

Open in app ↗


Sign up Sign in

Medium

Search

Write

# A Deep Dive Into RUNDLL32.EXE



Nasreddine Bencherchali · Follow

6 min read · Oct 10, 2020

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 12

On windows this can be a little tricky to achieve because of the complexity of the OS (after all it’s a 30+ years’ operating system).

Knowing this fact, malware authors write their malware to mimic normal windows processes. So you’ll see malware disguising itself as an “svchost.exe”, “rundll32.exe” or “lsass.exe” process, exploiting the fact that the majority of people using windows don’t know how these system processes behave in normal conditions.

Last time we’ve talked about the “svchost.exe” process and its command line

# 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 most basic syntax for using “rundll32.exe” is the following.

```
rundll32 <DLLname>
```

The “rundll32.exe” executable can be a child or a parent process, it all depend on the context of the execution. And to determine if an instance of “rundll32.exe” is malicious or not we need to take a look at a couple of things. First is the path from which its being launched and second is its

## 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

Always check the location from where the DLL is called, for example kernel32.dll being called from %temp% is obviously malicious. And as a side note always check the hash on sites like VT.

## SHELL32.DLL — “OpenAs\_RunDLL”

“rundll32.exe” can also execute specific functions in DLL’s. For example, when selecting a file and performing a right click on it, a context menu will be shown that offers multiple options. One of the options is the “OpenWith” option. Once selected a pop-up will appear that’ll let’s select from a set of applications on the system.

# Medium

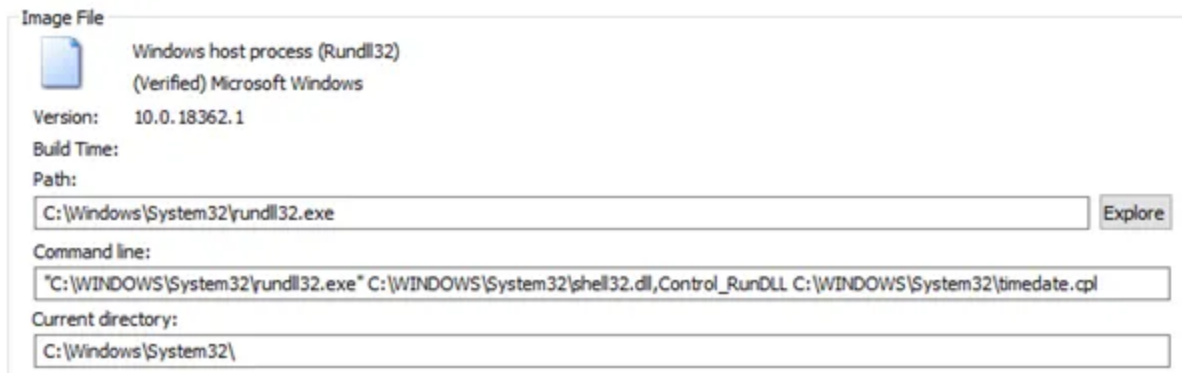
Sign up to discover human stories that deepen your understanding of the world.

## 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



Another common function we’ll see used with the “**shell32.dll**” is “**Control\_RunDLL**” / “**Control\_RunDLLAsUser**”. These two are used to run

## 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

CPL or Control Panel Items are programs that represent a functionality provided by the control panel or in other terms, they are DLL's that exports the **CPIApplet** Function.

A “.CPL” file can contain multiple applets that can be referred to by an applet index and each applet can contain multiple tabs that can be referred to by a tab index.

We can access and request this information via the “rundll32.exe” utility as follows

## 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 a normal case scenario, the parent process of a “rundll32.exe” instance with the “Control\_RunDLL” function should be “explorer.exe” or “control.exe”

Other processes can also launch “rundll32.exe” with that function. For example, it can be a child of “Google Chrom”, “MSGEDGE” or “IE” when launching the “inetctl.cpl” for proxy / network configuration.

If you want more details about CPL and how malware is using it, you can [read this trend micro research paper called CPL Malware](#)

## 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



```
C:\Windows\system32\svchost.exe -k LocalService -p -s WebClient
```

Malware like Emotet has already used this technique in the past. So always analyze the host that is present in this type of command line and make sure that everything is legitimate.

## RUNDLL32.EXE — “-sta” / “-localserver” Flags

A lesser known command line arguments are the “-sta” and “-localserver”. Which both can be used to load malicious registered COM objects

# Medium

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

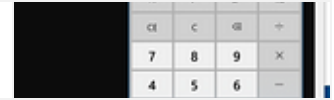
### Free

- ✓ 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

bohops.com



## RUNDLL32.EXE — Executing HTML / JAVASCRIPT

One other command line argument that attackers may use with “rundll32.exe” is the “javascript” flag.

In fact a “rundll32.exe” instance can run HTML / JavaScript code using the “mshtml.dll” and the “javascript” keyword (See Below).

# 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

Thanks for reading and I hope you enjoyed this quick look at Rundll32.

If you have any feedback or suggestions, send them my way via twitter [@nas\\_bench](https://twitter.com/nas_bench)

## References

- <https://bohops.com/2018/06/28/abusing-com-registry-structure-clsid-localserver32-inprocserver32/>
- <https://threathunternlavbook.com/evals/ant29/report.html>

# 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



Written by Nasreddine Bencherchali

2.1K Followers

Follow

I write about #Detection, #Sigma and #Windows. Follow <https://github.com/nasbench/Misc-Research> for interesting Windows tidbits

# 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