Orcus RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:53:37 UTC

Tool: Orcus RAT

Names	Orcus RAT Orcus Schnorchel
Category	Malware
Type	Backdoor, Keylogger, Credential stealer, Info stealer, DDoS
Description	(Morphisec) In a successful attack, the Orcus RAT can steal browser cookies and passwords, launch server stress tests (DDoS attacks), disable the webcam activity light, record microphone input, spoof file extensions, log keystrokes and more. The Orcus RAT masquerades as a legitimate remote administration tool, although it is clear from its features and functionality that it is not and was never intended to be. (Brian Krebs published an interesting expose on the man behind the supposed administration tool.) Until two weeks ago, it was publicly sold and licensed by a company calling itself Orcus Technologies. The project is now closed, according to this “press release” issued, and a license-free version available for download, as well as software development tools and documentation. Interestingly, the author also claims there is a “kill switch” available for download by security researchers to remotely shut down and lock out any Orcus control server that they find are being used for malicious purposes.
Information	<https://blog.morphisec.com/new-campaign-delivering-orcus-rat> <https://orcusremote.com/> <https://krebsonsecurity.com/2016/07/canadian-man-is-author-of-popular-orcus-rat/> <https://krebsonsecurity.com/2019/04/canadian-police-raid-orcus-rat-author/> <https://unit42.paloaltonetworks.com/unit42-orcus-birth-of-an-unusual-plugin-builder-rat/> <https://www.fortinet.com/blog/threat-research/a-peculiar-case-of-orcus-rat-targeting-bitcoin-investors.html> <https://asec.ahnlab.com/en/45462/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.orcus_rat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Orcus%20RAT>

Last change to this tool card: 15 February 2023

Download this tool card in JSON format

All groups using tool Orcus RAT

Changed	Name	Country	Observed	
APT groups				
	Pusikurac	[Unknown]	2019	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=9c969fa3-3382-4713-901d-a864b6c55549