

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:45:53 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool PLANKWALK

## Tool: PLANKWALK

|             |   |
|-------------|---|
| Names       | PLANKWALK   |
| Category    | <a href="#">Malware</a>   |
| Type        | <a href="#">Backdoor</a>  |
| Description | ( <a href="#">Mandiant</a> ) UNC2970 largely employs the PLANKWALK backdoor during phishing operations as well as other malware families that share code with multiple tools leveraged by UNC577. |
| Information | < <a href="https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970">https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970</a> >                                     |

Last change to this tool card: 25 April 2023

Download this tool card in [JSON](#) format

### All groups using tool PLANKWALK

| Changed           | Name  | Country  | Observed  |
|-------------------|---|--|---|
| <b>APT groups</b> |   |  |   |
|                   | <a href="#">Lazarus Group, Hidden Cobra, Labyrinth Chollima</a> |  | 2007-May 2025  |

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6595da50-1a03-4915-ad0c-ecfd1eaf4ccc>