

Bahamut (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:54:54 UTC

apk.bahamut ([Back to overview](#))

Bahamut

Actor(s): [Bahamut](#), Dropping Elephant



According to PCrisk, Bahamut is the name of Android malware with spyware functionality. Threat actors use Bahamut to steal sensitive information. The newest malware version targets various messaging apps and personally identifiable information.

References

2022-11-23 · [ESET Research](#) · [Lukáš Štefanko](#)

Bahamut cybermercenary group targets Android users with fake VPN apps

[Bahamut](#)

2022-06-29 · [cyble](#) · [Cyble Research Labs](#)

Bahamut Android Malware Returns With New Spying Capabilities

[Bahamut](#)

2022-04-12 · [360 Threat Intelligence Center](#) · [360 Beacon Lab](#)

Recent attacks by Bahamut group revealed

[Bahamut](#)

2020-10-06 · [Blackberry](#) · [Blackberry Research](#)

BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps

[Bahamut Bahamut](#)

2018-08-29 · [Trend Micro](#) · [Daniel Lunghi](#), [Ecular Xu](#)

The Urpage Connection to Bahamut, Confucius and Patchwork

[AndroRAT Bahamut](#)

2018-08-29 · [Trend Micro](#) · [Daniel Lunghi](#), [Ecular Xu](#)

Bahamut, Confucius and Patchwork Connected to Urpage

[Bahamut Confucius Urpage](#)

2017-10-27 · [Bellingcat](#) · [Collin Anderson](#)

Bahamut Revisited, More Cyber Espionage in the Middle East and South Asia

[Bahamut Bahamut Bahamut](#)

2017-06-12 · [Bellingcat](#) · [Collin Anderson](#)

Bahamut, Pursuing a Cyber Espionage Actor in the Middle East

[Bahamut Bahamut Bahamut](#)

There is no Yara-Signature yet.

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/apk.bahamut>