# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:38:39 UTC



## Tool: NimbleMamba

| | |
|---|---|
| Names | NimbleMamba |
| Category | Malware |
| Type | Backdoor, Info stealer, Downloader, Exfiltration |
| Description | (Proofpoint) Each variant of TA402's attack chain led to a RAR file containing one or multiple malicious compressed executables. These executables include a TA402 implant Proofpoint dubbed NimbleMamba and oftentimes an additional trojan Proofpoint named BrittleBush. NimbleMamba is almost certainly meant to replace LastConn, which Proofpoint reported about in June 2021.<br><br>NimbleMamba uses guardrails to ensure that all infected victims are within TA402's target region. NimbleMamba uses the Dropbox API for both command and control as well as exfiltration. The malware also contains multiple capabilities designed to complicate both automated and manual analysis. |
| Information | <https://www.proofpoint.com/us/blog/threat-insight/ugg-boots-4-sale-tale-palestinian-aligned-espionage> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.nimblemamba> |

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

### All groups using tool NimbleMamba

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Molerats, Extreme Jackal, Gaza Cybergang | [Gaza] | 2012-Jul 2023 | |

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

---