Detection Strategy for Lua Scripting Abuse, Detection Strategy DET0101

Archived: 2026-04-05 16:50:19 UTC

AN0278

Detects execution of Lua interpreters or scripts (.lua), especially when correlated with suspicious parent processes or file drop events, indicating malicious use of embedded scripting.

Log Sources

Mutable Elements

Field	Description
ParentProcessName	May vary depending on delivery vector (e.g., explorer.exe, cmd.exe, rundll32.exe)
TimeWindow	Used to correlate file drop and execution of Lua scripts in close succession.

AN0279

Detects invocation of lua or luajit interpreters by users or services outside of expected packages, chained with script drop or memory artifacts.

Log Sources

Mutable Elements

Field	Description
ExecutablePath	Lua interpreter path may vary based on distro or adversary staging.
UserContext	May need to exclude service or admin accounts that use Lua legitimately.

AN0280

Detects Lua script execution via native or 3rd party interpreters, chained with unsigned binaries or unexpected parent lineage.

Log Sources

Mutable Elements

Field	Description
ParentProcessName	Adjustable based on system activity patterns (e.g., Terminal vs GUI)
SignatureStatus	Helps filter unsigned or self-signed Lua payloads.

AN0281

Detects embedded Lua interpreter execution or script injection on devices supporting Lua scripting (e.g., routers, firewalls), often seen in modified firmware or abused APIs.

Log Sources

Mutable Elements

Field	Description
FirmwareBuildHash	Used to baseline known good versions versus injected scripts.
ScriptInjectionPath	Path to where scripts are allowed or denied based on config.
