禪

[illegible]

[illegible] 10 [illegible]

[illegible] 10 [illegible] API [illegible] 10 [illegible] 10 [illegible]

[illegible] 10 [illegible] API [illegible] AMSI [illegible] (Antimalware Scan Interface [illegible]

[illegible]

PowerShell
VBScript
Other Application
Other Application
MsMpEng.exe
(Windows Defender Service)
Win32 API Layer
AMSI.h + AMSI.lib + AMSI.dll
AmsiScanBuffer()
AmsiScanString()
COM API Layer
Amsi.h - Amsi.dll
IAntimalware::Scan()
Provider Class registration
MpEngine.dll
(Defender Scan Engine)
MpSvc.dll
(Defender RPC Server)
AV Provider Layer
Windows Defender Provider Class
IAntimalwareProvider::Scan()
3rd Party AV Provider Class
RPC