Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:02:21 UTC

Tool: MOPSLED

Names	MOPSLED
Category	Malware
Type	Reconnaissance, Backdoor
Description	(Mandiant) MOPSLED is a shellcode-based modular backdoor that has the capability to communicate over HTTP or a custom binary protocol over TCP to its C2 server. The core functionality of MOPSLED involves expanding its capabilities by retrieving plugins from the C2 server. MOPSLED also uses a custom ChaCha20 encryption algorithm to decrypt embedded and external configuration files. Mandiant observed sharing of MOPSLED between other Chinese cyber espionage groups including APT41. Mandiant considered MOPSLED to be an evolution of CrossWalk, which can act as a network proxy.
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 MOPSLED

Changed	Name	Country	Observed	
APT groups				
	UNC3886		2021-Early 2025	

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