A comprehensive analysis of malware's interactions with the system can be achieved through the examination of the following APIs:

Process Enumeration and Manipulation:

- **Process Enumeration:** `EnumProcesses`, `EnumProcessModules`, `EnumProcessModulesEx`, `NtQuerySystemInformation`, `CreateToolhelp32Snapshot`, `Process32First`, `Process32Next`, `Module32First`, `Module32Next`, `Heap32First`, `Heap32Next`, `Thread32First`, and `Thread32Next`.
- **Process Creation:** `CreateProcessA`, `CreateProcessW`, `CreateProcessInternalA`, `CreateProcessInternalW`, `NtCreateProcess`, and `NtCreateProcessEx`.

Memory Management:

- **Memory Allocation:** `VirtualAlloc`, `VirtualAllocEx`, `VirtualProtect`, `HeapAlloc`, `GlobalAlloc`, and `LocalAlloc`.

Network Communication:

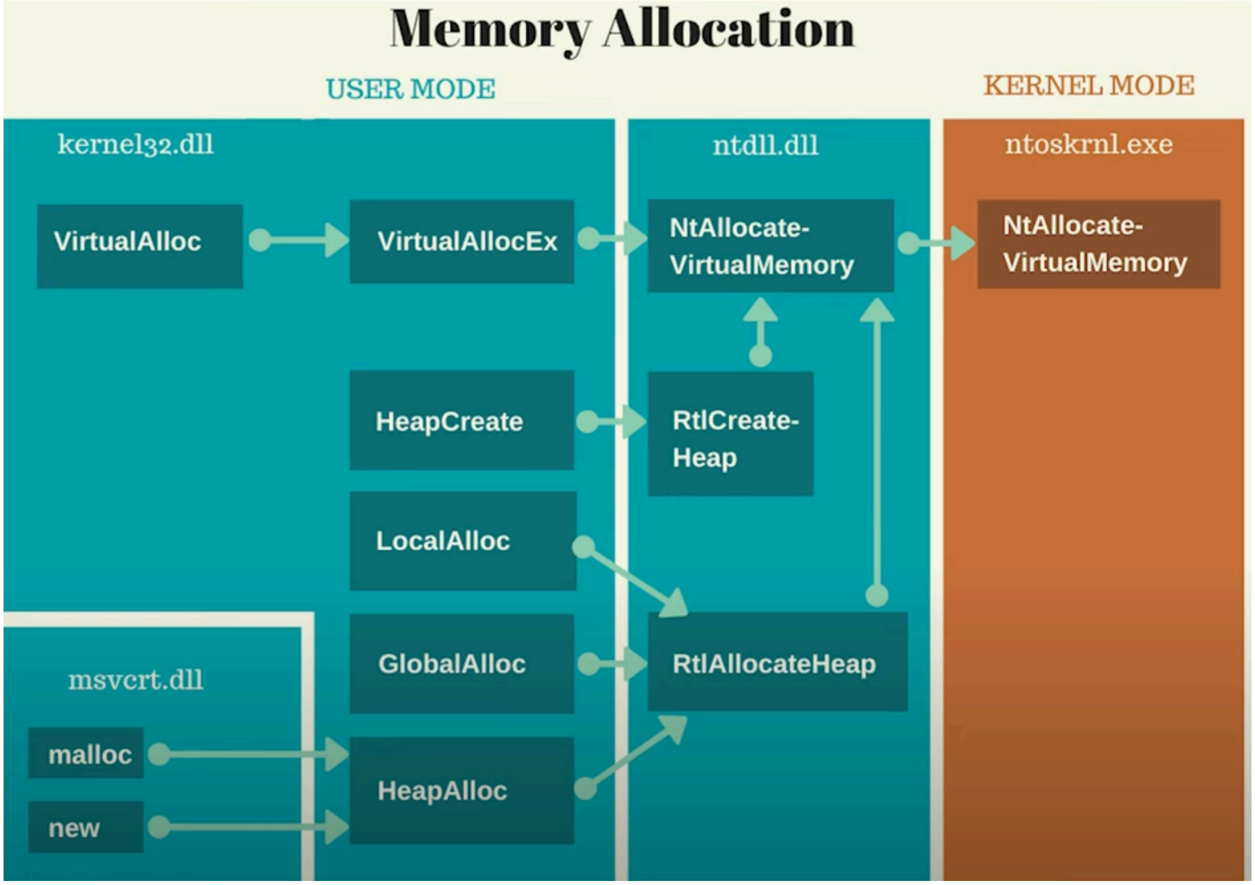
- **Network Operations:** `WSASend`, `WSARecv`, `send`, `recv`, `InternetOpenUrlA`, `InternetOpenUrlW`, `HttpSendRequestA`, and `HttpSendRequestW`.

File and Registry Operations:

- **File Operations:** `CreateFileA`, `CreateFileW`, `ReadFile`, `WriteFile`, `DeleteFileA`, and `DeleteFileW`.
- **Registry Operations:** `RegCreateKeyExA`, `RegCreateKeyExW`, `RegSetValueExA`, `RegSetValueExW`, `RegDeleteKeyA`, and `RegDeleteKeyW`.

DLL Loading:

- **DLL Loading:** `LoadLibraryA`, `LoadLibraryW`, `LoadLibraryExA`, `LoadLibraryExW`, and `GetProcAddress`.



Memory Allocation

USER MODE

KERNEL MODE

kernel32.dll

VirtualAlloc

VirtualAllocEx

HeapCreate

LocalAlloc

GlobalAlloc

HeapAlloc

msvcrt.dll

malloc

new

ntdll.dll

NtAllocate-VirtualMemory

RtlCreate-Heap

RtlAllocateHeap

ntoskrnl.exe

NtAllocate-VirtualMemory