

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:28:52 UTC

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

Tool: Ratankba

Names	Ratankba Ratabanka QUICKRIDE
Category	Malware
Type	Backdoor , Info stealer
Description	(Trend Micro) During our analysis, we collected a copy of the RATANKBA malware’s Lazarus Remote Controller tool. The remote controller provides a user interface that allows attackers to send jobs to any compromised endpoint. The controller gives the attackers the ability to manipulate the victims’ host by queueing tasks on the main server. RATANKBA retrieves and executes the tasks, and retrieves the collected information.
Information	< https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-campaign-targeting-cryptocurrencies-reveals-remote-controller-tool-evolved-ratankba/ >
MITRE ATT&CK	< https://attack.mitre.org/software/S0241/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.ratankba >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:ratankba >

Last change to this tool card: 29 December 2022

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

All groups using tool Ratankba

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.eta.da.or.th/cgi-bin/listgroups.cgi?u=86175fff-3f01-49ba-8057-ef28c8f619c9>