Hide Artifacts: NTFS File Attributes, Sub-technique T1564.004 - Enterprise

Archived: 2026-04-05 17:17:42 UTC

Adversaries may use NTFS file attributes to hide their malicious data in order to evade detection. Every New Technology File System (NTFS) formatted partition contains a Master File Table (MFT) that maintains a record for every file/directory on the partition. [1] Within MFT entries are file attributes, [2] such as Extended Attributes (EA) and Data [known as Alternate Data Streams (ADSs) when more than one Data attribute is present], that can be used to store arbitrary data (and even complete files). [1] [3] [4] [5]

Adversaries may store malicious data or binaries in file attribute metadata instead of directly in files. This may be done to evade some defenses, such as static indicator scanning tools and anti-virus. [6] [4]

Source: https://attack.mitre.org/techniques/T1096