Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:20:28 UTC

APT group: Bahamut

Names	Bahamut *(Bellingcat)*	
Country	[Middle East]	
Motivation	Information theft and espionage	
First seen	2016	
Description	(Bellingcat) Bahamut was first noticed when it targeted a Middle Eastern human rights activist in the first week of January 2017. Later that month, the same tactics and patterns were seen in attempts against an Iranian women's activist – an individual commonly targeted by Iranian actors, such as Magic Hound, APT 35, Cobalt Illusion, Charming Kitten and the Sima campaign documented in our 2016 Black Hat talk. Recurrent patterns in hostnames, registrations, and phishing scripts provided a strong link between the two incidents, and older attempts were found that directly overlapped with these attacks. Over the course of the following months, several more attempts against the same individuals were observed, intended to steal credentials for iCloud and Gmail accounts. Bahamut was also observed engaging in reconnaissance and counter-reconnaissance attempts, intended to harvest IP addresses of emails accounts. One attempt impersonated BBC News Alerts, using timely content related to the diplomatic conflict between Qatar and other Gulf states as bait. This message used external images embedded in the email to track where the lure would be opened.	
Observed	Sectors: Political, economic and social. Countries: Egypt, Iran, Pakistan, Palestine, Qatar, Tunisia, Turkey, UAE.	
Tools used	Bahamut, DownPaper.	
Operations performed	Dec 2016	Beginning in December 2016, unconnected Middle Eastern human rights activists began to receive spear-phishing messages in English and Persian that were not related to any previously-known groups. These attempts differed from other tactics seen by us elsewhere, such as those connected to Iran, with better attention paid to the operation of the campaign.

	<https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/>
Oct 2017	For three months there was no apparent further activity from the actor. However, in the same week of September a series of spear-phishing attempts once again targeted a set of otherwise unrelated individuals, employing the same tactics as before. Bahamut remains active, and its operations are more extensive than first disclosed. <https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/>
Jun 2018	Cisco Talos has identified a highly targeted campaign against 13 iPhones which appears to be focused on India. The attacker deployed an open-source mobile device management (MDM) system to control enrolled devices. <https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM.html>
Jul 2018	Android-based malware with some similarities to the iOS malware we identified. That post kickstarted our investigation into any potential overlap between these campaigns and how they are potentially linked. The new MDM platform we identified has similar victimology with Middle Eastern targets, namely Qatar, using a U.K. mobile number issued from LycaMobile. Bahamut targeted similar Qatar-based individuals during their campaign. <https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM-Part2.html>
Jun 2020	Bahamut Possibly Responsible for Multi-Stage Infection Chain Campaign <https://www.anomali.com/blog/bahamut-possibly-responsible-for-multi-stage-infection-chain-campaign>
Aug 2021	Bahamut Threat Group Targeting Users Through Phishing Campaign <https://blog.cyble.com/2021/08/10/bahamut-threat-group-targeting-users-through-phishing-campaign/>
Jan 2022	Bahamut cybermercenary group targets Android users with fake VPN apps <https://www.welivesecurity.com/2022/11/23/bahamut-cybermercenary-group-targets-android-users-fake-vpn-apps/>
Apr 2022	Bahamut Android Malware returns with New Spying Capabilities <https://blog.cyble.com/2022/06/29/bahamut-android-malware-

		returns-with-new-spying-capabilities/>
	Nov 2022	APT Bahamut Attacks Indian Intelligence Operative using Android Malware <https://www.cyfirma.com/outofband/apt-bahamut-attacks-indian-intelligence-operative-using-android-malware/>
	Jul 2023	APT Bahamut Targets Individuals with Android Malware Using Spear Messaging <https://www.cyfirma.com/outofband/apt-bahamut-targets-individuals-with-android-malware-using-spear-messaging/>
Information	<https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/> <https://www.blackberry.com/us/en/forms/enterprise/bahamut-report>	

Last change to this card: 06 September 2023

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=90fb0276-a977-4d3e-a148-85a95778aebe