

Forum:[Hack Forums](#)

Thread: [Comparison of Various Injection techniques widely used.](#)

Infinity. - October 5, 2024, 10:19 am

Hi guys, today I will be comparing various Injection techniques widely used by Pentesters and developers.

Remote thread injection

Risk Level: Low

Evasion Level: Medium

This technique is widely used by developers or pentester needs to inject a DLL into a target process for monitoring, debugging, or testing purposes. It's commonly seen in tools that require interaction with other applications (e.g., for modifying behaviors or functionality). However, it can also be exploited by malware to execute malicious code in a victim's process.

APC Injection

Risk Level: Medium

Evasion Level: High

Asynchronous Procedure Call (APC) injection allows an attacker to queue a DLL to be executed in the context of a target thread. This method can be stealthy, as it doesn't require direct manipulation of the target process's memory and can avoid detection by security tools. It's often used in more sophisticated attacks where stealth and evasion are priorities.

Process Hollowing

Risk Level: High

Evasion Level: High

This method involves creating a new process in a suspended state and then replacing its memory space with the code from a malicious DLL. It's often used by malware to run in the context of a legitimate process, making detection difficult. For example, a malware author might hollow out a legitimate process to execute malicious payloads while appearing benign to antivirus solutions.

Reflective DLL Injection

Risk Level: High

Evasion Level: Very High

This technique allows a DLL to be injected into a process without relying on standard Windows API functions like LoadLibrary. It is often used by penetration testers to test the security of applications or by malware to evade detection and load malicious payloads in a stealthy manner. Its reflective nature allows for greater flexibility in DLL handling, making it a favorite amongst attackers.

Thread Hijacking

Risk Level: High

Evasion Level: High

This technique allows an attacker to take control of an existing thread in a target process. It can be particularly stealthy, as it avoids creating new threads that might raise suspicion. Thread hijacking is commonly used in advanced persistent threats (APTs) and other stealthy malware campaigns, allowing attackers to execute their code without detection.

SetWindowsHookEx Injection

Risk Level: Low

Evasion Level: Low

This method utilizes the Windows API to set hooks that monitor and modify messages sent to GUI components. It's often used in applications that require interaction with user input or other GUI events. For example, keyloggers may use this technique to capture keystrokes and other input without raising suspicion. While it's primarily used for legitimate applications, it can also be exploited by malicious software.

Inline Hooking

Risk Level: Medium

Evasion Level: Medium

Inline hooking allows an attacker to modify the behavior of specific functions by replacing the first few bytes of a target function with a jump to custom code. This technique can be used for debugging, monitoring, or malicious purposes, such as altering the execution flow of an application to execute arbitrary code or to hide malicious behavior.

Risk Level: Low
Evasion Level: Low

This technique takes advantage of the way Windows searches for DLLs. By placing a malicious DLL in a location that is searched before the real DLL, an attacker can execute their code when the application attempts to load the library. This is often used to substitute legitimate functionality with malicious behavior, such as redirecting API calls or stealing credentials.

Section Object Injection

Risk Level: High
Evasion: Very High

This technique involves creating a memory section that can be shared between processes. The attacker injects the DLL by manipulating this shared memory, which can be particularly stealthy and allows for sophisticated injection scenarios. It is often used in advanced malware and exploitation techniques, particularly in targeted attacks where evasion is a priority.

IAT Hooking

Risk Level: Medium
Evasion: Medium

Import Address Table (IAT) hooking allows an attacker to redirect calls to specific functions by modifying the IAT of the target process. This technique is often used in malware to alter the behavior of legitimate applications, such as redirecting function calls to malicious payloads or modifying the application's functionality without direct code alteration.

I will be posting various examples of the various techniques mentioned here.
Have a great day Everyone!

Py_Dev - October 8, 2024, 2:07 pm

Great post brother! Very informative and detailed. Keep up the good work!

Vinavil - October 8, 2024, 5:24 pm

Super useful, thanks for the great resources!

Flantoni - October 9, 2024, 5:02 pm

I have a file that won't get through windows defender if you/someone can help me get it through the defender using reverse reflective shell or dll hijacking

I'll pay that

Btw is a c2 agent