

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:57:15 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool NineRAT

Tool: NineRAT

Names	NineRAT
Category	Malware
Type	Backdoor
Description	(Talos) Once the credential dumping is complete, Lazarus deploys a previously unknown RAT we're calling "NineRAT" on the infected systems. NineRAT was first seen being used in the wild by Lazarus as early as March 2023. NineRAT is written in DLang and indicates a definitive shift in TTPs from APT groups falling under the Lazarus umbrella with the increased adoption of malware being authored using non-traditional frameworks such as the Qt framework, including MagicRAT and QuiteRAT .
Information	< https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.ninerat >

Last change to this tool card: 17 January 2024

Download this tool card in [JSON](#) format

All groups using tool NineRAT

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group , Hidden Cobra , Labyrinth Chollima		2007-May 2025	

1 group listed (1 APT, 0 other, 0 unknown)