Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:08:35 UTC

Tool: LOSTKEYS

Names	LOSTKEYS
Category	Malware
Type	Reconnaissance, Info stealer, Exfiltration
Description	(Mandiant) It is a piece of malware that is capable of stealing files from a hard-coded list of extensions and directories, along with sending system information and running processes to the attacker.
Information	<https://cloud.google.com/blog/topics/threat-intelligence/coldriver-steal-documents-western-targets-ngos>

Last change to this tool card: 27 June 2025

Download this tool card in JSON format

All groups using tool LOSTKEYS

Changed	Name	Country	Observed	
APT groups				
	Cold River		2019-Jan 2025	

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