

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:57:41 UTC

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

## Tool: CI Wiper

Names	CI Wiper
Category	<a href="#">Malware</a>
Type	<a href="#">Wiper</a>
Description	<a href="#">(Check Point)</a> How it works: cl.exe gets arguments from the command line and uses a legitimate driver by ElRawDisk, called rdsk.sys. The use of ElRawDisk is relatively common among wipers and has been previously used by several wiper families, some of them associated with Iranian actors. Additionally, the license key used in the wiper is the same as the one used in the <a href="#">ZeroCleare</a> wiper, which is known to be used by several actors with links to MOIS. ElRawDisk enables interaction with files, disks, and partitions, proxying the wiping procedures and allowing raw access to the disk.
Information	< <a href="https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel/">https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel/</a> > < <a href="https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a">https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a</a> >

Last change to this tool card: 18 June 2024

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

## All groups using tool CI Wiper

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">HomeLand Justice</a>		2022-Jan 2024

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=4b8d6551-2aed-451d-adc9-7070a040f833>