Detection of Local Data Collection Prior to Exfiltration, Detection Strategy DET0380

Archived: 2026-04-02 10:48:12 UTC

AN1070

Adversaries collecting local files via PowerShell, WMI, or direct file API calls often include recursive file listings, targeted file reads, and temporary file staging.

Log Sources

Mutable Elements

Field	Description
TargetFilePathRegex	Allows tuning for file extensions or paths of sensitive data (e.g., *.xls, *.db, *.pdf).
ParentProcessFilter	Used to scope monitoring to suspicious parent/child process trees like PowerShell or WMI spawning file reads.

AN1071

Adversaries using bash scripts or tools to recursively enumerate user home directories, config files, or SSH keys.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time span to correlate multiple file access events indicative of scripted or bulk access.
ScriptToolName	List of tools (e.g., `find`, `grep`, `tar`, `scp`) that may be benign but are context-sensitive.

AN1072

Adversary use of bash/zsh or AppleScript to locate files and exfil targets like user keychains or documents.

Log Sources

Mutable Elements

Field	Description
UserContext	Useful for excluding known admin or scheduled jobs.
TargetVolume	Focus monitoring on removable drives or external paths.

AN1073

Collection of device configuration via CLI commands (e.g., `show running-config`, `copy flash`, `more`), often followed by TFTP/SCP transfers.

Log Sources

Mutable Elements

Field	Description
CommandScope	Defines list of configuration or diagnostic commands to monitor.
AuthenticatedUserList	Helps reduce false positives by whitelisting known admins.

AN1074

Adversaries accessing datastore or configuration files via `vim-cmd`, `esxcli`, or SCP to extract logs, VMs, or host configurations.

Log Sources

Mutable Elements

Field	Description
AccessPathRegex	Regex for filtering targeted VM paths or files like *.vmdk, *.vmx.
InteractiveShellUsage	Tune to distinguish between interactive and script-driven data access.
