Detect Multi-Stage Command and Control Channels, Detection Strategy DET0228

Archived: 2026-04-05 18:38:15 UTC

AN0637

Initial process initiates outbound connection to first-stage C2, receives payloads or commands, then spawns or injects into a second process that establishes a new outbound connection to an unrelated destination (second-stage C2).

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlate two-stage behavior occurring within a short window (e.g., 1-5 minutes)
ParentProcess	Tune to exclude known legitimate updaters and management agents
DestinationHostname	May be customized to exclude known corporate domains and CDNs

AN0638

Shell script or binary initiates curl/wget request to staging domain, writes output to disk or memory, and shortly afterward launches another process that establishes new outbound connection to a different IP or hostname.

Log Sources

Mutable Elements

Field	Description
BinaryPath	Tune for suspicious binaries like curl, wget, python, netcat
IPDistance	Detect multiple different external IPs contacted within short timeframe

AN0639

Initial process using NSURLSession or similar APIs reaches out to known staging domains, followed by creation of a reverse shell or RAT connecting to a second unrelated server.

Log Sources

Mutable Elements

Field	Description
UserContext	Detect activity outside normal user behavior (e.g., automation or daemon context)
EntropyScore	Optional for detecting encoded payloads delivered via stage 1

AN0640

CLI-based or API-based network call from the hypervisor to external staging host, shortly followed by a connection to a second external IP by a spawned process or scheduled task.

Log Sources

Mutable Elements

Field	Description
ScheduledTaskName	Detect unknown or obfuscated task names launching follow-up stages
DestinationIP	Scope multiple IP destinations outside corporate ranges in short sequence

---