

Data from Information Repositories: Databases, Sub-technique T1213.006 - Enterprise

Archived: 2026-04-05 14:21:55 UTC

Adversaries may leverage databases to mine valuable information. These databases may be hosted on-premises or in the cloud (both in platform-as-a-service and software-as-a-service environments).

Examples of databases from which information may be collected include MySQL, PostgreSQL, MongoDB, Amazon Relational Database Service, Azure SQL Database, Google Firebase, and Snowflake. Databases may include a variety of information of interest to adversaries, such as usernames, hashed passwords, personally identifiable information, and financial data. Data collected from databases may be used for [Lateral Movement](#), [Command and Control](#), or [Exfiltration](#). Data exfiltrated from databases may also be used to extort victims or may be sold for profit.^[1]

Source: <https://attack.mitre.org/techniques/T1213/006>