<https://www.bilibili.com/read/cv841855>

<https://www.freebuf.com/articles/terminal/195721.html>

所谓未知攻焉知防，了解了常见的攻击方法，才能更好的进行防御，在应急事件中也能更快的做出响应，阻断攻击行为，找到攻击源头。

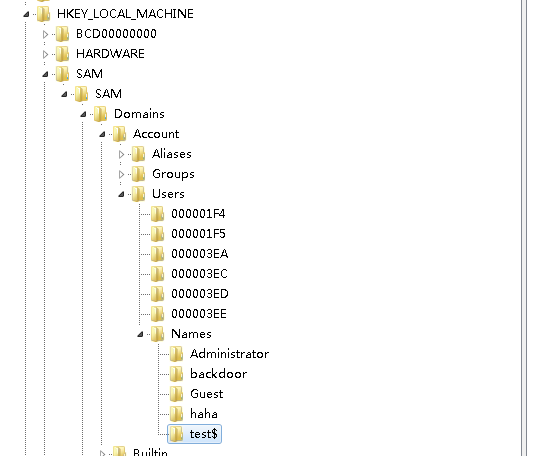
**一、账户隐藏**

隐藏方法：

新建用户时利用如下命令：net user test$ abc-123 /add，此种方式新建的用户无法通过net user cmd下查看，但是可以控制面板用户账户中查看；还可通过将隐藏用户的F值替换管理员值方式将隐藏账户才控制面板隐藏。

查看隐藏账户：

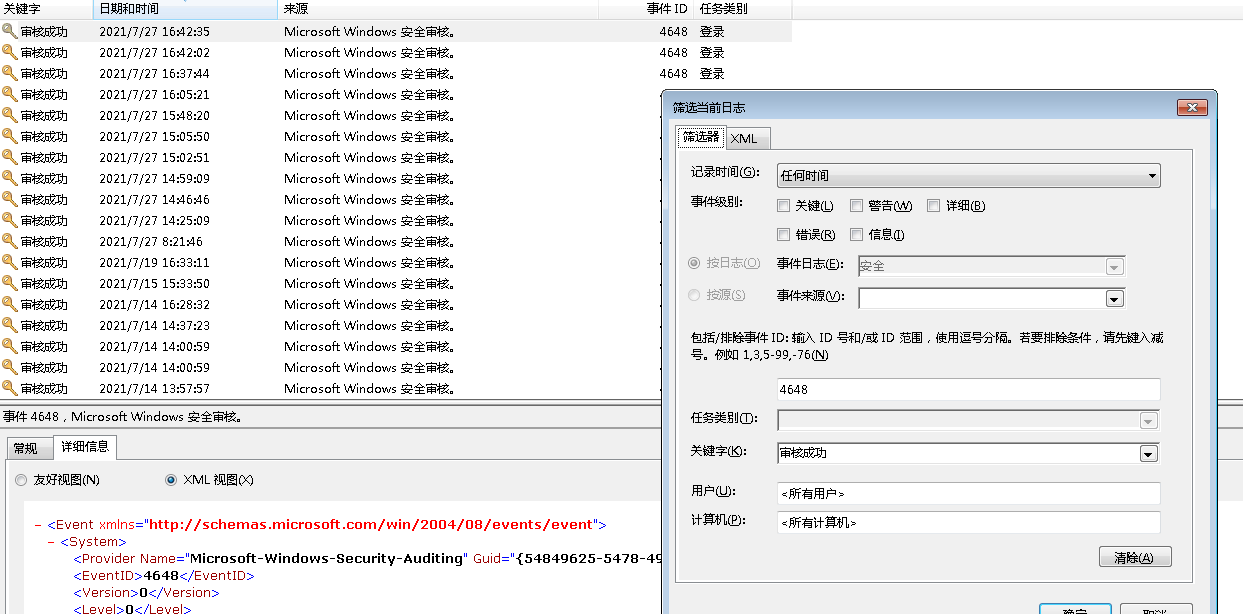
查看注册表（regedit）可查看隐藏账户，test$为建的隐藏账户



**查看工具：**

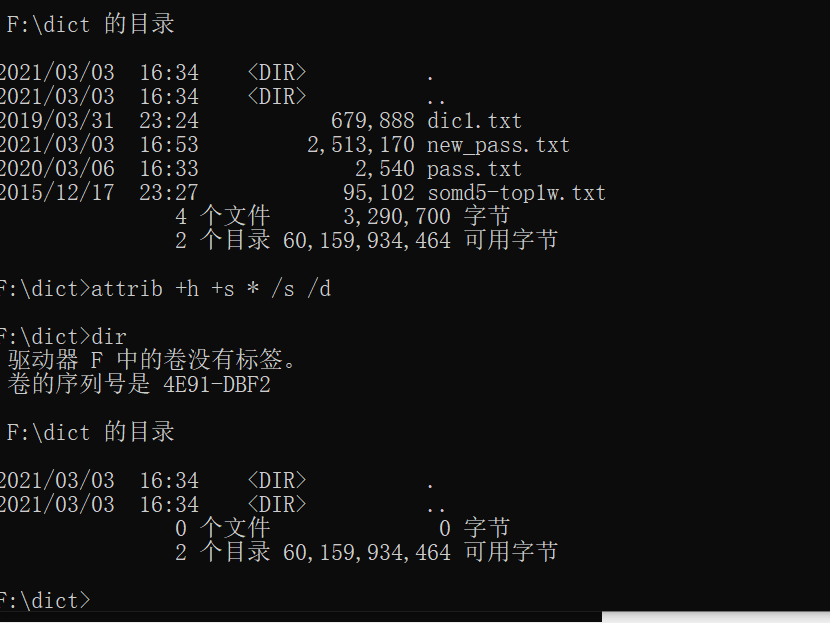
D盾工具可以检测出隐藏账户、克隆账户

查看登录日志（eventvwr打开系统日志）：通过筛选事件id 4648（登录成功），查看用户登录情况，从而确定是否有异常用户登录系统



**二、文件隐藏**

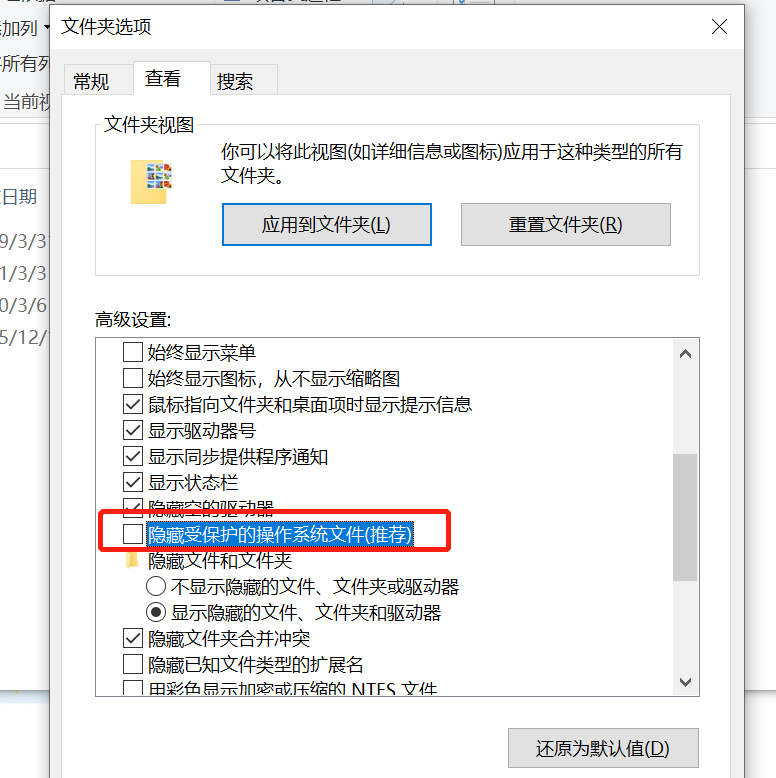
1、利用 attrib 命令来隐藏文件，例如隐藏F盘下的dict文件，可输入如下命令：attrib +h +s \* /s /d，命令执行成功后dir无法看到相关文件



**查看方法：**

输入相反命令：attrib -h -s \* /s /d 即可查看相关文件

文件夹选项，查看设置中去掉“隐藏受保护的操作系统文件”的选择，也可查看隐藏文件



2、CLSID方法

CLSID是指windows系统对于不同的应用程序，文件类型，OLE对象，特殊文件夹以及各种系统组件分配一个唯一表示它的ID代码，用于对其身份的标示和与其他对象进行区分，CLSID是一个128位的随机数，CLSID应用编辑常见组件类对应的CLSID

我的文档：450D8FBA-AD25-11D0-98A8-0800361B1103

我的电脑：20D04FE0-3AEA-1069-A2D8-08002B30309D

网上邻居：208D2C60-3AEA-1069-A2D7-08002B30309D

回收站：645FF040-5081-101B-9F08-00AA002F954E

Internet Explorer：871C5380-42A0-1069-A2EA-08002B30309D

控制面板：21EC2020-3AEA-1069-A2DD-08002B30309D

拨号网络/网络连接：992CFFA0-F557-101A-88EC-00DD010CCC48

任务计划：D6277990-4C6A-11CF-8D87-00AA0060F5BF

打印机(和传真)：2227A280-3AEA-1069-A2DE-08002B30309D

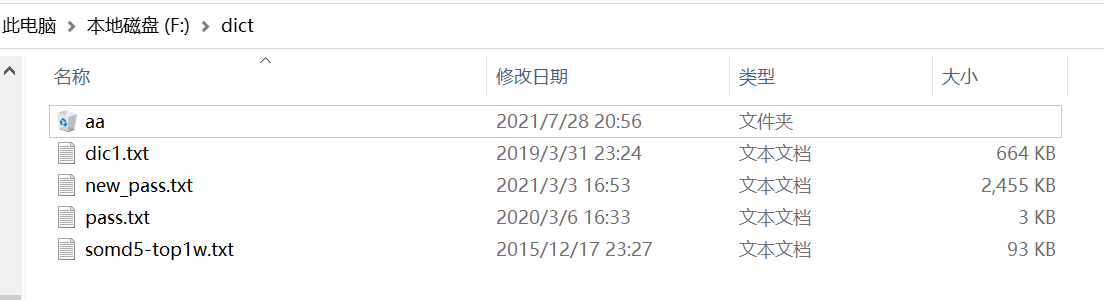
历史文件夹：7BD29E00-76C1-11CF-9DD0-00A0C9034933

公文包：85BBD920-42A0-1069-A2E4-08002B30309D

Web文件夹：BDEADF00-C265-11d0-BCED-00A0C90AB50F

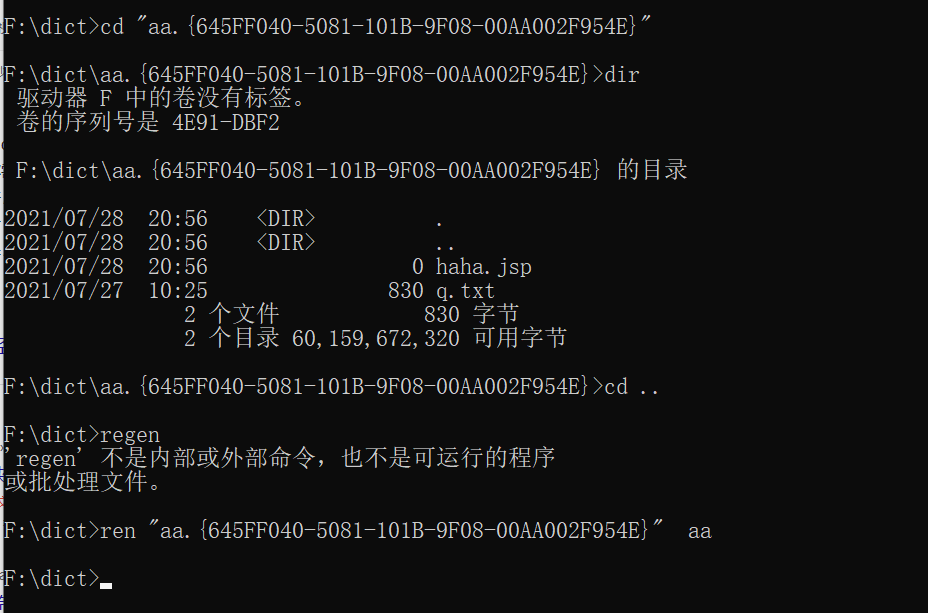
网页：25336920-03F9-11CF-8FD0-00AA00686F13

将aa文件夹命令为aa.{645FF040-5081-101B-9F08-00AA002F954E}，发现之前的文件夹真的变为一个回收站的图标，即使双击打开的依然是垃圾桶



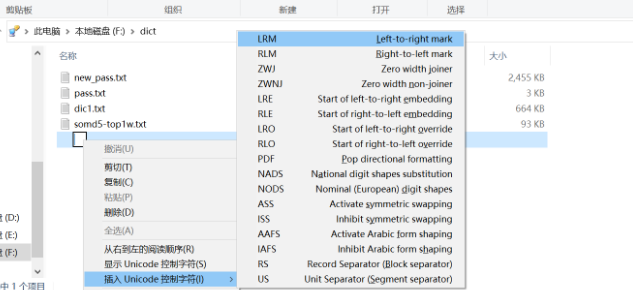
**查看方法：**

通过命令查看可发现该文件，利用ren对其进行重命名后，就可以还原文件。

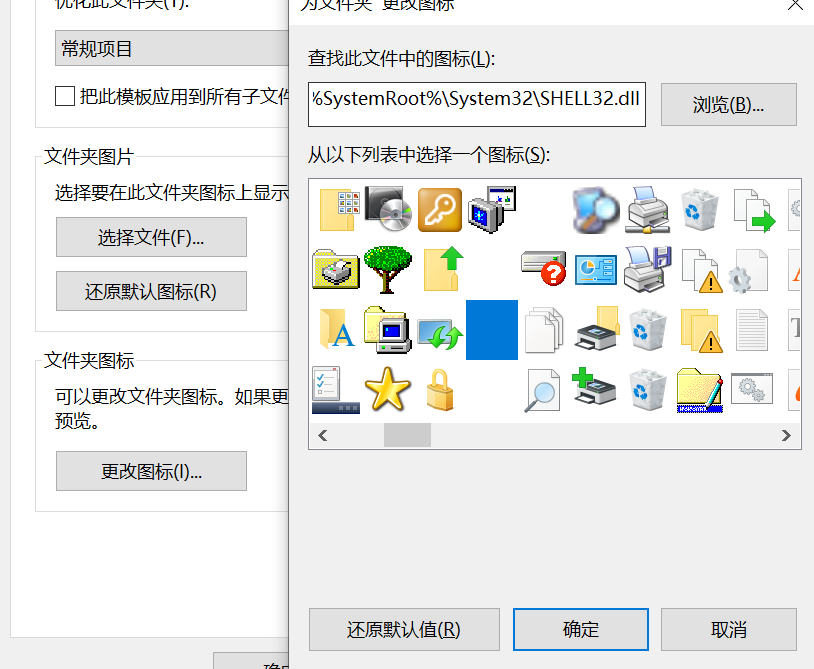


3、unicode重命名

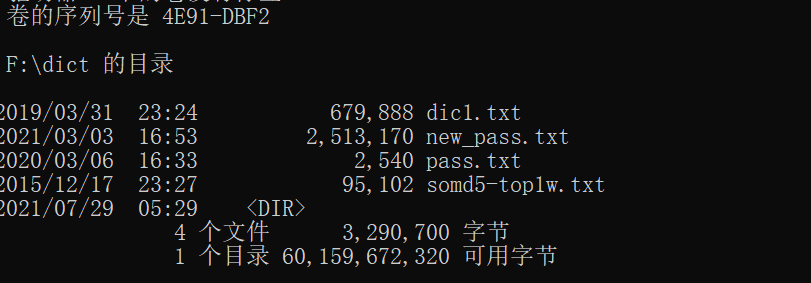
新建文件夹，重命名时选择插入unicode控制字符，即可删除该文件夹的名称



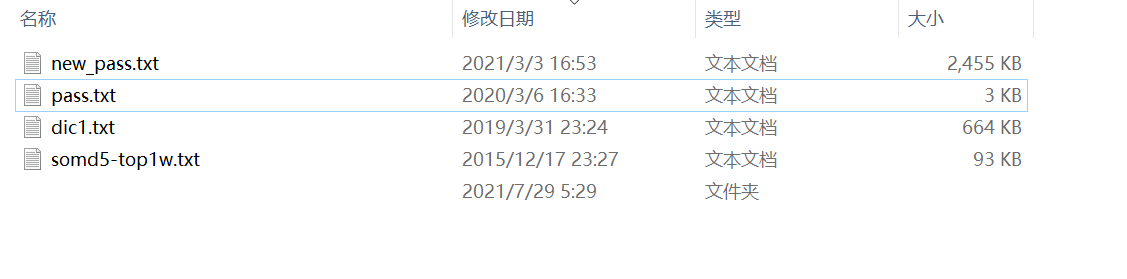
在将该文件夹替换的图标替换为透明图标，即可隐藏该文件夹



利用该方法在命令行下也无法发现



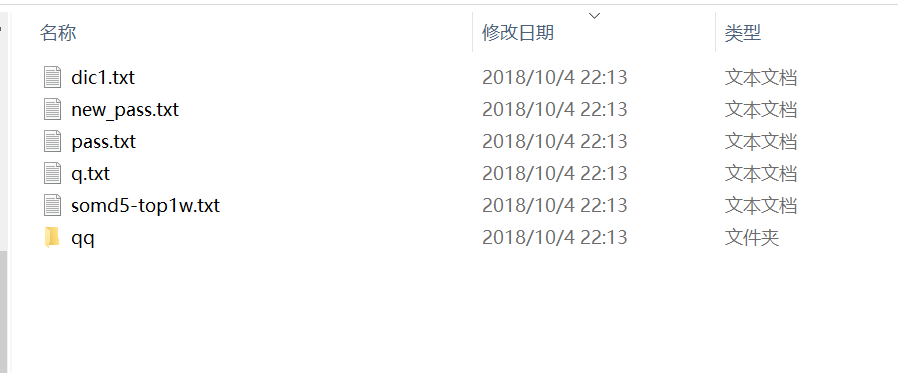
但是界面上仍然会存在修改日期、类型等相关信息



4、修改文件时间

为了更好的隐藏文件，需要修改文件创建时间，可利用powershell语句进行修改，利用此语句是将dict目录下文件创建时间以及修改时间，将时间改为2018年

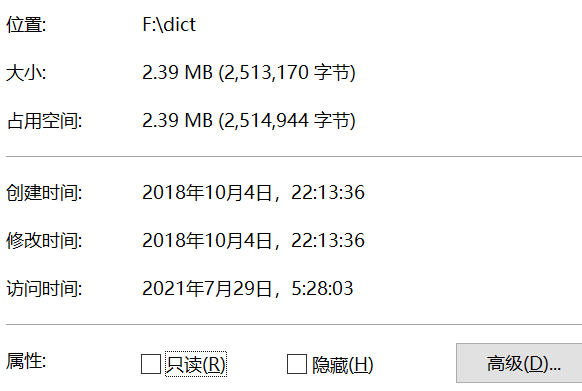
powershell.exe -command "Get-Childitem -path 'F:\dict\' -Recurse | foreach-object { $\_.LastWriteTime = '10/4/2018 22:13:36'; $\_.CreationTime = '10/4/2018 22:13:36' }"



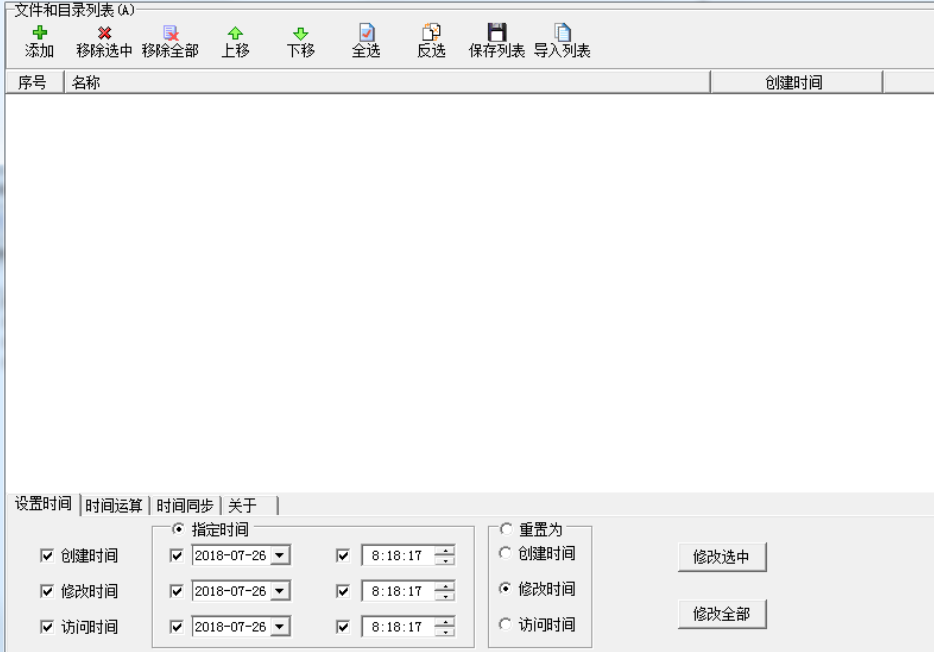
只修改某一文件的时间，如只是修改F盘下dict目录下的q.txt，可使用如下命令：

powershell.exe -command "ls 'F:\dict\q.txt' | foreach-object { $\_.LastWriteTime = '01/11/2004 22:13:36'; $\_.CreationTime = '01/11/2004 22:13:36' }"

利用这种方式修改的文件时间，只是修改了创建时间和修改时间，如果细心点会看到访问时间是没有修改的，可以采用FileTimeSync进行修改



FileTimeSync界面如下：



**查看方法：**

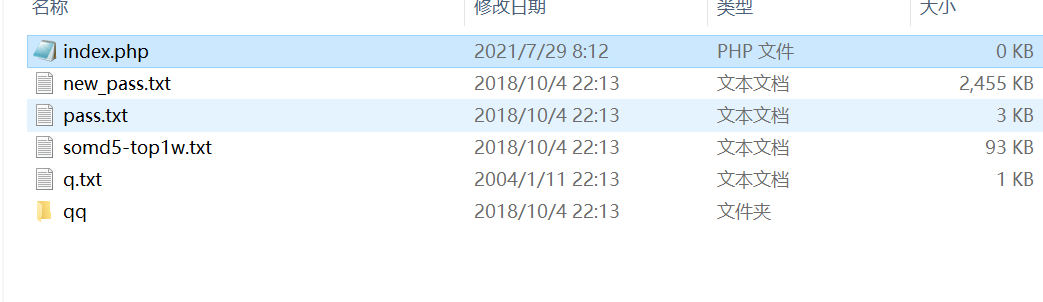
这种情况下就不大好去发现了，只能通过流量监测、进程查看去定位到该恶意文件。

5、ADS隐藏

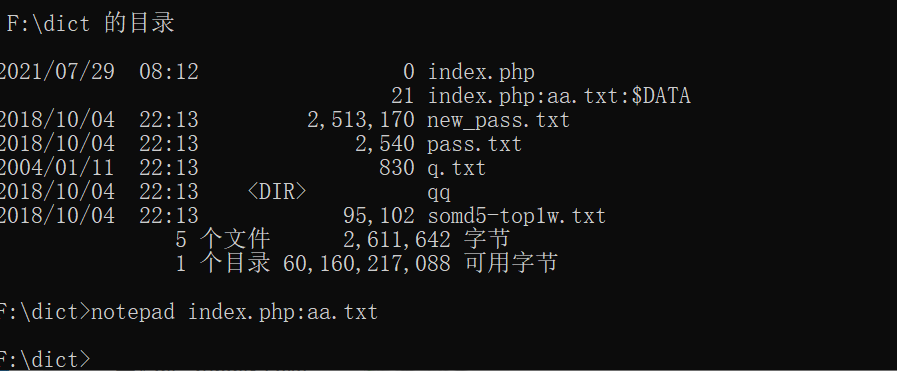
NTFS交换数据流（Alternate　Data　Streams，简称 ADS）是 NTFS 磁盘格式的一个特性，在 NTFS文件系统下，每个文件都可以存在多个数据流。利用该方法无法直接进行调用，需要配合文件包含去查看文件。利用ADS写入如下webshell

echo ^<?php phpinfo();?^> > index.php:aa.txt

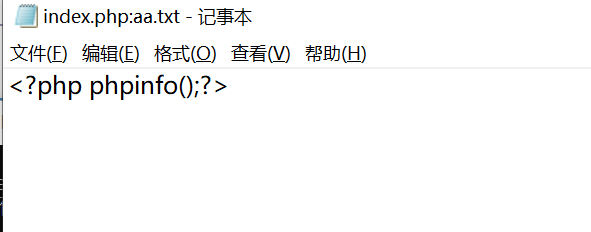
通过页面查看文件夹，显示数据大小为空



可以通过dir /r命令查看



打开文件内容为写入的一句话木马



再调用文件包含脚本test.php，内容如下，$a为文件名称的hex编码（<https://www.107000.com/T-Hex/>）696E6465782E7068703A61612E747874

<?php

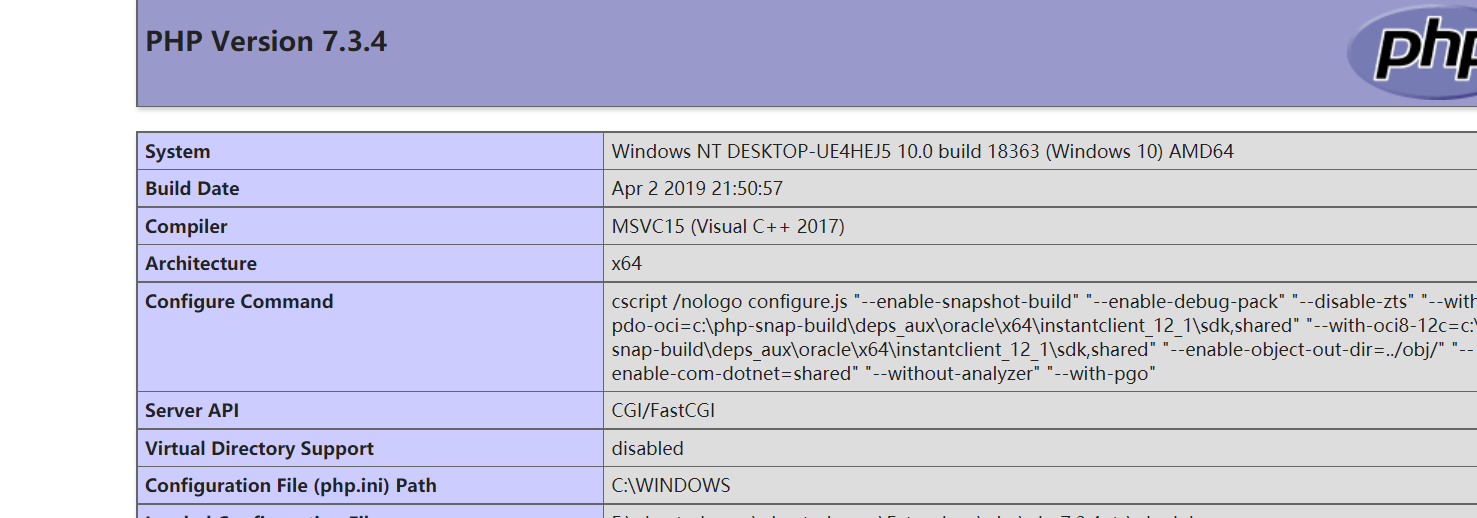
$a="696E6465782E7068"."703A61612E747874";

$b="a";

include(PACK('H\*',$$b))

?>

最终通过访问test.php即可查看phpinfo信息

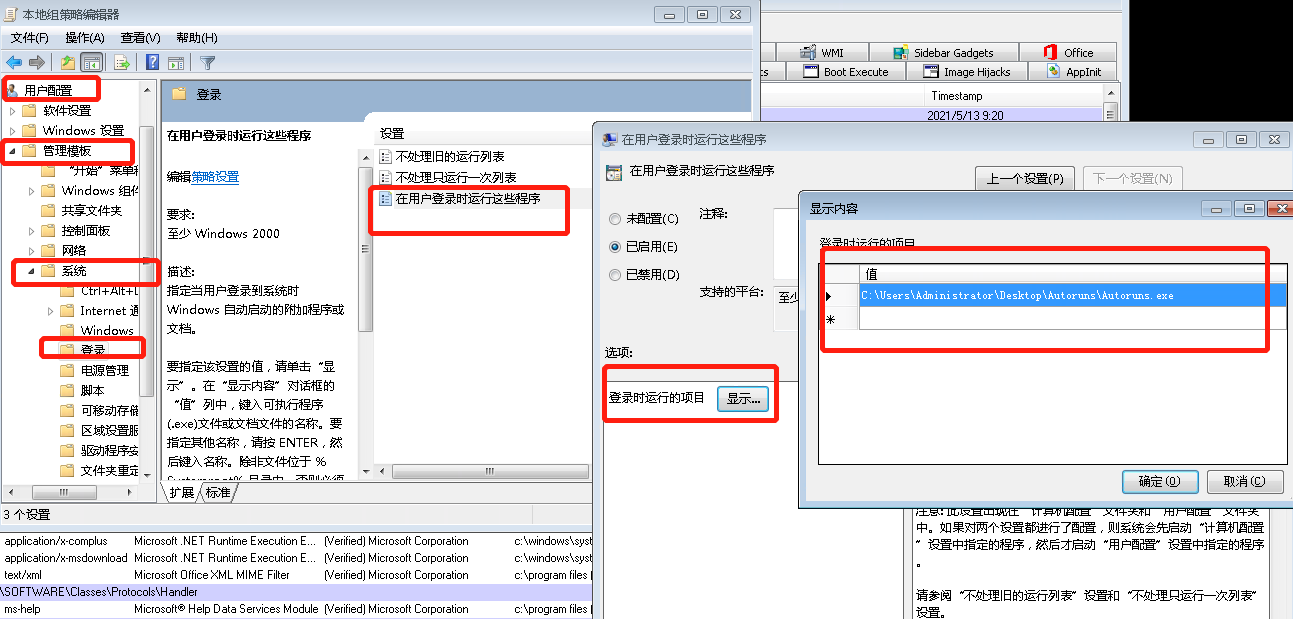


**查看方法：**

通过测试发现利用该方法，D盾无法扫描成功，此种方法较为隐蔽，可在命令行下利用dir /r查看，确定是否存在隐藏文件，也可通过异常进程、连接追踪到此文件。

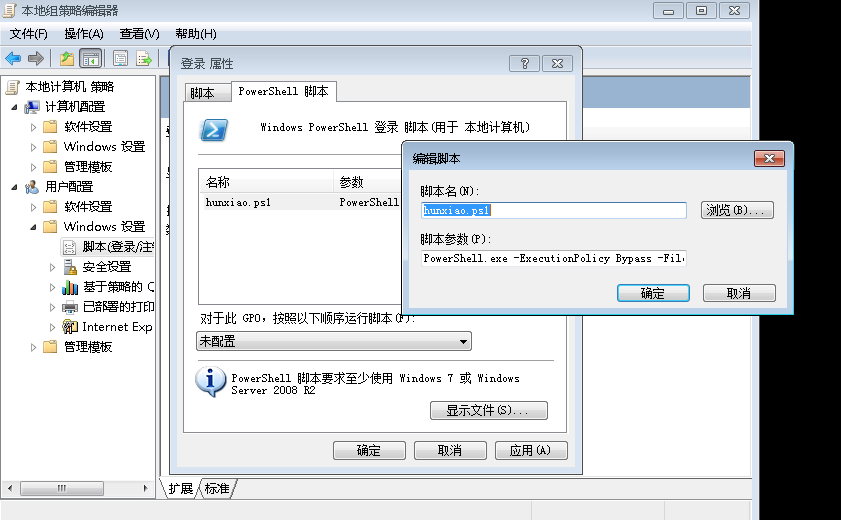
**三、开机启动项**

1、在“开始→运行”中键入“gpedit.msc”，启动“组策略”，展开“用户配置→管理模板→系统→登录”，启用“在用户登录时运行这些程序”项，并单击“显示”按钮，添加某个程序，重新登录后该程序就会自动运行

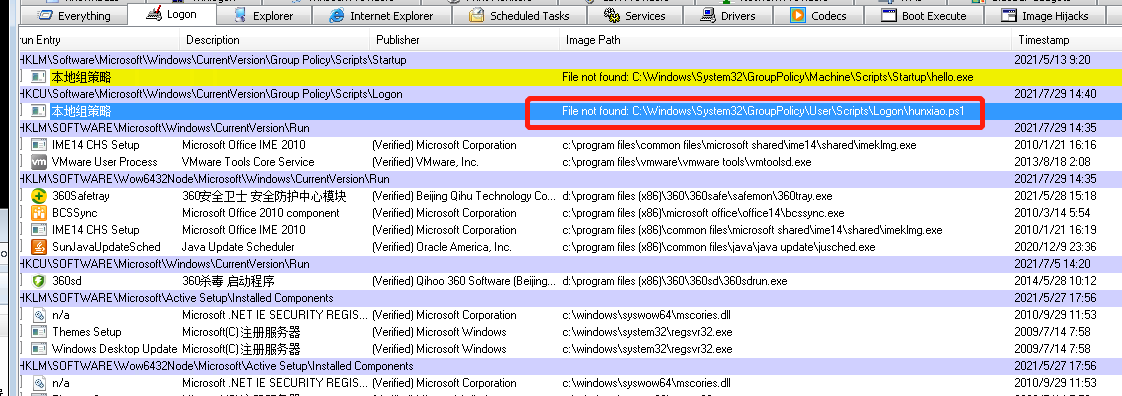


2、组策略设置脚本启动

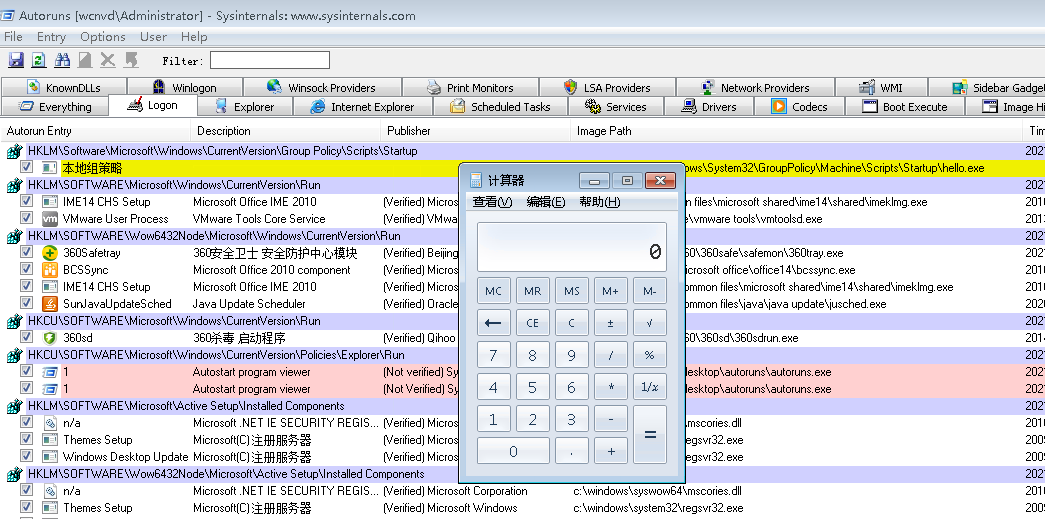
设置好后，等系统下次启动后，设置的脚本会自动运行，如下图设置powershell脚本自动运行



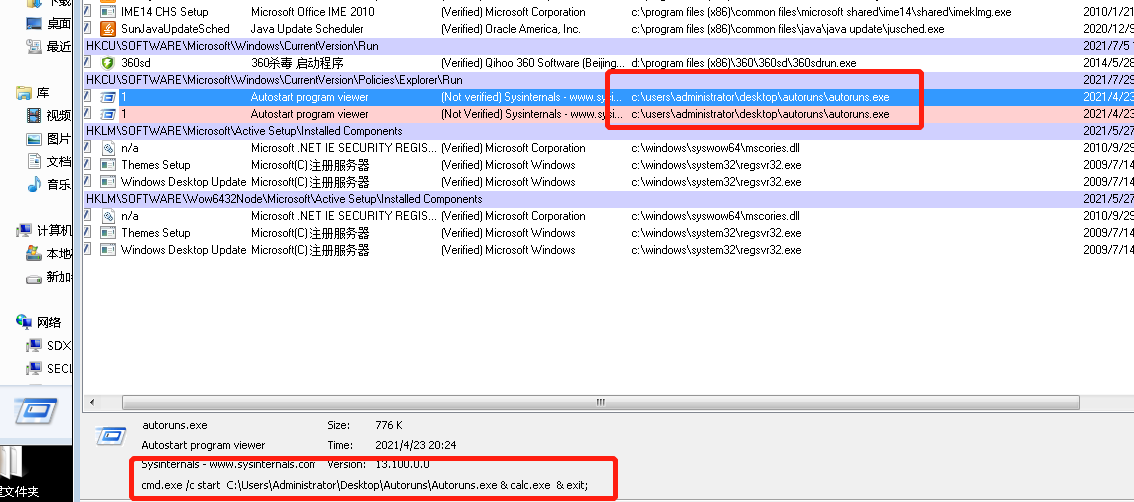
3、但是利用上述两种方法，如果直接将恶意文件加入启动项目容易被发现，利用Autoruns很容易发现启动的恶意文件，如下图



可以利用逻辑操作符&，将非法程序和合法程序连接在一起，例如在启动程序时，同时打开计算器，修改C:\UsersAdministrator\Desktop\Autoruns\Autoruns.exe为 cmd.exe /c start C:\UsersAdministrator\Desktop\Autoruns\Autoruns.exe & calc.exe &exit;



利用Autoruns.exe查看进程，无法发现异常进程，但是查看下面的详细信息，可发现连带的calc的启动项



但是当打开Autoruns”过滤Microsoft签名的程序“时，可将恶意程序绑定在微软关系的程序如rundll32.exe，这样就可以不显示相关信息，具体可参考如下文章

<https://m0nst3r.me/pentest/%E9%80%8F%E8%BF%87Autoruns%E7%9C%8B%E6%8C%81%E4%B9%85%E5%8C%96%E7%BB%95%E8%BF%87%E5%A7%BF%E5%8A%BF%E7%9A%84%E5%88%86%E4%BA%AB.html>

常见的开机启动项排查位置：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

**查看方法：**

建议安装杀毒软件，一般杀毒软件会重点关注开机启动项关键位置，也可配合Autoruns工具自行查看系统启动项，并且还要注意查看启动项详细信息，也能发现一些想不到的进程。

四、注册表后门

Windows提供了专门的开机自启动注册表。在每次开机完成后，它都会在这个注册表键下遍历键值，以获取键值中的程序路径，并创建进程启动程序。所以，要想修改注册表实现开机自启动，只需要在这个注册表键下添加想要设置自启动程序的程序路径就可以了。通过修改注册表自启动键值，添加一个木马程序路径，实现开机自启动，在存在杀软的情况下，修改注册表操作通常被拦截。

可利用如下命令修改注册表：

常用的注册表启动键：

# Run键

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

# Winlogon\Userinit键

HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

**查看方法：**

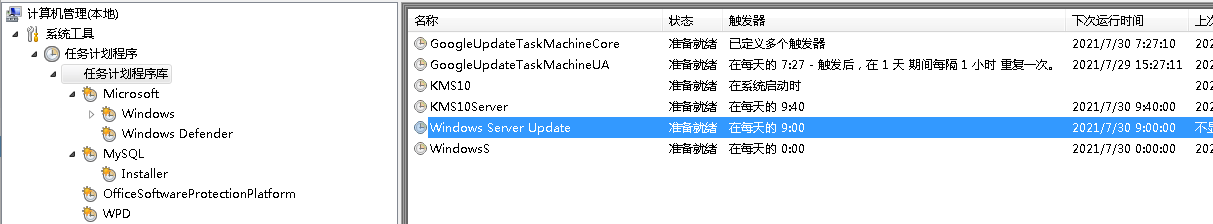
对常见的注册表位置进行查看，安装杀毒软件。

五、计划任务

通过window系统的任务计划程序功能实现定时启动某个任务，执行某个脚本。可利用如下命令创建任务计划名称为Windows Server Update，每天9点执行1.ps1

schtasks /create /RL HIGHEST /F /tn "Windows Server Update" /tr "PowerShell.exe -ExecutionPolicy Bypass -File 1.ps1" /sc DAILY /mo 1 /ST 09:00 /RU SYSTEM

可通过任务计划查看已经存在的任务计划，还可利用schtasks /query命令查看



**查看方法：**

查看任务计划是否存在异常计划。