Detection Strategy for Hidden Virtual Instance Execution, Detection Strategy DET0321

Archived: 2026-04-05 17:05:04 UTC

AN0909

Unusual execution of virtualization binaries (VBoxManage.exe, vmware-vmx.exe, vmwp.exe) with headless or suppressed notification arguments. Registry and service modifications linked to virtualization installs. Defender view: anomalies in process creation, service metadata, and registry writes tied to enabling hidden VMs.

Log Sources

Mutable Elements

Field	Description
VirtualizationBinaryWhitelist	Exclude known administrative VM software usage in enterprise environments.
TimeWindow	Correlate registry and service modifications with VM process starts within a narrow time frame.

AN0910

Execution of QEMU, KVM, or VirtualBox processes with unusual flags (e.g., '-nographic', '-snapshot'). File creation of VM images in atypical directories. Defender view: monitoring audit logs for process executions and file modifications linked to hidden virtualization.

Log Sources

Mutable Elements

Field	Description
ImageDirectoryWhitelist	Legitimate VM image storage paths to reduce false positives.
UserContext	Correlate suspicious VM execution with non-admin or service accounts.

AN0911

Execution of virtualization binaries (Parallels, VMware Fusion, VirtualBox) with arguments to hide UI. File monitoring for plist modifications indicating hidden virtualization behavior. Defender perspective: tracking

process lineage and file modifications in system configs.

Log Sources

Mutable Elements

Field	Description
PlistKeyScope	Focus monitoring on UI suppression or VM auto-run keys.

AN0912

Direct execution of /bin/vmx or presence of rogue .vmx files not registered in vCenter inventory. Defender perspective: anomalous commands in shell history, edits to rc.local.d/local.sh for persistence.

Log Sources

Mutable Elements

Field	Description
VMInventorySync	Cross-verify running VMs with vCenter inventory for rogue instances.
