# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:09:15 UTC



## Tool: KARAE

| | |
|---|---|
| Names | KARAE |
| Category | Malware |
| Type | Reconnaissance, Backdoor, Info stealer, Exfiltration |
| Description | (FireEye) Karae backdoors are typically used as first-stage malware after an initial compromise. The backdoors can collect system information, upload and download files, and may be used to retrieve a second-stage payload. The malware uses public cloud-based storage providers for command and control.<br><br>In March 2016, KARAE malware was distributed through torrent file-sharing websites for South Korean users. During this campaign, the malware used a YouTube video downloader application as a lure. |
| Information | <https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf> |
| MITRE ATT&CK | <https://attack.mitre.org/software/S0215/> |

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

### All groups using tool KARAE

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | Reaper, APT 37, Ricochet Chollima, ScarCruft |  | 2012-Mar 2025 |  |

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=4ad9ed1b-37c5-4253-9f67-07f705c084a2