

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:06:25 UTC

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

Tool: GearShift

Names	GearShift
Category	Malware
Type	Dropper , Keylogger
Description	According to FireEye, GEARSHIFT is a memory-only dropper for two keylogger DLLs. It is designed to replace a legitimate Fax Service DLL.
Information	< http://content.fireeye.com/apt41/rpt-apt41 >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.gearshift >

Last change to this tool card: 24 April 2021

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

All groups using tool GearShift

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ade7195f-aad1-4fa1-8951-a2c79aba24c1>