# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:51:09 UTC



## Tool: DRIGO

| | |
|---|---|
| Names | DRIGO |
| Category | Malware |
| Type | Exfiltration |
| Description | (Trend Micro) PLEAD also uses the document-targeting exfiltration tool DRIGO, which mainly searches the infected machine for documents. Each copy of DRIGO contains a refresh token tied to specific Gmail accounts used by the attackers, which are in turn linked to a Google Drive account. The stolen files are uploaded to these Google Drives, where the attackers can harvest them. |
| Information | <https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:DRIGO> |

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

### All groups using tool DRIGO

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | BlackTech, Circuit Panda, Radio Panda |  | 2010-Oct 2020 | |

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