

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:12:53 UTC

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

Tool: HeavyLift

Names	HeavyLift
Category	Malware
Type	Loader
Description	(Talos) A previously unknown Electron-based malware loader family distributed via malicious installers targeting the Windows operating system.
Information	< https://blog.talosintelligence.com/cosmic-leopard/ >

Last change to this tool card: 19 June 2024

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

All groups using tool HeavyLift

Changed	Name	Country	Observed
APT groups			
	Cosmic Leopard, Operation Celestial Force		2018

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3f7ceb54-35ec-4c1b-9fcb-ca8534a4d147>