Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:05:07 UTC

APT group: WIP26

Names	WIP26 *(SentinelLabs)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2022
Description	(SentinelLabs) In collaboration with QGroup GmbH, SentinelLabs is monitoring a threat activity we track as WIP26. The threat actor behind WIP26 has been targeting telecommunication providers in the Middle East. WIP26 is characterized by the abuse of public Cloud infrastructure – Microsoft 365 Mail, Microsoft Azure, Google Firebase, and Dropbox – for malware delivery, data exfiltration, and C2 purposes. The WIP26 activity is initiated by precision targeting of employees through WhatsApp messages that contain Dropbox links to a malware loader. Tricking employees into downloading and executing the loader ultimately leads to the deployment of backdoors that leverage Microsoft 365 Mail and Google Firebase instances as C2 servers. We refer to these backdoors as CMD365 and CMDEmber, respectively. The main functionality of CMD365 and CMDEmber is to execute attacker-provided system commands using the Windows command interpreter.
Observed	Sectors: Telecommunications. Countries: Middle East.
Tools used	CMD365, CMDEmber.
Information	<https://www.sentinelone.com/labs/wip26-espionage-threat-actors-abuse-cloud-infrastructure-in-targeted-telco-attacks/>

Last change to this card: 17 February 2023

Download this actor card in PDF or JSON format