Detection of Suspicious Compiled HTML File Execution via hh.exe, Detection Strategy DET0342

Archived: 2026-04-05 15:55:08 UTC

Analytics

- Windows

AN0968

Execution of hh.exe to open a .chm file followed by suspicious child processes or script engine invocation (VBScript, JScript, mshta, powershell). Behavior includes loading a CHM file from untrusted locations, or immediately spawning commands indicative of payload execution.

Log Sources

Mutable Elements

Field	Description
CHMPathRegex	Regex matching CHM file locations; tune to exclude trusted internal software help files
ChildProcessList	List of suspicious children of hh.exe (powershell.exe, cmd.exe, mshta.exe, wscript.exe)
NetworkDestinationAllowlist	Filter for legitimate update/help servers accessed by hh.exe
TimeWindow	Threshold time between hh.exe execution and suspicious follow-on activity

---