# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:27:36 UTC



## Tool: DADJOKE

| | |
|---|---|
| Names | DADJOKE |
| Category | Malware |
| Type | Backdoor, Exfiltration |
| Description | 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. |
| Information | <https://www.mycert.org.my/portal/advisory?id=MA-770.022020> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.dadjoke> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:DADJOKE> |

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

### All groups using tool DADJOKE

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Leviathan, APT 40, TEMP.Periscope |  | 2013-Jul 2021 |  |

*1 group listed (1 APT, 0 other, 0 unknown)*