Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:15:11 UTC

Tool: MoonWalk

Names	MoonWalk CurveLast SneakCross
Category	Malware
Type	Backdoor
Description	(ZScaler) APT41, a China-based nation-state threat actor known for campaigns in Southeast Asia, has been observed using a new backdoor called MoonWalk. MoonWalk shares a common development toolkit with DUSTTRAP, reusing code that implements evasive techniques such as DLL hollowing, import resolution, DLL unhooking, and call stack spoofing. Additionally, MoonWalk employs further evasion tactics, including the use of Google Drive as its C2 channel to blend in with legitimate network traffic and the utilization of Windows Fibers to evade AV/EDR security solutions. MoonWalk's modular design allows attackers to easily update its capabilities, modify its behavior, and customize functionality for different scenarios.
Information	<https://www.zscaler.com/blogs/security-research/moonwalk-deep-dive-updated-arsenal-apt41-part-2>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.moonwalk>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool MoonWalk

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

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