Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:35:05 UTC

Tool: KamiKakaBot

Names	KamiKakaBot
Category	Malware
Type	Backdoor
Description	(Group-IB) They created two custom modules, named by Group-IB as TelePowerBot and KamiKakaBot, which are written in PowerShell and .NET, respectively. These two pieces of malware are designed to read and execute commands from a threat actor-controlled Telegram channel via Telegram bot. Group-IB researchers noted that all communication between the devices of the threat actors and victims was based entirely on Telegram API, and they utilized numerous evasion techniques, including Bypass User Account Control, to remain undetected.
Information	<https://www.group-ib.com/media-center/press-releases/dark-pink-apt/>

Last change to this tool card: 15 February 2023

Download this tool card in JSON format

All groups using tool KamiKakaBot

Changed	Name	Country	Observed	
APT groups				
	Dark Pink	[Unknown]	2022-Feb 2023	

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