Detection of Data Destruction Across Platforms via Mass Overwrite and Deletion Patterns, Detection Strategy DET0146

Archived: 2026-04-05 14:46:06 UTC

AN0411

Adversary spawns command-line tools (e.g., del, cipher /w, SDelete) or scripts to recursively delete or overwrite user/system files. This may be correlated with abnormal file IO activity, registry writes, or tampering in critical system directories.

Log Sources

Mutable Elements

Field	Description
TargetFilename	Filter file deletion activity to sensitive locations (e.g., %System32%, Documents, DB paths).
ProcessCommandLine	Tune for aggressive overwrite flags (e.g., /w, /q, /s) or temp file overwrites.
VolumeThreshold	Threshold of unique file deletions or modifications within time window.
TimeWindow	Correlate rapid file delete/overwrite behavior from same process/user.

AN0412

Massive recursive deletions or overwrites via `rm -rf`, `shred`, `dd`, or wiper binaries. May include unlink syscalls, deletion of known config/data paths, or sequential overwrite patterns.

Log Sources

Mutable Elements

Field	Description
ExecutablePath	Focus on binaries like shred, dd, wipe, custom wipers, or bash execution chains.
DeletedPathPattern	Tune for critical mount points or home/data directories.
SyscallBurstRate	Rate of unlink/unlinkat syscalls to indicate mass deletion in a short period.

AN0413

Destruction via `rm -rf`, overwrite with `dd` or `srm`, often executed by script in /tmp or /private/tmp, may also involve file overwrite to political or decoy image data.

Log Sources

Mutable Elements

Field	Description
CommandPattern	Focus on high-risk patterns in temporary directories or key system paths.
EntropyChangeRate	Optional anomaly detection on overwritten files with high-entropy payloads.

AN0414

Adversary deletes critical infrastructure: EC2 instances, S3 buckets, snapshots, or volumes using elevated IAM credentials. Frequently includes batch API calls with `Delete*` or `TerminateInstances`.

Log Sources

Mutable Elements

Field	Description
OperationType	Correlate multiple destructive API calls over short intervals.
UserAgent	Flag non-console/API clients initiating destructive behavior.
RegionScope	Observe whether deletions span multiple regions or org accounts.

AN0415

Adversary destroys virtual disks (VMDK), images, or VMs by invoking `vim-cmd`, deleting datastore contents, or purging snapshots.

Log Sources

Mutable Elements

Field	Description
DatastorePath	Targeted deletion of critical VMDKs or VM configuration files.
InitiatingUser	Detect deletions from users outside normal maintenance windows.

AN0416

Container process executes destructive file operations inside volume mounts or host paths. Includes `rm -rf /mnt/volumes/`, container breakout followed by host deletion attempts.

Log Sources

Mutable Elements

Field	Description
MountPoint	Identify when deletions occur inside persistent or shared volume paths.
ContainerImage	Correlate destructive behavior with unknown or untrusted container sources.
