Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:20:01 UTC

Tool: RomeoMike

Names	RomeoMike
Category	Malware
Type	Backdoor
Description	(Novetta) A component of the reported Ten Days of Rain attacks, RomeoMike is a RAT with a very limited set of capabilities yet exhibits a great deal of functional and procedural similarity to SierraJuliett (see Section 17) and DeltaCharlie with regards to the way commands are processed through signed command files. RomeoMike is a service DLL that, after establishing the scaffolding code to appear as a legitimate Windows service.
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 RomeoMike

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

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