kernel32.dll

- **VirtualAllocEx** (Reflective DLL Injection, DLL Injection, PE Injection, Process Hollowing, Doppelganging, EarlyBird Injection, APC Injection)
- **WriteProcessMemory** (Reflective DLL Injection, DLL Injection, PE Injection, Process Hollowing, Doppelganging, APC Injection, EarlyBird Injection)
- **CreateRemoteThread** (Reflective DLL Injection, DLL Injection, PE Injection, Process Hollowing, EarlyBird Injection, APC Injection)
- **CreateProcess (CREATE_SUSPENDED)** (Process Hollowing, EarlyBird Injection)
- **ResumeThread** (Process Hollowing, EarlyBird Injection)
- **LoadLibraryA/B** (Reflective DLL Injection, DLL Injection - Optional)
- **GetProcAddress** (Reflective DLL Injection - Optional)
- **VirtualProtect** (Reflective DLL Injection - Optional, PE Injection)
- **SetThreadContext** (Process Hollowing - Optional)
- **NtUnmapViewOfSection/ZwUnmapViewOfSection** (Process Hollowing, PE Injection - Optional)
- **NtContinue** (Doppelganging - Optional)
- **QueueUserAPC** (APC Injection, EarlyBird Injection)
- **OpenProcess** (DLL Injection, APC Injection)
- **NtWaitForSingleObject/WaitForSingleObject** (APC Injection - Optional)
- **NtWriteVirtualMemory** (EarlyBird Injection - Optional)
- **NtProtectVirtualMemory/ZwProtectVirtualMemory** (API Hooking - Optional)
- **NtCreateThread/CreateRemoteThread** (API Hooking - Optional)
- **ZwWriteVirtualMemory** (API Hooking - Optional)
- **ZwAllocateVirtualMemory** (API Hooking - Optional)
- **CreateFileTransacted** (Doppelganging)
- **CreateTransaction** (Doppelganging)
- **RollbackTransaction** (Doppelganging)
- **CreateFile** (Doppelganging - Optional)
- **WriteFile** (Doppelganging - Optional)
- **OpenFile** (Doppelganging - Optional)
- **ReadFile** (Doppelganging - Optional)
- **DeviceIoControl** (Doppelganging - Optional)
- **SetFilePointer** (Doppelganging - Optional)

---

ntdll.dll

- **NtQuerySystemInformation** (Reflective DLL Injection, DLL Injection, PE Injection)
- **NtCreateProcessEx** (DLL Injection, Doppelganging - Optional)
- **NtCreateProcess** (DLL Injection)
- **NtContinue** (Doppelganging - Optional)

- **NtWriteVirtualMemory** (EarlyBird Injection - Optional)
- **NtUnmapViewOfSection/ZwUnmapViewOfSection** (Process Hollowing, PE Injection - Optional)
- **ZwMapViewOfSection** (API Hooking - Optional)
- **ZwWriteVirtualMemory** (API Hooking - Optional)
- **ZwAllocateVirtualMemory** (API Hooking - Optional)
- **ZwProtectVirtualMemory** (API Hooking - Optional)

---

user32.dll

- **SetWindowsHookEx** (API Hooking)
- **UnhookWindowsHookEx** (API Hooking)

---

psapi.dll

- **EnumProcesses** (Reflective DLL Injection, DLL Injection, PE Injection)
- **EnumProcessModules** (Reflective DLL Injection, DLL Injection, PE Injection)
- **EnumProcessModulesEx** (Reflective DLL Injection, DLL Injection, PE Injection)

---

advapi32.dll

- **RegCreateKeyExA** (DLL Injection)
- **RegCreateKeyExW** (DLL Injection)
- **RegSetValueExA** (DLL Injection)
- **RegSetValueExW** (DLL Injection)
- **RegDeleteKeyA** (DLL Injection)
- **RegDeleteKeyW** (DLL Injection)

---

ws2_32.dll

- **WSASend** (Network Communication)
- **WSARecv** (Network Communication)
- **send** (Network Communication)
- **recv** (Network Communication)

---

wininet.dll

- **InternetOpenUrlA** (Network Communication)
- **InternetOpenUrlW** (Network Communication)
- **HttpSendRequestA** (Network Communication)
- **HttpSendRequestW** (Network Communication)

Summary of Key DLLs:

- `kernel32.dll`: Handles most memory, process, thread, and file operations.
- `ntdll.dll`: Manages low-level system functions, process management, and memory manipulation.
- `user32.dll`: Provides functionality for setting and removing system-wide event hooks (API Hooking).
- `psapi.dll`: Used for enumerating processes and modules.
- `advapi32.dll`: Manages registry operations, often used for malicious manipulation of the system registry.
- `ws2_32.dll`: Handles network-related operations for socket communication.
- `wininet.dll`: Provides Internet functionality, including sending and receiving HTTP requests.