Detection Strategy for Reflective Code Loading, Detection Strategy DET0300

Archived: 2026-04-05 15:12:10 UTC

AN0838

Detect anomalous chains of memory allocation and execution inside the same process (e.g., VirtualAlloc → memcpy → VirtualProtect → CreateThread). Unlike process injection, reflective code loading does not perform cross-process memory writes — the suspicious activity occurs entirely within the process's own PID context.

Log Sources

Mutable Elements

Field	Description
ParentProcessWhitelist	Certain processes may legitimately use Assembly.Load(); defenders may whitelist known developer/admin tools.
MemoryRegionPermissions	Detection logic can tune for RWX memory allocations; some legitimate tools may allocate with RW permissions only.

AN0839

Monitor for in-process mmap + mprotect + execve/execveat activity where memory permissions are changed from writable to executable inside the same process without a corresponding ELF on disk.

Log Sources

Mutable Elements

Field	Description
ProcessNameScope	Uncommon for service binaries to call memfd_create; detection tuned for high-risk processes.
RWXMemoryThreshold	Adjust threshold for allowed RWX allocations to reduce false positives in JIT runtimes.

AN0840

Suspicious calls to dlopen(), dlsym(), or mmap with RWX flags in processes that do not typically perform dynamic module loading. Monitor anonymous memory regions executed by user processes.

Log Sources

Mutable Elements

Field	Description
ApplicationScope	Developer tools may legitimately call dlopen/dlsym; narrow scope to production workloads.
ExecutionTimeWindow	Correlate suspicious loads with subsequent process activity in a defined window.
