Compromise Accounts: Email Accounts, Sub-technique T1586.002 - Enterprise

Archived: 2026-04-05 14:37:46 UTC

Adversaries may compromise email accounts that can be used during targeting. Adversaries can use compromised email accounts to further their operations, such as leveraging them to conduct Phishing for Information, Phishing, or large-scale spam email campaigns. Utilizing an existing persona with a compromised email account may engender a level of trust in a potential victim if they have a relationship with, or knowledge of, the compromised persona. Compromised email accounts can also be used in the acquisition of infrastructure (ex: Domains).

A variety of methods exist for compromising email accounts, such as gathering credentials via Phishing for Information, purchasing credentials from third-party sites, brute forcing credentials (ex: password reuse from breach credential dumps), or paying employees, suppliers or business partners for access to credentials.[1][2] Prior to compromising email accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation. Adversaries may target compromising well-known email accounts or domains from which malicious spam or Phishing emails may evade reputation-based email filtering rules.

Adversaries can use a compromised email account to hijack existing email threads with targets of interest.

Source: https://attack.mitre.org/techniques/T1586/002