Input Capture: Credential API Hooking, Sub-technique T1056.004 - Enterprise

Archived: 2026-04-05 15:48:07 UTC

Adversaries may hook into Windows application programming interface (API) functions and Linux system functions to collect user credentials. Malicious hooking mechanisms may capture API or function calls that include parameters that reveal user authentication credentials.[1] Unlike Keylogging, this technique focuses specifically on API functions that include parameters that reveal user credentials.

In Windows, 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.[2][3]
- **Import address table (IAT) hooking**, which use modifications to a process's IAT, where pointers to imported API functions are stored.[3][4][5]
- **Inline hooking**, which overwrites the first bytes in an API function to redirect code flow.[3][6][5]

In Linux and macOS, adversaries may hook into system functions via the `LD_PRELOAD` (Linux) or `DYLD_INSERT_LIBRARIES` (macOS) environment variables, which enables loading shared libraries into a program's address space. For example, an adversary may capture credentials by hooking into the `libc read` function leveraged by SSH or SCP.[7]

Source: https://attack.mitre.org/techniques/T1056/004