Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:10:41 UTC

Tool: Castov

Names	Castov
Category	Malware
Type	Credential stealer, Info stealer
Description	Also in 2013, researchers spotted a piece of malware called Castov (Downloader.Castov and Infostealer.Castov) targeting South Korean financial institutions and their customers. In these attacks, which are also believed to originate from Lazarus, Castov was used to steal passwords, account details, and digital certificates from the computers it infected. Castov (Trojan.Castov) was also used in further DDoS attacks against South Korean targets in June 2013.
Information	<https://medium.com/threat-intel/lazarus-attacks-wannacry-5fdeddee476c>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Castov

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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