

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:18:47 UTC

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

Tool: RIFLESPINE

Names	RIFLESPINE
Category	Malware
Type	Backdoor
Description	(Mandiant) RIFLESPINE is a cross-platform backdoor that leverages Google Drive to transfer files and execute commands. It adopts the CryptoPP library to implement the AES algorithm to encrypt and decrypt the data transmitted between an affected machine and the threat actor.
Information	< https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations >

Last change to this tool card: 26 August 2024

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

All groups using tool RIFLESPINE

Changed	Name	Country	Observed
APT groups			
	UNC3886		2021-Early 2025

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d9c072a3-0aa5-426c-b55c-1dc582c5596d>