MoonBounce (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 03:21:34 UTC

MoonBounce is a malware embedded into a modified UEFI firmware. Placed into SPI flash, it can provide persistence across full reinstall and even disk replacements. MoonBounce deploys user-mode malware through in-memory staging with a small footprint.

▶ [TLP:WHITE] win_moonbounce_auto (20251219 | Detects win.moonbounce.)
