Threat Group Cards: A Threat Actor Encyclopedia

Tool: COLDCAT

Names	COLDCAT
Category	Malware
Type	Downloader
Description	(Mandiant) COLDCAT is a complex downloader. COLDCAT generates unique host identifier information, and beacons it to a C2 that is specified in a separate file via POST request with the data in the cookie header. After a brief handshake, the malware expects base64 encoded shellcode to execute in response.
Information	<https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise>

Last change to this tool card: 26 April 2023

Download this tool card in JSON format

All groups using tool COLDCAT

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

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