Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:45:46 UTC

Tool: TriangleDB

Names	TriangleDB
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Kaspersky) The implant, which we dubbed TriangleDB, is deployed after the attackers obtain root privileges on the target iOS device by exploiting a kernel vulnerability. It is deployed in memory, meaning that all traces of the implant are lost when the device gets rebooted. Therefore, if the victim reboots their device, the attackers have to reinfect it by sending an iMessage with a malicious attachment, thus launching the whole exploitation chain again. In case no reboot occurs, the implant uninstalls itself after 30 days, unless this period is extended by the attackers.
Information	<https://securelist.com/triangledb-triangulation-implant/110050/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1216>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ios.triangledb>

Last change to this tool card: 28 June 2025

Download this tool card in JSON format

All groups using tool TriangleDB

Changed	Name	Country	Observed	
APT groups				
	Operation Triangulation	[Unknown]	2023	

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