Uroburos (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:46:05 UTC

Uroburos is a driver for Windows, including a bypass of PatchGuard. According to Andrzej Dereszowski and Matthieu Kaczmarek, "the techniques used demonstrate [their] excellent knowledge of Windows kernel internals."

▶ [TLP:WHITE] win_uroburos_auto (20241030 | Detects win.uroburos.)
