Threat Group Cards: A Threat Actor Encyclopedia

Tool: RomeoHotel

Names	RomeoHotel
Category	Malware
Type	Backdoor, Info stealer
Description	(Novetta) Functionally, RomeoHotel is nearly identical to RomeoAlfa: RomeoHotel supports the same commands within the R-C1 portion of itself, has an identical configuration data structure in both size and field meaning to that of RomeoAlfa-Two, and uses fake TLS for communication. RomeoHotel supports the same command set found in RomeoAlfa-Two, but supports all commands fully, while RomeoAlfa-Two does not fully support all of its commands. For example, RomeoHotel supports the RunAs command fully while the RomeoAlfa variants will accept the command but will perform not action as a result of the instruction from the C2 server.
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 RomeoHotel

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

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