Detection Strategy for Double File Extension Masquerading, Detection Strategy DET0366

Archived: 2026-04-05 14:23:09 UTC

AN1033

Detects adversary behavior where a file with a benign-looking first extension (e.g., .txt, .jpg) ends with a dangerous second extension (e.g., .exe, .scr), and is subsequently executed. The behavior chain includes file creation with misleading naming and user or system-initiated process execution from the disguised file.

Log Sources

Mutable Elements

Field	Description
benign_extensions	List of extensions typically used to masquerade malicious files (.txt, .jpg, .doc, .pdf)
dangerous_extensions	List of true executable extensions that may be abused (.exe, .scr, .hta, .lnk)
monitored_paths	Specific directories to focus on (e.g., Downloads folder, %TEMP%, Desktop)
TimeWindow	Duration between file creation and process execution to correlate activity
UserContext	Whether the behavior occurs in a standard user session or elevated context

---