Being able to call a function without using GetProcAddress is not a security vulnerability

devblogs.microsoft.com/oldnewthing/20090409-00

April 9, 2009

Raymond Chen

Another genre in the sporadic category of dubious security vulnerability is people who find an unusual way of accomplishing something perfectly normal but declare it a security vulnerability because they found an unusual way of doing it.

> Security is important to all computers users, from families at home to employees of government agencies, and people who use Microsoft Windows are no exception. Trojans, backdoors, and spyware (collectively known as *malware*) have taken many forms, most recently those of so-called *rootkits*, which modify the operating system itself in order to prevent their detection. Firewalls are an important tool in the defense against malware.
>
> Through the following sequence of tricks, we can obtain the address of any function without using the `GetProcAddress` function. Once that address is obtained, the function can be called in the normal manner. First, obtain the module base address by calling the `LoadLibrary` function. The headers of the image are mapped into memory at the base address. From there, you can parse the headers of the module, look for the export directory, then manually parse the exported function name table until you find the function you want. In this way you can call functions like `RegSetValue` without detection.

Well, sure, you can manually perform all the operations that the `GetProcAddress` would perform, but what's the point? Once you call `RegSetValue` all the normal registry security checks take place. You haven't bypassed anything. If you were so keen on calling functions surreptitiously, you could scan memory looking for the byte pattern that corresponds to the function you're looking for, or heck, just cut out the middle man and just take the code from the DLL you are trying to gain secret access to and copy it into your program!

In other words, you just found a complicated way of doing something perfectly mundane. You can't make up for the absence of any actual vulnerability by piling on style points and cranking up the degree of difficulty.

Raymond Chen

Follow