BLUEHAZE (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:09:22 UTC

Mandiant associates this with UNC4191, this malware is a launcher for NCAT to establish a reverse tunnel.

▶ [TLP:WHITE] win_bluehaze_auto (20251219 | Detects win.bluehaze.)

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.bluehaze