

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:05:21 UTC

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

Tool: CMDEmber

Names	CMDEmber
Category	Malware
Type	Backdoor
Description	(SentinelLabs) CMDEmber interacts with a Google Firebase Realtime Database instance that has the role of a C2 server.
Information	< https://www.sentinelone.com/labs/wip26-espionage-threat-actors-abuse-cloud-infrastructure-in-targeted-telco-attacks/ >

Last change to this tool card: 17 February 2023

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

All groups using tool CMDEmber

Changed	Name	Country	Observed
APT groups			
	WIP26	[Unknown]	2022

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=65a9b500-18f7-4049-8f52-7d3609741718>