DLL与UEFI的故事之一：Windows下运行Dll的三种方式

老狼

2021 年度新知答主

DLL（动态链接库）是Windows下最常见的模块，它的引入曾经让微软引以为傲，有着古老的历史。而UEFI是计算机等固件的标准，两者似乎完全没有关系。实际上，UEFI初试啼声就借鉴了PE格式而与dll产生了紧密的联系，真是“**金风玉露一相逢，便胜却人间无数。**”为了参透UEFI模块的本质，我们不得不从dll开始本系列。因为它的基本知识已经深入人心，本系列不打算介绍它的浅层内容。我们打算另辟蹊径，介绍以下几个方面：

1. Windows下直接运行Dll的三种方式

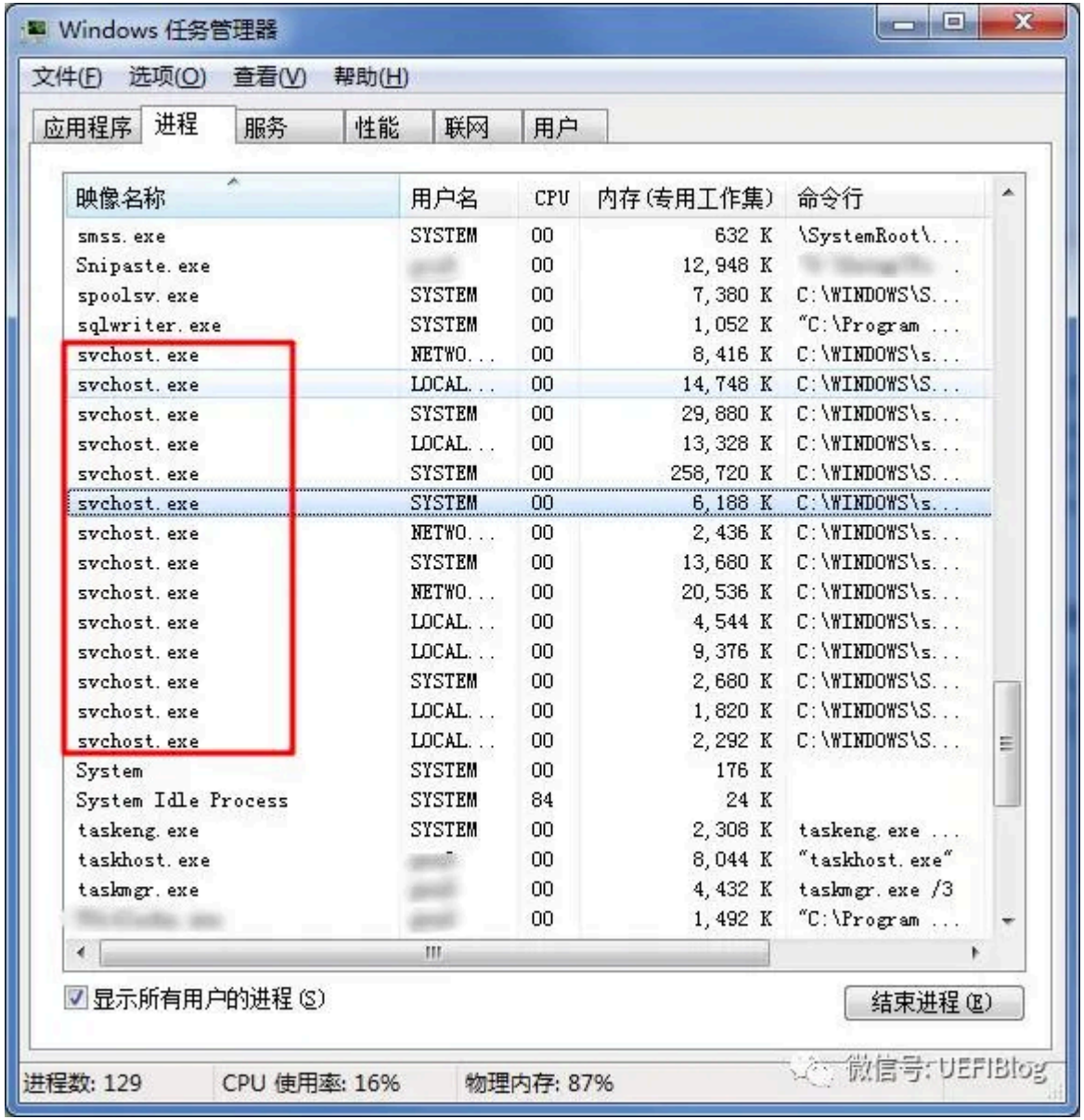
预备知识包括：什么是Dll、为什么要有dll、dll与exe的关系等。他们并不在本系列的涵盖范围内。

楔子

在Windows系统中，Dll的使用已经遍及各个角落。众所周知dll是被映射到exe进程的地址空间中去，换句话说，它可以被认为寄生在exe之上，没有自己独立存在的可能。但是你有没有发现，有很多软件安装后并没有exe文件，而仅仅是几个dll文件，这究竟是怎么回事呢？他们的主人Host在哪里呢？其实Windows早已经为它们安排好了容身之所：svchost.exe、dllhost.exe和rundll32.exe。

svchost.exe

如果你和我一样经常查看任务管理器，你就会惊奇的发现在进程栏里有一大票svchost.exe，它们占据了半个屏幕，大小不一、摩肩接踵、好不热闹：



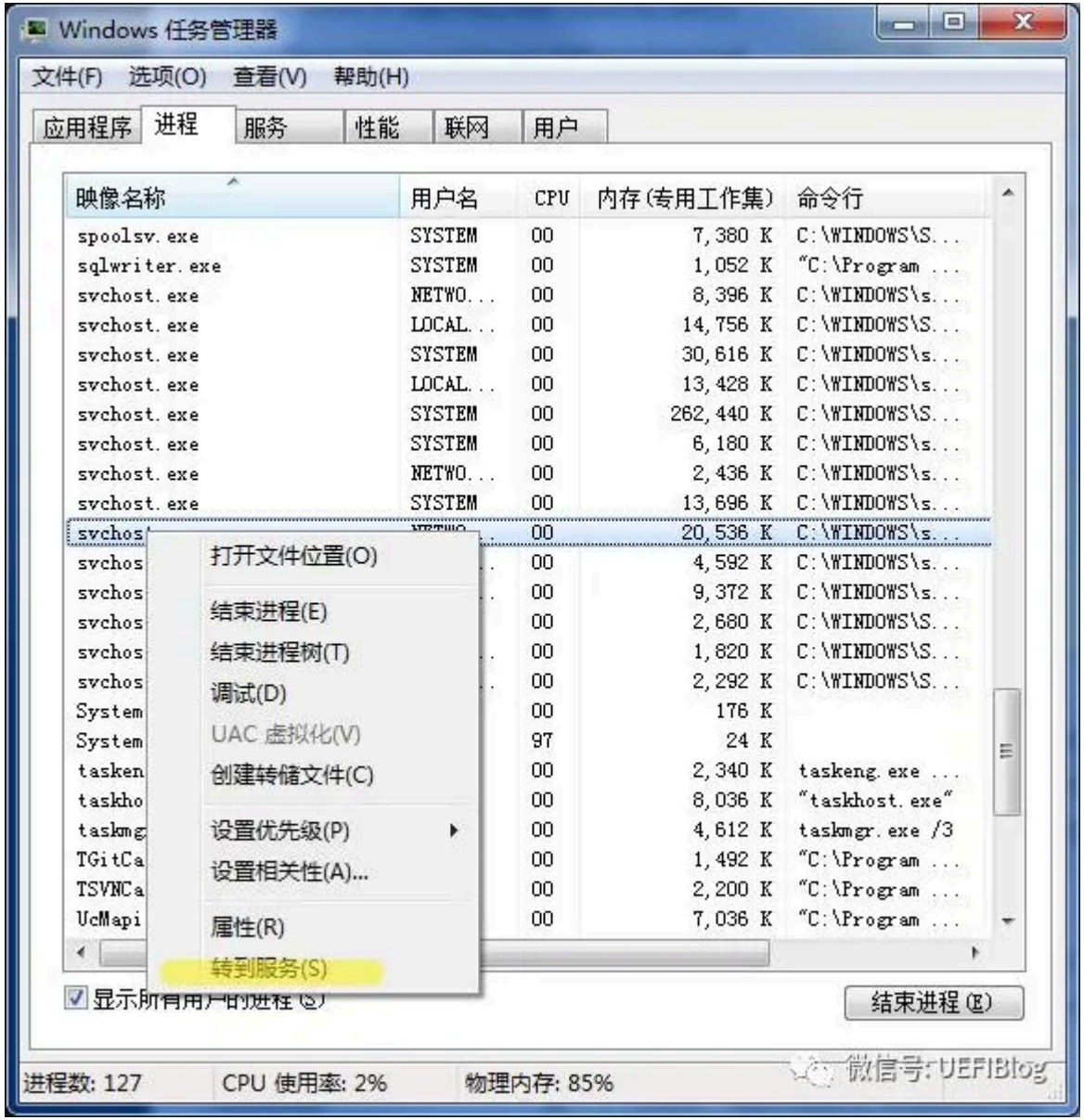
你还不能干掉它们，你也并没有打开它们，它们会不会是病毒呢?

微软的官方解释是：Svchost.exe is a generic host process name for services that run from dynamic-link libraries.

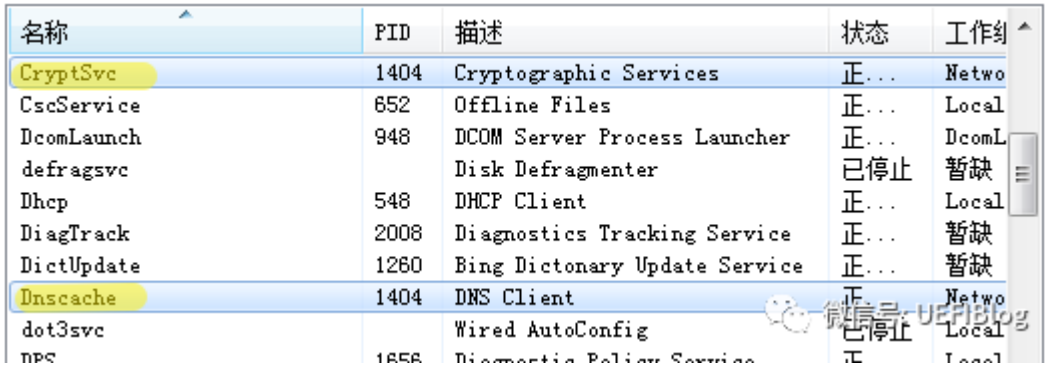
它的真正的名字叫做 Service Host process，它为Windows上的Dll类服务例程驱动提供了运行空间，这也是微软所提倡的。

有同学也许会问为什么有这么多svchost，是不是每个dll单独开启一个呢？是也不是，微软没有搞出一个大svchost来包容所有dll服务例程，是因为如果某个dll产生错误，可能会造成该host被强制关闭，从而导致所有服务例程重启；微软也没有为每个例程单独开启一个svchost，这样我们就不仅仅看到十几个exe而是几十个exe了。微软将它们根据类别进行了分组，将相互有关联的并入一个svchost。我们可以通过进程管理器来查看一下他们的关联。

在Win7中，打开进程管理器，在某个svchost上点击右键，选择转到服务：

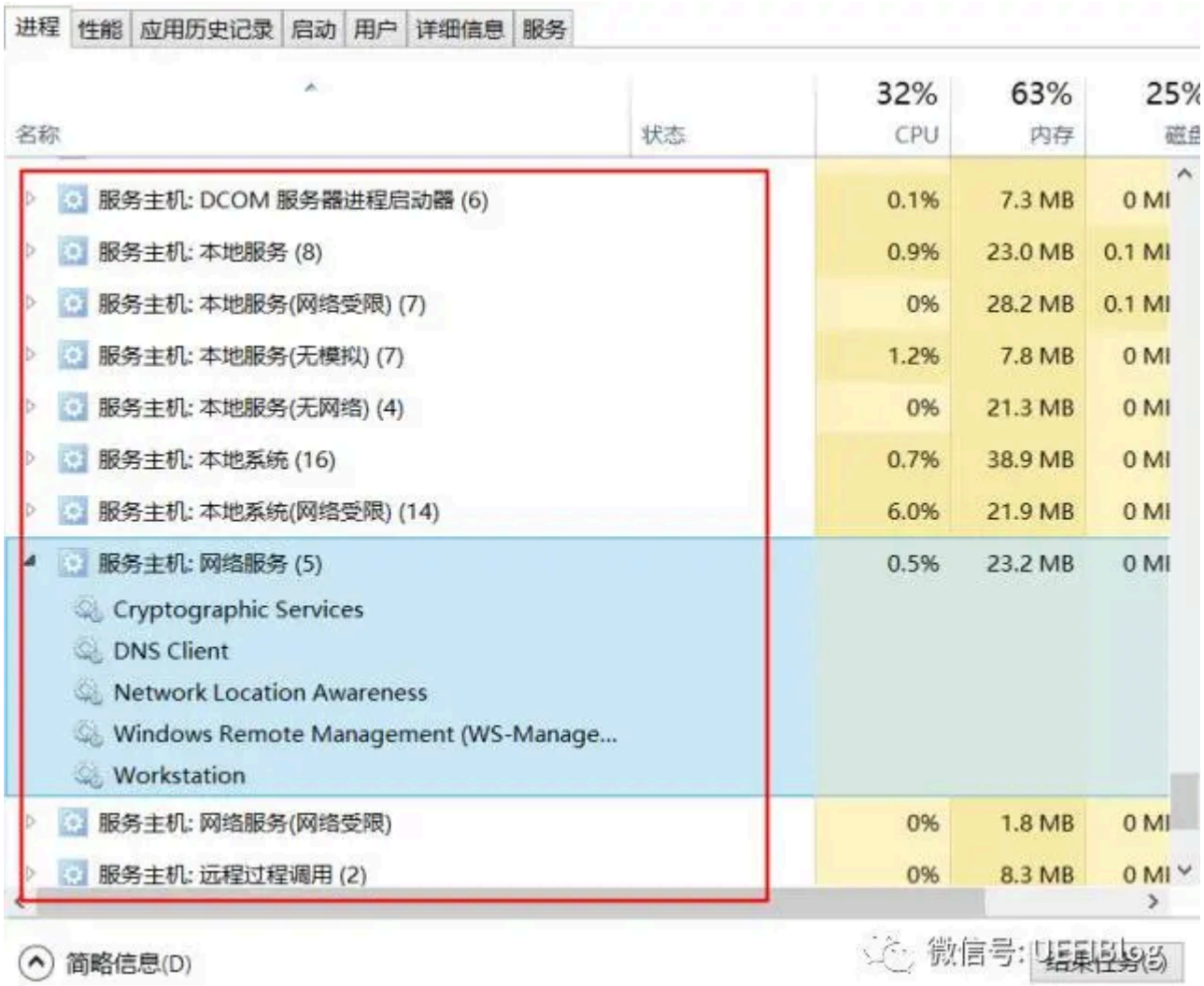


我们在服务栏里面会看到该svchost关联的服务例程：



名称	PID	描述	状态	工作组
CryptSvc	1404	Cryptographic Services	正...	Netwo
CscService	652	Offline Files	正...	Local
DcomLaunch	948	DCOM Server Process Launcher	正...	DcomL
defragsvc		Disk Defragmenter	已停止	暂缺
Dhcp	548	DHCP Client	正...	Local
DiagTrack	2008	Diagnostics Tracking Service	正...	暂缺
DictUpdate	1260	Bing Dictonary Update Service	正...	暂缺
Dnscache	1404	DNS Client	正...	Netwo
dot3svc		Wired AutoConfig	已停止	Local
DPS	1656	Diagnostic Policy Service	正	Local

在win8中，资源管理器中的名字就友善多了：



每个“服务主机”就是一个svchost。大家可以右键点选后选择属性确认一下。评论区有同学说到Win10每个服务有个svchost，我确认了一下，是**几乎**所有的服务都是这样的（有个别例外）。感谢 @aNT Te ，找到了微软的官方说明：

Announcing Windows 10 Insider Preview Build 14942 for PC

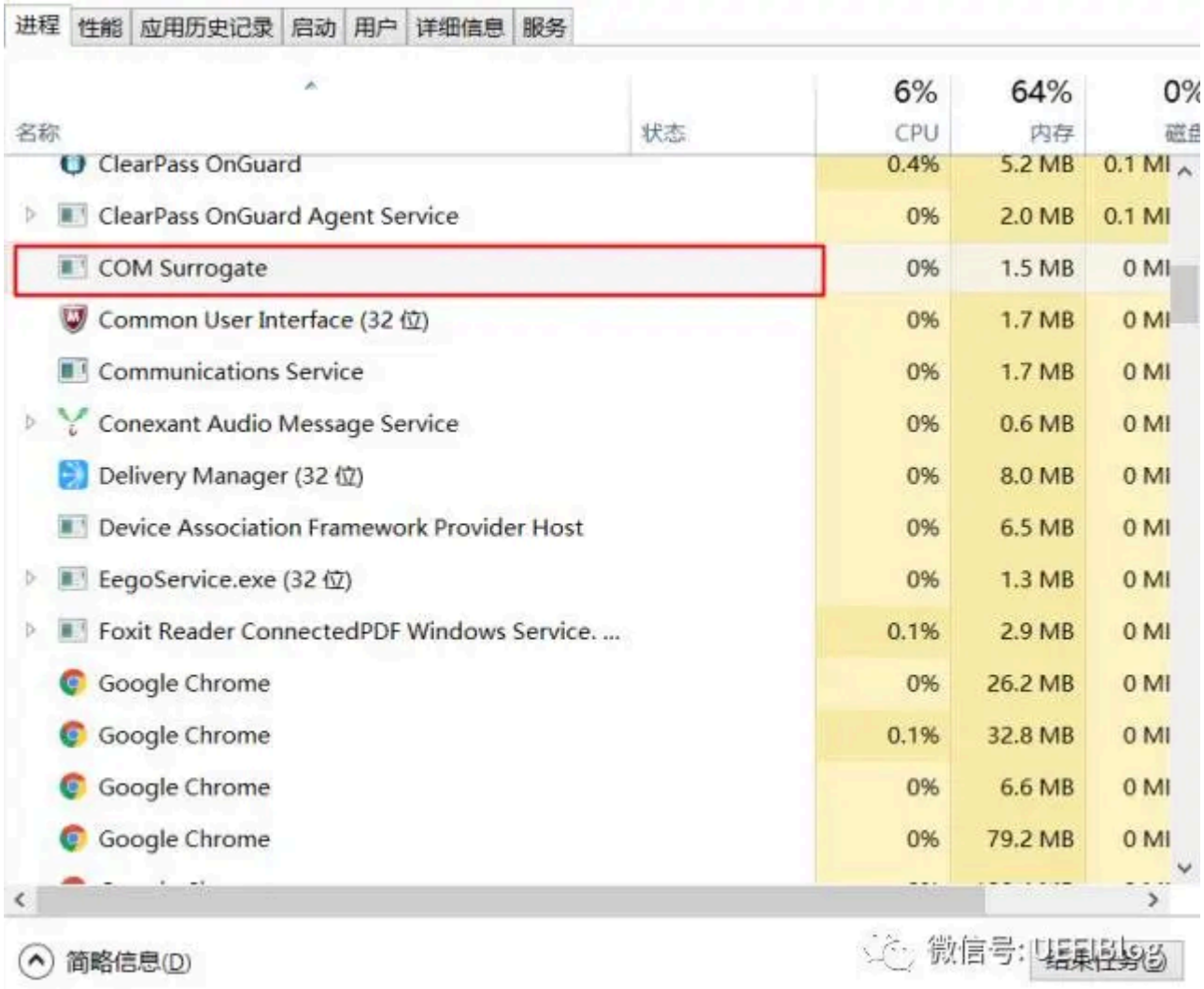
在win10 insider build 14942中加入了新的特性：当内存为3.5GB+的时候，svchost会被切分为每个service一个单独的线程。这回导致进程的明显增加，但也会带来好处：稳定性增加、安全性增加、透明和减少管理成本。

dllhost.exe

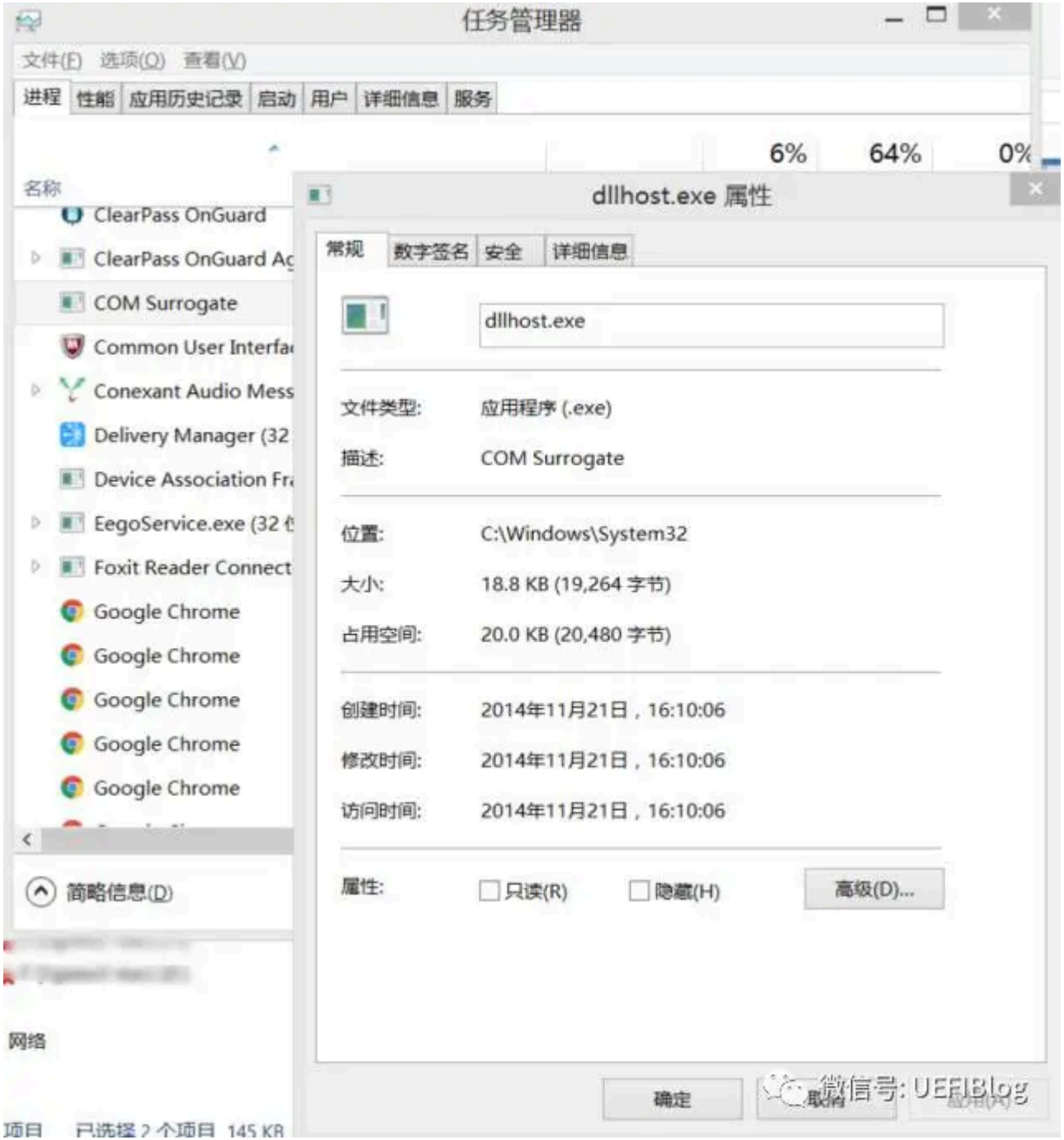
它的存在是为了容纳COM组件。提起COM，DCOM和COM+，那是相当有名，曾经的明星技术，微软的DirectX就是基于此技术。它的好处是跨语言，并且没有bytecode的效率问题，既平台无关性，无论你是远程的、本地的还是进程内的，编程是一样的。IUnknown接口虽然名字怪异但影响深远，曾经微软内核不少扩展都依赖于COM技术。大部分COM组件是以DLL形式存在，对于本地模式的组件一般是有EXE存在，所以它本身就已经是一个进程。对于远程DLL，我们必须找一个进程，这个进程必须包含了调度代码以实现基本的调度。这个进程就是dllhost.exe。这是COM默认的DLL代理。

也许你觉得这些概念很陌生，但是打开系统注册表，在看到一大堆GUID的时候你就会发现COM技术仍然活跃在Windows系统中。我们的Explore中就大量使用了COM技术做扩展，包括缩略图等等。

举个例子，在win8/win10任务管理器中我们会找到名叫“COM Surrogate”的进程：



右键选择属性，我们可以看到它是：


任务管理器
文件(F) 选项(O) 查看(V)
进程 性能 应用历史记录 启动 用户 详细信息 服务
6% 64% 0%
名称
ClearPass OnGuard
ClearPass OnGuard Ag
COM Surrogate
Common User Interfa
Conexant Audio Mess
Delivery Manager (32
Device Association Fra
EegoService.exe (32 位
Foxit Reader Connect
Google Chrome
Google Chrome
Google Chrome
Google Chrome
Google Chrome
简略信息(D)
网络
项目 已选择 2 个项目 145 KB
dllhost.exe 属性
常规 数字签名 安全 详细信息
dllhost.exe
文件类型: 应用程序 (.exe)
描述: COM Surrogate
位置: C:\Windows\System32
大小: 18.8 KB (19,264 字节)
占用空间: 20.0 KB (20,480 字节)
创建时间: 2014年11月21日，16:10:06
修改时间: 2014年11月21日，16:10:06
访问时间: 2014年11月21日，16:10:06
属性: 只读(R) 隐藏(H) 高级(D)...
确定
取消
微信号: UEFIBlog

在Win7中，我们在观看图片缩略图时，会看到有dllhost.exe出现在进程列表中，有时还不只一个。

有没有奇怪为什么explorer会使用dllhost.exe打开COM组件而不是自己打开？毕竟explorer本身就是个exe，完全有能力host一个COM组件。微软著名的The Old New Thing blogs.msdn.microsoft.com...）。原因是explorer不信任基于COM的扩展插件，毕竟谁都可以遵照接口写个插件（我就曾经写过预览pdf内容的插件），而糟糕的插件宕机后会连累explorer被关掉。explorer于是祸水东引，让dllhost来背锅。Dllhost当背锅侠的同时，背上了经常宕机的罪名，不过换来了Windows整体稳定性的提升，也算是当代雷锋了。

rundll32.exe

自从windows9x年代后，Rundll32.exe和Rundll.exe就广为大众所熟识。顾名思义，rundll就是运行dll。这个dll并不是普通的dll, 而是要符合rundll接口规范，详见：

support.microsoft.com/e...

它是Windows系统自带的一个直接执行DLL中导出函数的小工具，很多工具和语言都利用它来执行一些有趣的功能，譬如打开控制面板：

```
rundll32.exe shell32.dll,Control_RunDLL
```

关机:

```
rundll32.exe shell32.dll,SHExitWindowsEx 1
```

等等。

The Old New Thing上也有一篇有意思的rundll32的文章：

blogs.msdn.microsoft.com...

大家有空可以一读。

结论

这三种是Windows下直接运行Dll的主要方式，但他们出现在任务管理器中常常会造成误解：

1. 它们都不是病毒，但却可能被病毒利用或者篡改。尤其是rundll32，曾经蠕虫病毒W32.Miroot.Worm，和它只有一字之差（rundl132.exe）。

2. 在windows9x时代，经常有优化文章介绍要求关掉svchost部分进程，甚至发布script这么做，在win8/win10时代这样做完全没有必要。比较我们现在CPU和内存都很大，远远不是win9x时代可比，这么做往往得不偿失。

最后推荐大家下载良心软件：被微软收购的Sysinternals的免费工具：Process Explorer（Process Explorer）。它可以提供更完整的进程内容。同时在闲暇时间看看The Old New Thing网站上的blog，上面有不少微软某些设计背后的故事，有不少冷知识哦。

参考资料

[1]: blogs.msdn.microsoft.com...

[2]: support.microsoft.com/e...

编辑于 2017-10-28 20:41

Weasley Frank

当前版本的win10真是一个服务一个svchost了……

2017-10-11 · 热评 回复 11

aNT Te

搜了搜相关资料，确切地说是14942(preview版本)加入了这个新特性，关键词:"3.5GB内存以上的电脑，seevice host将分离成独立的进程。"创意者更新的时候正式发布，当时加入了insider preview，有一个更新说明就是说分离svhost的服务，映像比较深。

2017-10-12 · 热评 回复 7

aNT Te

是创意者更新之后才更新成每个服务单独进程，应该是15063(1703)以后的版本。

2017-10-12 回复 2

展开其他 1 条回复 ›

Tim Chen

the old new thing，漏掉一个单词

2017-10-13 回复 2

老狼 作者

谢谢，已改

2017-10-13 回复 喜欢

nukacolamania

同捉虫： “有没有奇怪为什么explore会使用dllhost.exe打开COM组件而不是自己打开？”
该段explore都应为explorer

2017-10-12 回复 2

nukacolamania ▸ **老狼**

白璧微瑕，不掩其美。

2017-10-12 回复 4

老狼 作者

Good catch!

2017-10-12 回复 1

aNT Te

blogs.windows.com/windo...

2017-10-12 回复 1

老狼 作者

谢谢，已更新正文反应这个变化。

2017-10-13 回复 1

fhg0129

白璧微瑕...强迫症提个醒:“广为”非“光为”； “篡改”非“串改”。

2017-10-12 回复 1

老狼 作者

bug好多啊，谢谢。

2017-10-12 回复 喜欢

Bubble Berry

好文章。

顺便捉个bug，是「楔子」不是「契子」啦。

2017-10-12 回复 1

老狼 作者

我也快成半文盲了:(，我改。

2017-10-12 回复 1

RECAP PACER

「在windows9x时代，经常有优化文章介绍要求关掉svchost部分进程，甚至发布script这么做，在win8/win10时代这样做完全没有必要。」

黑的好

2017-10-12 回复 1

神烦狗

红石好评

2022-10-13 回复 喜欢

这破平台谁用真名

那怎么没有很多个dllhost.exe进程呢？就不怕一个COM组建挂掉然后全部死掉？

2018-10-25 回复 喜欢

草履虫

vc6.0过来的、瞬间亲切感爆棚、

2017-11-30 回复 喜欢

茄子

点击查看全部评论 ›

我的Windows 10 1703下有77个svchost

2017-10-13 回复 喜欢