Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:12:13 UTC

Tool: RomeoNovember

Names	RomeoNovember
Category	Malware
Type	Backdoor, Tunneling
Description	(Novetta) RomeoNovember is a client-mode RAT that has a strong structural and familial relationship to both RomeoAlfa (see Section 3) and RomeoBravo (see Section 4). Romeo-CoreOne-based, structurally RomeoNovember is most like RomeoAlfa, as it operates as a standalone executable, constructs its configuration data structure from hardcoded values, and leverages the same scaffolding for supporting R-C1. Functionally, however, RomeoNovember is closer to RomeoBravo than RomeoAlfa. Like RomeoBravo, RomeoNovember uses DNSCALC-style encoding to obfuscate network communication instead of RomeoAlfa's reliance on fake TLS. The similarity to RomeoBravo also extends to the use of the same base command number (0x523B) and channel ID (0x3456). The commands within R-C1 supported by RomeoNovember are the nearly the same as those supported by RomeoBravo, to the extent that RomeoNovember and RomeoBravo both implement the Secure Delete command with the same code. Only the Upload Directory as Archive command is missing from RomeoNovember. RomeoNovember's hybrid nature may indicate an active development period for the developer(s).
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 RomeoNovember

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=c0f7cd3b-3b65-47f7-8188-2b8b89e51fea