Web Service: Bidirectional Communication, Sub-technique T1481.002 - Mobile

Archived: 2026-04-05 13:45:23 UTC

Adversaries may use an existing, legitimate external Web service channel as a means for sending commands to and receiving output from a compromised system. Compromised systems may leverage popular websites and social media to host command and control (C2) instructions. Those infected systems can then send the output from those commands back over that Web service channel. The return traffic may occur in a variety of ways, depending on the Web service being utilized. For example, the return traffic may take the form of the compromised system posting a comment on a forum, issuing a pull request to development project, updating a document hosted on a Web service, or by sending a Tweet.

Popular websites and social media, acting as a mechanism for C2, may give a significant amount of cover. This is due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Source: https://attack.mitre.org/techniques/T1481/002