LIGHTRAIL (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:17:08 UTC

According to Mandiant, this is a tunneler, likely based on an open-source Socks4a proxy, that communicates using Azure cloud infrastructure.

▶ [TLP:WHITE] win_lightrail_auto (20251219 | Detects win.lightrail.)
