Threat Group Cards: A Threat Actor Encyclopedia

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)