Warzone RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:22:30 UTC

Tool: Warzone RAT

Names	Warzone RAT Warzone
Category	Malware
Type	Backdoor, Credential stealer, Keylogger, Downloader, Remote command
Description	(Anomali) Warzone RAT is a commodity info stealer written in C++ that is widely available for purchase on criminal forums. Warzone is a commodity malware, with cracked versions hosted on GitHub. The RAT reuses code from the Ave Maria stealer.
Information	<https://www.anomali.com/blog/aggah-using-compromised-websites-to-target-businesses-across-asia-including-taiwan-manufacturing-industry> <https://www.justice.gov/opa/pr/international-cybercrime-malware-service-dismantled-federal-authorities-key-malware-sales>
MITRE ATT&CK	<https://attack.mitre.org/software/S0670/>

Last change to this tool card: 06 March 2024

Download this tool card in JSON format

All groups using tool Warzone RAT

Changed	Name	Country	Observed	
APT groups				
	Aggah	[Unknown]	2018-Jun 2022	
	Blind Eagle		2018-Nov 2024	
	Operation Armor Piercer		2020	
	Sandworm Team, Iron Viking, Voodoo Bear		2009-Dec 2024	

	Tomiris	[Unknown]	2020	
	YoroTrooper		2022	

6 groups listed (6 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a5646599-1634-4e8d-9a26-e2c5a5f71726