

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:16:03 UTC

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

Tool: Behinder

Names	Behinder
Category	Malware
Type	Backdoor
Description	(Trend Micro) Behinder is a web shell management toolkit that encrypts traffic — making it stand out from other web shell management tools, Encrypted payloads are more difficult for web application firewalls or intrusion prevention systems to discover.
Information	< https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/php.behinder >

Last change to this tool card: 27 December 2022

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

All groups using tool Behinder

Changed	Name	Country	Observed
APT groups			
	Earth Lusca		2019-Sep 2024

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=e0858e5e-e744-46ef-b898-1e56a982ea6f>