Obfuscated Files or Information: Compression, Sub-technique T1027.015 - Enterprise

Archived: 2026-04-05 17:48:05 UTC

Adversaries may use compression to obfuscate their payloads or files. Compressed file formats such as ZIP, gzip, 7z, and RAR can compress and archive multiple files together to make it easier and faster to transfer files. In addition to compressing files, adversaries may also compress shellcode directly - for example, in order to store it in a Windows Registry key (i.e., Fileless Storage).[1]

In order to further evade detection, adversaries may combine multiple ZIP files into one archive. This process of concatenation creates an archive that appears to be a single archive but in fact contains the central directories of the embedded archives. Some ZIP readers, such as 7zip, may not be able to identify concatenated ZIP files and miss the presence of the malicious payload.[2]

File archives may be sent as one Spearphishing Attachment through email. Adversaries have sent malicious payloads as archived files to encourage the user to interact with and extract the malicious payload onto their system (i.e., Malicious File).[3] However, some file compression tools, such as 7zip, can be used to produce self-extracting archives. Adversaries may send self-extracting archives to hide the functionality of their payload and launch it without requiring multiple actions from the user.[4]

Compression may be used in combination with Encrypted/Encoded File where compressed files are encrypted and password-protected.

Source: https://attack.mitre.org/techniques/T1027/015