Stage Capabilities: Upload Tool, Sub-technique T1608.002 - Enterprise

Archived: 2026-04-05 18:09:32 UTC

Adversaries may upload tools to third-party or adversary controlled infrastructure to make it accessible during targeting. Tools can be open or closed source, free or commercial. Tools can be used for malicious purposes by an adversary, but (unlike malware) were not intended to be used for those purposes (ex: PsExec). Adversaries may upload tools to support their operations, such as making a tool available to a victim network to enable Ingress Tool Transfer by placing it on an Internet accessible web server.

Tools may be placed on infrastructure that was previously purchased/rented by the adversary (Acquire Infrastructure) or was otherwise compromised by them (Compromise Infrastructure).[1] Tools can also be staged on web services, such as an adversary controlled GitHub repo, or on Platform-as-a-Service offerings that enable users to easily provision applications.[2][3][4]

Adversaries can avoid the need to upload a tool by having compromised victim machines download the tool directly from a third-party hosting location (ex: a non-adversary controlled GitHub repo), including the original hosting site of the tool.

Source: https://attack.mitre.org/techniques/T1608/002