# TTP Detail – T1129

## TTP Information

Name: Shared Modules

Description: Adversaries may execute malicious payloads via loading shared modules. Shared modules are executable files that are loaded into processes to provide access to reusable code, such as specific custom functions or invoking OS API functions (i.e., [Native API](https://attack.mitre.org/techniques/T1106)).

Adversaries may use this functionality as a way to execute arbitrary payloads on a victim system. For example, adversaries can modularize functionality of their malware into shared objects that perform various functions such as managing C2 network communications or execution of specific actions on objective.

The Linux & macOS module loader can load and execute shared objects from arbitrary local paths. This functionality resides in `dlfcn.h` in functions such as `dlopen` and `dlsym`. Although macOS can execute `.so` files, common practice uses `.dylib` files.(Citation: Apple Dev Dynamic Libraries)(Citation: Linux Shared Libraries)(Citation: RotaJakiro 2021 netlab360 analysis)(Citation: Unit42 OceanLotus 2017)

The Windows module loader can be instructed to load DLLs from arbitrary local paths and arbitrary Universal Naming Convention (UNC) network paths. This functionality resides in `NTDLL.dll` and is part of the Windows [Native API](https://attack.mitre.org/techniques/T1106) which is called from functions like `LoadLibrary` at run time.(Citation: Microsoft DLL)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Astaroth
* Attor
* BLINDINGCAN
* BOOSTWRITE
* Bumblebee
* DarkWatchman
* Dtrack
* Ebury
* FoggyWeb
* Hydraq
* KillDisk
* LightSpy
* Metamorfo
* OSX\_OCEANLOTUS.D
* PUNCHBUGGY
* PipeMon
* RotaJakiro
* Stuxnet
* TajMahal
* VersaMem
* gh0st RAT