Clipboard Data Access with Anomalous Context, Detection Strategy DET0341

Archived: 2026-04-05 15:46:31 UTC

AN0965

Detection of clipboard access via OS utilities (e.g., clip.exe, Get-Clipboard) by non-interactive or abnormal parent processes, potentially chained with staging or exfiltration commands.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Defines how far back to look for parent-child relationships and follow-on network activity.
UserContext	Filters based on service vs interactive users to reduce noise.
ParentProcessName	Tunable list of expected/benign clipboard accessors.

AN0966

Detection of pbpaste/pbcopy clipboard access by processes without terminal sessions or linked to launch agents, potentially staged for collection.

Log Sources

Mutable Elements

Field	Description
ExecutionChainLength	How many chained or embedded processes to track for correlation.
TerminalSession	Whether the pbpaste/pbcopy action is tied to a user terminal.
BinaryPath	Adjust if clipboard tooling is relocated (e.g., /opt/empyre/pbpaste).

AN0967

Detection of xclip or xsel access to clipboard buffers outside of user terminal context, especially when chained to staging (gzip, base64) or network exfiltration (curl, scp).

Log Sources

Mutable Elements

Field	Description
ClipboardCommand	Tool used (xclip, xsel, custom clipboard-read binary).
CorrelationWindow	Temporal window to chain staging or network activity with clipboard access.
TTYLinked	Was access linked to interactive user TTY?
