# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:35:58 UTC



## Tool: NavRAT

| | |
|---|---|
| Names | NavRAT<br>JinhoSpy |
| Category | Malware |
| Type | Backdoor, Keylogger, Info stealer |
| Description | (Talos) Talos has discovered a new malicious Hangul Word Processor (HWP) document targeting Korean users. If a malicious document is opened, a remote access trojan that we're calling 'NavRAT' is downloaded, which can perform various actions on the victim machine, including command execution, and has keylogging capabilities. |
| Information | <https://blog.talosintelligence.com/2018/05/navrat.html> |
| MITRE ATT&CK | <https://attack.mitre.org/software/S0247/> |
| Malpedia | <https://malpedia.caad.fkie.fraunhofer.de/details/win.navrat> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:navrat> |

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

### All groups using tool NavRAT

| 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=b38c64f4-8c44-4c8a-b4c4-8fdd33cba785