Behavioral Detection for Service Stop across Platforms, Detection Strategy DET0021

Archived: 2026-04-05 13:58:13 UTC

AN0061

Adversary disables or stops critical services (e.g., Exchange, SQL, AV, endpoint monitoring) using native utilities or API calls, often preceding destructive actions (T1485, T1486). Behavioral chain: Elevated execution context + stop-service or sc.exe or ChangeServiceConfigW + terminated or disabled service + possible follow-up file manipulation.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time span between elevated privilege use and critical service stop
ServiceName	Service names of interest (e.g., MSExchangeIS, SQLSERVERAGENT)
ParentProcess	Upstream process lineage leading to service stop

AN0062

Adversary executes systemctl or service stop targeting high-value services (e.g., mysql, sshd), possibly followed by rm or shred against data stores. Behavioral chain: sudo/su usage + stop command + /var/log/messages or syslog entries + file access/delete.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Window between service stop and suspicious file deletion
ExecUser	Username or UID executing service stop command

AN0063

Use of launchctl to stop services or kill critical background processes (e.g., securityd, com.apple.*), typically followed by command-line tools like rm or diskutil. Behavioral chain: Terminal or remote shell + launchctl bootout/disable + process termination + follow-on modification.

Log Sources

Mutable Elements

Field	Description
ServiceLabel	Launch daemon label or name targeted by command
LaunchType	Whether the command disables or boots out the service

AN0064

Attacker disables VM-related services or stops VMs forcibly to target vmdk or logs. Behavioral chain: esxcli or vim-cmd stop + audit log showing user privilege use + datastore file manipulation.

Log Sources

Mutable Elements

Field	Description
VMName	Targeted virtual machine name
InitiatorUser	User who issued stop or disable command
