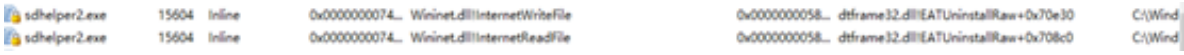
软件构成：

公司加密软件经过分析，是由两个模块组成：

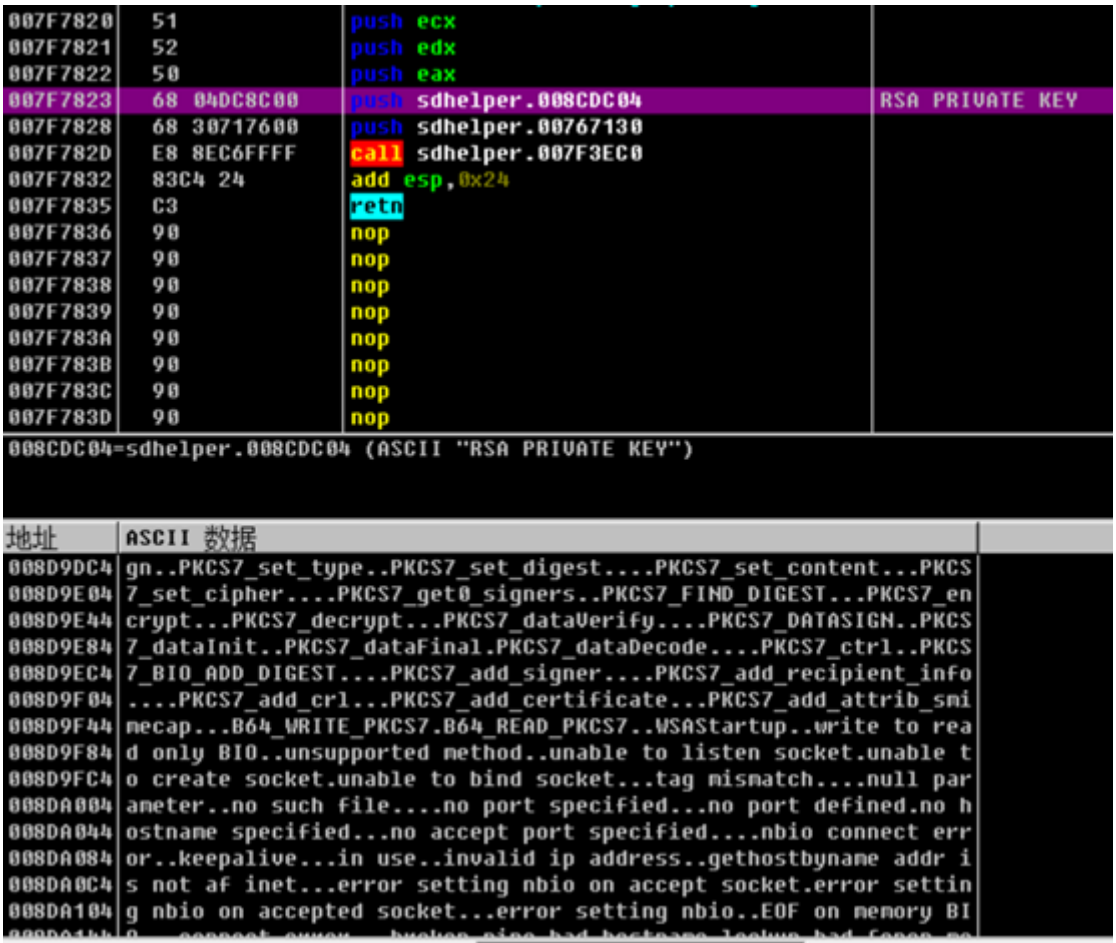
(1) 加密系统：加密系统一般都会遍历电脑所有的文档类文件(当然也包括规则的文件)，并且对其存储的数据进行可逆的加密，所以一般存储在文件里的数据实际上已经被改写过，前面提到的，加密系统本身是主动去遍历加密的，所以一旦我们在系统中产生了新文件，加密系统的模块均会主动去尝试对产生的新文件进行加密工作，由于遍历操作的存在，电脑的性能急剧下降。

(2) 解密系统：解密系统的机制，据我研究，其主要的技术应该是通过解密钩子来完成，原本在未安装加密软件系统上的执行流程为：文件->应用程序 变成为文件->解密模块->应用程序。解密系统模块使用钩子去拦截系统中所有读取文件的请求，然后由解密模块为代理去读取文件，将加密的文件解密后再转发给应用程序。

解密系统拦截读取文件如图：



解密系统的算法(可以看到不仅仅是只用RSA算法)



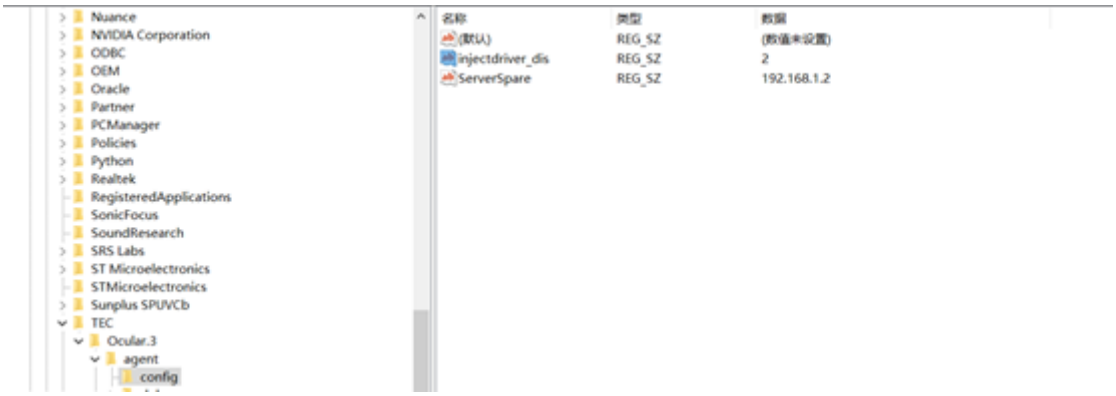
攻击

既然这个软件分为两个模块，那我们就只要把加密模块给弄掉，只留解密模块工作。

当然我在逆向加密模块的过程中，发现加密软件的配置信息位置：

```
push    20019h          ; phkResult
push    offset aSoftwareTecOcu ; "software\\TEC\\Ocular.3\\Agent\\config"
push    80000002h       ; hKey
lea     ecx, [esp+38h+var_14]
mov     [esp+38h+var_4], 0
call    sub_4434E0
```

打开注册表：

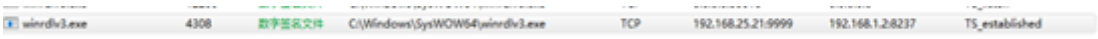


据分析应该192.168.1.2为文件服务器地址。

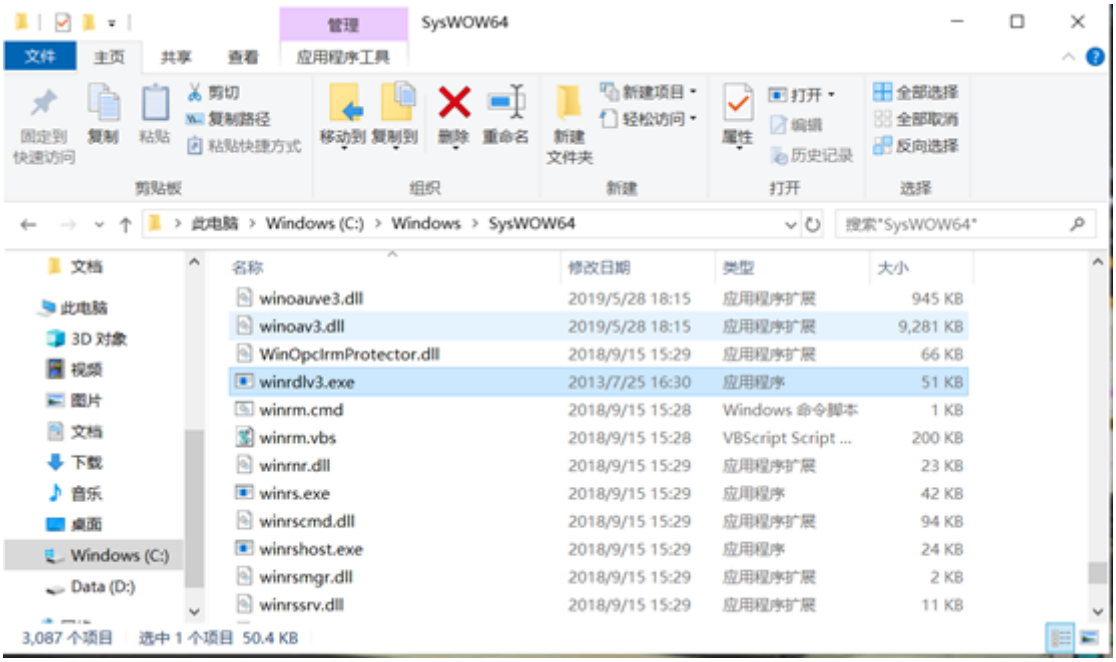
我们可以找到该加密系统的驱动

攻击1(此方法只能把加密软件给禁用，并不能阻止文档被加密)

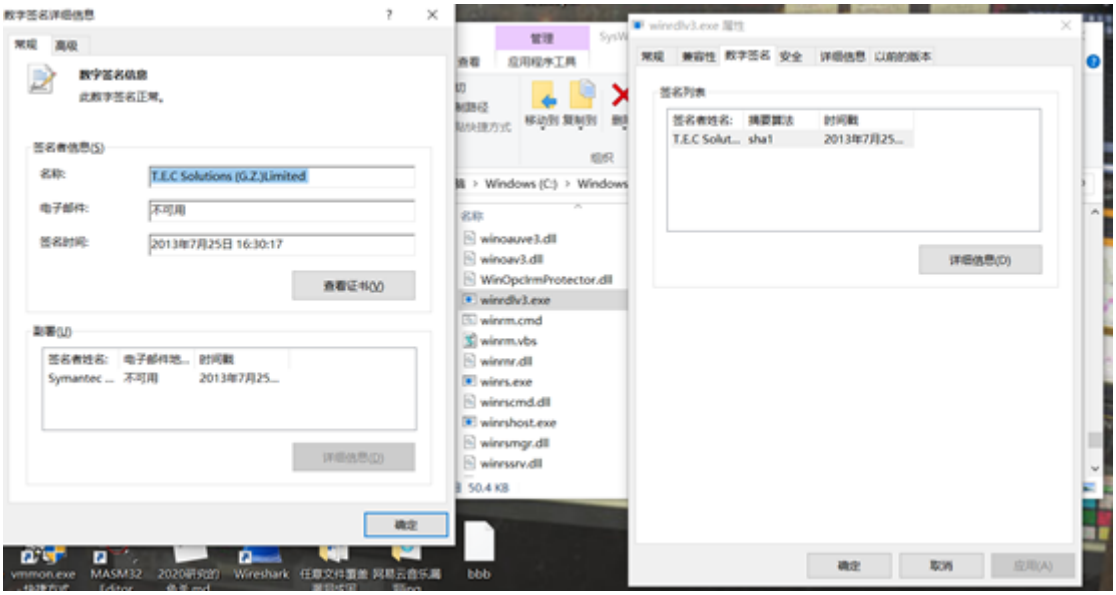
首先我们需要流量查看工具找到加密模块的进程;



在文件中找到:

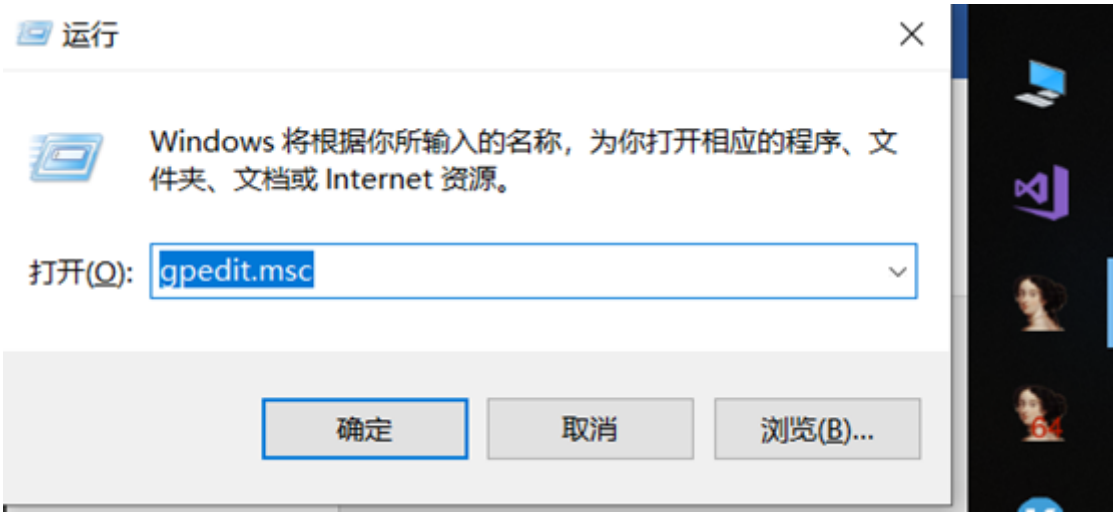


提取其签名:

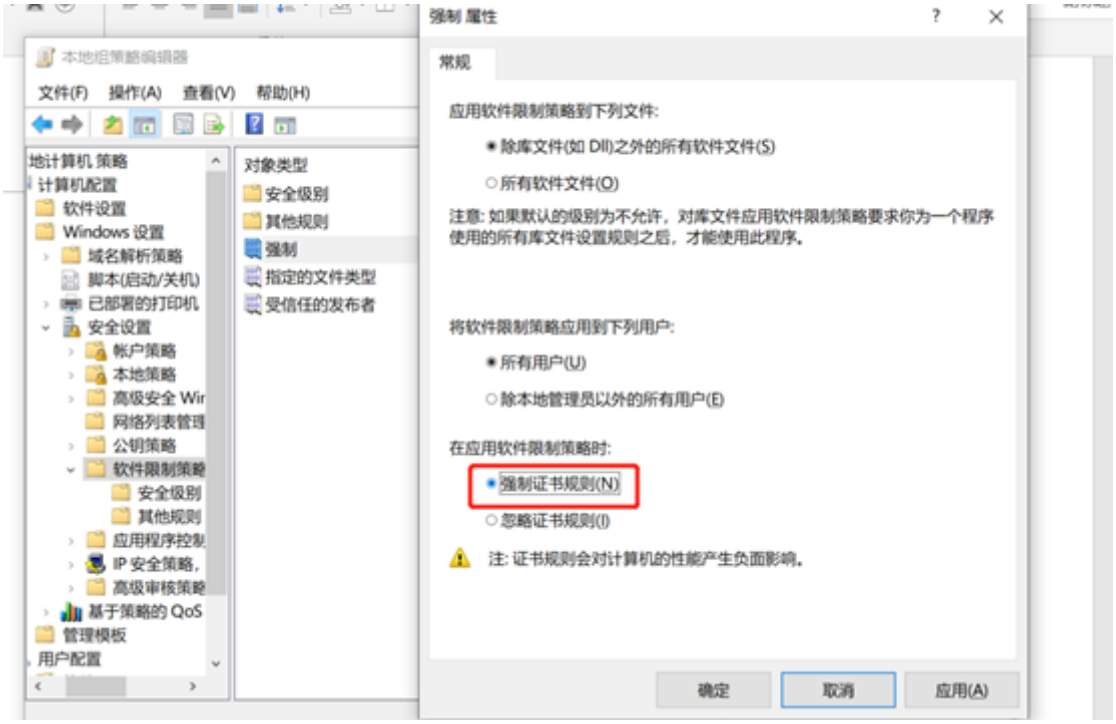


禁用其数字证书：

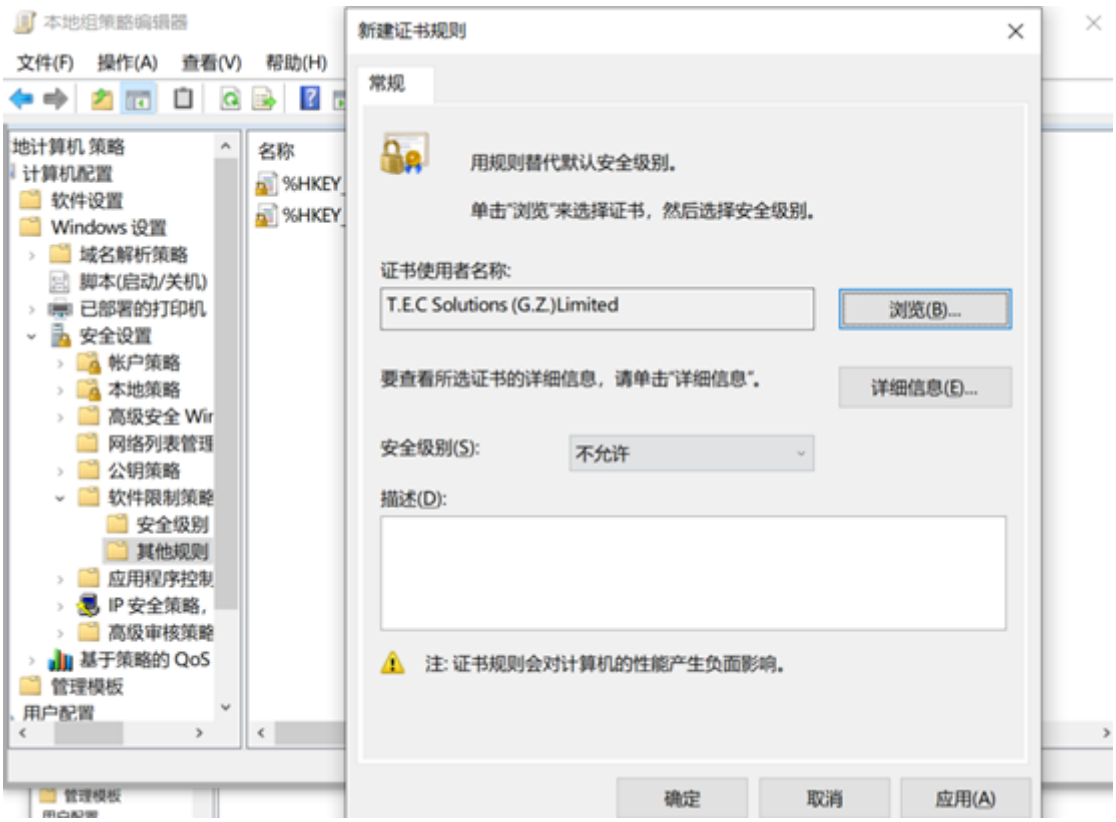
启动命令行:



创建新的软件策略:

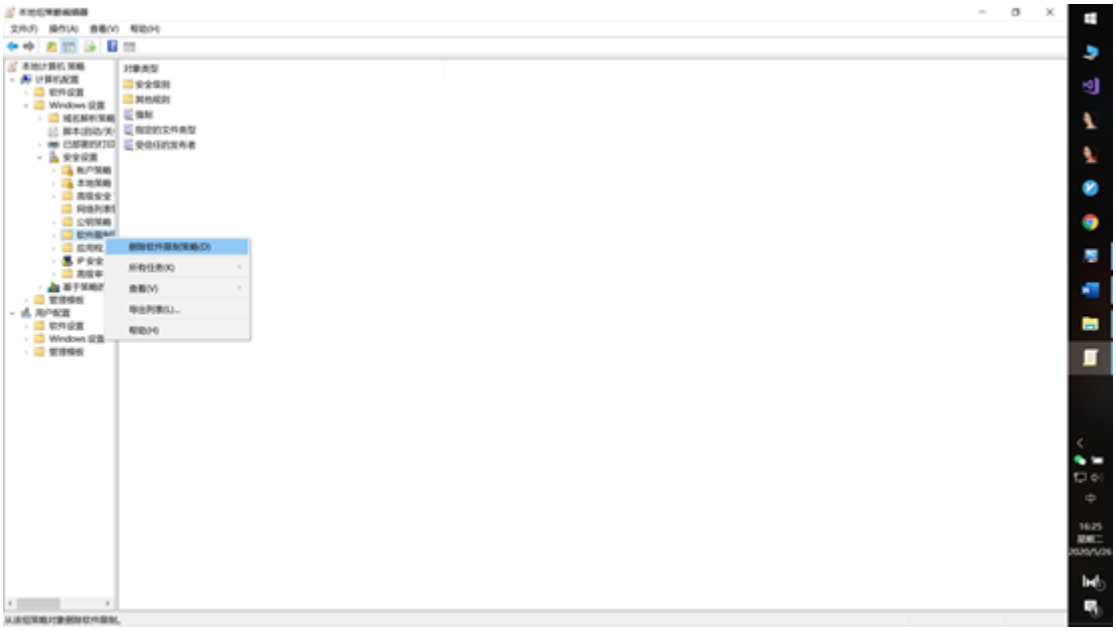


新建证书规则:



重启发现进程中不存在加密软件，右下角也没有图标:

需要恢复时，直接删除软件限制策略

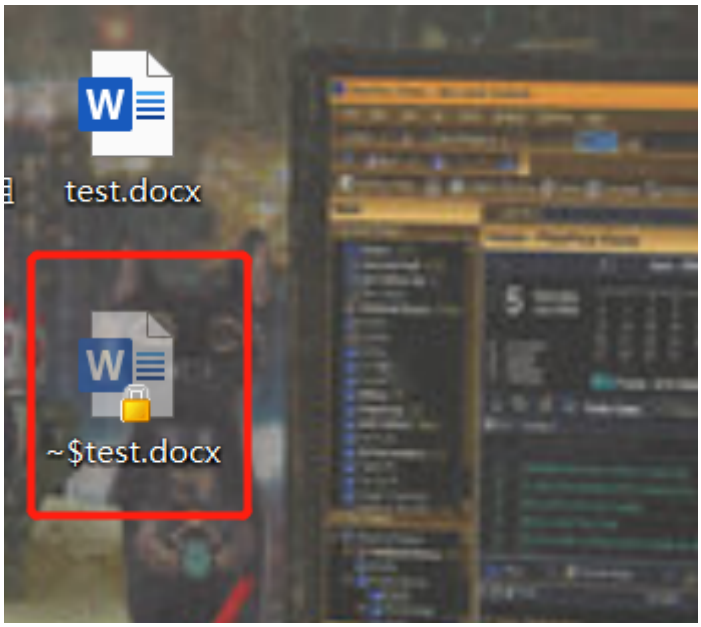


攻击方式二(有局限性)

注:此方法只能针对word、ppt等系列文档

首先，先把文件的隐藏项打开:

在编辑新的文档时，先不要着急保存，只需要删除红色框框的文件即可(注：每次保存过后此文件又会出现，需要重新删除)



攻击方式三(极端(终极卸载))

方法一:

将驱动删除

TsdEncrypt.sys	0xFFFFF807561B0000	0x000DA000	0xFFFFB9088681ABA0	C:\Windows\system32\drivers\TsdEncrypt.sys
THlpDrv64.sys	0xFFFFF80756150000	0x0000C000	0xFFFFB90886A68CB0	C:\Windows\System32\Drivers\THlpDrv64.sys
TIjtdrv64.sys	0xFFFFF80756E20000	0x00019000	0xFFFFB90886803880	C:\Windows\System32\Drivers\TIjtdrv64.sys

系统回调删除

0xFFFFF807561E9374	CreateProcess	C:\Windows\system32\drivers\TsdEncrypt.sys	TEC Solutions Limited.
0xFFFFF80756E28F14	CreateProcess	C:\Windows\System32\Drivers\TIjtdrv64.sys	TEC Solutions Limited.
0xFFFFF80756E28F7C	LoadImage	C:\Windows\System32\Drivers\TIjtdrv64.sys	TEC Solutions Limited.
0xFFFFF80756229D4C	Shutdown	C:\Windows\system32\drivers\TsdEncrypt.sys	TEC Solutions Limited.
0xFFFFF807562286E0	FsNotifyChange	C:\Windows\system32\drivers\TsdEncrypt.sys	TEC Solutions Limited.

把钩子全都卸载

0x000100F5	WH_GETMESSAGE	0x00000000000A250	winrdlv3.exe	7872	7620	C:\Windows\SysWOW64\winrdlv3.exe
0x000100F7	WH_KEYBOARD_LL	0x00000000000A020	winrdlv3.exe	7872	7620	C:\Windows\SysWOW64\winrdlv3.exe
0x00060115	WH_KEYBOARD	0x0000000000009800	winrdlv3.exe	8344	7688	C:\Windows\SysWOW64\winrdlv3.exe
0x000102DE	WH_GETMESSAGE	0x0000000000003720	winrdlv3.exe	9608	7688	C:\Windows\SysWOW64\winrdlv3.exe
0x00080731	WH_MOUSE	0x00000000000A170	winrdlv3.exe	8344	7688	C:\Windows\SysWOW64\winrdlv3.exe
0x00080739	WH_SYSMSGFILTER	0x0000000000009550	winrdlv3.exe	8344	7688	C:\Windows\SysWOW64\winrdlv3.exe
0x00040761	WH_GETMESSAGE	0x00000000000008F90	winrdlv3.exe	8344	7688	C:\Windows\SysWOW64\winrdlv3.exe
0x00060113	WH_SYSMSGFILTER	0x00000000000A200	winrdlv3.exe	8648	8552	C:\Windows\System32\winrdlv3.exe
0x00060117	WH_MOUSE	0x00000000000A3D0	winrdlv3.exe	8648	8552	C:\Windows\System32\winrdlv3.exe
0x00060119	WH_GETMESSAGE	0x00000000000A1A0	winrdlv3.exe	8648	8552	C:\Windows\System32\winrdlv3.exe
0x0001011F	WH_GETMESSAGE	0x00000000001466F90	winrdlv3.exe	8876	8552	C:\Windows\System32\winrdlv3.exe
0x00010121	WH_KEYBOARD_LL	0x0000000001332480	winrdlv3.exe	8876	8552	C:\Windows\System32\winrdlv3.exe
0x00020269	WH_GETMESSAGE	0x00000000000008470	winrdlv3.exe	10316	8552	C:\Windows\System32\winrdlv3.exe
0x00070741	WH_KEYBOARD	0x00000000000A260	winrdlv3.exe	8648	8552	C:\Windows\System32\winrdlv3.exe

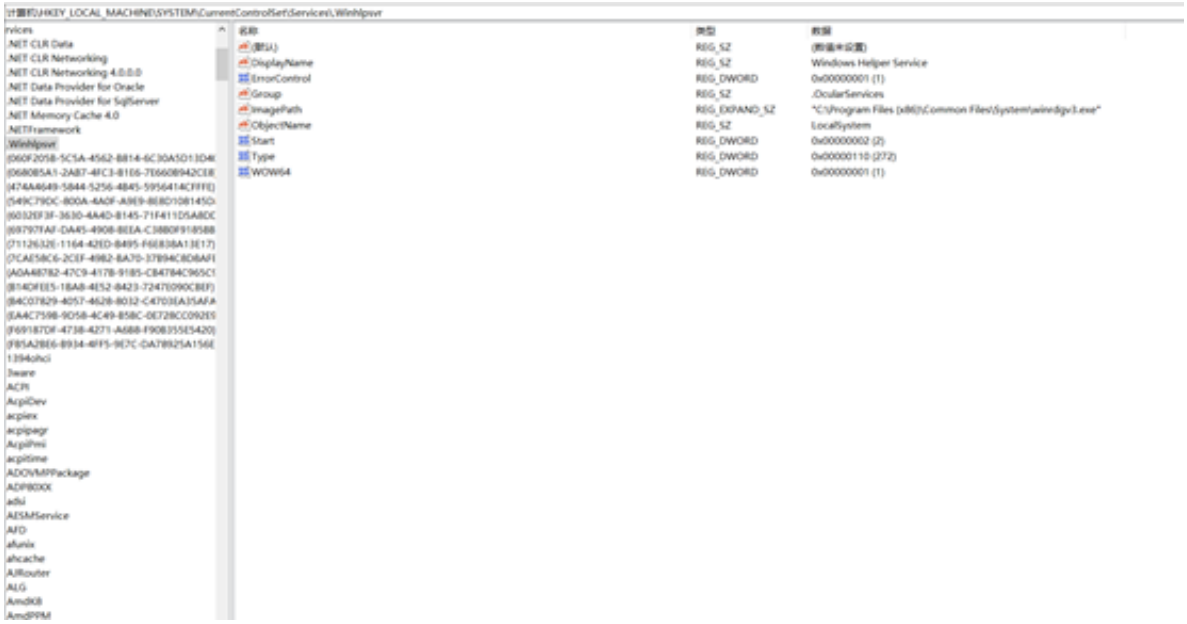
恢复inline

len(5) KERNEL32.DLL->CreateProcessA	0x0000000076A33CE0->_
len(5) KERNEL32.DLL->CreateProcessInternalW	0x0000000076A33D60->_
len(5) KERNEL32.DLL->CreateProcessW	0x0000000076A18BA0->_
len(5) KERNELBASE.dll->CreateProcessInternalW	0x000000007570A4E0->_
len(5) WS2_32.dll->accept	0x0000000074874AE0->_
len(5) WS2_32.dll->closesocket	0x000000007487EAC0->_
len(5) WS2_32.dll->connect	0x0000000074875650->_
len(5) WS2_32.dll->recv	0x0000000074881460->_
len(5) WS2_32.dll->recvfrom	0x0000000074874D50->_
len(5) WS2_32.dll->send	0x0000000074875750->_
len(5) WS2_32.dll->sendto	0x0000000074875550->_
len(5) WS2_32.dll->shutdown	0x00000000748808D0->_
len(5) WS2_32.dll->socket	0x000000007487BFA0->_
len(5) WS2_32.dll->GetAddrInfoExW	0x000000007487B420->_
len(5) WS2_32.dll->GetAddrInfoW	0x0000000074877B50->_
len(5) WS2_32.dll->WSAConnect	0x00000000748A3C20->_
len(5) WS2_32.dll->gethostbyname	0x000000007489DE30->_
len(5) WS2_32.dll->WSAGetOverlappedResult	0x0000000074886DC0->_
len(5) WS2_32.dll->WSAIoctl	0x000000007487EDD0->_
len(5) WS2_32.dll->WSARecv	0x000000007487E0C0->_
len(5) WS2_32.dll->WSASend	0x000000007487DDC0->_
len(5) Wininet.dll->HttpEndRequestA	0x00000000736DA520->_
len(5) Wininet.dll->HttpEndRequestW	0x00000000736DCBD0->_
len(5) Wininet.dll->HttpOpenRequestA	0x0000000073771FC0->_
len(5) Wininet.dll->HttpOpenRequestW	0x0000000073684B60->_
len(5) Wininet.dll->HttpQueryInfoA	0x000000007368DD80->_
len(5) Wininet.dll->HttpQueryInfoW	0x000000007368BD80->_
len(5) Wininet.dll->HttpSendRequestA	0x00000000736DAE40->_
len(5) Wininet.dll->HttpSendRequestExA	0x00000000736DCAA0->_
len(5) Wininet.dll->HttpSendRequestExW	0x00000000736D96B0->_
len(5) Wininet.dll->HttpSendRequestW	0x00000000736986A0->_
len(5) Wininet.dll->InternetCloseHandle	0x000000007368B410->_
len(5) Wininet.dll->InternetConnectA	0x0000000073747E40->_
len(5) Wininet.dll->InternetConnectW	0x000000007367C150->_
len(5) Wininet.dll->InternetReadFile	0x000000007368C090->_
len(5) Wininet.dll->InternetWriteFile	0x0000000073667830->_

把启动项删除

```
trmenushl64.dll(TRMenuShlExt)
trmenushl64.dll(TRMenuShlExt)
sdiskcontext64.dll(TSafeDiskContext)
sdcontext64.dll(TSafeDocContext)
sdcontext64.dll(TSafeDocContext)
```

把注册表中的数值改为0



方法二:

弄个PE系统，进入winPE之后：

1. 打开系统盘->右键->分组依据->更多->勾选(公司)->确定
2. 右键->分组依据->公司
3. 查看->选项->查看->应用到文件夹
4. 在C盘中找到所有公司为T.E.C.Solutions(G.Z)Limited的文件，删除

技术免责声明

本文仅作技术性研究.请酌情使用,由此引发的一系列后果请自行承担.

By:AhRMo