BOLDMOVE (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:56:38 UTC

According to Mandiant, this malware family is attributed to potential chinese background and its Linux variant is related to exploitation of Fortinet's SSL-VPN (CVE-2022-42475).

▶ [TLP:WHITE] win_boldmove_auto (20251219 | Detects win.boldmove.)
