SpyNote RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:37:59 UTC

Tool: SpyNote RAT

Names	SpyNote RAT SpyNote CypherRat
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	SpyNote RAT (Remote Access Trojan) is a family of malicious Android apps. The SpyNote RAT builder tool can be used to develop malicious apps with the malware's functionality.
Information	<https://threatpost.com/new-trojan-spynote-installs-backdoor-on-android-devices/119560/> <https://www.zscaler.com/blogs/research/spynote-rat-posing-netflix-app> <https://www.cleafy.com/cleafy-labs/spynote-continues-to-attack-financial-institutions> <https://blog.f-secure.com/take-a-note-of-spynote/> <https://www.bleepingcomputer.com/news/security/spynote-android-malware-spreads-via-fake-volcano-eruption-alerts/> <https://www.fortinet.com/blog/threat-research/android-spynote-moves-to-crypto-currencies> <https://www.cyfirma.com/research/spynote-unmasking-a-sophisticated-android-malware/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0305/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.spynote>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:spynote>

Last change to this tool card: 26 December 2024

Download this tool card in JSON format

All groups using tool SpyNote RAT

Changed	Name	Country	Observed

APT groups

	OilAlpha		2022	
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	
	Syrian Electronic Army (SEA), Deadeye Jackal		2011-Aug 2021	
	↳ Subgroup: Pat Bear, APT-C-37		2015	

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

↑
