Detection Strategy for Process Doppelgänging on Windows, Detection Strategy DET0544

Archived: 2026-04-05 16:53:18 UTC

Analytics

- Windows

AN1501

Detects adversary abuse of Transactional NTFS (TxF) and undocumented process loading mechanisms (e.g., NtCreateProcessEx) to create a hollowed process from an uncommitted, maliciously tainted file image in memory, later executed via NtCreateThreadEx.

Log Sources

Mutable Elements

Field	Description
TransactionExecutableNamePattern	Pattern of legitimate executables often used as doppelgänging targets (e.g., svchost.exe, calc.exe)
TimeWindow_TransactionToExecution	Time delta between TxF rollback and thread creation in hollowed process
ThreadStartEntropyThreshold	Entropy level of thread start address in memory used to detect obfuscated shellcode
TxF API Call Frequency Threshold	Limit on CreateTransaction + RollbackTransaction sequences per process

---