Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:22:46 UTC

Tool: WolfRAT

Names	WolfRAT W1_RAT
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Info stealer, Exfiltration
Description	(Talos) Cisco Talos has discovered a new Android malware based on a leak of the Dendroid malware family. We named this malware 'WolfRAT' due to strong links between this malware (and the command and control (C2) infrastructure) and Wolf Research, an infamous organization that developed interception and espionage-based malware and was publicly described by CSIS during Virus Bulletin 2018. We identified infrastructure overlaps and string references to previous Wolf Research work. The organization appears to be shut down, but the threat actors are still very active. We identified campaigns targeting Thai users and their devices. Some of the C2 servers are located in Thailand. The panels also contain Thai JavaScript comments and the domain names also contain references to Thai food, a tactic commonly employed to entice users to click/visit these C2 panels without much disruption.
Information	<https://blog.talosintelligence.com/2020/05/the-wolf-is-back.html> <https://www.virusbulletin.com/uploads/pdf/conference_slides/2018/AncelKuprins-VB2018-WolfSheep.pdf> <https://www.africacybersecurityconference.com/document/CrowdStrike_GTR_2019.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0489/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.wolf_rat>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool WolfRAT

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ee2b0b06-f227-4523-b696-da3c1cae3a7c