# TTP Detail – T1056.004

## TTP Information

Name: Credential API Hooking

Description: 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.(Citation: Microsoft TrojanSpy:Win32/Ursnif.gen!I Sept 2017) Unlike [Keylogging](https://attack.mitre.org/techniques/T1056/001), 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.(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)  
  
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.(Citation: Intezer Symbiote 2022)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: collection

**•** mitre-attack: credential-access

## Malware

* Carberp
* FinFisher
* NOKKI
* RDFSNIFFER
* TrickBot
* Ursnif
* VersaMem
* Zebrocy
* Zeus Panda
* ZxShell

## Tools

* Empire

## APTs (Intrusion Sets)

* PLATINUM