

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:57:26 UTC

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

## Tool: MagicRAT

Names	MagicRAT
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a>
Description	( <a href="#">Talos</a> ) MagicRAT is programmed in C++ programming language and uses the Qt Framework by statically linking it to the RAT on 32- and 64-bit versions. The Qt Framework is a programming library for developing graphical user interfaces, of which this RAT has none. Talos believes that the objective was to increase the complexity of the code, thus making human analysis harder. On the other hand, since there are very few examples (if any) of malware programmed with Qt Framework, this also makes machine learning and heuristic analysis detection less reliable.
Information	< <a href="https://blog.talosintelligence.com/2022/09/lazarus-magicrat.html">https://blog.talosintelligence.com/2022/09/lazarus-magicrat.html</a> >
MITRE ATT&CK	< <a href="https://attack.mitre.org/software/S1182">https://attack.mitre.org/software/S1182</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.magic_rat">https://malpedia.caad.fkie.fraunhofer.de/details/win.magic_rat</a> >

Last change to this tool card: 28 June 2025

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

## All groups using tool MagicRAT

Changed	Name	Country	Observed	
<b>APT groups</b>				
	<a href="#">Lazarus Group</a> , <a href="#">Hidden Cobra</a> , <a href="#">Labyrinth Chollima</a>		2007-May 2025	

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

---

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=8894b29c-bd50-4b79-a549-6b2fd2d5d93b>