# TTP Detail – T1107

## TTP Information

Name: File Deletion

Description: Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.

There are tools available from the host operating system to perform cleanup, but adversaries may use other tools as well. Examples include native [cmd](https://attack.mitre.org/software/S0106) functions such as DEL, secure deletion tools such as Windows Sysinternals SDelete, or other third-party file deletion tools. (Citation: Trend Micro APT Attack Tools)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion