

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:38:06 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool RomeoGolf

Tool: RomeoGolf

Names	RomeoGolf
Category	Malware
Type	Backdoor , Info stealer , Exfiltration
Description	(Novetta) Observed as the payload of IndiaEcho and loaded by LimaBravo, RomeoGolf is a RAT with some similarity to the families derived from Romeo-CoreOne (see Section 2) and as RomeoFoxtrot-Two (see Section 8) in terms of the commands supported. Structurally, however, RomeoGolf is a family unto its own.
Information	< https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-RAT-and-Staging-Report.pdf >

Last change to this tool card: 20 April 2020

Download this tool card in [JSON](#) format

All groups using tool RomeoGolf

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=4caddf1c-bd8f-44d4-81d1-2c32143511c6>