Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:01:01 UTC

Tool: AZORult

Names	AZORult PuffStealer Rultazo
Category	Malware
Type	Info stealer, Credential stealer, Downloader
Description	(Kaspersky) The AZORult Trojan is one of the most commonly bought and sold stealers in Russian forums. Despite the relatively high price tag ($100), buyers like AZORult for its broad functionality (for example, the use of .bit domains as C&C servers to ensure owner anonymity and to make it difficult to block the C&C server), as well as its high performance. Many comment leavers recommend it. AZORult is a Trojan stealer that collects various data on infected computers and sends it to the C&C server, including browser history, login credentials, cookies, files from folders as specified by the C&C server (for example, all TXT files from the Desktop folder), cryptowallet files, etc.; the malware can also be used as a loader to download other malware. Kaspersky Lab products detect the stealer as Trojan-PSW.Win32.Azorult. Our statistics show that since the start of 2019, users in Russia and India are the most targeted.
Information	<https://securelist.com/azorult-analysis-history/89922/> <https://threatvector.cylance.com/en_us/home/threat-spotlight-analyzing-azorult-infostealer-malware.html> <https://blog.minerva-labs.com/puffstealer-evasion-in-a-cloak-of-multiple-layers> <https://blog.minerva-labs.com/azorult-now-as-a-signed-google-update> <https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside> <https://www.blueliv.com/blog-news/research/azorult-crydbrox-stops-sells-malware-credential-stealer/> <https://research.checkpoint.com/the-emergence-of-the-new-azorult-3-3/> <https://www.netskope.com/blog/from-delivery-to-execution-an-evasive-azorult-campaign-smuggled-through-google-sites>

MITRE ATT&CK	<https://attack.mitre.org/software/S0344/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.azorult>

Last change to this tool card: 22 April 2024

Download this tool card in JSON format

All groups using tool AZORult

Changed	Name	Country	Observed	
APT groups				
	FIN11	[Unknown]	2016-Mar 2025	
	Operation Epic Manchego	[Unknown]	2020	
	TA558	[Unknown]	2018-Jun 2023	
Other groups				
	TA516	[Unknown]	2016-Feb 2020	

4 groups listed (3 APT, 1 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ce88f834-afbf-4d8b-8ca6-43b7fde7bdf2