Behavioral Detection Strategy for Exfiltration Over Symmetric Encrypted Non-C2 Protocol, Detection Strategy DET0503

Archived: 2026-04-05 18:10:25 UTC

AN1389

Detects the execution of non-browser processes establishing outbound encrypted network connections using uncommon symmetric encryption protocols (e.g., AES via PowerShell or custom scripts) to alternate external destinations.

Log Sources

Mutable Elements

Field	Description
PayloadEntropyThreshold	Flag high-entropy payloads sent over unexpected protocols.
TimeWindow	Define allowable transfer window (e.g., abnormal traffic outside business hours).
ExecutableAllowlist	List of known-good binaries for encrypted traffic (e.g., Chrome, Outlook).

AN1390

Detects command-line utilities or scripts using encryption libraries or symmetric algorithms (e.g., OpenSSL AES, GPG, Python + PyCrypto) in conjunction with outbound file transfers or traffic to external destinations.

Log Sources

Mutable Elements

Field	Description
FileTransferIndicator	Threshold for transferred data size or extension type.
LibraryCallTracking	Hooks into use of encryption libraries like `libcrypto.so`, `pycrypto`, `gpg`.

AN1391

Detects symmetric key-based encryption operations (e.g., AES via Python, AppleScript, or OpenSSL) followed by unusual outbound connections from non-browser applications or scripted tools.

Log Sources

Mutable Elements

Field	Description
ApplicationProfileBaseline	Expected outbound connection profiles per app.
EncryptionRoutinePattern	Indicators of manual encryption operations (e.g., script strings invoking AES).

AN1392

Detects unexpected encrypted egress traffic from management services (e.g., hostd) or guest VMs utilizing symmetric encryption without traditional protocols (e.g., FTP with embedded AES ciphertext).

Log Sources

Mutable Elements

Field	Description
GuestVMExfilWatchlist	VMs with data sensitivity labels or outside normal behavior.
ServiceEgressProfile	Expected egress destinations and volume for core services.
