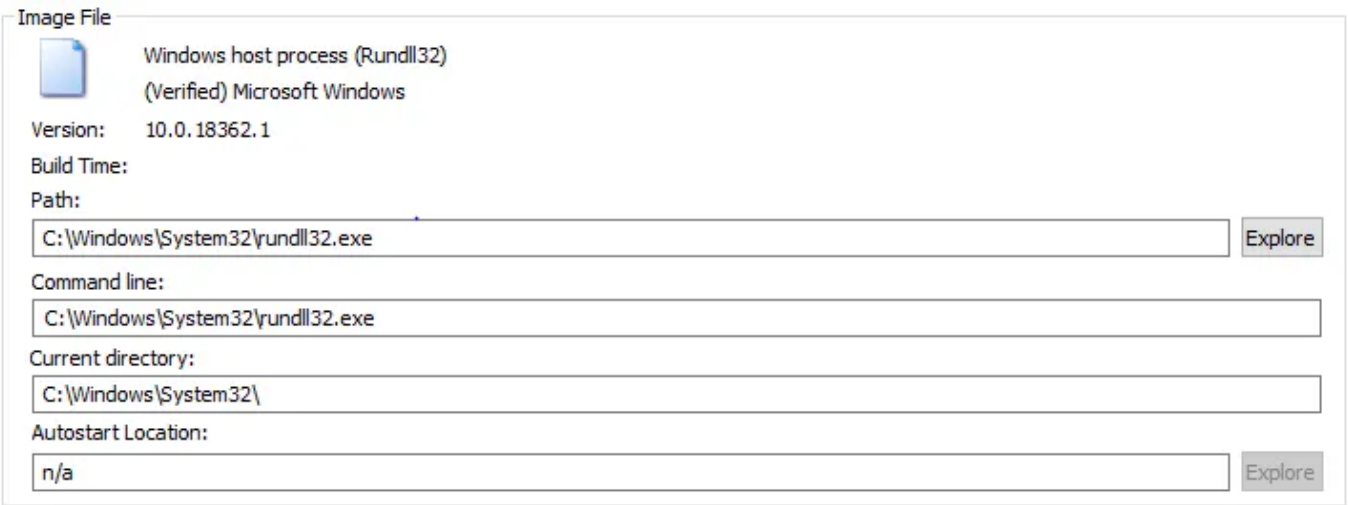
A Deep Dive Into RUNDLL32.EXE

Nasreddine Bencherchali · Follow
6 min read · Oct 10, 2020



Rundll32

When threat hunting malware one of the key skills to have is an understanding of the platform and the OS. To make the distinction between the good and the bad one has to know what’s good first.

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).

RUNDLL32.EXE

As [redacted] or Dynamic Link Libraries (Below is the definition of a DLL from MSDN):

> *A* dynamic-link library *(DLL) is a module that contains functions and data that can be used by another module (application or DLL) —* *MSDN*

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 command line.

The valid “RUNDLL32.EXE” process is always located at:

```
\Windows\System32\rundll32.exe
\Windows\SysWOW64\rundll32.exe (32bit version on 64bit systems)
```

As for the command line of a “rundll32.exe” instance it all depends on what’s being launched whether be it a CPL file, a DLL install…etc.

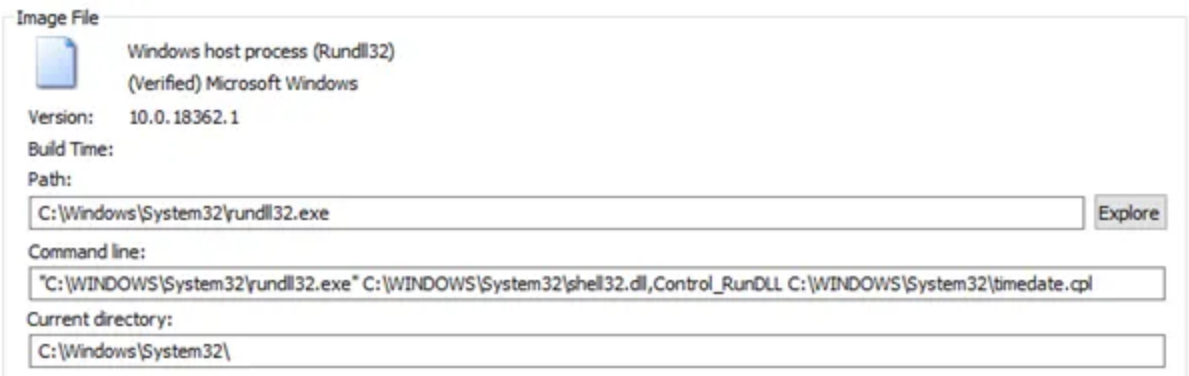
Behind the scene this is actually launching the “rundll32.exe” utility with the “sl


```
C:\Windows\System32\rundll32.exe
C:\Windows\System32\shell32.dll,OpenAs_RunDLL <file_path>
```

This behavior of calling specific functions in a DLL is very common and it can be tricky to know all of them in advance. Below is a list containing a batch of “rundll32.exe” calls and their meaning.

- https://www.tenforums.com/tutorials/77458-rundll32-commands-list-windows-10-a.html
- http://chagdali.free.fr/dcs/RunDll.htm

SHELL32.DLL — “Control_RunDLL”, “Control_RunDLLAsUser” and Control Panel Applets



Another common function we’ll see used with the **“shell32.dll”** is **“Control_RunDLL” / “Control_RunDLLAsUser”.** These two are used to run “.CPL” files or control panel items.

Behind the scene, windows launched a “rundll32.exe” instance with the following command line.

```
C:\WINDOWS\System32\rundll32.exe
C:\WINDOWS\System32\shell32.dll,Control_RunDLL
C:\WINDOWS\System32\timedate.cpl
```

In addition to verifying the legitimacy of a DLL. When using the **“Control_RunDLL” / “Control_RunDLLAsUser”** functions, you should always check the legitimacy of a “.CPL” file.

Control Panel Items (.CPL)

properties and change the pointer, we’ll do it like this


```
C:\WINDOWS\System32\rundll32.exe
C:\WINDOWS\System32\shell32.dll,Control_RunDLL
C:\WINDOWS\System32\main.cpl,@0,1
```

As you can see, one can easily replace the “main.cpl” file with a malicious version and come by unnoticed to the untrained eye. In fact, that’s what malware authors have been doing to infect users.

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 **“inetcpl.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**.

DEVCLNT.DLL — “DavSetCookie” (Web Dav Client)

One of the mysterious command lines in a “rundll32.exe” instance that’ll show up a lot in the logs, takes the following format.

```
C:\WINDOWS\System32\rundll32.exe
C:\Windows\system32\davclnt.dll,DavSetCookie <Host> <Share>
```

A lesser known command line arguments are the “-sta” and “-localserver”

W

If you see in your logs or a process running with one of the following command line arguments.

```
rundll32.exe -localserver <CLSID_GUID>
rundll32.exe -sta <CLSID_GUID>
```

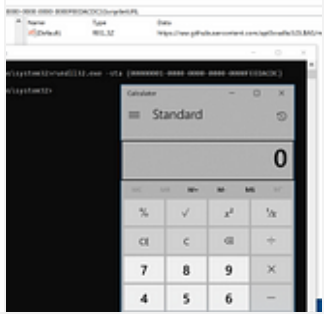
You need to verify the corresponding registry key **[\HKEY_CLASSES_ROOT\CLSID\<GUID>]** and its sub-keys and values for any malicious **DLL** or **SCT** script.

I highly suggest you read **@bohops** blog post for a detailed explanation on this technique and check hexacorn **blog** for the “-localserver” variant.

Abusing the COM Registry Structure: CLSID, LocalServer32, & InprocServer32

TL;DR Vendors are notorious for including and/or leaving behind Registry artifacts that could potentially be abused by...

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

Co

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

References

- https://bohops.com/2018/06/28/abusing-com-registry-structure-clsid-localserver32-inprocserver32/
- https://threathunterplaybook.com/evals/apt29/report.html
- https://www.hexacorn.com/blog/2020/02/13/run-lola-bin-run/
- https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf
- https://support.microsoft.com/en-us/help/149648/description-of-control-panel-cpl-files
- https://isc.sans.edu/forums/diary/Lets+Trade+You+Read+My+Email+Ill+Read+Your+Password/24062/
- https://blog.didierstevens.com/2017/11/13/webdav-traffic-to-malicious-sites/

Windows 10 | Threat Hunting | Malware Analysis | Windows Internals | Infosec

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

What is the “DLLHOST.EXE” Process Actually Running

A Deep Dive Into “DLLHOST.EXE”

Oct 17, 2020 122

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, “taskhostw.exe” and its command line...

Nov 1, 2020 18 1

“Fr[redacted]h
Re[redacted]w…

Lists

Our Favorite Productivity Advice
9 stories · 721 saves

Kostas

Telemetry on Linux vs. Windows: A Comparative Analysis

A look at how Windows and Linux manage telemetry to support incident response…

Sep 3 · 177

Dean

Setting Up Velociraptor for Forensic Analysis in a Home Lab |…

Before I start, Update you will not find article related to setting up Velociraptor in home la…

Oct 6