# Backup Software Discovery via CLI, Registry, and Process Inspection (T1518.002), Detection Strategy DET0088

Archived: 2026-04-05 14:54:36 UTC

### AN0240

Defender observes execution of commands like `tasklist`, `sc query`, `reg query`, or PowerShell WMI/Registry queries targeting known backup products (e.g., Veeam, Acronis, CrashPlan). Behavior often includes parent-child lineage involving PowerShell or cmd.exe with discovery syntax, and enumeration of services, directories, or registry paths tied to backup software.

#### Log Sources

#### Mutable Elements

| Field | Description |
|---|---|
| KnownBackupVendors | List of software vendors to match in command-line or registry queries |
| UserContextScope | Focus on low-privilege or interactive user contexts rather than service accounts |
| SuspiciousParentProcesses | Flag execution from scripting tools, interpreters, or LOLBins |

### AN0241

Defender observes use of CLI tools (`find`, `grep`, `ls`, `dpkg`, `rpm`, `systemctl`, `ps aux`) to discover backup agents or config files (e.g., rsnapshot, duplicity, veeam). This often includes command lines that recursively search `/etc/`, `/opt/`, or `/var/` directories for keywords like `backup`, and parent-child relationships involving shell or Python scripts.

#### Log Sources

| Data Component | Name | Channel |
|---|---|---|
| Process Creation (DC0032) | auditd:SYSCALL | execve: Execution of discovery commands targeting backup binaries, processes, or config paths |
| File Access (DC0055) | auditd:PATH | Read access to known backup software configuration files (e.g., /etc/rsnapshot.conf, /opt/veeam/config.ini) |

#### Mutable Elements

| Field | Description |
| --- | --- |
| BackupConfigPaths | Directory paths and filenames related to backup agents |
| ToolchainScope | Shells, interpreters, or binaries used by attacker scripts for discovery |

### AN0242

Defender detects execution of `mdfind`, `launchctl`, or GUI-based enumeration (e.g., `/Applications/Time Machine.app`) along with command-line usage of `find`, `grep`, or `system_profiler` to identify installed backup tools like Time Machine, Carbon Copy Cloner, or Backblaze. Often triggered from Terminal sessions or within post-exploitation scripts.

#### Log Sources

| Data Component | Name | Channel |
| --- | --- | --- |
| Process Creation (DC0032) | macos:unifiedlog | Process execution logs showing discovery commands like mdfind, system_profiler, or launchctl list |
| File Access (DC0055) | macos:unifiedlog | Read access to Time Machine plist files or CCC configurations in ~/Library/Preferences/ |

#### Mutable Elements

| Field | Description |
| --- | --- |
| InstallLocationScope | Directories or bundles where backup tools are commonly installed |
| KnownAppPlistPaths | Plist files related to backup software configurations |

---

Source: https://attack.mitre.org/detectionstrategies/DET0088#AN0241