Detection Strategy for Extra Window Memory (EWM) Injection on Windows, Detection Strategy DET0217

Archived: 2026-04-05 13:50:32 UTC

Analytics

- Windows

AN0608

Detects adversary manipulation of Extra Window Memory (EWM) in a GUI process, where the attacker uses SetWindowLong or SetClassLong to redirect function pointers to injected shellcode stored in shared memory, then triggers execution via a window message like SendNotifyMessage.

Log Sources

Mutable Elements

Field	Description
TargetWindowClassRegex	Regex to scope suspicious or uncommon GUI class names registered by user-created processes
ExecutionTriggerWindowMessage	API calls like SendNotifyMessage or PostMessage that deliver execution to the shellcode location
SharedSectionWriteThreshold	Set byte count thresholds on suspicious memory writes to known shared sections
TimeWindowSetWindowLongToMessageTrigger	Define max time (e.g., <10s) between API call to set window memory and the message call to trigger it

---