Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:55:50 UTC

Tool: ElizaRAT

Names	ElizaRAT
Category	Malware
Type	Backdoor
Description	(Check Point) ElizaRAT, a Windows Remote Access Tool disclosed in September 2023, is employed by Transparent Tribe in targeted attacks. Infections typically start via executable files shared through Google Storage links, likely due to phishing efforts. Earlier variants relied on Telegram for Command and Control (C2) communication. Since its initial detection, ElizaRAT has evolved in execution methods, detection evasion, and C2 communication, as demonstrated in three distinct campaigns from late 2023 to early 2024. Each campaign utilized a different variant of ElizaRAT to deploy specific payloads for automated information gathering.
Information	<https://blog.checkpoint.com/research/the-evolution-of-transparent-tribes-new-malware/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.eliza_rat>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool ElizaRAT

Changed	Name	Country	Observed	
APT groups				
	Transparent Tribe, APT 36		2013-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=99c550ef-5f9a-49e5-b4d1-f05d18c4cc9f