**枚举进程的所有模块**

* 项目
* 2023/06/13
* 4 个参与者

反馈

若要确定哪些进程加载了特定的 DLL，必须枚举每个进程的模块。 以下示例代码使用 [**EnumProcessModules**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Psapi/nf-psapi-enumprocessmodules) 函数枚举系统中当前进程的模块。

C++复制

#include <windows.h>

#include <tchar.h>

#include <stdio.h>

#include <psapi.h>

// To ensure correct resolution of symbols, add Psapi.lib to TARGETLIBS

// and compile with -DPSAPI\_VERSION=1

int PrintModules( DWORD processID )

{

HMODULE hMods[1024];

HANDLE hProcess;

DWORD cbNeeded;

unsigned int i;

// Print the process identifier.

printf( "\nProcess ID: %u\n", processID );

// Get a handle to the process.

hProcess = OpenProcess( PROCESS\_QUERY\_INFORMATION |

PROCESS\_VM\_READ,

FALSE, processID );

if (NULL == hProcess)

return 1;

// Get a list of all the modules in this process.

if( EnumProcessModules(hProcess, hMods, sizeof(hMods), &cbNeeded))

{

for ( i = 0; i < (cbNeeded / sizeof(HMODULE)); i++ )

{

TCHAR szModName[MAX\_PATH];

// Get the full path to the module's file.

if ( GetModuleFileNameEx( hProcess, hMods[i], szModName,

sizeof(szModName) / sizeof(TCHAR)))

{

// Print the module name and handle value.

\_tprintf( TEXT("\t%s (0x%08X)\n"), szModName, hMods[i] );

}

}

}

// Release the handle to the process.

CloseHandle( hProcess );

return 0;

}

int main( void )

{

DWORD aProcesses[1024];

DWORD cbNeeded;

DWORD cProcesses;

unsigned int i;

// Get the list of process identifiers.

if ( !EnumProcesses( aProcesses, sizeof(aProcesses), &cbNeeded ) )

return 1;

// Calculate how many process identifiers were returned.

cProcesses = cbNeeded / sizeof(DWORD);

// Print the names of the modules for each process.

for ( i = 0; i < cProcesses; i++ )

{

PrintModules( aProcesses[i] );

}

return 0;

}

main 函数使用 [**EnumProcesses**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Psapi/nf-psapi-enumprocesses) 函数获取进程列表。 对于每个进程，main 函数调用 PrintModules 函数，向其传递进程标识符。 PrintModules 依次调用 [**OpenProcess**](https://learn.microsoft.com/zh-cn/windows/desktop/api/processthreadsapi/nf-processthreadsapi-openprocess) 函数来获取进程句柄。 如果 **OpenProcess** 失败，则输出仅显示进程标识符。 例如，对于 Idle 和 CSRSS 进程， **OpenProcess** 会失败，因为它们的访问限制阻止用户级代码打开它们。 接下来，PrintModules 调用 [**EnumProcessModules**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Psapi/nf-psapi-enumprocessmodules) 函数以获取模块句柄函数。 最后，PrintModules 为每个模块调用 [**一次 GetModuleFileNameEx**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Psapi/nf-psapi-getmodulefilenameexa) 函数以获取模块名称。