HOTWAX (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:58:01 UTC

HOTWAX is a module that upon starting imports all necessary system API functions, and searches for a .CHM file. HOTWAX decrypts a payload using the Spritz algorithm with a hard-coded key and then searches the target process and attempts to inject the decrypted payload module from the CHM file into the address space of the target process.

▶ [TLP:WHITE] win_hotwax_auto (20251219 | Detects win.hotwax.)
