Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:36:03 UTC

Tool: CMD365

Names	CMD365
Category	Malware
Type	Backdoor
Description	(SentinelLabs) The main functionality of CMD365 is to execute commands from a C2 hosted on a Microsoft 365 Mail instance. This capability was used to conduct a variety of activities, such as reconnaissance, privilege escalation, staging of additional malware, and data exfiltration.
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 CMD365

Changed	Name	Country	Observed	
APT groups				
	WIP26	[Unknown]	2022	

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