Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:39:57 UTC

Tool: BEATDROP

Names	BEATDROP
Category	Malware
Type	Downloader
Description	(Mandiant) BEATDROP is a downloader written in C that makes use of Trello for C2. Once executed, BEATDROP first maps its own copy of `ntdll.dll` into memory for the purpose of executing shellcode in its own process. BEATDROP first creates a suspended thread with RtlCreateUserThread which points to NtCreateFile.
Information	<https://www.mandiant.com/resources/blog/tracking-apt29-phishing-campaigns>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.beatdrop>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool BEATDROP

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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