Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:20:25 UTC

Tool: MAGICDROP

Names	MAGICDROP
Category	Malware
Type	Dropper
Description	(Mandiant) MAGICDROP is a dropper written in C++. It decrypts files from its .data section and writes them to disk in the system's %TEMP% directory. The files dropped often include a decoy file, a next-stage payload, and sometimes an installer for the payload.
Information	<https://www.mandiant.com/media/17826>

Last change to this tool card: 13 September 2022

Download this tool card in JSON format

All groups using tool MAGICDROP

Changed	Name	Country	Observed	
APT groups				
	APT 42		2015-Feb 2024	

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