Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:26:41 UTC

Tool: RomeoWhiskey

Names	RomeoWhiskey Winsec
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Novetta) In terms of sophistication and functionality, RomeoWhiskey is a mid-tier RAT. At its core, RomeoWhiskey provides the basic functionality one would expect in a RAT: file transfer commands, program execution, basic intelligence gathering, etcetera. Observed as early as May 2011, RomeoWhiskey, also known as Winsec, is one of the older family members used by the Lazarus Group, and, over the course of its lifetime, it has undergone at least one major revision. The first variant of RomeoWhiskey, RomeoWhiskey–One, has been observed with compile dates from May 2011 to late January/early February 2012, while RomeoWhiskey-Two, the second variant, was compiled from late February 2012 until at least March 2014. RomeoWhiskey uses numerical constants to identify specific commands, reflective of the way RATs like the Romeo-CoreOne-based families (see Section 2) identify commands by unique numerical constants. There are two sets of constants for identifying commands within the RomeoWhiskey samples that do not necessarily align with variant boundaries: command base 0x7D50 and command base 0x1E10.
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 RomeoWhiskey

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=cef31157-132a-4436-8a09-076be4a1747d