

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:45:09 UTC

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

## Tool: SIDESHOW

Names	SIDESHOW
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a>
Description	( <a href="#">Mandiant</a> ) SIDESHOW is a backdoor written in C/C++ that communicates via HTTP POST requests with its C2 server. The backdoor is multi-threaded, uses RC6 encryption, and supports at least 49 commands.
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 SIDESHOW

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=e2f6c1f6-86c5-4fc8-bda6-26ca19484eff>