Virtualization/Sandbox Evasion via System Checks across Windows, Linux, macOS, Detection Strategy DET0168

Archived: 2026-04-05 14:22:16 UTC

AN0478

Script or binary performs a rapid sequence of system discovery checks (e.g., CPU count, RAM size, registry keys, running processes) indicative of VM detection

Log Sources

Mutable Elements

Field	Description
TimeWindow	Sequence of system enumeration events within X seconds
ProcessAncestry	Parent-child lineage to identify potentially suspicious launch sources (e.g., Office, browser, WMI, PowerShell)
UserContext	Limit to non-admin or interactive sessions if desired

AN0479

Shell script or binary uses multiple system commands (e.g., dmidecode, lscpu, lspci) in quick succession to detect virtualization environment

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	execve of system tools like dmidecode, lspci, lscpu, dmesg, systemd-detect-virt

Mutable Elements

Field	Description
TimeWindow	Burst of system info commands within X seconds
CommandPattern	Regex or substring matching virtualization artifact checks

AN0480

Bash, Swift, or Objective-C programs enumerate system profile, I/O registry, or inspect kernel extensions to identify VM artifacts

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	exec or spawn of 'system_profiler', 'ioreg', 'kextstat', 'sysctl', or calls to sysctl API

Mutable Elements

Field	Description
ExecutionBurst	Threshold of sequential system checks or tools used in a short time
ToolName	Specific tools used for querying device and system metadata

---