# TsDefenseBt.sys分析报告

该驱动主要用于和各类竞品做对抗用，本文为2015.7.23版本的Tsdefensebt.sys的分析。该驱动使用TsFltMgr和TsSysKit提供的接口，和另外几个驱动一样存在验签名机制。

目录

[TsDefenseBt.sys分析报告 1](#_Toc437536305)

[一、 入口点 2](#_Toc437536306)

[Ntfs创建回调NtfsFsdCreateHooker： 2](#_Toc437536307)

[RegisterShutdown： 2](#_Toc437536308)

[ClearThread 2](#_Toc437536309)

[ShutdownDispatch： 3](#_Toc437536310)

[UnloadDispatch： 3](#_Toc437536311)

[CreateDispatch： 3](#_Toc437536312)

[CloseDispatch： 3](#_Toc437536313)

[IoCtlDispatch： 3](#_Toc437536314)

[删除360注册表项： 3](#_Toc437536315)

[解除baidu驱动回调： 6](#_Toc437536316)

[删除360快捷方式： 6](#_Toc437536317)

[删除360服务项： 6](#_Toc437536318)

[删除baidu注册表项： 7](#_Toc437536319)

[NtCreateProcessNotifyHooker1： 8](#_Toc437536320)

[NtSetValueKeyHooker： 9](#_Toc437536321)

[ZwRequestWaitReplyPortHooker/ZwAlpcSendWaitReceivePortHooker 9](#_Toc437536322)

[NtWriteVirtualMemoryHooker/NtCreateThreadHooker 9](#_Toc437536323)

[FakeObReferenceObjectByHandle 9](#_Toc437536324)

[CmCallback 10](#_Toc437536325)

## 入口点

1.设置ZwQueryValueKey的PrevFilter为ZwQueryValueKeyHooker

ZwQueryValueKeyHooker中拦截Service.exe对qqpcrtp服务的查询

2.检查HookPort, 360SelfProtection若存在则设置360存在标志位，baidu标志位默认设置为存在

若baidu存在，则解除baidu驱动进程创建、映像加载、线程创建回调

若360存在，则对TsDefensebt本身做ObOpenObjectByName的IAT hook，并记录iat信息(防止360 hook)，初始化360tray.exe, zhudongfangyu.exe, 360se.exe, 360chrome.exe, wscript.exe到进程id监视表

3.获取系统api真实地址

4.获取关机回调队列头

5.获取TsSyskit接口

6.设置UnloadDispatch,CreateDispatch,CloseDispatch,IoCtlDispatch,ShutdownDispatch

7.挂钩进程创建为NtCreateProcessNotifyHooker1，若360存在则挂钩NtSetValueKey为NtSetValueKeyHooker，挂钩ZwRequestWaitReplyPort为ZwRequestWaitReplyPortHooker，挂钩ZwAlpcSendWaitReceivePort为ZwAlpcSendWaitReceivePortHooker，挂钩ZwWriteVirtualMemory为ZwWriteVirtualMemoryHooker，挂钩ZwCreateThread为ZwCreateThreadHooker，挂钩ObReferenceObjectByHandle为FakeObReferenceObjectByHandle

8.注册注册表回调CmCallback

9.创建TSDFStategy设备，作为穿透驱动第二通道

10.保存TsDefenseBt映像起始地址处4096字节

若ShutdownTime被修改，若360存在则从SysOpt.ini删除指定的启动项，若baidu存在则删除服务项BDMWrench,BDArKit,BDSGRTP,BDMiniDlUpdate,bd0001,bd0002,bd0003,bd0004,BDDefense,BDEnhanceBoost,BDFileDefend,BDMNetMon,BDSafeBrower,BDSandBox,Bprotect,Bhbase,Bfmon,Bfilter

11.加密TsDefenseBt->DriverObject->DriverSection中存储的驱动路径

### Ntfs创建回调NtfsFsdCreateHooker：

若当前进程为360Tray.exe, Zhudongfangyu.exe, 360se.exe, 360chrome.exe, rundll32.exe, 360tray.exe，目标目录为

appdata\roaming\microsoft\windows\start menu\programs\startup,

\「开始」菜单\程序\启动,

\local settings\defend,

\local\defend,

且目标文件为.lnk后缀则拒绝

若当前进程为svchost.exe，目标目录为\360safe\则拒绝

若当前进程为explorer.exe或runonce.exe，目标路径为\360safe\且目标文件为.lnk .slnk .flnk .plnk .zlnk .xlnk .qlnk .qqlnk则拒绝

若当前进程为360tray.exe或zhudongfangyu.exe，目标路径为\360safe\且目标文件为.lnk .slnk .flnk .plnk .zlnk .xlnk .qlnk .qqlnk则拒绝；目标匹配

\\*\WINDOWS\TEMP\\*.EXE,

\\*\LOCAL SETTINGS\TEMP\\*.EXE,

\\*\LOCAL\TEMP\\*.EXE,

\\*\LOCAL\*\F9\\*.EXE,

\\*\APPDATA\SAFERUN\\*.EXE\\*\APPDATA\\*\\*.EXE\*\PROGRAMDATA\\*\\*.EXE

则拒绝

若当前进程为cmd.exe 360se.exe wscript.exe 360chrome.exe，且目标文件为360tray.exe zhudongfangyu.exe则拒绝

### RegisterShutdown：

重置TsDefenseBt关机回调

若发现ShutdownTime被修改则执行ClearThread

将\Driver\WMIxWDM,\Driver\mountmgr,\FileSystem\RAW,\Driver\volmgr,\Driver\ksecdd,\Driver\BDArKit关机回调置无效

设置注册表[\\Registry\\Machine\\System\\CurrentControlSet\\Control\\Windows](file:///\\Registry\\Machine\\System\\CurrentControlSet\\Control\\Windows)键回调为RegisterShutdown

### ClearThread

若360存在则清除SysOpt.ini指定的启动项

删除baidu注册表项

### ShutdownDispatch：

打开360文件

\safemon\safeloader.exe,

\safemon\BAK\_safeloader.exe,

\safemon\ok\_safeloader.exe,

\safemon\zz\_safeloader.exe,

\safemon\agesafe.exe,

\safemon\sssafefix.exe,

\safemon\safe505.exe并存储句柄

创建ClearThread线程

删除360注册表项

删除360快捷方式(文件和注册表)

删除360服务项

删除baidu注册表项

### UnloadDispatch：

删除ZwQueryValueKey的PrevFilter

### CreateDispatch：

检查进程是否处于监视列表

检查进程是否为Ts文件，并加入监视列表

### CloseDispatch：

无

### IoCtlDispatch：

IoCtlCode= 0x222044 TSDFStategy 记录文件注册表(加密)数据用于增删查改

IoCtlCode= 0x222048 文件、注册表穿透操作新通道

IoCtlCode= 0x222054|0x222058 穿透加载驱动新通道

IoCtlCode= 0x222014 设置开自保

IoCtlCode= 0x222004 用于同步

IoCtlCode= 0x222028| 0x22202C 设置注册表服务项标识位

IoCtlCode= 0x222030 设置关自保

### 删除360注册表项：

删除

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

\Registry\Machine\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

\Registry\Machine\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\RunOnce

和\Registry\User下每个用户的

\Software\Microsoft\Windows\CurrentVersion\Run

\Software\Microsoft\Windows\CurrentVersion\RunOnce

\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\RunOnce

下的键：

Fix360Safe

"{7B03EE23-306B-47a7-B9A5-4B4783FBB2A6}"

"{7A03EE23-306B-47a7-B9A5-4B4783FBB2A6}"

Repair360Safe

360安全卫士应急修复

360Safe安全卫士应急修复

360应急修复程序

360SafeEmergencyRepair

Safe安全卫士应急修复

360卫士自我修复程序

应急修复360卫士程序

360卫士用户应急自修复程序

360卫士应急自修复程序

360卫士应急自修复程序7896

360安全卫士应急修复工具

360安全卫士异常修复工具

360卫士异常修复工具

360卫士异常应急修复工具

360卫士异常应急修复程序

360卫士异常应急修复服务程序

360卫士应急修复服务程序

360卫士应急修复服务工具

360安全卫士应急修复服务工具

360安全卫士异常应急修复服务工具

360安全卫士异常应急修复服务程序

360安全卫士修复服务工具

360安全卫士修复服务工具7787

3-6-0安全卫士-异常应急修复-Fix2

3-6-0-F-i-x-3

360卫士异常应急修复服务程序7xi

360卫士异常应急修复服务程序Ok

360卫士-异常应急修复服务程序

卫士-修复程序

360-卫士-修复程序

卫士-360-修复

360-Tray-修复

tray-360-修复

修复-tray-360

卫士安全修复应急

卫士修复安全应急

修复安全卫士应急

异常安全卫士应急修复

360安全卫士应急修复异常组件程序

"My360Helper"

"MyDefend360"

"36ORepair"

"Safe360Tray"

"360Safe360TrayFix"

"360SafeTrayFix"

"360SafeTrayFix123"

"360SafeTrayFix1"

"360SafeTrayFix2"

"Rep36O"

"Rep36Osafes"

"Rep36OFixsafe"

"360SafeTrayFix3"

"Defend360TrayFix"

"360Safe\_TrayFix"

"36OFix\_360safe"

"36OFix\_360safe1"

"36OFix\_safe"

"3 6 0 F i x"

"3 6 O F i x"

"3-6-O-F-i-x"

"3-6-0 F-i-x"

"36 0 Fi x"

"36 0 F i-x"

"360-Fi-x"

"-360Fix-"

"-3 6-0 F-i x-"

"-3-6-0 F-i x-"

"-3-6-0F-i x-"

"3-6-0-Fix-0"

"360fiix\_69"

"360fiix\_419"

"fixfixfixfix"

"QFiPCTray"

"QFiPCTray\_1"

"PCTray360"

"PCFTray360"

"OKJPCTray"

"sdCFTrayJHSDSDF"

"TrayFixSVC"

"Traydsfsdffs"

"FTrayPCsss"

"120FTray"

"361FTray"

"361FTrayFix"

"GFFsFTray"

"s1aGFFsFTray"

"31aGFFsFTray"

"31FixQFTray"

"FwwwixQFTray"

"DdFFdOTA"

"AlchemistFAA"

"BearFixAW"

"DestroyerUHSFSS"

"AxeWUDIZHAN"

"spiderManSAD"

"BaneZhiYuan"

"ursaXiongZi"

"BMShouWangZ"

"gondarSanJin"

"KunkkaChuanZhang"

"Azwraithnver"

和项：

"360\_FIX\*"

"360FIX\*"

"3-60FIX\*"

"360FIIX\*"

"QFIPCTRAY\*"

删除\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{FC6354A7-BACD-47C3-A989-312F7FADA3E2}\LocalServer32

删除TSDFStategy指定的键值

### 解除baidu驱动回调：

分别对\Driver\BDMWrench,\Driver\BDArKit,\Driver\bd0001,\Driver\bd0002,\FileSystem\bd0003,

\Driver\bd0004,\Driver\BdSandBox,\Driver\BDMNetMon几个驱动，从映像起始地址处4096字节范围内，以1为步长的4096个地址，做摘除进程回调、映像加载回调、线程回调操作

### 删除360快捷方式：

删除\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup键，以及\Registry\User下每个用户\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellFolders, Startup键 (lnk文件及注册表)：

\safe505.lnk

\safeFY.lnk

\FYFY.lnk

\OKFOU.lnk

\OKFix.lnk

\OKZFix.lnk

\OKAgeFix.lnk

\sssafeFix.lnk

\SafeFix360.lnk

\ss360safeFix.lnk

\yy360safeFix.lnk

\Fixs360safeFix.lnk

\FixMy360safe.lnk

\MyFix360safe.lnk

\ProFixSafe.lnk

\DoFix360Safe.lnk

\RunHelper60safe.lnk

\360

\360safe.lnk

\360trayfix.lnk

\360

\360safe505Fixs.lnk

\360safe110Fixs.lnk

\safe505110Fixs.lnk

### 删除360服务项：

360FixSvc

3600FixSvc

360SFixSvc

Fix360SafeService

SafeFix

360XFixSvc

Fix360Service

360FixService

360FixSafe

FixSafeService

RepairSafezage

360csvcsFix

360Fixcsvcs

360ServiceFixs

360SafeFixService

360SafeFixOk

360Fix360Safe

360Fix360tray

Fix360trayService

360Fix360trayService

360Fix360trayServices

360Fix360trayServicess

360Fix360trayFix

360trayFixService

360trayFixsSvc

360trayFixsSvcx

360trayRunFix

360trayRunFixs

360traysRunFix

360sRunFix

360ssxxaRunFix

360stxaFix

FixSafe360

FixsvcSafe360

FixsvcServiceSafe360

FixServiceSafe360tary

FixSafe360taryServices

505Fix360Safe

505360Safe

repair505

505repair

saferepair

repairtray

repair360

startrep

SoS360Safe

S0S360Safe

360Sos

36OSosSafe

36OOKS0SSafe

360OKS0SSafe

3600KSOSSafe

36O0OKSOSafe

36000KSOSSafe

36000OKSOSSafe

36O00OKSOSSafe

36O00OsKSOSSafe

36O0OOKSOSSafe

36O00OsKSOSSafe

3605050Safe

36OSOSFixSafe

### 删除baidu注册表项：

"BDMWrench"

"BDArKit"

"BDSGRTP"

"BDMiniDlUpdate"

"bd0001"

"bd0002"

"bd0003"

"bd0004"

"BDDefense"

"BDEnhanceBoost"

"BDFileDefend"

"BDMNetMon"

"BDSafeBrower"

"BDSandBox"

"Bprotect"

"Bhbase"

"Bfmon"

"Bfilter"

### NtCreateProcessNotifyHooker1：

若当前进程为360tray.exe, zhudongfangyu.exe, 360se.exe, 360chrome.exe, wscript.exe则添加到进程id监视表safemonfilehandle

若360存在，且目标进程为\SystemRoot\system32\sc.exe或\SystemRoot\system32\rundll32.exe则添加到监视列表

若目标进程为explorer.exe且当前进程为Userinit.exe或Taskmgr.exe则删除进程id监视表safemonfilehandle

若目标文件为Userinit.exe，则打开360文件\safemon\safeloader.exe, \safemon\BAK\_safeloader.exe, \safemon\ok\_safeloader.exe, \safemon\zz\_safeloader.exe, \safemon\agesafe.exe, \safemon\sssafefix.exe, \safemon\safe505.exe并存储句柄

若目标进程为baiduprotect.exe

若 当前进程为explorer.exe或svchost.exe且目标进程为safe505.exe：

当前进程为runonce.exe且目标进程为360tray.exe

当前进程为360se.exe或360chrome.exe且目标进程为360tray.exe, zhudongfangyu.exe, safe505.exe, liveupdate360.exe：

目标进程为safe505.exe, safefix.exe, safeloader.exe, 360xfix505.exe：

若目标进程为

\360safe\softmgr\softmanager.exe

\360safe\safemon\360realpro.exe

\360safe\uninst.exe

\360safe\utils\filesmasher.exe

\360safe\utils\360fileunlock.exe

\360safe\360shellpro.exe

\360safe\360safe.exe

\360safe\mobilemgr\360mobilemgr.exe

\360safe\360apploader.exe

\360safe\deepscan\dsmain.exe

\360safe\safemon\360tray.exe

则强制结束进程

若创建目标进程为explorer.exe或winlogon.exe，则

若baidu存在则解除baidu驱动回调

若360存在则删除360启动项和快捷方式

若结束目标进程为explorer.exe或winlogon.exe，则

若baidu存在则解除baidu驱动回调

若360存在则：执行FuckCompeete1，删除360启动项和快捷方式；清除SysOpt.ini指定的启动项；删除\Registry\User下每个用户\Software\Microsoft\Windows\CurrentVersion\Run和\Software\Microsoft\Windows\CurrentVersion\RunOnce的360safetray和360sd项；删除360服务项；删除baidu服务项^\_^

FuckCompete1：将\\FileSystem\\360boost的关机回调设置为无效；挂钩Ntfs创建例程；重置自身关机回调；创建随机名驱动及设备执行并设置其关机回调为ShutdownDispatch

### NtSetValueKeyHooker：

若系统关机/注销，且ValueName存在360或当前进程为zhudongfangyu.exe，且目标注册表路径为：

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost

\REGISTRY\\*\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\*

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\360

\REGISTRY\MACHINE\SYSTEM\\*CONTROLSET\*\CONTROL\SESSION MANAGER

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

\REGISTRY\MACHINE\SYSTEM\\*CONTROLSET\*\SERVICES\\*

\REGISTRY\\*\SOFTWARE\CLASSES\CLSID\\*\LOCALSERVER32\*

则拒绝

### ZwRequestWaitReplyPortHooker/ZwAlpcSendWaitReceivePortHooker

若当前进程为360se.exe或360chrome.exe，目标进程为360tray.exe或zhudongfangyu.exe则拒绝

若当前进程为zhudongfangyu.exe或wmiprvse.exe系统正在关机，或当前进程为360tray.exe，且目标操作存在关键字Win32\_Service, Create, :\\WINDOWS\\system32\\svchost.exe –k, Win32\_Process, Defend360, Fix360, FixRundll, \SoftMgr\, 360Safe, .dll, .dat, .exe, .cp, DllGetClassObject, 360csvcs, RERDVGYBHNJ, REPA, REPAIR则拒绝

### NtWriteVirtualMemoryHooker/NtCreateThreadHooker

若当前进程为360se.exe或360chrome.exe且目标进程为explorer.exe，则拒绝(explorer.exe被注入)

### FakeObReferenceObjectByHandle

若当前进程为zhudongfangyu.exe且目标对象路径为

\\*\WINDOWS\CURRENTVERSION\RUN

\\*\WINDOWS\CURRENTVERSION\RUN\\*

\\*\WINDOWS\CURRENTVERSION\RUNONCE

\\*\WINDOWS\CURRENTVERSION\RUNONCE\\*

\\*\CURRENTVERSION\SVCHOST

\\*\SYSTEM\CONTROLSET\*\SERVICES\QQ\*

\\*\SYSTEM\CONTROLSET\*\SERVICES\TS\*

则拒绝

若当前进程为zhudongfangyu.exe, 360tray.exe, svchost.exe，且目标对象位于监视链表中则拒绝

若系统正在关机或注销：

若当前进程为services.exe, svchost.exe且目标路径为

\\REGISTRY\\MACHINE\\SYSTEM\\\*CONTROLSET\*\\SERVICES\\\*FIX\*SERV\*

\\REGISTRY\\MACHINE\\SYSTEM\\\*CONTROLSET\*\\SERVICES\\\*FIX\*SAFE\*

\\REGISTRY\\\*\\SOFTWARE\\CLASSES\\CLSID\\\*\\LOCALSERVER32\*

则拒绝

若当前进程为zhudongfangyu.exe, 360tray.exe，且目标对象路径为

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost

\REGISTRY\\*\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\*

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\360

\REGISTRY\MACHINE\SYSTEM\\*CONTROLSET\*\CONTROL\SESSION MANAGER

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

\REGISTRY\MACHINE\SYSTEM\\*CONTROLSET\*\SERVICES\\*

\REGISTRY\\*\SOFTWARE\CLASSES\CLSID\\*\LOCALSERVER32\*

则拒绝

### CmCallback

若存在修改ShutdownTime的行为，则执行FuckCompete1：

将\FileSystem\360boost关机回调置无效

挂钩NtfsFsdCreate或NtfsCreateDispatch为NtfsFsdCreateHooker

设置监视\Registry\Machine\System\CurrentControlSet\Control\Windows，回调设置为RegisterShutdown

创建随机名驱动及设备执行并设置其关机回调为ShutdownDispatch