Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:33:39 UTC

Tool: JRat

Names	JRat Jacksbot
Category	Malware
Type	Backdoor
Description	(Electronic Frontier Foundation) One of the common malware samples used over the course of Operation Manul is known as JRat or Jacksbot. JRat is a commercially available remote access tool (RAT), written in Java. JRat is currently available for purchase at jrat[.]io for the price of $40USD. JRat has been continuously developed for the last four years, seemingly by a single developer who goes by the name “redp0ison”. While JRat itself is closed source, many modules and helpful utilities are open source and are available on github.
Information	<https://www.eff.org/files/2016/08/03/i-got-a-letter-from-the-government.pdf> <https://blog.trendmicro.com/trendlabs-security-intelligence/jacksbot-has-some-dirty-tricks-up-its-sleeves/> <https://maskop9.wordpress.com/2019/02/06/analysis-of-jacksbot-backdoor/> <https://research.checkpoint.com/malware-against-the-c-monoculture/> <https://www.intego.com/mac-security-blog/new-multiplatform-backdoor-jacksbot-discovered>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/jar.jrat>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool JRat

Changed	Name	Country	Observed
APT groups			

	Operation Manul		2015	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c9a2dfe0-4dca-44f4-a310-08d7efe3e726