Masquerading: Double File Extension, Sub-technique T1036.007 - Enterprise

Archived: 2026-04-05 14:31:02 UTC

Adversaries may abuse a double extension in the filename as a means of masquerading the true file type. A file name may include a secondary file type extension that may cause only the first extension to be displayed (ex: `File.txt.exe` may render in some views as just `File.txt`). However, the second extension is the true file type that determines how the file is opened and executed. The real file extension may be hidden by the operating system in the file browser (ex: explorer.exe), as well as in any software configured using or similar to the system's policies.[1][2]

Adversaries may abuse double extensions to attempt to conceal dangerous file types of payloads. A very common usage involves tricking a user into opening what they think is a benign file type but is actually executable code. Such files often pose as email attachments and allow an adversary to gain Initial Access into a user's system via Spearphishing Attachment then User Execution. For example, an executable file attachment named `Evil.txt.exe` may display as `Evil.txt` to a user. The user may then view it as a benign text file and open it, inadvertently executing the hidden malware.[2]

Common file types, such as text files (.txt, .doc, etc.) and image files (.jpg, .gif, etc.) are typically used as the first extension to appear benign. Executable extensions commonly regarded as dangerous, such as .exe, .lnk, .hta, and .scr, often appear as the second extension and true file type.

Source: https://attack.mitre.org/techniques/T1036/007