# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:49:21 UTC



## Tool: Scote

| | |
|---|---|
| Names | Scote |
| Category | Malware |
| Type | Backdoor |
| Description | (Palo Alto) Scote provides backdoor access for an attacker and we have observed it collecting command and control (C2) information from Pastebin links as well as Google+ profiles. The bit.ly links obscured the C2 URLs so victims could not evaluate the legitimacy of the final site prior to clicking it. We are calling their recent activity the “TopHat” campaign. |
| Information | <https://unit42.paloaltonetworks.com/unit42-the-tophat-campaign-attacks-within-the-middle-east-region-using-popular-third-party-services/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.scote> |

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

### All groups using tool Scote

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

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