

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:59:25 UTC

[Home](#) > [List all groups](#) > Operation Triangulation

APT group: Operation Triangulation

Names	Operation Triangulation (<i>Kaspersky</i>)
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2023
Description	<p>(Kaspersky) While monitoring the network traffic of our own corporate Wi-Fi network using the Kaspersky Unified Monitoring and Analysis Platform (KUMA), we discovered a previously unknown mobile APT campaign targeting iOS devices. The targets are infected using zero-click exploits via the iMessage platform, and the malware runs with root privileges, gaining complete control over the device and user data. We are calling this campaign “Operation Triangulation”.</p> <p>This is an ongoing investigation, the amount of material we collected is substantial and will take time to analyze. Given the complexity of the attack, we are confident that we are not the only target, and invite everyone to join the research.</p>
Observed	
Tools used	TriangleDB .
Information	<p><https://securelist.com/trng-2023/> <https://securelist.com/operation-triangulation/109842/> <https://securelist.com/find-the-triangulation-utility/109867/> <https://securelist.com/triangulation-validators-modules/110847/> <https://securelist.com/operation-triangulation-catching-wild-triangle/110916/> <https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/></p>

Last change to this card: 17 January 2024

Download this actor card in [PDF](#) or [JSON](#) format