Application Layer Protocol: File Transfer Protocols, Sub-technique T1071.002 - Enterprise

Archived: 2026-04-05 12:44:16 UTC

Adversaries may communicate using application layer protocols associated with transferring files to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Protocols such as SMB[1], FTP[2], FTPS, and TFTP that transfer files may be very common in environments. Packets produced from these protocols may have many fields and headers in which data can be concealed. Data could also be concealed within the transferred files. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

Source: https://attack.mitre.org/techniques/T1071/002