# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:45:32 UTC



## Tool: Bandook

| | |
|---|---|
| Names | Bandook<br>Bandok |
| Category | Tools |
| Type | Backdoor |
| Description | Bandook is a commercially available RAT, written in Delphi, which has been available since roughly 2007. |
| Information | <https://www.eff.org/files/2016/08/03/i-got-a-letter-from-the-government.pdf><br><https://www.fortinet.com/blog/threat-research/bandook-persistent-threat-that-keeps-evolving> |
| MITRE ATT&CK | <https://attack.mitre.org/software/S0234/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.bandook> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:Bandook> |

Last change to this tool card: 16 January 2024

Download this tool card in JSON format

### All groups using tool Bandook

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Dark Caracal | | 2007-Jun 2024 | |
| | Operation Bandidos | [Unknown] | 2021 | |
| | Operation Manul | | 2015 | |

*3 groups listed (3 APT, 0 other, 0 unknown)*

---