Mobile Threat of the Month

February 2025

Spyrtacus & Graphite

Active families of spyware targeting mobile devices

Spyrtacus

Spyrtacus is a sophisticated form of mobile spyware developed by SIO, an Italy-based spyware producer known for supplying its products to government clients. First identified and analyzed in 2019 by mobile security researchers at Lookout, Spyrtacus has recently resurfaced in counterfeit versions of applications impersonating major Italian telecom providers, including TIM, Vodafone, and WINDTRE. These malicious apps were deployed in highly targeted campaigns.

Graphite

A group of 90 journalists and members of civil society using WhatsApp, were targeted by spyware developed by Paragon, an Israeli company specializing in hacking software. The attack was a "zero-click" exploit, meaning the targets did not need to interact with or click on any malicious links to become infected. Meta, the parent company of WhatsApp, suspects that the spyware was delivered through a malicious PDF file sent to specific individuals who were added to group chats.

Potential Impact

Spyware like Spyrtacus and Graphite possess advanced functionalities designed to covertly monitor targets without detection. These capabilities include extracting contact lists, intercepting text messages and chats from popular communication platforms such as Facebook Messenger, Signal, and WhatsApp, as well as recording phone calls, ambient sounds, and capturing images. Such comprehensive surveillance can lead to the exposure of sensitive information, including the compromise of login credentials, posing significant risks to privacy and security.

Lookout Mobile Security

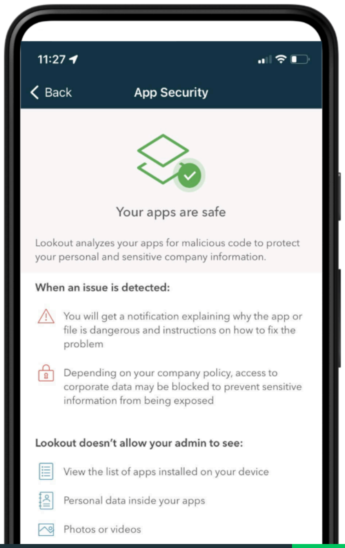
Lookout provides a multi-layered defence strategy to safeguard iOS, Android, and ChromeOS devices against mobile threats. Key features to protect against mobile-delivered spyware include:

Unparalleled Visibility and Detection: Advanced tools to identify and block mobile malware and spyware, ensuring robust protection against evolving threats.

Sideloaded App Detection: Detect apps downloaded from untrusted or unauthorized sources outside of official app stores reduces the risk of malicious software.

Risk-Based Access Control: The option to block devices with unresolved security risks from accessing sensitive company data enhances organizational security.

App Management: Restrict the use of specific app families or versions, allowing organizations to enforce compliance and mitigate potential vulnerabilities.



Your apps are safe

Lookout analyzes your apps for malicious code to protect your personal and sensitive company information.

When an issue is detected:

- You will get a notification explaining why the app or file is dangerous and instructions on how to fix the problem
- Depending on your company policy, access to corporate data may be blocked to prevent sensitive information from being exposed

Lookout doesn't allow your admin to see:

- View the list of apps installed on your device
- Personal data inside your apps
- Photos or videos

Sources: TechCrunch / The Guardian