# DADJOKE (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:22:10 UTC

DADJOKE was discovered as being distributed via email, targeting a South-East Asian Ministry of Defense. It is delivered as an embedded EXE file in a Word document using remote templates and a unique macro using multiple GET requests. The payload is deployed using load-order hijacking with a benign Windows Defender executable. Stage 1 has only beacon+download functionality, made to look like a PNG file. Additional analysis by Kaspersky found 8 campaigns over 2019 and no activity prior to January 2019, DADJOKE is attributed with medium confidence to APT40.

▶ [TLP:WHITE] win_dadjoke_auto (20251219 | Detects win.dadjoke.)

---

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