

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:40:16 UTC

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


Tool: Cuthead

Names	Cuthead
Category	Malware
Type	Info stealer
Description	(Kaspersky) Recently, ToddyCat started using a new tool we named cuthead to search for documents. The name originated from the “file description” field of the sample we found. It is a .NET compiled executable designed to search for files and store those it finds inside an archive. The tool can search for specified file extensions or words in the file name.
Information	< https://securelist.com/toddycat-traffic-tunneling-data-extraction-tools/112443/ >

Last change to this tool card: 23 April 2024

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

All groups using tool Cuthead

Changed	Name	Country	Observed
APT groups			
	ToddyCat		2020-2024

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=5f231d6e-d68b-4e07-94a2-3427697d13df>