# TTP Detail – T1564.001

## TTP Information

Name: Hidden Files and Directories

Description: Adversaries may set files and directories to be hidden to evade detection mechanisms. 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).

On Linux and 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 folders 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.

Files on macOS can also 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). On Windows, users can mark specific files as hidden by using the attrib.exe binary. 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.

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

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Agent Tesla
* AppleJeus
* Attor
* BackConfig
* COATHANGER
* Calisto
* Carberp
* Clambling
* CoinTicker
* Cuckoo Stealer
* Dacls
* DarkGate
* EnvyScout
* Explosive
* FruitFly
* InvisiMole
* Ixeshe
* Komplex
* Lokibot
* LoudMiner
* MacSpy
* Machete
* Micropsia
* NETWIRE
* OSX/Shlayer
* OSX\_OCEANLOTUS.D
* Okrum
* PlugX
* PoetRAT
* QakBot
* Rising Sun
* SLOTHFULMEDIA
* SysUpdate
* ThiefQuest
* WannaCry
* WastedLocker
* XCSSET
* ccf32
* iKitten

## Tools

* Imminent Monitor
* QuasarRAT
* attrib

## APTs (Intrusion Sets)

* APT28
* APT32
* FIN13
* HAFNIUM
* Lazarus Group
* LuminousMoth
* Mustang Panda
* RedCurl
* Rocke
* Transparent Tribe
* Tropic Trooper