Named Pipe Metadata, Data Component DC0048

Archived: 2026-04-05 17:47:30 UTC

Contextual data about a named pipe on a system, including pipe name and creating process (ex: Sysmon EIDs 17-18)

Data Collection Measures:

- Windows:
  - Sysmon Event ID 17: Logs the creation of a named pipe.
  - Sysmon Event ID 18: Logs connection attempts to a named pipe.
  - Windows Security Event ID 5145: Logs access attempts to named pipes via SMB shares.
  - ETW (Event Tracing for Windows): Provides deep telemetry into named pipe interactions.
- Linux/macOS:
  - AuditD (`mkfifo` , `open` , `read` , `write` syscalls): Tracks FIFO (named pipe) creation and usage.
  - Lsof (`lsof -p <PID>` or `lsof | grep PIPE`): Lists active named pipes and associated processes.
  - Strace (`strace -e open <process>`): Monitors named pipe interactions.
- Endpoint Detection & Response (EDR):
  - Capture named pipe events as part of process tracking.
- Memory Forensics:
  - Volatility Plugin (`pipescan`): Enumerates named pipes in system memory.
  - Rekall Framework: Identifies active named pipes and associated processes.

Source: https://attack.mitre.org/datacomponents/DC0048