

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:28:21 UTC

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

## Tool: LIGHTSHOW

Names	LIGHTSHOW FudModule
Category	<a href="#">Malware</a>
Type	<a href="#">Poisoning</a>
Description	( <a href="#">Mandiant</a> ) LIGHTSHOW is a utility that was used by UNC2970 to manipulate kernel data-structures and represents an advancement in DPRK's capabilities to evade detection.
Information	< <a href="https://www.mandiant.com/resources/blog/lightshift-and-lightshow">https://www.mandiant.com/resources/blog/lightshift-and-lightshow</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.fudmodule">https://malpedia.caad.fkie.fraunhofer.de/details/win.fudmodule</a> >

Last change to this tool card: 13 October 2023

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

### All groups using tool LIGHTSHOW

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=c28d6028-a6c9-4eba-acfb-62579e176b64>