# TTP Detail – T1158

## TTP Information

Name: Hidden Files and Directories

Description: To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a ‘hidden’ file. These files don’t show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (<code>dir /a</code> for Windows and <code>ls –a</code> for Linux and macOS).

Adversaries can use this to their advantage to hide files and folders anywhere on the system for persistence and evading a typical user or system analysis that does not incorporate investigation of hidden files.

### Windows

Users can mark specific files as hidden by using the attrib.exe binary. Simply do <code>attrib +h filename</code> to mark a file or folder as hidden. Similarly, the “+s” marks a file as a system file and the “+r” flag marks the file as read only. Like most windows binaries, the attrib.exe binary provides the ability to apply these changes recursively “/S”.

### Linux/Mac

Users can mark specific files as hidden simply by putting a “.” as the first character in the file or folder name (Citation: Sofacy Komplex Trojan) (Citation: Antiquated Mac Malware). Files and folder that start with a period, ‘.’, are by default hidden from being viewed in the Finder application and standard command-line utilities like “ls”. Users must specifically change settings to have these files viewable. For command line usages, there is typically a flag to see all files (including hidden ones). To view these files in the Finder Application, the following command must be executed: <code>defaults write com.apple.finder AppleShowAllFiles YES</code>, and then relaunch the Finder Application.

### Mac

Files on macOS can be marked with the UF\_HIDDEN flag which prevents them from being seen in Finder.app, but still allows them to be seen in Terminal.app (Citation: WireLurker).
Many applications create these hidden files and folders to store information so that it doesn’t clutter up the user’s workspace. For example, SSH utilities create a .ssh folder that’s hidden and contains the user’s known hosts and keys.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence