Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:36:03 UTC

Tool: CollectionRAT

Names	CollectionRAT
Category	Malware
Type	Backdoor
Description	(Talos) CollectionRAT has standard remote access trojan (RAT) capabilities, including the ability to run arbitrary commands on an infected system. Based on our analysis, CollectionRAT appears to be connected to Jupiter/EarlyRAT, another malware family Kaspersky recently wrote about and attributed to Andariel, a subgroup within the Lazarus Group umbrella of threat actors.
Information	<https://blog.talosintelligence.com/lazarus-collectionrat/>

Last change to this tool card: 06 September 2023

Download this tool card in JSON format

All groups using tool CollectionRAT

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2c3ec378-cfba-4bfb-b04d-19d79f5ef66a