

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:39:56 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Bahamut


Tool: Bahamut

Names	Bahamut
Category	Malware
Type	Backdoor
Description	(Bellingcat) The malware is also of low quality – in version 1.1 of Khuai Translator, the URLs to report back to the attacker contain typos (e.g. “http://”) that would lead to them being non-functional. This was resolved in a subsequent update, but other typos are present in both applications across web properties, internal functions, and application dialogues, suggesting that quality was not a priority for the attackers.
Information	< https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/ > < https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/apk.bahamut > < https://malpedia.caad.fkie.fraunhofer.de/details/win.bahamut >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:Bahamut >

Last change to this tool card: 13 May 2020

Download this tool card in [JSON](#) format

All groups using tool Bahamut

Changed	Name	Country	Observed
APT groups			
	Bahamut	[Middle East]	2016-Jul 2023
	Patchwork , Dropping Elephant		2013-Jun 2025

2 groups listed (2 APT, 0 other, 0 unknown)

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=f70c41f5-703e-4dcd-9594-6646e837a195>