Detection Strategy for T1497 Virtualization/Sandbox Evasion, Detection Strategy DET0046

Archived: 2026-04-05 14:21:54 UTC

AN0127

Execution of discovery commands or API calls for virtualization artifacts (e.g., registry keys, device drivers, services), sleep/skipped execution behavior, or sandbox evasion DLLs before payload deployment.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time range in which multiple discovery processes or sleep/delay operations are executed to avoid sandbox detonation.
KnownVMArtifactList	Registry paths, DLLs, services or device names indicative of sandbox/VM environments.

AN0128

Execution of commands to enumerate virtualization-related files or processes (e.g., '/sys/class/dmi/id/product_name', dmesg, lscpu, lspci), or querying hypervisor interfaces prior to malware execution.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	execve or syscall invoking vm artifact check commands (e.g., dmidecode, lspci, dmesg)
Command Execution (DC0064)	auditd:SYSCALL	sleep function usage or loops (nanosleep, usleep) in scripts

Mutable Elements

Field	Description
TimeWindow	Duration between VM discovery commands and payload execution
CommandArtifactMatchList	Command-line regex patterns indicative of sandbox evasion (e.g., grep QEMU, strings vmware)

AN0129

Execution of scripts or binaries that check for virtualization indicators (e.g., system_profiler, ioreg -l, kextstat), combined with delay functions or anomalous launchd activity.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	execution of system_profiler, ioreg, kextstat with argument patterns related to VM/sandbox checks
Module Load (DC0016)	macos:unifiedlog	dynamic loading of sleep-related functions or sandbox detection libraries

Mutable Elements

Field	Description
ProcessCommandPattern	Detection regex or substring matching sandbox-related checks
SleepThreshold	Maximum duration of sleep execution before alert (e.g., > 5 minutes)
