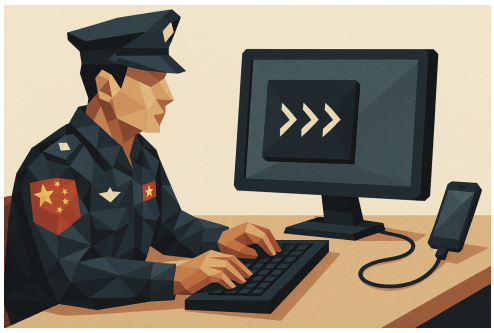
Lookout

Mobile Threat of the Month

August 2025

Lookout Discovers Massistant Mobile Forensic Tool



Lookout Threat Lab researchers have identified Massistant, a mobile forensic application used by Chinese law enforcement to extract extensive data from mobile devices. Meiya Pico, the company behind Massistant, and previously MFSocket in 2019, has been frequently reported for its involvement in the Chinese commercial surveillance market, with its tools used by law enforcement and for the surveillance of minority groups.

Massistant is not distributed through app stores; it is installed using specialist desktop forensic software over a physical port connection to a mobile device. Once installed, it can gain access to a wide range of data, including: device GPS location., SMS messages, contacts, images, audio files, phone service data and third-party app data from messaging apps such as Signal, Telegram, and Letstalk.

Potential Impact

In 2024, the Ministry of State Security introduced new legislation that allows Chinese law enforcement to collect and analyse devices without a warrant. The existence and use of forensic tools such as Massistant pose significant risks, particularly for those travelling to China:

Data Acquisition Risk for Travellers: Potential for tourists, business travellers, and persons of interest to have their confidential mobile data acquired as part of lawful intercept initiatives by the Chinese state police.

Persistent Surveillance: There are anecdotal reports of Chinese law enforcement collecting and analysing devices, and installing persistent, headless surveillance modules that continue to monitor device activity even after the device is returned.

Organisational Risk: These tools can pose a risk to organisations with executives and employees who travel abroad, especially to countries with policies that allow for the temporary confiscation of mobile devices upon entry.

Indication of Compromise: Even if Massistant doesn't exfiltrate data after a device is returned, its presence or any logging details would indicate to a device owner that their mobile data had been compromised.

Lookout Mobile Security

How would your team know if a mobile device is compromised? The challenge isn't just spotting these threats—it's achieving complete visibility, real-time detection, and rapid response across every mobile device. Securing mobile devices requires a purpose-built solution that understands mobile behaviour and continuously evaluates risk.

Lookout's AI-first approach to mobile endpoint security is purpose-built for the unique mobile environment, acting as the first line of defence to block mobile threats before execution. Designed expressly for iOS and Android ecosystems, Lookout delivers the visibility, context, and control needed to transform mobile security from a gap into a core strength of your cybersecurity strategy. Lookout customers are protected from Massistant.