

Behavioral Detection for T1490 - Inhibit System Recovery, Detection Strategy DET0329

Archived: 2026-04-02 11:38:46 UTC

AN0933

Process chains that use native utilities (vssadmin, wbadmin, diskshadow, bcdedit, REAgentC, wmic) with arguments to delete shadow copies, disable recovery, or remove backup catalogs

Log Sources

Mutable Elements

| Field | Description |
|----------------------|---|
| TimeWindow | Used to track rapid recovery feature changes over short intervals |
| CommandLinePattern | Can be tuned to catch variations in destructive flags (/all, /quiet, -delete) |
| ParentProcessContext | Tune based on common parent-child chains (e.g., powershell → diskshadow) |

AN0934

Shell utilities or scripts deleting `/etc/systemd/system/rescue.target`, `/etc/fstab` backups, or `/boot/efi` partitions; chattr used to block snapshot auto-recovery

Log Sources

Mutable Elements

| Field | Description |
|------------------|---|
| WatchedFilePaths | Modify to include specific OS backup configs or LVM snapshots |
| ShellProcessUser | Restrict detection to root or sudo users |

AN0935

ESXi shell or vim-cmd execution that deletes all VM snapshots using vmsvc/snapshot.removeall or rm on snapshot paths

Log Sources

Mutable Elements

| Field | Description |
|---------------|--|
| TargetVMNames | Limit to critical VM names to reduce false positives |

AN0936

Execution of `erase` , `format` , and `reload` in immediate sequence from a privileged AAA session

Log Sources

Mutable Elements

| Field | Description |
|-----------------------|--|
| CommandSequenceWindow | Time between erase and reload command to establish causality |
| UserPrivilegeLevel | Filter for high-privilege user sessions |

AN0937

Cloud API calls disabling snapshot scheduling, backup policies, versioning, followed by DeleteSnapshot/DeleteVolume operations

Log Sources

Mutable Elements

| Field | Description |
|--------------|--|
| UserAgent | Tune for legitimate backup automation vs unknown tools |
| ResourceType | Filter only on production images or vaults |

Source: <https://attack.mitre.org/detectionstrategies/DET0329#AN0933>