Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:17:31 UTC

Tool: Adwind

Names	Adwind Adwind RAT Frutas jFrutas UnReCoM Alien Spy AlienSpy JSocket Sockrat jBiFrost JBifrost RAT Unknown RAT jConnectPro RAT Unrecom Trojan.Maljava
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Credential stealer, Info stealer, Exfiltration, Miner

Description	(Proofpoint) The AlienSpy RAT is very powerful in the hands of an attacker. Some of the key features supported by the RAT include: • Collection of system information for fingerprinting and displaying on the attacker's controller dashboard • File system, process and registry explorer with ability to view and modify • Ability to run console commands • Keylogging to capture user inputs • Ability to download and execute secondary payloads • Credential theft from various browser stores • Ability to spy on victim through screenshots, webcam, microphone • Ability to RDP (Remote Desktop) to infected clients • Ability to mine various type of digital currency such as bitcoin, litecoin, dogecoin etc.
Information	<https://www.proofpoint.com/us/threat-insight/post/You-Dirty-RAT> <https://unit42.paloaltonetworks.com/the-legend-of-adwind-a-commodity-rat-saga-in-eight-parts/> <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07195002/KL_AdwindPublicReport_2016.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0283/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/jar.adwind>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:alienspy>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Adwind

Changed	Name	Country	Observed	
APT groups				
	LazyScripter	[Unknown]	2018	
	Packrat	[Latin America]	2008	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=90747400-bb9d-427d-8cc3-cd341f598860