LOWBALL (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 02:08:48 UTC

LOWBALL, uses the legitimate Dropbox cloud-storage
service to act as the CnC server. It uses the Dropbox API with a hardcoded bearer access token and has the ability to download, upload, and execute files. The communication occurs via HTTPS over port 443.

▶ [TLP:WHITE] win_lowball_auto (20251219 | Detects win.lowball.)
