Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:35:05 UTC

Tool: Trochilus RAT

Names	Trochilus RAT
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Downloader
Description	Despite that the RAT was designed to execute in the memory of the machine (thus evading detection by AV software), ASERT researchers obtained the RAT's source code and connected it to a GitHub profile of a user named 5loyd. On the GitHub page, the RAT has been advertised as a fast and free Windows remote administration tool. Other details include: • Written in CC+; • Supports various communication protocols; • Has a file manager module, a remote shell, a non-UAC mode; • Able to uninstall itself; • Able to upload information from remote machines; • Able to download an execute files. Researchers believe that 5loys is not a part of Group 27. More likely, the user's profile has been hijacked by the group and used for their own purposes.
Information	<https://sensorstechforum.com/trochilus-plugx-rats-in-targeted-attacks-on-governments/> <https://github.com/5loyd/trochilus/> <https://asert.arbornetworks.com/uncovering-the-seven-pointed-dagger/> <https://github.com/m0n0ph1/malware-1/tree/master/Trochilus> <https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.trochilus_rat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Trochilus>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool Trochilus RAT

Changed	Name	Country	Observed	
APT groups				
	APT 31, Judgment Panda, Zirconium		2016-Mar 2024	
	Earth Berberoka		2022	
	Nightshade Panda, APT 9, Group 27		2013-Sep 2016	
	Space Pirates		2017-Nov 2024	
	Stone Panda, APT 10, menuPass		2006-Mar 2025	

5 groups listed (5 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=cfb2355d-e43d-43b7-8033-0fcba988db50