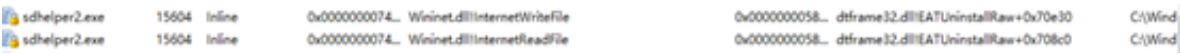


软件构成：

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 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)

007F7820	51	push ecx	
007F7821	52	push edx	
007F7822	50	push eax	
007F7823	68 04DC8C00	push sdhelper.008CDC04	RSA PRIVATE KEY
007F7828	68 30717600	push sdhelper.00767130	
007F782D	E8 8EC6FFFF	call sdhelper.007F3EC0	
007F7832	83C4 24	add esp,0x24	
007F7835	C3	ret	
007F7836	90	nop	
007F7837	90	nop	
007F7838	90	nop	
007F7839	90	nop	
007F783A	90	nop	
007F783B	90	nop	
007F783C	90	nop	
007F783D	90	nop	

008CDC04=sdhelper.008CDC04 (ASCII "RSA PRIVATE KEY")

地址	ASCII 数据
008D9DC4	gn..PKCS7_set_type..PKCS7_set_digest...PKCS7_set_content...PKCS
008D9E04	7_set_cipher...PKCS7_get0_signers..PKCS7_FIND_DIGEST...PKCS7_en
008D9E44	crypt...PKCS7_decrypt...PKCS7_dataVerify...PKCS7_DATASIGN..PKCS
008D9E84	7_dataInit..PKCS7_dataFinal.PKCS7_dataDecode...PKCS7_ctrl..PKCS
008D9EC4	7_BIO_ADD_DIGEST...PKCS7_add_signer...PKCS7_add_recipient_info
008D9F04	...PKCS7_add_crl...PKCS7_add_certificate...PKCS7_add_attrib_sni
008D9F44	meap...B64_WRITE_PKCS7.B64_READ_PKCS7..WSAStartup..write to rea
008D9F84	d only BIO..unsupported method..unable to listen socket.unable t
008D9FC4	o create socket.unable to bind socket...tag mismatch...null par
008DA004	ameter..no such file....no port specified...no port defined.no h
008DA044	ostname specified...no accept port specified...nbio connect err
008DA084	or..keepalive...in use..invalid ip address..gethostbyname addr i
008DA0C4	s not af inet...error setting nbio on accept socket.error settin
008DA104	g nbio on accepted socket...error setting nbio..EOF on memory BI
008DA144	o connect error...broken pipe had hostame lookup had connec

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。

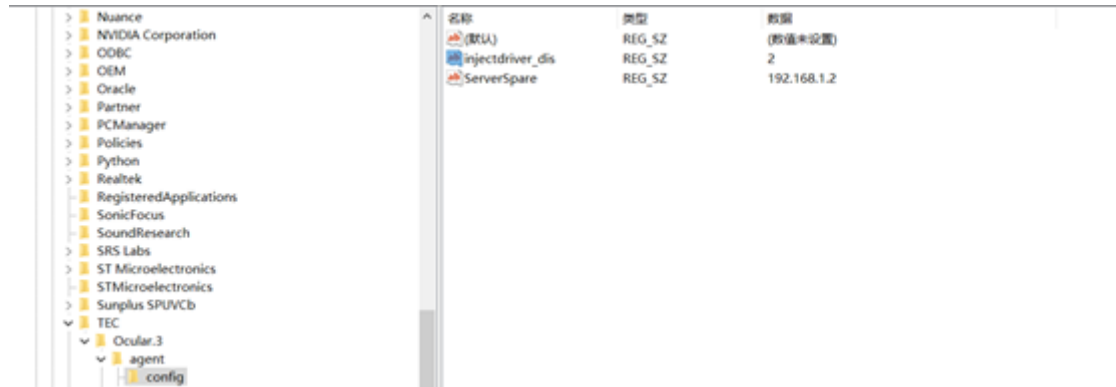
当然我在逆向加密模块的过程中，发现加密软件的配置信息位置：

```

push    20019h          ; phkResult
push    offset aSoftwareTec0cu ; "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

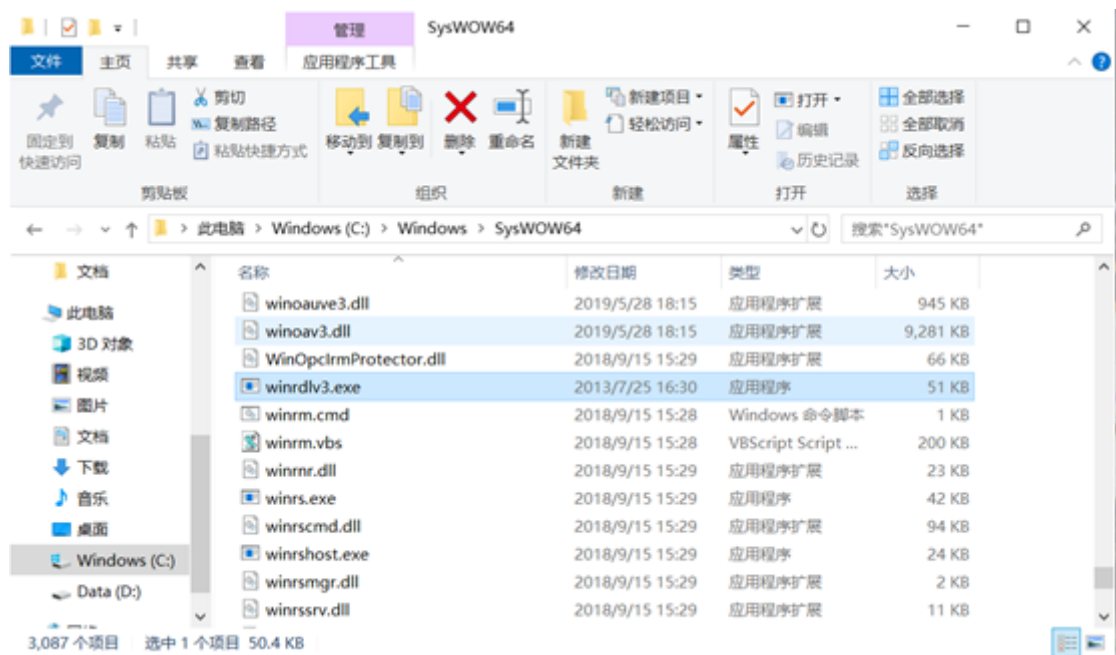
[DRV] \Driver\Tsfldrv	数字签名文件	0xFFFFBF02... C:\Windows\system32\drivers\Tsfldrv.sys	TEC Solutions Limited.	Ocular fs filter
[DRV] \Driver\ThlpDrv	数字签名文件	0xFFFFBF02... C:\Windows\System32\Drivers\ThlpDrv64.sys	TEC Solutions Limited.	Thelper Driver
[DRV] \Driver\Tjdrv	数字签名文件	0xFFFFBF02... C:\Windows\System32\Drivers\Tjdrv64.sys	TEC Solutions Limited.	Tjdrv.sys
[DRV] \Driver\TPacket7	数字签名文件	0xFFFFBF02... C:\Windows\system32\DRIVERS\TPacket7.sys	TEC Solutions Limited.	TPacket Network Driver
[DRV] \Driver\TsdEncrypt	数字签名文件	0xFFFFBF02... C:\Windows\system32\drivers\TsdEncrypt.sys	TEC Solutions Limited.	File System Filter Driver

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)

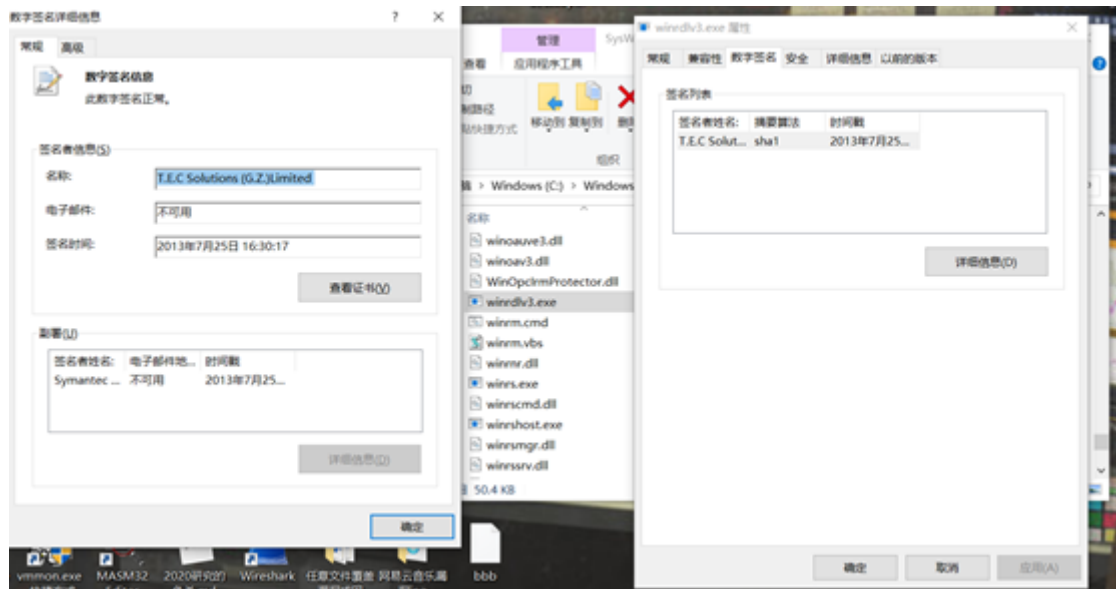
首先我们需要流量查看工具找到加密模块的进程：

winrdlv3.exe	4308	数字签名文件	C:\Windows\SysWOW64\winrdlv3.exe	TCP	192.168.25.21-9999	192.168.1.2:8237	TS_established
--------------	------	--------	----------------------------------	-----	--------------------	------------------	----------------

在文件中找到：

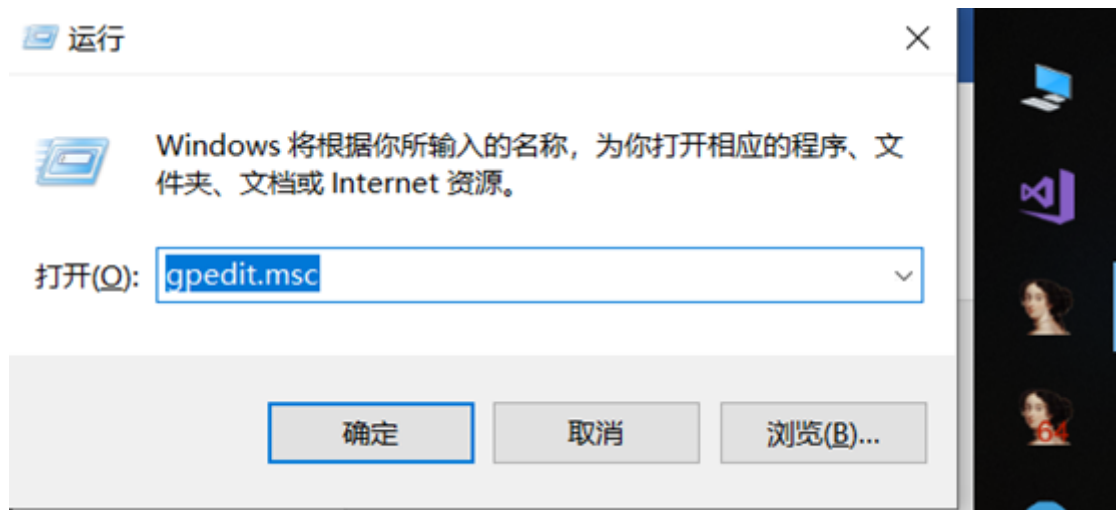


提取其签名：

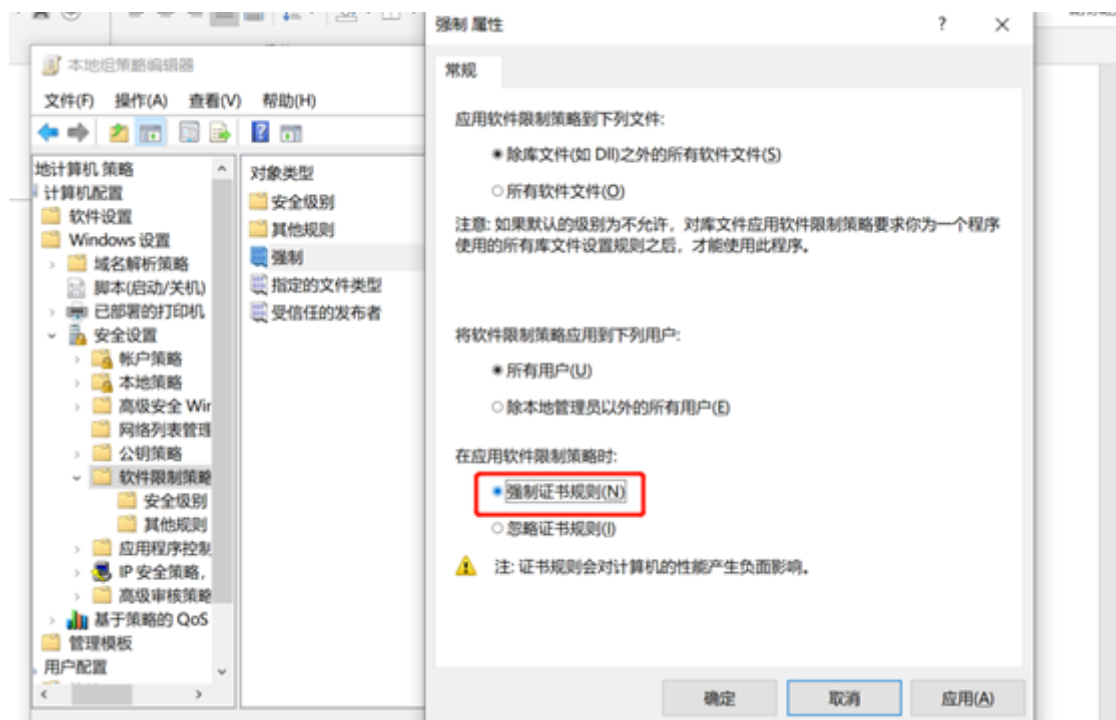


禁用其数字证书：

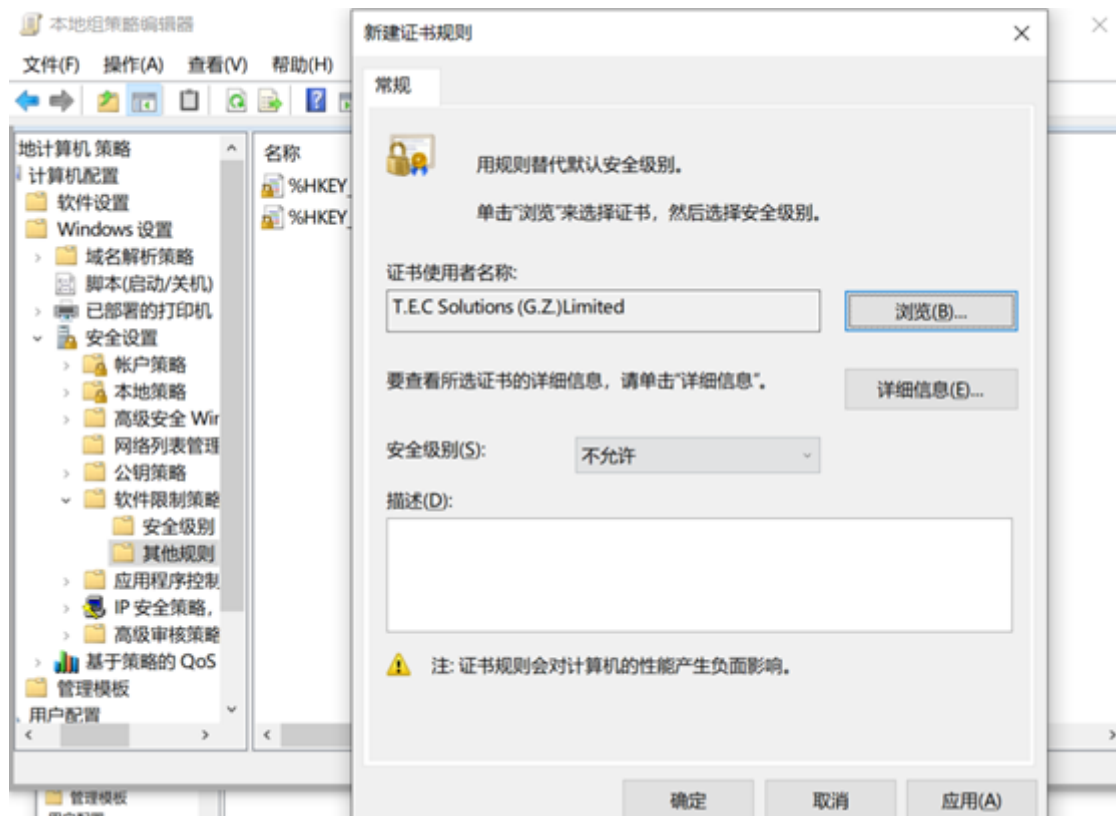
启动命令行：



创建新的软件策略：



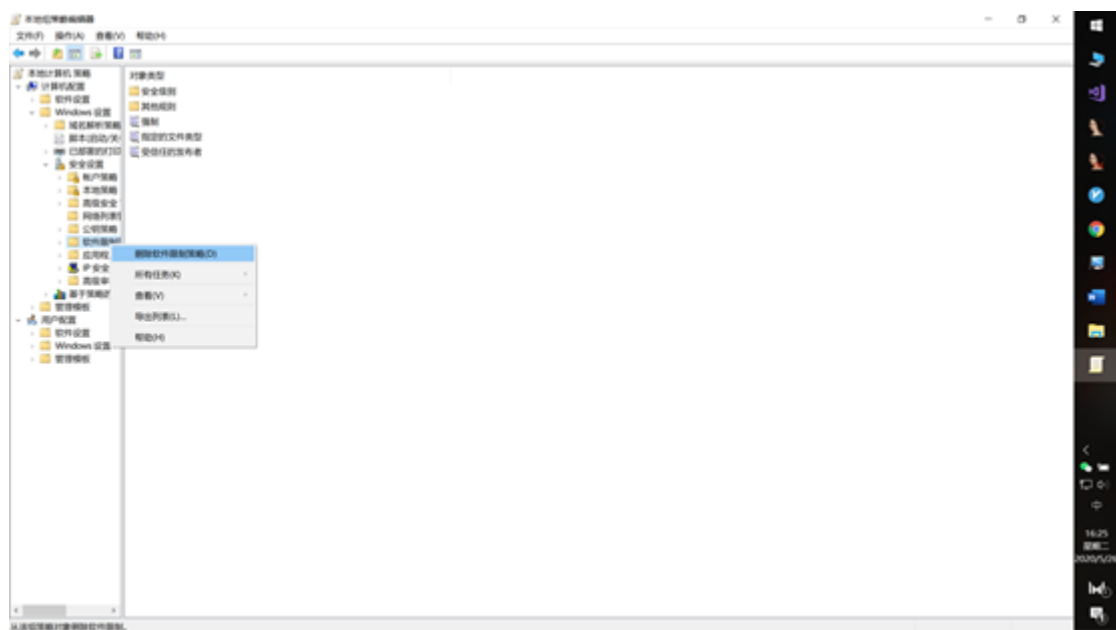
新建证书规则：



重启发现进程中不存在加密软件，右下角也没有图标:

winrdlv3.exe	6176	6176	TEC Solutions Limited.	Winrdlv3	C:\Windows\SysWOW64\winrdlv3.exe
winrdlv3.exe	8072	6176	TEC Solutions Limited.	Winrdlv3	C:\Windows\SysWOW64\winrdlv3.exe
winrdlv3.exe	8744	6176	TEC Solutions Limited.	Winrdlv3	C:\Windows\SysWOW64\winrdlv3.exe
winrdlv3.exe	9692	6176	TEC Solutions Limited.	Winrdlv3	C:\Windows\SysWOW64\winrdlv3.exe
winrdlv3.exe	8928	6176	TEC Solutions Limited.	Winrdlv3	C:\Windows\SysWOW64\winrdlv3.exe
ONacAgent.exe	8948	6176	TEC Solutions Limited.	ONacAgent	C:\Windows\SysWOW64\ONacAgent.exe
winrdlv3.exe	10184	6176	TEC Solutions Limited.	Winrdlv3	C:\Windows\SysWOW64\winrdlv3.exe
winrdlv3.exe	11288	6176	TEC Solutions Limited.	Winrdlv3	C:\Windows\System32\winrdlv3.exe
igfxEM.exe	7104	7104	Intel Corporation	igfxEM Module	C:\Windows\System32\DriverStore\...
explorer.exe	7740	0	Microsoft Corporation	Windows 资源管理器	C:\Windows\explorer.exe

需要恢复时，直接删除软件限制策略



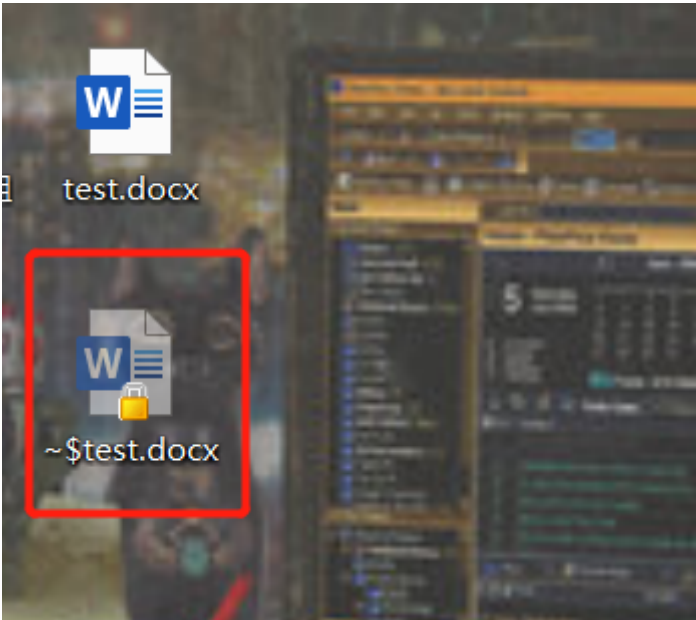
攻击方式二(有局限性)

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	0xFFFFF80756180000	0x000DA000	0xFFFFB9088681ABA0	C:\Windows\system32\drivers\TsdEncrypt.sys
THlpDrv64.sys	0xFFFFF80756150000	0x0000C000	0xFFFFB90886A68CB0	C:\Windows\System32\Drivers\THlpDrv64.sys
TJtdrv64.sys	0xFFFFF80756E20000	0x00019000	0xFFFFB90886803880	C:\Windows\System32\Drivers\TJtdrv64.sys

系统回调删除

0xFFFFF807561E9374	CreateProcess	C:\Windows\system32\drivers\TsdEncrypt.sys	TEC Solutions Limited.
0xFFFFF80756E28F14	CreateProcess	C:\Windows\System32\Drivers\TJtdrv64.sys	TEC Solutions Limited.
0xFFFFF80756E28F7C	LoadImage	C:\Windows\System32\Drivers\THlpDrv64.sys	TEC Solutions Limited.
0xFFFFF8075622904C	Shutdown	C:\Windows\system32\drivers\TsdEncrypt.sys	TEC Solutions Limited.
0xFFFFF807562286E0	FalselyChange	C:\Windows\system32\drivers\TsdEncrypt.sys	TEC Solutions Limited.

把钩子全都卸载

0x000100F5	WH_GETMESSAGE	0x000000000000A250	winrdv3.exe	7872	7620	C:\Windows\System32\winrdv3.exe
0x000100F7	WH_KEYBOARD_LL	0x000000000000A020	winrdv3.exe	7872	7620	C:\Windows\System32\winrdv3.exe
0x00060115	WH_KEYBOARD	0x0000000000000980	winrdv3.exe	8344	7688	C:\Windows\System32\winrdv3.exe
0x000102DE	WH_GETMESSAGE	0x0000000000003720	winrdv3.exe	9608	7688	C:\Windows\System32\winrdv3.exe
0x00080731	WH_MOUSE	0x000000000000A170	winrdv3.exe	8344	7688	C:\Windows\System32\winrdv3.exe
0x00080739	WH_SYSMSGFILTER	0x0000000000009950	winrdv3.exe	8344	7688	C:\Windows\System32\winrdv3.exe
0x00040761	WH_GETMESSAGE	0x0000000000009F90	winrdv3.exe	8344	7688	C:\Windows\System32\winrdv3.exe
0x00060113	WH_SYSMSGFILTER	0x000000000000A200	winrdv3.exe	8648	8552	C:\Windows\System32\winrdv3.exe
0x00060117	WH_MOUSE	0x000000000000A300	winrdv3.exe	8648	8552	C:\Windows\System32\winrdv3.exe
0x00060119	WH_GETMESSAGE	0x000000000000A1A0	winrdv3.exe	8648	8552	C:\Windows\System32\winrdv3.exe
0x0001011F	WH_GETMESSAGE	0x00000000000146F0	winrdv3.exe	8876	8552	C:\Windows\System32\winrdv3.exe
0x00010121	WH_KEYBOARD_LL	0x0000000000013240	winrdv3.exe	8876	8552	C:\Windows\System32\winrdv3.exe
0x00020269	WH_GETMESSAGE	0x0000000000000870	winrdv3.exe	10316	8552	C:\Windows\System32\winrdv3.exe
0x00070741	WH_KEYBOARD	0x000000000000A260	winrdv3.exe	8648	8552	C:\Windows\System32\winrdv3.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	0x0000000074878FA0->
len(5) WS2_32.dll->GetAddrInfoExW	0x0000000074878420->
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	0x0000000073684860->
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	0x00000000736D9680->
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

计算机\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Winlogon	名称	类型	数据
nvins			
NET CLR Data	Display	REG_SZ	(未设置)
NET CLR Networking 4.0.0.0	DisplayName	REG_SZ	Windows Helper Service
NET Data Provider for Oracle	ErrorControl	REG_DWORD	0x00000001 (1)
NET Data Provider for SqlServer	Group	REG_SZ	.OcularServices
NET Memory Cache 4.0	ImagePath	REG_DWORD	"C:\Program Files (x86)\Common-File\System\winlogon.exe"
NETFramework	ObjectName	REG_SZ	LocalSystem
Winlogon	Start	REG_DWORD	0x00000002 (2)
{00F2058-5C5A-4562-B814-6C3DA5D13D4E}	Type	REG_DWORD	0x00000110 (272)
{06085A1-2A87-4FC3-B106-7060B942C8E}	WOW64	REG_DWORD	0x00000001 (1)
{47AA4649-5844-5256-4845-595641ACFFFE}			
{549C790C-80DA-4A4F-A8B9-8E8D138145D}			
{6032F3F-3630-4A4D-B145-71F4112SAMDC}			
{69797AF-DA45-4908-BE1A-C3880F918588}			
{7112632E-1164-42ED-B495-F6E83A13E17}			
{7CAE58C6-2CE4-48B2-BA70-37B9AC8DBAF}			
{ADA8782-47C9-417B-9185-CB4784C965C1}			
{B14DFE5-1BA8-4E52-8423-7247090CBF}			
{B4C07829-4057-4628-B032-C4703A3A5AFA}			
{BAAC798B-9D58-4C4B-85BC-DE728CC092E}			
{B6F1870F-4738-4271-A6B8-F90B35E5420}			
{B8A28E6-8934-4F55-9E7C-DA7825A156E}			
1384dc6c			
lsass			
ACR			
AspDev			
acpiex			
acpiexgr			
AspHms			
acptime			
ADOXAIPackage			
ADP800K			
adsi			
AESMSERVICE			
AFO			
afunix			
afcache			
AIRouter			
ALG			
Amdb8			
AmdbPM			

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