Threat Group Cards: A Threat Actor Encyclopedia

Tool: COLDJAVA

Names	COLDJAVA
Category	Malware
Type	Loader
Description	(FireEye) The compromised CCleaner update (which we call DIRTCLEANER) is believed to download a second-stage loader (MD5: 748aa5fcfa2af451c76039faf6a8684d) that contains a 32-bit and 64-bit COLDJAVA DLL payload. The COLDJAVA payload contains shellcode that loads a variant of BlackCoffee.
Information	<https://docplayer.net/161018432-Double-dragon-apt41-a-dual-espionage-and-cyber-crime-operation.html>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool COLDJAVA

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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