


What is the “DLLHOST.EXE” Process Actually Running



Nasreddine Bencherchali · Follow

5 min read · Oct 17, 2020

👏

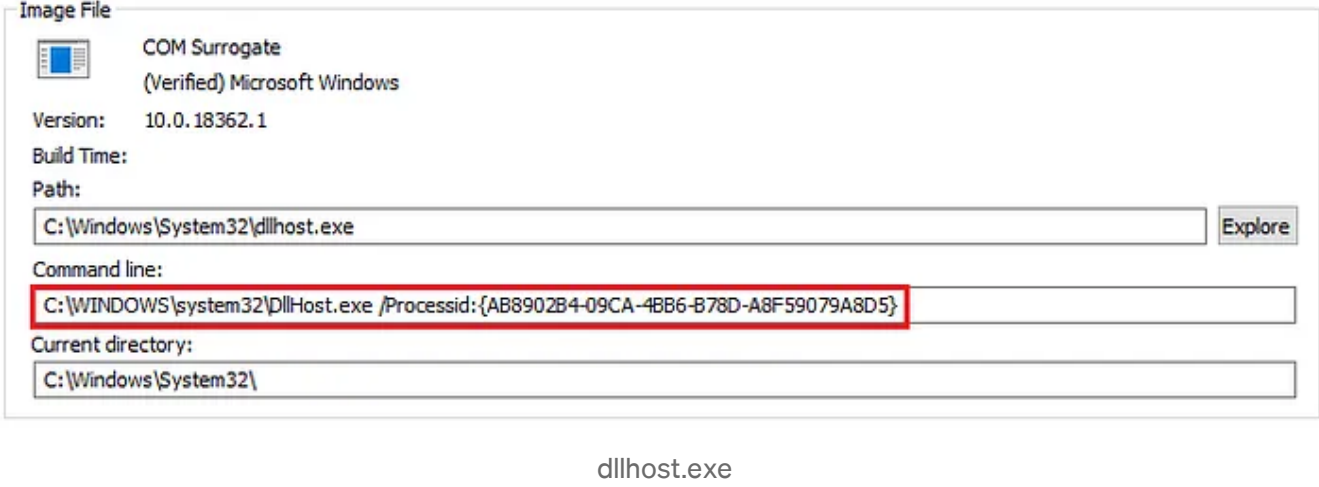
122

💬

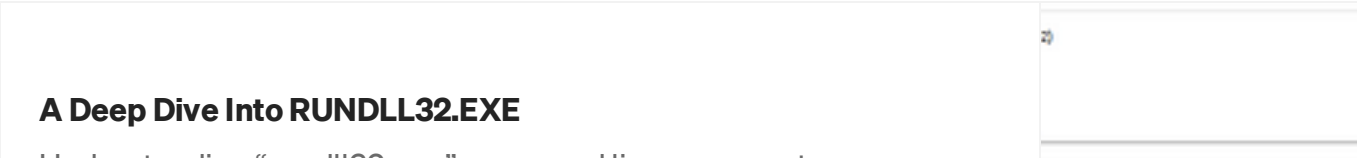
🔖

▶

📄



If you’ve been reading my recent blog posts, you’ll notice that I’ve taken an interest in windows processes. If you haven’t yet check my two recent posts on “svchost.exe” and “rundll32.exe”. Please do.



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

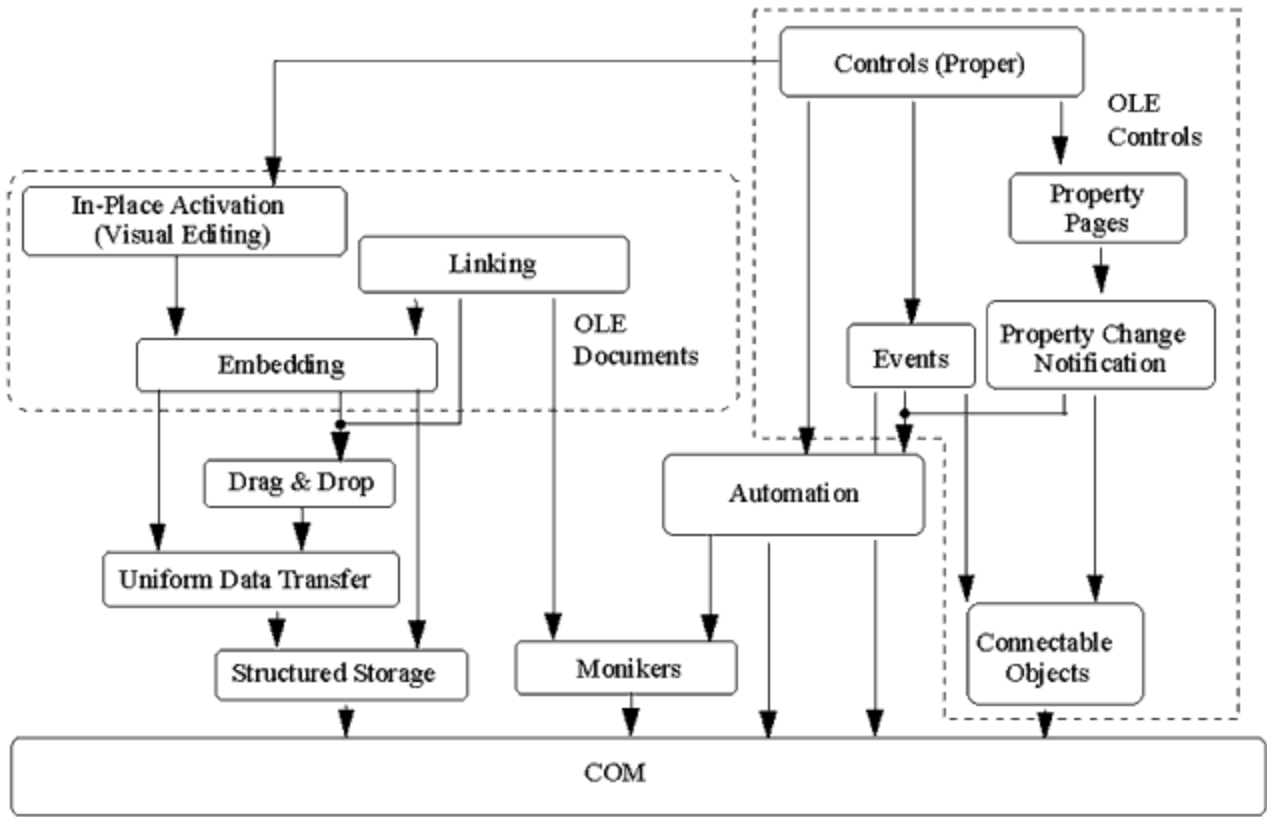
✓ Read offline with the Medium app

Try for 5 \$/month

Page 1 of 9

The Microsoft Component Object Model (COM) is a platform-independent distributed component architecture (DCA) for developing and invoking software components that communicate with each other via standardized interfaces. COM defines a standard way of creating objects and defining how those objects interact. COM enables the development of software components and the ability to use those components in a wide variety of applications. COM is used in a wide range of applications, including documents, ActiveX (Internet-enabled components), as well as others. — MSDN

In other words, COM provides a mechanism for developers to create and control objects (components) that can be used by and from applications, frameworks and the OS itself (I.e Code Reusability). It also allows inter-process communication even across machines and networks with (DCOM) and all of this while being language agnostic.



<https://networkencyclopedia.com/wp-content/uploads/2019/09/component-object-model-com.gif>

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

✓

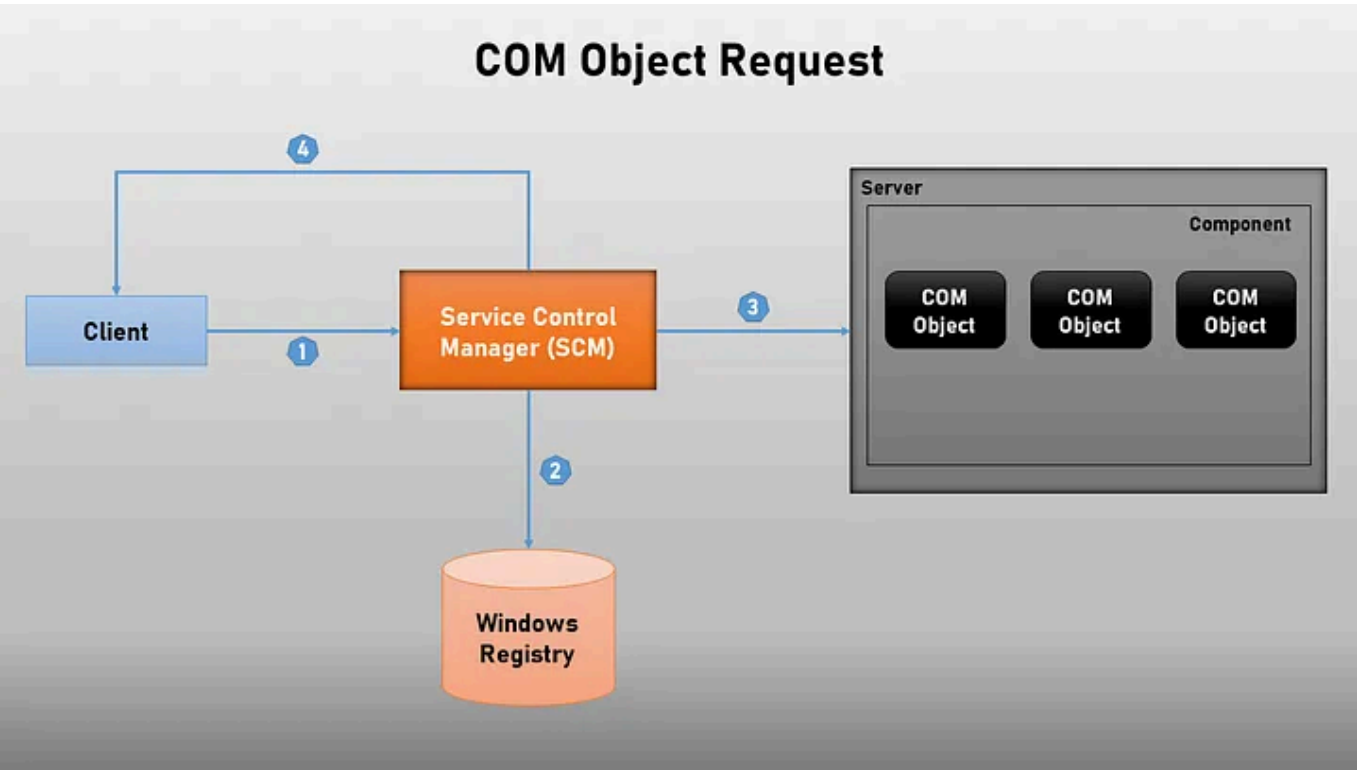
Read offline with the Medium app

Inside these CLSID keys you'll see sub keys containing the word "Server" the

ar

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

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



COM Object Example Request

1. Client request a COM Object
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 then forwards back to the client which requests

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

implement the requested class.

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Its `ProgID` is `CLSID` of the class.

case of an executable object.

ProgID

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*”

The COM factory is registered and can be found in the registry via its CLSID {AB8902B4–09CA-4BB6-B78D-A8F59079A8D5} and since this object is designed to run as a DLL you’ll notice the “InprocServer32” key that contain a reference to the DLL that will get loaded when this object is requested.

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

Page 4 of 9

“explorer.exe” was using a COM object to compute folder thumbnails, but as the process was not designed to host COM objects, it crashed. To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

To solve this issue, Microsoft created the COM SURROGATE process.

COM Surrogate (DLLHOST.EXE)

Here is a description of the COM Surrogate process from the official Microsoft blog “*The Old New Thing*”

The COM Surrogate is the I don’t feel good about this code, so I’m going to ask COM to host it in another process — Old New Thing

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.

And when the system requests the DLL it’ll launch the default surrogate process (which is “dllhost.exe”) and you’ll see something like the following in your process tree or logs.

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

{3E000D72-A845-4CD9-BD82-80C07C3B881E} to bypass UIAC (User

Ac

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

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.

. . .

Conclusion

This conclude our discussion on “dllhost.exe”. I hope you enjoyed reading and that you learned something along the way.

Please if you have any feedback or suggestions regarding this topic or any other send them my way on twitter [@nas_bench](#)

Happy Hunting

Resources

- <https://docs.microsoft.com/en-us/windows/win32/com/com-objects-and-interfaces>
- <https://docs.microsoft.com/en-us/windows/win32/com/dll-surrogates>
- <https://www.gdatasoftware.com/blog/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence>
- http://www.indigoo.com/dox/wsmw/1_Middleware/COM.pdf
- <https://devblogs.microsoft.com/oldnewthing/20090212-00/?p=19173>

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

I write about #Detection, #Sigma and #Windows. Follow
https://medium.com/@nasreddinebencherchali

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

More from Nasreddine Bencherchali

 Nasreddine Bencherchali

Demystifying the “SVCHOST.EXE” Process and Its Command Line...

Understanding the “svchost.exe” process and its command line options

Sep 26, 2020  366  1 

 Nasreddine Bencherchali

Windows System Processes—An Overview For Blue Teams

An overview into windows system process and their parent child relationship.

Oct 24, 2020  77  3 

 Nasreddine Bencherchali

A Deep Dive Into Windows Scheduled Tasks and The...

Understanding the task scheduler service.

 Nasreddine Bencherchali

A Deep Dive Into RUNDLL32.EXE

Understanding “rundll32.exe” command line arguments

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

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.


 theUnknown

Malware Reverse Engineering Basics. Part 1.

This is the beginning of the series of my brief notes on reverse engineering and assembly.

★ Jul 11 🖱 24



 Aardvark Infinity in Aardvark Infinity

Set Up a Windows 11 Malware Analysis Lab for Reverse...

★ Aug 29 🖱 12



Lists

Our Favorite Productivity Advice

9 stories · 721 saves

Tech & Tools

21 stories · 332 saves

Icon Design

36 stories · 438 saves

Productivity

242 stories · 594 saves

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

The Windows Assistant is a tool for managing your Windows settings. It helps you find and install updates, troubleshoot problems, and manage your files. (All rights reserved. All trademarks are the property of their respective owners.)

See more recommendations

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