Automated File and API Collection Detection Across Platforms, Detection Strategy DET0186

Archived: 2026-04-05 14:21:46 UTC

AN0531

Automated execution of native utilities and scripts to discover, enumerate, and exfiltrate files and clipboard content. Focus is on detecting repeated file access, scripting engine use, and use of command-line utilities commonly leveraged by collection scripts.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Defines the lookback period for identifying burst activity or patterns in process/file events.
SuspiciousFileExtensions	Tunable list of file extensions associated with collection (e.g., .pdf, .docx).
ProcessCountThreshold	The number of times a process executes before considered anomalous.

AN0532

Repeated or automated access to user document directories or clipboard using shell scripts or utilities like xclip/pbpaste. Detectable via auditd syscall logs or osquery file events.

Log Sources

Mutable Elements

Field	Description
AccessPath	Tunable location for sensitive files like /home/*/Documents.
ScriptInterpreterList	Shells or scripting engines to monitor (e.g., bash, python, perl).

AN0533

Use of pbpaste, AppleScript, or third-party automation frameworks (e.g., Automator) to collect clipboard or file content in bursts. Observable via unified logs.

Log Sources

Mutable Elements

Field	Description
AutomationTool	Detectable script interpreters or clipboard tools (pbpaste, osascript).
ClipboardCheckRate	Threshold for how often clipboard access occurs within a given time window.

AN0534

Suspicious sign-ins to Graph API or sensitive resources using non-browser scripting agents (e.g., Python, PowerShell), often for programmatic access to mailbox or OneDrive content.

Log Sources

Mutable Elements

Field	Description
UserAgentFilter	Filter for scripting agents (e.g., Python, PowerShell) which may vary by org.
ExpectedClientIPList	Set of known internal or managed IPs to filter benign automation.
DeviceProperties	Expected managed device profiles used to detect unmanaged devices.
