

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:27:07 UTC

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

Tool: Ragnatela

Names	Ragnatela Ragnatela RAT
Category	Malware
Type	Backdoor , Info stealer , Keylogger , Downloader , Exfiltration
Description	<p>(Malwarebytes) We identified what we believe is a new variant of the BADNEWS RAT called Ragnatela being distributed via spear phishing emails to targets of interest in Pakistan. Ragnatela, which means spider web in Italian, is also the project name and panel used by Patchwork APT.</p> <p>Ragnatela RAT was built sometime in late November as seen in its Program Database (PDB) path “E:\new_ops\jlitest __change_ops -29no – Copy\Release\jlitest.pdb”. It features the following capabilities:</p> <ul style="list-style-type: none">• Executing commands via cmd• Capturing screenshots• Logging Keystrokes• Collecting list of all the files in victim’s machine• Collecting list of the running applications in the victim’s machine at a specific time periods• Downing addition payloads• Uploading files
Information	< https://blog.malwarebytes.com/threat-intelligence/2022/01/patchwork-apt-caught-in-its-own-web/ >

Last change to this tool card: 25 January 2022

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

All groups using tool Ragnatela

Changed	Name	Country	Observed
---------	------	---------	----------

APT groups

	Patchwork, Dropping Elephant		2013-Jun 2025	
--	--	---	---------------	--

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2e9285ec-5ef6-4191-b13a-7c871bfb6e9f>