# TTP Detail – T1179

## TTP Information

Name: Hooking

Description: Windows processes often leverage application programming interface (API) functions to perform tasks that require reusable system resources. Windows API functions are typically stored in dynamic-link libraries (DLLs) as exported functions.

Hooking involves redirecting calls to these functions and can be implemented via:

\* \*\*Hooks procedures\*\*, which intercept and execute designated code in response to events such as messages, keystrokes, and mouse inputs. (Citation: Microsoft Hook Overview) (Citation: Elastic Process Injection July 2017)
\* \*\*Import address table (IAT) hooking\*\*, which use modifications to a process’s IAT, where pointers to imported API functions are stored. (Citation: Elastic Process Injection July 2017) (Citation: Adlice Software IAT Hooks Oct 2014) (Citation: MWRInfoSecurity Dynamic Hooking 2015)
\* \*\*Inline hooking\*\*, which overwrites the first bytes in an API function to redirect code flow. (Citation: Elastic Process Injection July 2017) (Citation: HighTech Bridge Inline Hooking Sept 2011) (Citation: MWRInfoSecurity Dynamic Hooking 2015)

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), adversaries may use hooking to load and execute malicious code within the context of another process, masking the execution while also allowing access to the process's memory and possibly elevated privileges. Installing hooking mechanisms may also provide Persistence via continuous invocation when the functions are called through normal use.

Malicious hooking mechanisms may also capture API calls that include parameters that reveal user authentication credentials for Credential Access. (Citation: Microsoft TrojanSpy:Win32/Ursnif.gen!I Sept 2017)

Hooking is commonly utilized by [Rootkit](https://attack.mitre.org/techniques/T1014)s to conceal files, processes, Registry keys, and other objects in order to hide malware and associated behaviors. (Citation: Symantec Windows Rootkits)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation

**•** mitre-attack: credential-access