

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:54:29 UTC

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

Tool: RunningRAT

Names	RunningRAT Running RAT running_rat
Category	Malware
Type	Reconnaissance , Backdoor , Keylogger , Info stealer
Description	(McAfee) RunningRat is a remote access Trojan (RAT) that operates with two DLLs. It gets its name from a hardcoded string embedded in the malware. Upon being dropped onto a system, the first DLL executes. This DLL serves three main functions: killing antimalware, unpacking and executing the main RAT DLL, and obtaining persistence. The malware drops the Windows batch file dx.bat, which attempts to kill the task daumcleaner.exe; a Korean security program. The batch file then attempts to remove itself.
Information	< https://www.mcafee.com/blogs/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/ >
MITRE ATT&CK	< https://attack.mitre.org/software/S0253/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.runningrat >

Last change to this tool card: 28 December 2022

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

All groups using tool RunningRAT

Changed	Name	Country	Observed	
APT groups				
	Hades		2017-Oct 2020	

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=df6926cd-9c41-4db7-a233-54e6ebbb6ee>