Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:33:46 UTC

Tool: Kazuar

Names	Kazuar
Category	Malware
Type	Backdoor, Info stealer, Exfiltration, Loader
Description	(Palo Alto) Kazuar is a fully featured backdoor written using the .NET Framework and obfuscated using the open source packer called ConfuserEx. Kazuar has an extensive command set, many of which are similar in functionality as other backdoor Trojans. However, a few commands specific to Kazuar appear to be unique and are worth further discussion.
Information	<https://unit42.paloaltonetworks.com/unit42-kazuar-multiplatform-espionage-backdoor-api-access/> <https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity> <https://unit42.paloaltonetworks.com/pensive-ursa-uses-upgraded-kazuar-backdoor/https://unit42.paloaltonetworks.com/pensive-ursa-uses-upgraded-kazuar-backdoor/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0265/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.kazuar>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Kazuar>

Last change to this tool card: 29 November 2023

Download this tool card in JSON format

All groups using tool Kazuar

Changed	Name	Country	Observed

APT groups

	Turla, Waterbug, Venomous Bear		1996-2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=65bcba1a-e845-438b-9920-72bf6282af32