Detection of Multi-Platform File Encryption for Impact, Detection Strategy DET0215

Archived: 2026-04-05 14:07:57 UTC

AN0602

High-frequency file write operations using uncommon extensions, followed by ransom note creation, registry tampering, or shadow copy deletion. Often uses CLI tools like vssadmin, wbadmin, cipher, or PowerShell.

Log Sources

Mutable Elements

Field	Description
FileExtension	Non-standard or randomly generated file extensions may indicate encrypted content.
TargetFolder	Focus on user document folders, network shares, or system paths like %System32%.
TimeWindow	Correlate rapid writes and renames within seconds across high file count.
CommandLine	Flag common ransomware tools or functions (vssadmin delete shadows /all /quiet).

AN0603

Encryption via custom or open-source tools (e.g., openssl, gpg, aescrypt) recursively targeting user or system directories. Also includes overwrite of existing data and ransom note drops.

Log Sources

Mutable Elements

Field	Description
FilenamePattern	Look for creation of ransom note files (e.g., READ_ME.txt, HELP_DECRYPT.html).
SyscallBurstRate	High write/open/unlink activity in short intervals indicates encryption attempts.
DirectoryTargeted	Correlate activity in /home, /etc, /opt, or mounted volumes.

AN0604

Userland or kernel-level ransomware encrypting user files (Documents, Desktop) using `srm`, `gpg`, or compiled payloads. Often correlated with ransom note creation in multiple directories.

Log Sources

Mutable Elements

Field	Description
ExtensionPattern	Encrypted files may use .locked, .enc, or ransom-specific extensions.
VolumeTargeted	Detect activity targeting mounted external or backup volumes.

AN0605

Ransomware encrypts .vmdk, .vmx, .log, or VM config files in VMFS datastores. May rename to .locked or delete/overwrite with encrypted versions. Often correlates with shell commands run through `dcui`, SSH, or vSphere.

Log Sources

Mutable Elements

Field	Description
FileType	Detect renames or write patterns involving .vmdk, .vmx, .nvram.
UserContext	Identify shell sessions opened by root or unexpected users outside maintenance window.

AN0606

Encryption of cloud storage objects (e.g., S3 buckets) via Server-Side Encryption (SSE-C) or by replacing objects with encrypted variants. May include API patterns like PutObject with SSE-C headers.

Log Sources

Mutable Elements

Field	Description
SSEHeader	SSE-C headers indicate attacker-controlled encryption keys.
AffectedBucket	Prioritize logs, backups, or shared document storage buckets.
UserAgent	Detect scripted automation vs console-based API behavior.

Source: https://attack.mitre.org/detectionstrategies/DET0215#AN0602