What is the “DLLHOST.EXE” Process Actually Running

Nasreddine Bencherchali · Follow

×

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

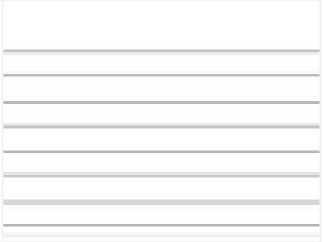
✓ Read offline with the Medium app

Try for 5 $/month

A Deep Dive Into RUNDLL32.EXE

Understanding “rundll32.exe” command line arguments

medium.com



Continuing with the same theme, today we’ll be taking a look at **“dllhost.exe”** and answering the simple question.

“What is the DLLHOST.EXE process actually running”

Medium

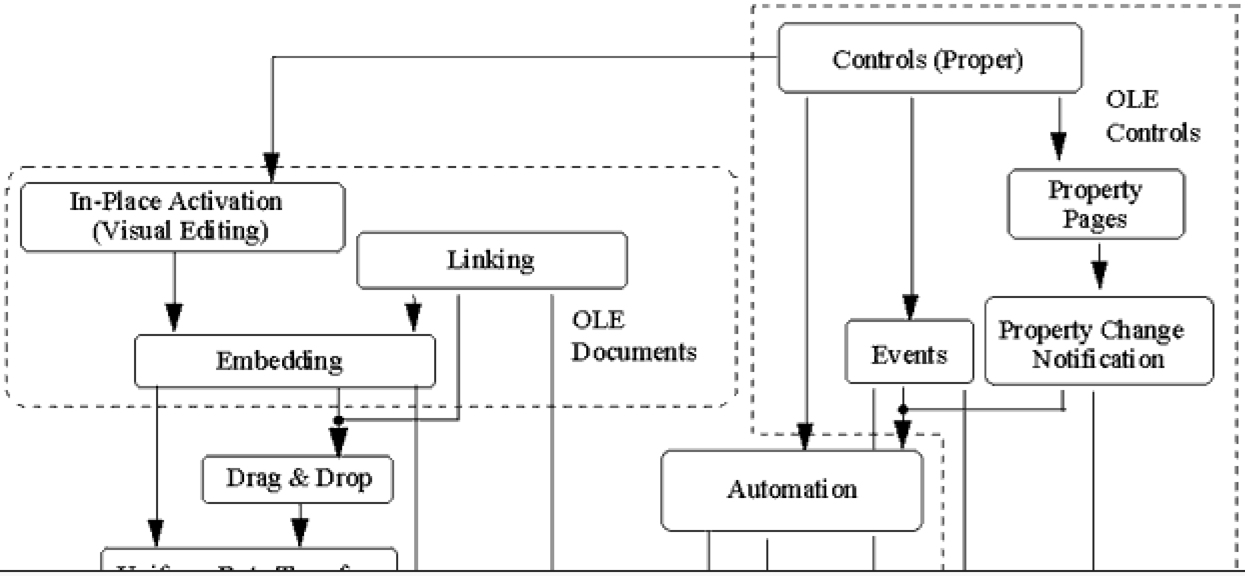
Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
"HKEY_LOCAL_MACHINE\Software\Classes"
"HKEY_CURRENT_USER\Software\Classes"
```

Inside these CLSID keys you'll see sub keys containing the word "Server" that's because COM communication is modeled after a Client/Server architecture.

The client is any application requesting a COM Object (CLSID) from the system, the server requests are handled by the Service Control Manager

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

2. The SCM locates the COM object on the registry via its CLSID
3. The SCM then makes a request to the server (be it local or remote) and grab a reference to the COM class.
4. The SCM passes the reference back to the client, which he can use to create the object.

For more information about COM and its technical details, please refer to MSDN.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Is another way to identify a COM object but with less precision as it's not guaranteed to be unique. (Note that this is an optional key)

AppId

The AppID is a key that groups the configuration of one or more (D)COM objects.

Let's illustrate all of this with an example and let's take the *"Thumbnail Cache Class Factory"*

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

And that's how a typical object is laid out in the registry in the general case.

DLL Surrogate

Now that we understand a little bit more about how things work in COM. Let's ask the following question.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

In short we can host COM Objects in a standalone process called **"dllhost.exe"** that runs, as the name suggest DLL's.

All you need is a value of type "REG_SZ" in the AppId key called **"DllSurrogate"** set to an empty string or NULL.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

One of the use cases is the usage of the CMSTP COM Interfaces such as ***CMSTPLUA {3E5FC7F9–9A51–4367–9063-A120244FBEC7}*** and ***CMLUAUTIL {3E000D72-A845–4CD9-BD83–80C07C3B881F}*** to bypass UAC (User Account Control).

So always monitor what’s being passed to a “DLLHOST.EXE” process and make sure that the COM interface is not hijacked or being used maliciously.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

- https://devblogs.microsoft.com/oldnewthing/20090212-00/?p=19173
- https://networkencyclopedia.com/com-component/
- https://networkencyclopedia.com/component-object-model-com/

Windows 10 Threat Hunting Malware Microsoft Windows Internals

--

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app