Gather Victim Identity Information: Credentials, Sub-technique T1589.001 - Enterprise

Archived: 2026-04-05 13:37:51 UTC

Adversaries may gather credentials that can be used during targeting. Account credentials gathered by adversaries may be those directly associated with the target victim organization or attempt to take advantage of the tendency for users to use the same passwords across personal and business accounts.

Adversaries may gather credentials from potential victims in various ways, such as direct elicitation via Phishing for Information. Adversaries may also compromise sites then add malicious content designed to collect website authentication cookies from visitors.[1] [2][3][4][5][6][7][8] Where multi-factor authentication (MFA) based on out-of-band communications is in use, adversaries may compromise a service provider to gain access to MFA codes and one-time passwords (OTP).[9]

Credential information may also be exposed to adversaries via leaks to online or other accessible data sets (ex: Search Engines, breach dumps, code repositories, etc.). Adversaries may purchase credentials from dark web markets, such as Russian Market and 2easy, or through access to Telegram channels that distribute logs from infostealer malware.[10][11][12]

Gathering this information may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Phishing for Information), establishing operational resources (ex: Compromise Accounts), and/or initial access (ex: External Remote Services or Valid Accounts).

Source: https://attack.mitre.org/techniques/T1589/001