Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:13:48 UTC

Tool: RomeoFoxtrot

Names	RomeoFoxtrot
Category	Malware
Type	Backdoor, Info stealer
Description	(Novetta) Operating as a server mode RAT, RomeoFoxtrot uses a simple handshake to establish a connection and variant-dependent encryption to transfer data making the malware significantly less sophisticated from a network perspective than other members of the Romeo class. Despite the lack of network sophistication, RomeoFoxtrot provides a large number of commands to handle aspects of file management, process management, network proxying, and victim computer information enumeration. **There are two known variants of RomeoFoxtrot: RomeoFoxtrot-One and RomeoFoxtrot-Two. The RomeoFoxtrot family has been observed as the payload of the IndiaCharlie variants, with IndiaCharlie-One observed dropping RomeoFoxtrot-One and IndiaCharlie-Two observed dropping RomeoFoxtrot-Two. Functionally, the two variants are very similar with only two distinctions. The primary distinction is the inclusion of a configuration file for RomoeFoxtrot-Two that specifies the listening port, while RomeoFoxtrot-One uses a hardcoded value. The second is a renumbering of command identifiers. Given the similarities, the remainder of this section will simply refer to them equally as RomeoFoxtrot unless a particular detail is specific to one variant over the other.**
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 RomeoFoxtrot

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=042f93fa-2adf-4e6e-af8c-ccf96872e4a8