



# Mobile Threat Landscape

June 2023

Omer Rafaeli | Mobile Security Expert

A circular logo with a white center containing the text "CPX 360" in red. The logo is surrounded by a red ring and is positioned over a background of horizontal bars in various colors (blue, red, purple, teal) and a large pink circle with a black arrow pointing towards it.

**CPX  
360**

YOU DESERVE THE  
BEST SECURITY

# Recent Threats

## Over 400 million infected with Android spyware — delete these apps right now

By [Anthony Spadafora](#) last updated 3 days ago

Malicious SpinOk spyware module found in 101 popular Android apps

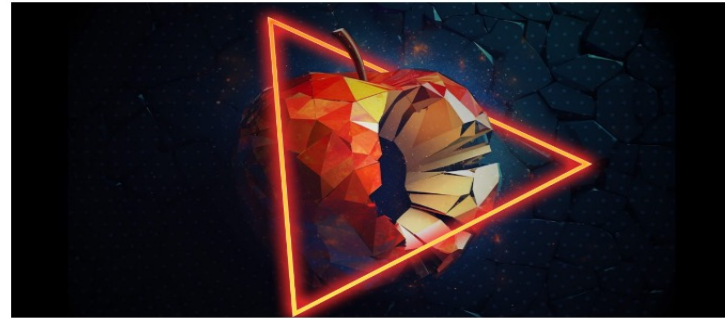
[f](#) [t](#) [g+](#) [p](#) [r](#) [m](#) [c](#) Comments (0)



## Operation Triangulation: iOS devices targeted with previously unknown malware

APT REPORTS 01 JUN 2023

5 minute read



# SpinOK

## WHAT?

- Trojanized SDK for ad-revenue
- Popular Android apps
- 400 million downloads
- Over 190 infected apps in GP

## HOW

App developers likely added the SpinOk module without knowing its malicious capabilities, as it appeared to be legitimate



- The trojanized SDK connects to a remote server in order to download a list of websites to display minigames.
- The minigames are displayed within the apps, while SpinOk performs its malicious activities.
- Most infected apps were already removed from the Google Play Store, but infected versions may still be present on mobile devices of the organization.

C&C  
connectivity &  
Data  
Exfiltration

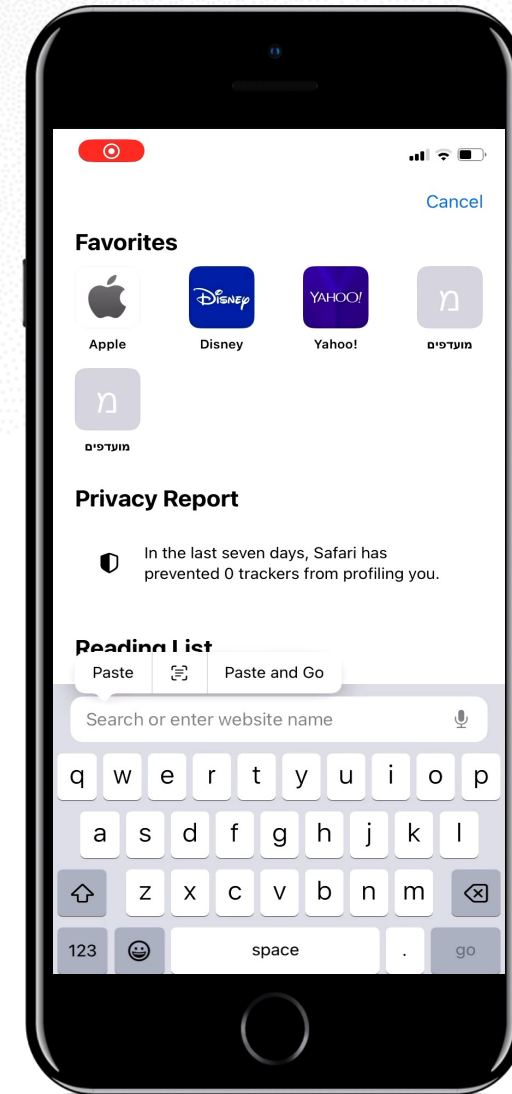
Data  
Exploitation

The hackers receives  
the entire phone's  
data: files,  
passwords, credit  
card data, etc.



# You are protected against SpinOK with Harmony Mobile

- All applications downloaded from the official or 3<sup>rd</sup> party mobile app stores are analyzed by Harmony Mobile.
- All existing and new applications using SpinOK SDK malware strain (regardless where they came from) will be detected by Harmony Mobile's Behavioral Risk Engine.
- All Harmony Mobile customers are fully protected!  
Check Point has recently prevented this attack in a major bank in South Africa and a large Telco in Asia





# iOS Triangulation

## WHAT?

iOS exploit raising permissions on the devices

## HOW

By exploiting a vulnerability in iMessage, the hackers can raise permissions for the malwares by installing a hidden executable into the device.



- The targets are infected using zero-click exploits via the iMessage platform.
- The malware runs with root privileges, gaining complete control over the device and user data.



Sideload

Indicator  
Removal

The initial message  
and the exploit in  
the attachment are  
deleted



# Protection against iMessage vulnerability with Harmony Mobile

- This vul
- By moni
- define a
- which is
- Harmon
- connect
- To explo
- into the
- been do

Security Alert - Apple just released new iOS and iPadOS versions 16\_5\_1

Critical vulnerabilities have recently been detected in the iOS WebKit.

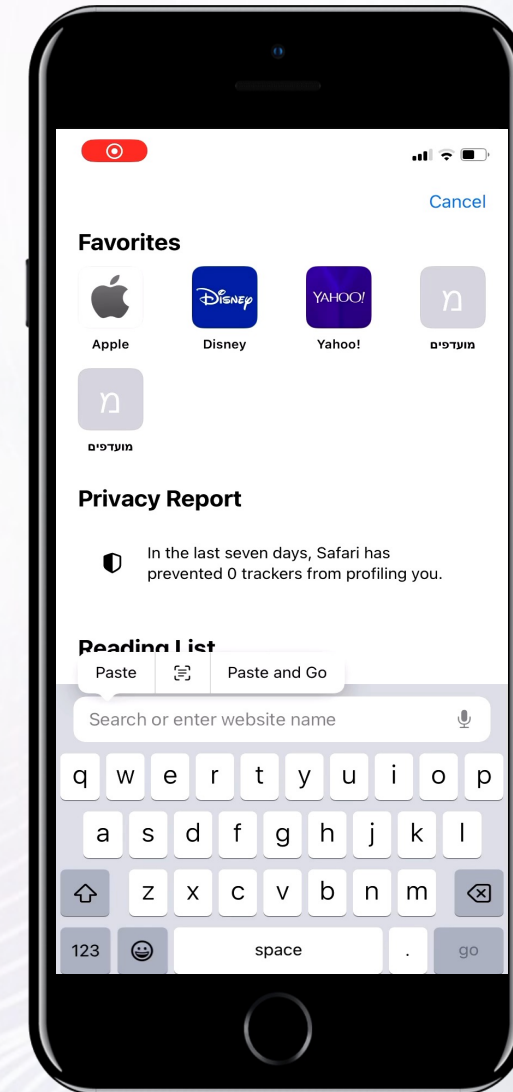
Several exploits known as Operation Triangulation and using those security flaws have already been reported.

To address those vulnerabilities, Apple just released new iOS and iPadOS versions 16.5.1.

We highly recommend you ensure your users' iPhone and iPad devices are updated to those new versions and are rebooted after upgrade.

Additionally, to prevent vulnerable devices from accessing your corporate resources, you can also set the risk level of the mobile devices not upgraded yet to high as follows:

Don't show me again. CLOSE



# TRIADA



**Malware family:** TRIADA



**Market segment:** Consumers



**Damage :**

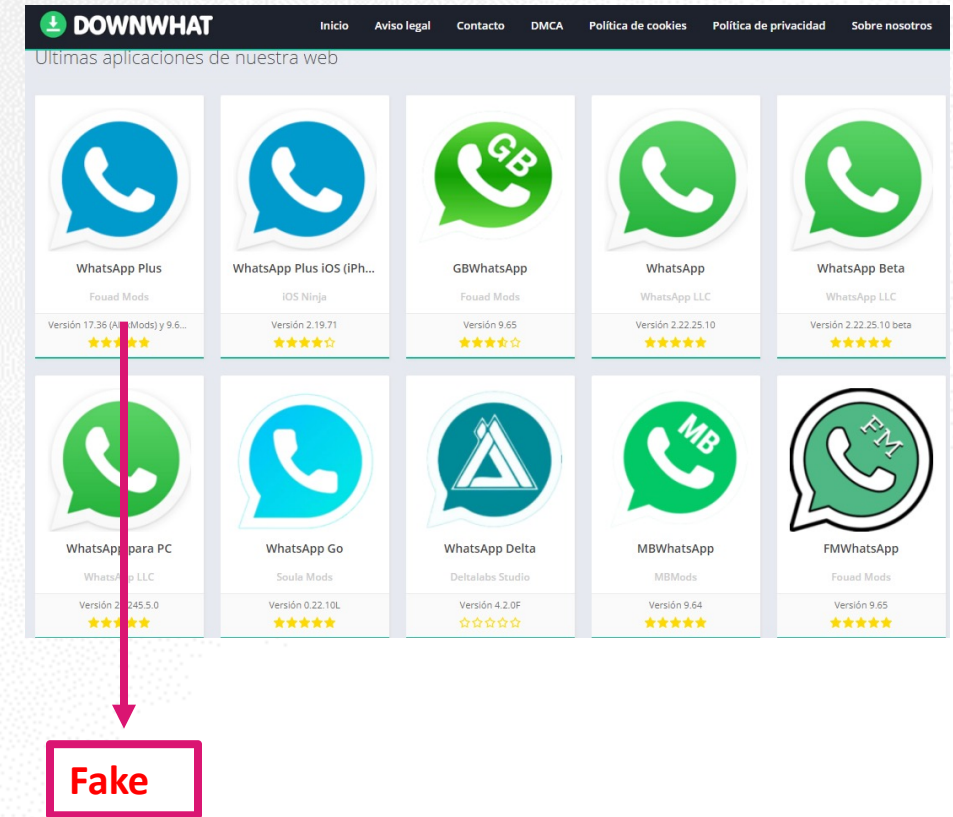
- Steal data from the device,
- Download and run additional malwares
- Privileges escalations.



**Anatomy of the attack**

Delivered via innocent applications or add-on to existing applications, that usually need to be paid for.

After installation TRIADA running on the background and start executing the malicious logic, which uploading sensitive data to the hacker C&C, and can perform any kind of malicious actions based on the hacker desire.



**Thank You!**

