

Forum:[Hack Forums](#)

Thread: [Manually mapping a .NET executable.](#)

oh9od - December 7, 2020, 3:55 am

So pretty much I've been working on a Manual Mapper, works like a charm with native executables but if I try to map a .NET executable (or anything that has .NET dependencies), it fails throwing this error:

I know that this can be fixed by using a compiler flag (/clr), but that's a bad solution because, while it'll allow .NET applications to be manually loaded, it will also require VC++ to be installed on the victim's machine (all of this is for a crypter's stub I am making, so I want zero dependencies whatsoever). So I manually load .NET assemblies with this code snippet:

```
Code ICLRRuntimeHost* LoadNETRuntimeStatic()
{
    DLL_DEBUG("Loading .NET Runtime...\n");

    HRESULT hr;
    ICLRMetaHost* pMetaHost = NULL;
    ICLRRuntimeInfo* pRuntimeInfo = NULL;
    ICLRRuntimeHost* pRuntimeHost = NULL;

    hr = CLRCREATEINSTANCE(CLSID_CLRMetaHost, IID_PPV_ARGS(&pMetaHost));

    if (FAILED(hr))
    {
        DLL_DEBUG("Could not create CLR instance.\n");
        return 0;
    }

    hr = pMetaHost->GetRuntime(L"v4.0.30319", IID_PPV_ARGS(&pRuntimeInfo));

    if (FAILED(hr))
    {
        DLL_DEBUG("Could not get .NET runtime.\n");
        return 0;
    }

    hr = pRuntimeInfo->GetInterface(CLSID_CLRRuntimeHost, IID_PPV_ARGS(&pRuntimeHost));

    if (FAILED(hr))
    {
        DLL_DEBUG("Could not get .NET interface.\n");
        return 0;
    }

    hr = pRuntimeHost->Start();
```

}

Indeed .NET assemblies get correctly loaded inside the executable, but the latter still won't run.

So before I tell what I want to achieve, let's gloss over some rules.

1. No dependencies, aka no usage of the /clr flag.
2. The executable is inside the stub (duh.), so no dropping files on disk, everything is done in memory.

My manual mapper does every required step, remapping to memory, base relocation, fixing imports etc etc, although .NET assemblies might require some sort of extra step since their PE structure is different.

Am I missing something? Is the /clr flag the only way out of this?