

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:42:32 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Cerberus

Tool: Cerberus

Names	Cerberus
Category	Malware
Type	Banking trojan , Backdoor , Info stealer , Credential stealer , Botnet
Description	(ThreatFabric) After the user grants the requested privilege, Cerberus starts to abuse it by granting itself additional permissions, such as permissions needed to send messages and make calls, without requiring any user interaction. It also disables Play Protect (Google's preinstalled antivirus solution) to prevent its discovery and deletion in the future. After conveniently granting itself additional privileges and securing its persistence on the device, Cerberus registers the infected device in the botnet and waits for commands from the C2 server while also being ready to perform overlay attacks.
Information	<p><https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html></p> <p><https://www.mcafee.com/blogs/consumer/consumer-threat-notice/cerberus-banking-trojan/></p> <p><https://threatpost.com/cerberus-android-malware-rental/147280/></p> <p><https://threatpost.com/cerberus-trojan-major-spyware-targeted-attack/155415/></p> <p><https://securityintelligence.com/news/cerberus-android-malware-gains-ability-to-steal-2fa-tokens-screen-lock-credentials/></p> <p><https://malware.wikia.org/wiki/Cerberus_(Banker)></p> <p><https://www.bleepingcomputer.com/news/security/cerberus-android-malware-source-code-offered-for-sale-for-100-000/></p> <p><https://www.zdnet.com/article/cerberus-banking-trojan-source-code-released-for-free-to-cyberattackers/></p> <p><https://www.bankinfosecurity.com/attacks-using-cerberus-banking-trojan-surge-a-15025></p> <p><https://www.threatfabric.com/blogs/alien_the_story_of_cerberus_demise.html></p>
MITRE ATT&CK	< https://attack.mitre.org/software/S0480/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/apk.cerberus >

AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:cerberus >
----------------	---

Last change to this tool card: 30 December 2022

Download this tool card in [JSON](#) format

All groups using tool Cerberus

Changed	Name	Country	Observed
Unknown groups			
	_ [Interesting malware not linked to an actor yet] _		

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=eafc48e5-6613-4d2d-aa69-0596a6d1f4d8>