

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:05:58 UTC

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

Tool: WINTERLOVE

Names	WINTERLOVE
Category	Malware
Type	Reconnaissance , Backdoor
Description	(FireEye) WINTERLOVE is a backdoor used by suspected Chinese cyber espionage actors. WINTERLOVE attempts to load and execute remote code in a running process and can enumerate system files and directories.
Information	< https://paper.bobylive.com/Security/APT_Report/APT-41.pdf >

Last change to this tool card: 20 April 2020

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

All groups using tool WINTERLOVE

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=f4083b38-7b04-46da-9ad4-5eed72a03841>