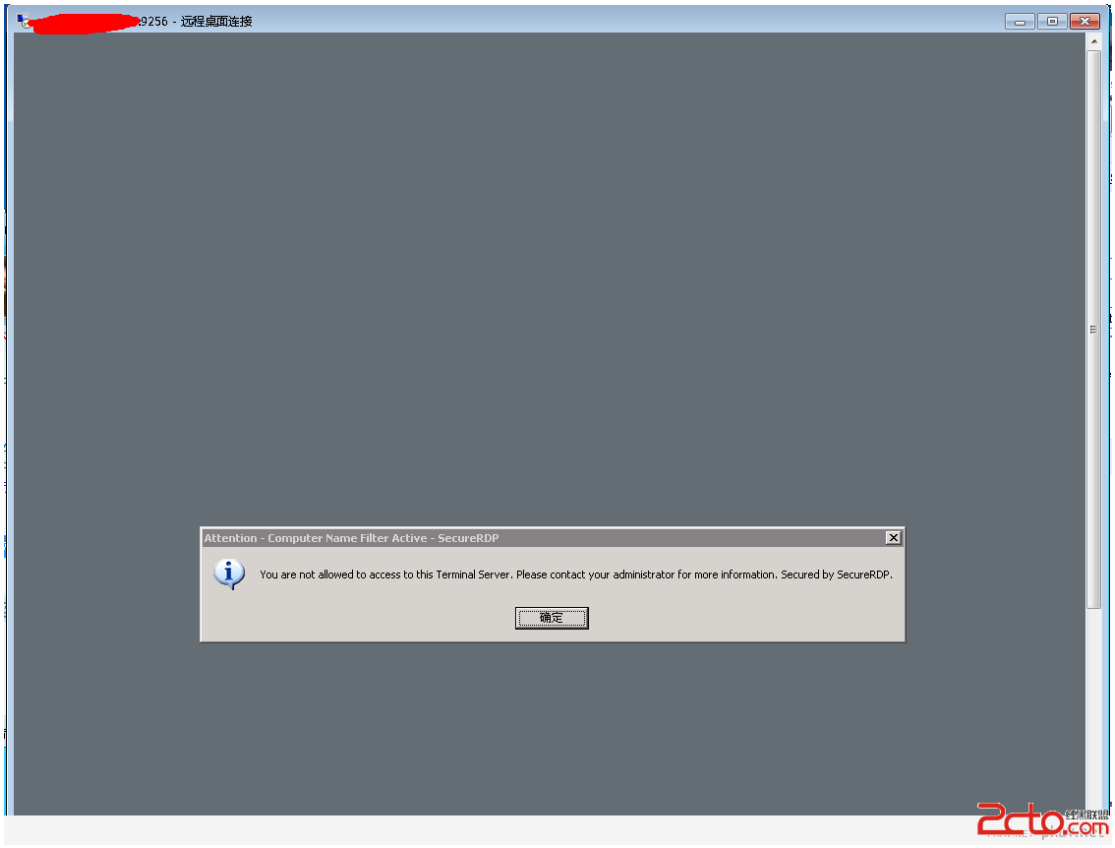

图 1

看来是对客户端的连接做了限制了，现在流行的 D 盾和安全狗都有这样的功能！
着实第一次见这个软件，好奇心也来了，也想顺便帮这位童鞋一把，下了软件
虚拟机装好，配置好限制 ip，一看软件目录，依然只有这几个文件，那么他的配置要么是写入其他目录了，要么写到注册表里面啦！

图 2

想想之前调试的某狗。Od 打开，加载软件

Aspack 壳无视之，运行起软件，直接下好注册表 API 断点 RegOpenKeyExA，直接保存配置断点断下了，注册表的路径显示出来了

HKEY_LOCAL_MACHINE\Software\Terminalsoft\WTSFilter

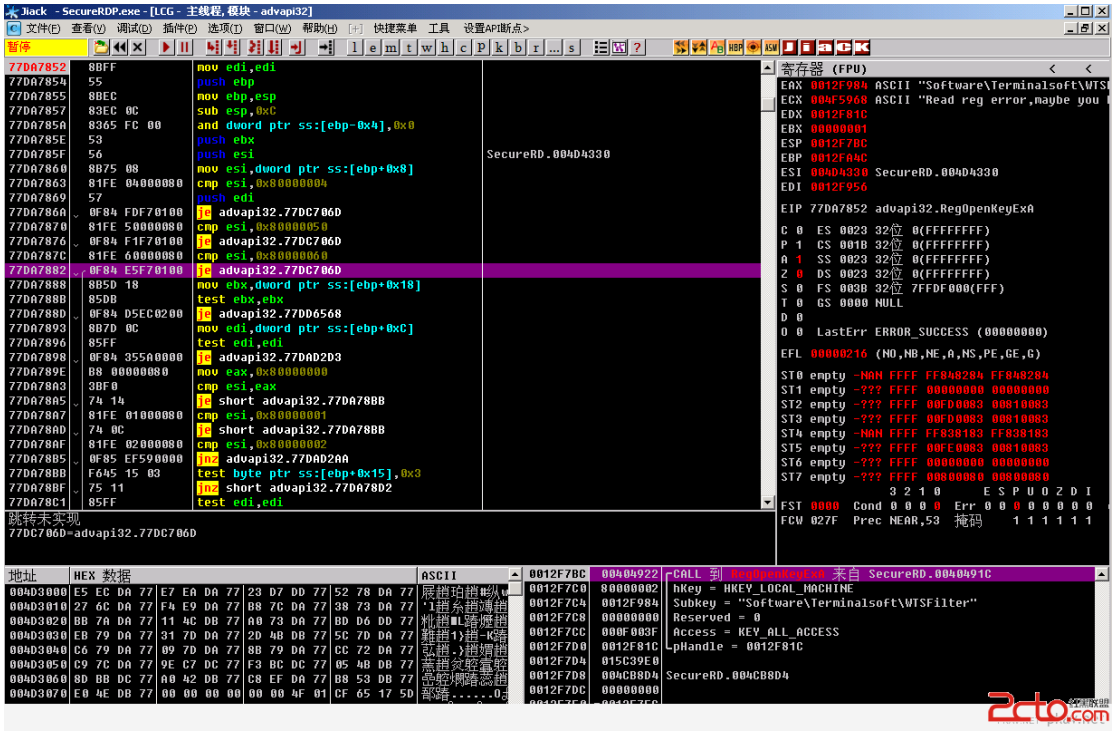

图 3

跑到注册表里面一看，果然是这个

邪恶的直接把 WTSFilter 项给删除了

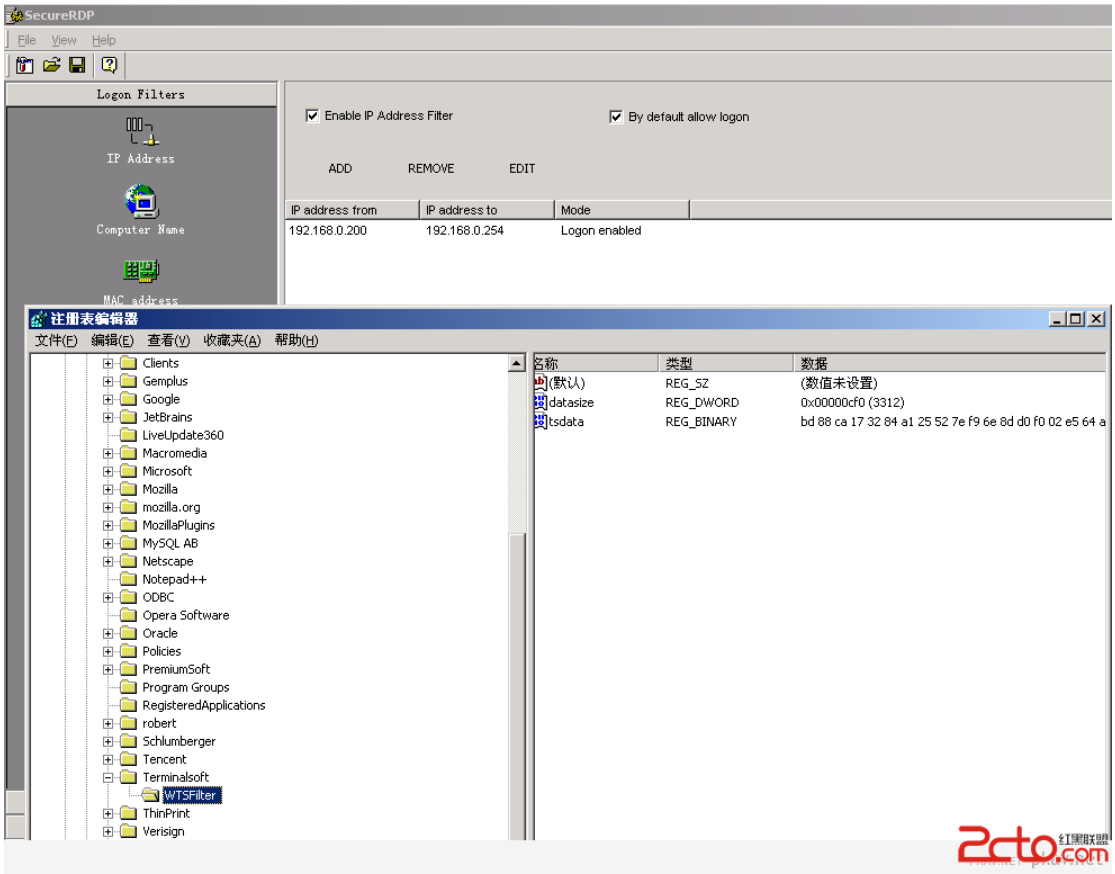

图 4

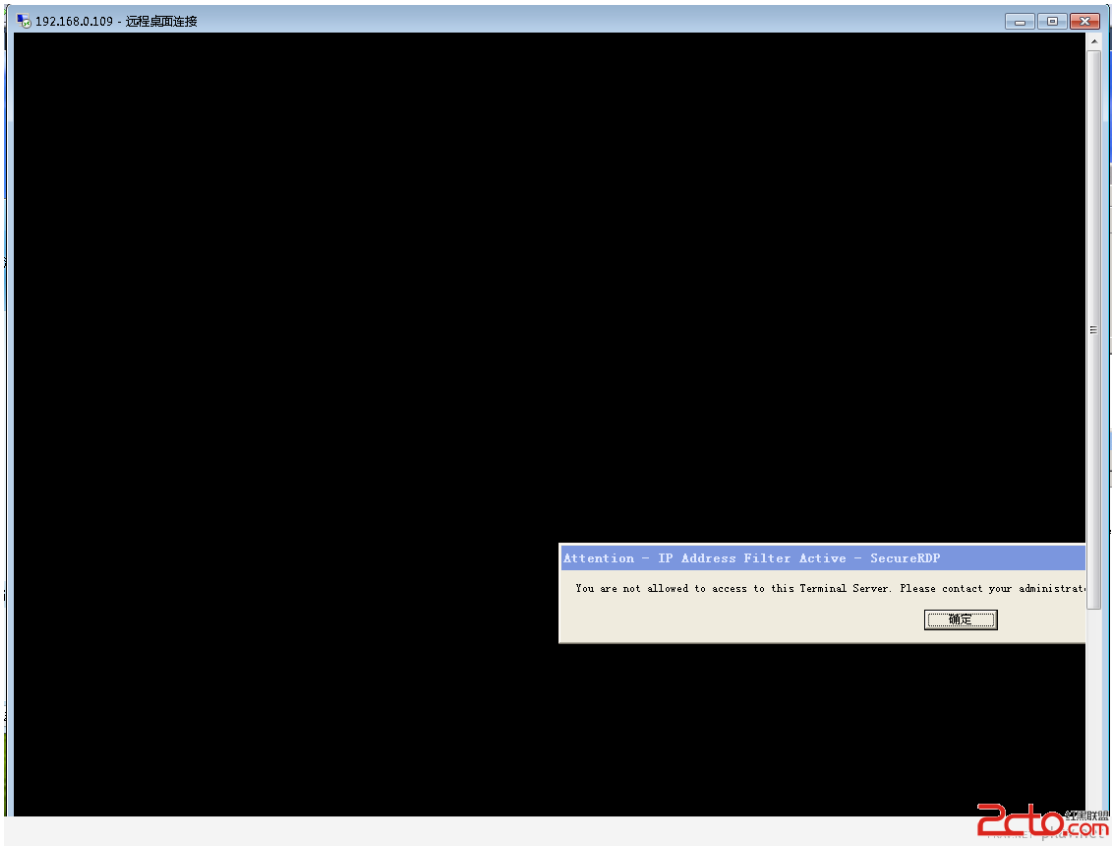

图 5

看在删除之前我是配置把自己的 ip 除外了的。提示不允许连接！

把注册表项删除以后，已经没有任何的限制了！

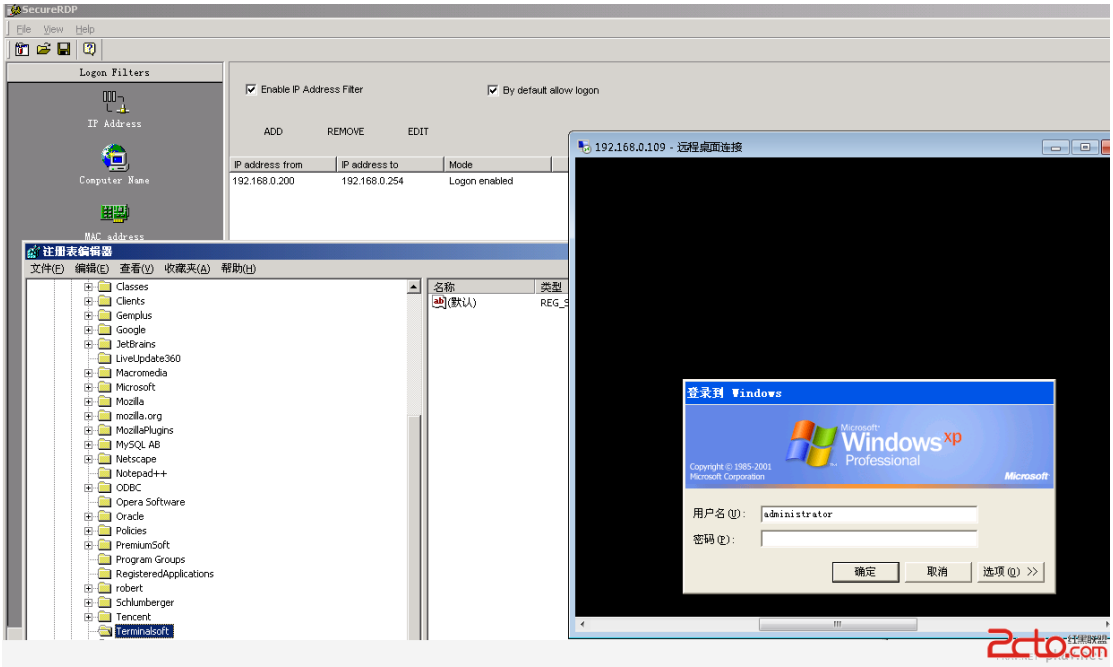

图 6

思路已经很清楚了。直接干掉那个注册表项，就能搞定啦！

我先是在 shell 上读取了这个注册表的值，的确存在的。

读取注册表值：

reg query "HKEY_LOCAL_MACHINE\Software\Terminalsoft\WTSFilter" /v tsdata

备份导出注册表项：

Cmd /c "regedit /e d:\freehost\jiqiren\web\Editor\js\wts.reg "HKEY_LOCAL_MACHINE\Software\Terminalsoft\WTSFilter""

然后就是删除注册表项：

reg delete "HKEY_LOCAL_MACHINE\Software\Terminalsoft\WTSFilter" /va /f

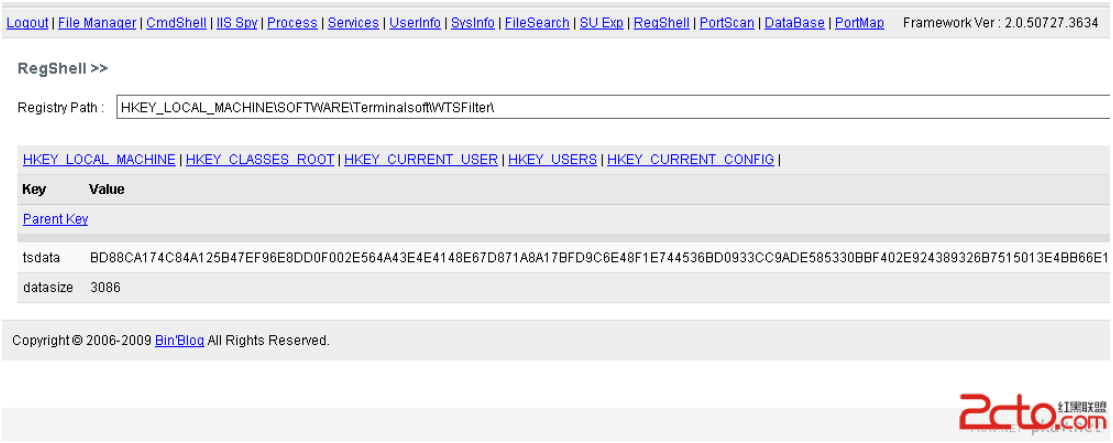

图 7

好吧，此时连接目标服务器，发现限制已经么有啦！

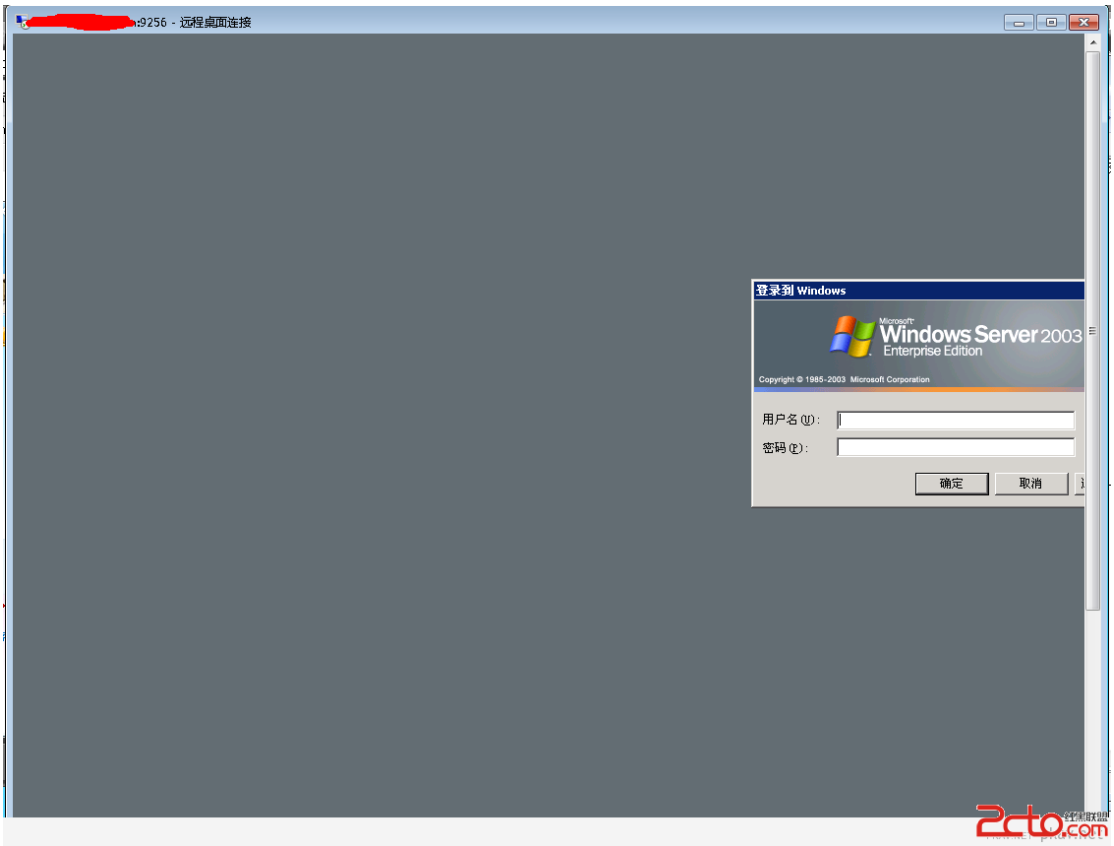

图 8

服务器已经提权，登录之后，恢复注册表项，看他的配置，发现对计算机名进行了限制！

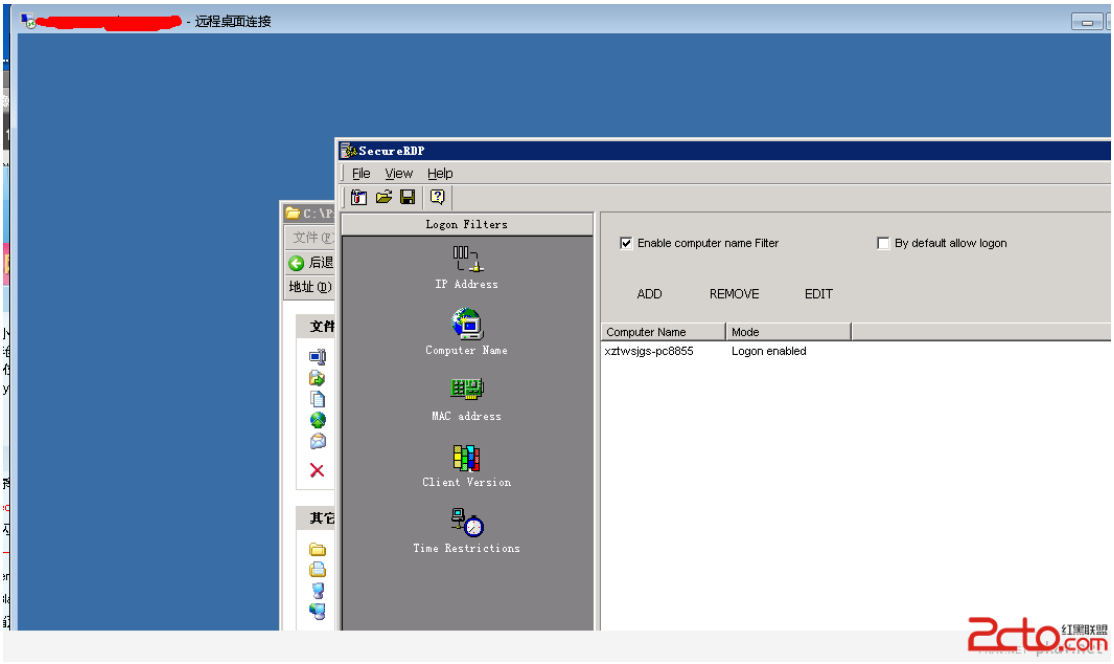

图 9

这次好玩的过程就结束啦。成功的 kill 掉了它的限制！

最后总结：

1. 开始没看清提示，以为是组策略或者是远程组的关系！
2. 发现软件时，直接 kill 掉进程是没用的，实现的手法还待探索！
3. 其实这些个小安全软件做的还真是不太“安全”！