# badbazaar (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:44:31 UTC

## badbazaar

Actor(s): APT15

---

BadBazaar is a type of malware primarily functioning as a spyware. Designed to compromise Android and iOS devices, it is often distributed through malicious apps downloaded from unofficial app stores, third-party websites, Telegram channels, and social engineering. Once installed, BadBazaar seeks to surveil the victim by intercepting SMS messages, performing screen recordings, and logging keystrokes on the device. Additionally, it can execute remote commands and download and install other malicious applications, further compromising the security of the affected device.

**References**

2025-04-09 · NCSC UK · ASD, BND, Bundesamt für Verfassungsschutz, Canadian Centre for Cyber Security (CCCS), FBI, NCSC UK, New Zealand National Cyber Security Centre (NZ NCSC), NSA
NCSC and partners share guidance for communities at high risk of digital surveillance
badbazaar

2025-04-09 · NCSC UK · ASD, BND, Bundesamt für Verfassungsschutz, Canadian Centre for Cyber Security (CCCS), FBI, NCSC UK, New Zealand National Cyber Security Centre (NZ NCSC), NSA
Advisory: BADBAZAAR and MOONSHINE: Spyware targeting Uyghur, Taiwanese and Tibetan groups and civil society actors
badbazaar

2025-04-09 · NCSC UK · ASD, BND, Bundesamt für Verfassungsschutz, Canadian Centre for Cyber Security (CCCS), FBI, NCSC UK, New Zealand National Cyber Security Centre (NZ NCSC), NSA
Advisory: BADBAZAAR and MOONSHINE: Technical analysis and mitigations
badbazaar

2023-01-22 · Lookout · Alemdar Islamoglu, Justin Albrecht, Kristina Balaam, Ruohan Xiong
BadBazaar: iOS and Android Surveillanceware by China’s APT15 Used to Target Tibetans and Uyghurs
badbazaar

There is no Yara-Signature yet.

---

---

Source: https://malpedia.caad.fkie.fraunhofer.de/details/apk.badbazaar