Stage Capabilities, Technique T1608 - Enterprise

Archived: 2026-04-05 16:11:20 UTC

Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed (Develop Capabilities) or obtained (Obtain Capabilities) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary (Acquire Infrastructure) or was otherwise compromised by them (Compromise Infrastructure). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.[1][2][3][4][5]

Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to):

- Staging web resources necessary to conduct Drive-by Compromise when a user browses to a site.[6][7][8]
- Staging web resources for a link target to be used with spearphishing.[9][10]
- Uploading malware or tools to a location accessible to a victim network to enable Ingress Tool Transfer.[1]
- Installing a previously acquired SSL/TLS certificate to use to encrypt command and control traffic (ex: Asymmetric Cryptography with Web Protocols).[11]

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