Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:31:16 UTC

Tool: Marcher

Names	Marcher
Category	Malware
Type	Banking trojan, Credential stealer
Description	(ZScaler) Upon infection, Marcher would inspect the victim's device and send a list of all installed apps to its command and control (C&C) server. If the malware found any German financial apps installed in the device, it would show a fake page asking for credentials of that particular institution. Unaware that the login page is a fake, the victim would provide their credentials where they would then be sent to the malware's C&C. The malware would also show a fake Google Play payment page if the infected device did not have any German financial firm apps.
Information	<https://www.zscaler.de/blogs/research/android-marcher-continuously-evolving-mobile-malware> <https://www.clientsidedetection.com/marcher.html> <https://www.clientsidedetection.com/exobot_v2_update___staying_ahead_of_the_competition.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0522/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.marcher>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Marcher>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Marcher

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

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