Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:27:16 UTC

Tool: ExoBot

Names	ExoBot
Category	Malware
Type	Banking trojan, Info stealer, Credential stealer, Botnet
Description	(IMB) ExoBot is Android malware that was based originally on a previous code known as Marcher. This code represents a banking Trojan that uses the overlay technique — that is, popping up fake windows that hide the original app users open — to trick victims into tapping their banking credentials into a fake interface. After stealing account access details, the malware can also intercept SMS messages and phone calls, thereby enabling criminals to take over the victim's bank account and other financial accounts at their discretion. Some of the capabilities that enable ExoBot to facilitate fraudulent activity on infected devices include gaining admin privileges, launching overlay screens, and exfiltrating SMS, data and other information from the infected device.
Information	<https://securityintelligence.com/ibm-x-force-delves-into-exobots-leaked-source-code/> <https://securityintelligence.com/news/unknown-actor-leaks-android-malware-exobot-source-code/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0522/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.exobot>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:ExoBot>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool ExoBot

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=becb3edc-a20e-4b0e-918d-db63051a137f