# TTP Detail – T1070.006

## TTP Information

Name: Timestomp

Description: Adversaries may modify file time attributes to hide new files or changes to existing files. Timestomping is a technique that modifies the timestamps of a file (the modify, access, create, and change times), often to mimic files that are in the same folder and blend malicious files with legitimate files.

In Windows systems, both the `$STANDARD\_INFORMATION` (`$SI`) and `$FILE\_NAME` (`$FN`) attributes record times in a Master File Table (MFT) file.(Citation: Inversecos Timestomping 2022) `$SI` (dates/time stamps) is displayed to the end user, including in the File System view, while `$FN` is dealt with by the kernel.(Citation: Magnet Forensics)

Modifying the `$SI` attribute is the most common method of timestomping because it can be modified at the user level using API calls. `$FN` timestomping, however, typically requires interacting with the system kernel or moving or renaming a file.(Citation: Inversecos Timestomping 2022)

Adversaries modify timestamps on files so that they do not appear conspicuous to forensic investigators or file analysis tools. In order to evade detections that rely on identifying discrepancies between the `$SI` and `$FN` attributes, adversaries may also engage in “double timestomping” by modifying times on both attributes simultaneously.(Citation: Double Timestomping)

In Linux systems and on ESXi servers, threat actors may attempt to perform timestomping using commands such as `touch -a -m -t <timestamp> <filename>` (which sets access and modification times to a specific value) or `touch -r <filename> <filename>` (which sets access and modification times to match those of another file).(Citation: Inversecos Linux Timestomping)(Citation: Juniper Networks ESXi Backdoor 2022)

Timestomping may be used along with file name [Masquerading](https://attack.mitre.org/techniques/T1036) to hide malware and tools.(Citation: WindowsIR Anti-Forensic Techniques)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* 3PARA RAT
* Attor
* BLINDINGCAN
* BPFDoor
* Bankshot
* BitPaymer
* BlackByte 2.0 Ransomware
* CHIMNEYSWEEP
* China Chopper
* Cobalt Strike
* Cyclops Blink
* Derusbi
* EVILNUM
* Elise
* FALLCHILL
* Gazer
* Gelsemium
* InvisiMole
* KeyBoy
* Kobalos
* MacMa
* Misdat
* MultiLayer Wiper
* NightClub
* Ninja
* OSX\_OCEANLOTUS.D
* OwaAuth
* POSHSPY
* PingPull
* PowerStallion
* Psylo
* SEASHARPEE
* Shamoon
* Stuxnet
* TAINTEDSCRIBE
* TDTESS
* UPSTYLE
* USBStealer
* Winnti for Windows
* metaMain

## Tools

* Empire

## APTs (Intrusion Sets)

* APT28
* APT29
* APT32
* APT38
* APT5
* Chimera
* Kimsuky
* Lazarus Group
* Rocke