# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:05:18 UTC



## Tool: BackConfig

| | |
|---|---|
| Names | BackConfig |
| Category | Malware |
| Type | Backdoor |
| Description | (Palo Alto) The BackConfig custom trojan has a flexible plug-in architecture for components offering various features, including the ability to gather system and keylog information and to upload and execute additional payloads. |
| Information | <https://unit42.paloaltonetworks.com/updated-backconfig-malware-targeting-government-and-military-organizations/> <https://ti.360.net/blog/articles/donot-group-is-targeting-pakistani-businessman-working-in-china-en/> |
| MITRE ATT&CK | <https://attack.mitre.org/software/S0475/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.backconfig> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:backconfig> |

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

### All groups using tool BackConfig

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Donot Team | | 2016-Oct 2024 | |
| | Operation HangOver, Monsoon, Viceroy Tiger | | 2010-Jan 2020 | |

*2 groups listed (2 APT, 0 other, 0 unknown)*

---