Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:10:36 UTC

Tool: RomeoCharlie

Names	RomeoCharlie
Category	Malware
Type	Backdoor, Info stealer, Tunneling
Description	(Novetta) With observed compile dates going back to February 5, 2014, RomeoCharlie is one of the oldest R-C1-based RATs (see Section 2) in the Lazarus Group's collection. A server-mode RAT, RomeoCharlie uses DNSCALC-style encoding for network communication and RSA encryption for client authentication. There are two observed variants, RomeoCharlie-One and RomeoCharlie-Two. The differences between the two are cosmetic in nature. With the configuration of the RomeoCharlie variants loaded into memory, the differences between RomeoCharlie-One and RomeoCharlie-Two cease (save for one exception that will be explained). RomeoCharlie is a server-mode RAT and, as such, must establish a listening port. Before a listening port is established at the Winsock level, RomeoCharlie first opens a hole in the Windows Firewall to allow incoming connections on the desired listening port (as specified in the configuration). The task of opening a firewall port consists of constructing and then issuing the command line.
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 RomeoCharlie

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=8b4f43d3-431c-4c8d-a553-0424f728312c