

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:22:19 UTC

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

Tool: TAXHAUL

Names	TAXHAUL
Category	Malware
Type	Dropper
Description	(Mandiant) TAXHAUL is a DLL that, when executed, decrypts a shellcode payload expected at C:\Windows\System32\config\TxR\TxR.0.regtrans-ms. Mandiant has seen TAXHAUL persist via DLL search order hijacking.
Information	< https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise >

Last change to this tool card: 26 April 2023

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

All groups using tool TAXHAUL

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=71b734a7-1ca4-457f97bd-d6112e85c41f>