

1. **AMSI API Layer**: Applications like PowerShell, VBScript, and Other Applications interact with the Win32 API Layer. The Win32 API Layer contains `AMSI.h + AMSI.lib + AMSI.dll` with functions `AmsiScanBuffer()` and `AmsiScanString()`.

2. **COM API Layer**: The Win32 API Layer interacts with the COM API Layer. The COM API Layer contains `Amsi.h - Amsi.dll` with the `IAntimalware::Scan()` interface. A `Provider Class registration` database is also present.

3. **AV Provider Layer**: The COM API Layer interacts with the AV Provider Layer. The AV Provider Layer contains the `Windows Defender Provider Class` (implementing `IAntimalwareProvider::Scan()`) and a `3rd Party AV Provider Class`.

4. **MsMpEng.exe (Windows Defender Service)**: This service contains `MpEngine.dll (Defender Scan Engine)` and `MpSvc.dll (Defender RPC Server)`. It communicates with the AV Provider Layer via **RPC**.

The diagram illustrates the flow of data and control between these layers. Applications call the Win32 API, which then calls the COM API. The COM API uses the Provider Class registration to find the appropriate AV Provider Class. This class then communicates with the Windows Defender Service via RPC.

AMSI API Layer

The AMSI API Layer is the first layer where applications interact with the scanning engine. It provides a simple interface for applications to scan data. The Win32 API Layer acts as a bridge between the applications and the COM API Layer.

The COM API Layer is responsible for managing the provider classes. It uses the `IAntimalware::Scan()` interface to request scans from the provider classes. The `Provider Class registration` is a database that maps the interface to the specific provider class.

The AV Provider Layer contains the actual scanning logic. The `Windows Defender Provider Class` is the default provider, but other 3rd party providers can be registered. The `MsMpEng.exe` service is the central component that manages the scanning process.

The `RPC` (Remote Procedure Call) mechanism is used for communication between the AV Provider Layer and the `MsMpEng.exe` service.

:
 :
 :
 :
 13:03 - 24/03/1394
 :

<https://www.shabakeh-mag.com/security/840>: معماری معماری