# TTP Detail – T1106

## TTP Information

Name: Native API

Description: Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes.(Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations.

Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system.

Native API functions (such as <code>NtCreateProcess</code>) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API <code>CreateProcess()</code> or GNU <code>fork()</code> will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations.(Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC)

Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation)

Adversaries may use assembly to directly or in-directly invoke syscalls in an attempt to subvert defensive sensors and detection signatures such as user mode API-hooks.(Citation: Redops Syscalls) Adversaries may also attempt to tamper with sensors and defensive tools associated with API monitoring, such as unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* ADVSTORESHELL
* Akira
* Amadey
* AppleSeed
* Aria-body
* Attor
* Avaddon
* AvosLocker
* BADHATCH
* BADNEWS
* BBK
* Babuk
* BackConfig
* Bad Rabbit
* Bandook
* Bankshot
* Bazar
* BendyBear
* Bisonal
* BitPaymer
* Black Basta
* BlackByte Ransomware
* BoxCaon
* Bumblebee
* CHIMNEYSWEEP
* CaddyWiper
* Carberp
* Chaes
* Chrommme
* Clop
* Cobalt Strike
* ComRAT
* Conti
* CostaBricks
* Cuba
* Cyclops Blink
* DCSrv
* DEADEYE
* DRATzarus
* DarkGate
* DarkTortilla
* Denis
* Diavol
* Dridex
* Egregor
* Emotet
* EvilBunny
* Exbyte
* Explosive
* FatDuke
* Flagpro
* FoggyWeb
* FunnyDream
* Gelsemium
* GoldenSpy
* Goopy
* Grandoreiro
* GrimAgent
* GuLoader
* HAWKBALL
* Hancitor
* HermeticWiper
* HermeticWizard
* HotCroissant
* HyperBro
* HyperStack
* IMAPLoader
* INC Ransomware
* IcedID
* InnaputRAT
* InvisiMole
* KOCTOPUS
* KONNI
* Kapeka
* Kevin
* KillDisk
* Latrodectus
* LightNeuron
* LitePower
* Lizar
* LockBit 3.0
* Lokibot
* MacMa
* Mafalda
* Mango
* MarkiRAT
* Maze
* MegaCortex
* Metamorfo
* Meteor
* Milan
* Mis-Type
* Misdat
* Mispadu
* Mosquito
* NETWIRE
* Nebulae
* Netwalker
* NightClub
* Ninja
* ODAgent
* OilBooster
* PLEAD
* Pikabot
* Pillowmint
* PipeMon
* PlugX
* PolyglotDuke
* Pony
* Prestige
* Pteranodon
* QUIETCANARY
* QakBot
* RCSession
* RDFSNIFFER
* REvil
* ROKRAT
* RTM
* RainyDay
* Ramsay
* Rising Sun
* RotaJakiro
* Royal
* Ryuk
* S-Type
* SUNSPOT
* SVCReady
* Sagerunex
* Saint Bot
* Samurai
* Sardonic
* SharpDisco
* ShimRat
* SideTwist
* Siloscape
* SodaMaster
* SombRAT
* StealBit
* StrifeWater
* Stuxnet
* SynAck
* SysUpdate
* Taidoor
* ThiefQuest
* TinyTurla
* Torisma
* TrickBot
* Uroburos
* Ursnif
* Volgmer
* WarzoneRAT
* WastedLocker
* Waterbear
* WhisperGate
* WindTail
* Winnti for Windows
* Woody RAT
* XAgentOSX
* XLoader
* ZeroCleare
* ZxShell
* ZxxZ
* build\_downer
* gh0st RAT
* metaMain
* njRAT
* xCaon

## Tools

* AsyncRAT
* BloodHound
* Brute Ratel C4
* Donut
* Empire
* Imminent Monitor
* PcShare
* SILENTTRINITY
* ShimRatReporter

## APTs (Intrusion Sets)

* APT37
* APT38
* BlackTech
* Chimera
* Gamaredon Group
* Gorgon Group
* Higaisa
* Lazarus Group
* Sandworm Team
* SideCopy
* Silence
* TA505
* ToddyCat
* Tropic Trooper
* Turla
* menuPass