Linux Detection Strategy for T1547.013 - XDG Autostart Entries, Detection Strategy DET0390

Archived: 2026-04-05 12:42:51 UTC

Analytics

- Linux

AN1096

Correlation of file creation/modification of `.desktop` files within XDG autostart directories, followed by execution of processes at user login initiated by the desktop environment. Malicious entries typically include suspicious Exec paths or anomalous names and are not associated with installed packages.

Log Sources

Mutable Elements

Field	Description
ExecCommandPattern	Regex or allowlist of expected Exec paths within .desktop files. Deviations may be suspicious.
AutostartDirectory	May vary by user config (e.g., $XDG_CONFIG_HOME). Must enumerate actual values per system.
TimeWindow	Correlate file creation/mod + exec within login window (e.g., 0–5 min of user logon).
UserContext	Should filter to non-system users, as XDG persistence typically targets interactive sessions.
PackageOriginBaseline	Compare .desktop entries to known package sources (e.g., `dpkg -S`). Unexpected origins may be suspicious.
