Compromise Infrastructure: Web Services, Sub-technique T1584.006 - Enterprise

Archived: 2026-04-05 17:40:56 UTC

Other sub-techniques of Compromise Infrastructure (8)

Adversaries may compromise access to third-party web services that can be used during targeting. A variety of popular websites exist for legitimate users to register for web-based services, such as GitHub, Twitter, Dropbox, Google, SendGrid, etc. Adversaries may try to take ownership of a legitimate user's access to a web service and use that web service as infrastructure in support of cyber operations. Such web services can be abused during later stages of the adversary lifecycle, such as during Command and Control (Web Service), Exfiltration Over Web Service, or Phishing.[1] Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. By utilizing a web service, particularly when access is stolen from legitimate users, adversaries can make it difficult to physically tie back operations to them. Additionally, leveraging compromised web-based email services may allow adversaries to leverage the trust associated with legitimate domains.

Source: https://attack.mitre.org/techniques/T1584/006