Common API Used in Malware

Topics:

- Networking
- Persistence
- Encryption
- Anti-Analysis
- Stealth
- Execution
- Miscellaneous

Networking:

Raw Sockets:

- socket()
- Server:
  - bind()
  - listen()
  - accept()
- Client:
  - connect()
- read()/recv()
- write()
- shutdown()

WinAPI Sockets:

- WSAStartup(), socket()
- Server:
  - bind()
  - listen()
  - accept()
- Client:
  - connect()
- send()
- recv()
- WSACleanup()

Persistence:

Registry Persistence:

- RegCreateKeyEx()
- RegOpenKeyEx()
- RegSetValueEx()
- RegDeleteKeyEx()
- RegGetValue()

File Persistence:

- GetTempPath()
- CopyFile()
- CreateFile()
- WriteFile()
- ReadFile()

Service Persistence:

- OpenSCManager()
- CreateService()
- StartServiceCtrlDispatcher()

Encryption:

WinCrypt API:

- CryptAcquireContext()
- CryptGenKey()
- CryptDestroyKey()
- CryptDeriveKey()
- CryptEncrypt()
- CryptDecrypt()
- CryptReleaseContext()

Anti-Analysis/VM

- IsDebuggerPresent()
- GetSystemInfo()
- GlobalMemoryStatusEx()
- GetVersion()
- Assembly Instructions:
  - CPUID()
  - IN()

Stealth:

- VirtualAlloc()
- VirtualProtect()
- ReadProcessMemory()
- WriteProcessMemory()
- CreateRemoteThread()
- NtUnmapViewOfSection()
- QueueUserAPC()

Execution:

- CreateProcess()
- ShellExecute()
- WinExec()
- ResumeThread()

Miscellaneous:

- GetAsyncKeyState()
- SetWindowsHookEx()
- GetForeGroundWindow()
- LoadLibrary(), GetProcAddress()
- CreateToolhelp32Snapshot()
- GetDC(), BitBlt()
- InternetOpen(), InternetOpenUrl(), InternetReadFile(), InternetWriteFile()
- FindResource(), LoadResource(), LockResource()

Thank you