Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:31:12 UTC

Tool: Romeos

Names	Romeos RomeoCore Romeo-CoreOne R-C1
Category	Malware
Type	Backdoor, Info stealer
Description	(Novetta) A large portion of the Lazarus Group's RAT collection stems from a common core, Romeo-CoreOne (R-C1); the individual families that use R-C1 need only provide the scaffolding to support the R-C1 code. At a minimum, each family that is built upon R-C1 must provide an interface to their specific communications abstraction and a method by which to activate the R-C1 functionality. The general flow of execution for families that use R-C1 is as follows: 1. Dynamically load API functions 2. Perform any configuration management tasks that the family may require (e.g., loading the configuration, opening listening ports, establishing persistence) 3. Establish a communication channel with controlling endpoint 4. Pass off the channel to the R-C1 component There are five known families that are based on, or that incorporate, R-C1 (Figure 2-1): RomeoAlfa, RomeoBravo, RomeoCharlie, RomeoHotel, and RomeoNovember. In addition to the four families having commonality through the use of R-C1, two of the families, RomeoAlfa and RomeoHotel, share the distinctive fake TLS communication scheme and use the Caracachs encryption scheme as their underlying communication encryption. RomeoBravo, RomeoCharlie, and RomeoNovember use DNSCALC-style encoding for communication encryption.
Information	<https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-RAT-and-Staging-Report.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.romeos>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Romeos

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=f9e598ab-266d-4460-9d22-d945de9498d3