Software Discovery: Backup Software Discovery, Sub-technique T1518.002 - Enterprise

Archived: 2026-04-05 17:14:32 UTC

Adversaries may attempt to get a listing of backup software or configurations that are installed on a system. Adversaries may use this information to shape follow-on behaviors, such as Data Destruction, Inhibit System Recovery, or Data Encrypted for Impact.

Commands that can be used to obtain security software information are netsh, `reg query` with Reg, `dir` with cmd, and Tasklist, but other indicators of discovery behavior may be more specific to the type of software or security system the adversary is looking for, such as Veeam, Acronis, Dropbox, or Paragon.[1]

Source: https://attack.mitre.org/techniques/T1518/002