

FalconFeeds.io Confirms Pro-Houthi Espionage Group OilAlpha Is Active in 2026

FalconFeeds.io: pro-Houthi group OilAlpha is active in 2026, using new SpyMax Android spyware, live C2 servers and a fake KSrelief WhatsApp lure on aid workers.

LONDON, LONDON, UNITED KINGDOM, September 29, 2026 /EINPresswire.com/ --

FalconFeeds.io, a real-time threat intelligence platform, today published new research showing that OilAlpha, a pro-Houthi cyber-espionage group first exposed in 2023, remains fully operational in 2026 and continues to target humanitarian organisations, journalists and political figures connected to the Yemen conflict.

The report, "OilAlpha 2026: Pro-Houthi Mobile Espionage," presents the first public identification of the group's 2026 campaign. Working with OSINT partner Sycek, FalconFeeds.io analysts identified two previously unreported Android spyware samples built on the commodity SpyMax/SpyNote remote access trojan, live command-and-control (C2) infrastructure operated through at least August 2026, and a KSrelief-themed WhatsApp lure that circulated among Yemeni users in May 2026.

Key findings include:

Rebuild, launch, expand. Between December 2025 and February 2026, OilAlpha re-pointed its entire 2024 hostname set to a new server. The first 2026 sample appeared two weeks later, six new hostnames followed in May, and the most recent was added on 18 August 2026.

Live infrastructure, not sinkholes. 47 of 51 historical OilAlpha C2 domains still resolve to two DigitalOcean-hosted servers assessed as actor-controlled. Earlier "probable sinkhole" assessments are withdrawn.

Evolving delivery. The May 2026 lure was a roughly 13 MB ZIP-wrapped APK spread through forwarded WhatsApp chains, impersonating Saudi Arabia's King Salman Humanitarian Aid and Relief Centre (KSrelief) with an Arabic-language "Inquiry" theme.

Maturing tradecraft. Operator-chosen package names from 2022 have given way to randomised builds with anti-analysis checks and staged code loading, while APK sizes have grown from under 1 MB to 12.48 MB.

A language gap. English-language visibility of OilAlpha ended in mid-2024. The only public warning of the 2026 campaign appeared in Arabic-language Yemeni media and was surfaced through Sycek collection.

Once installed, OilAlpha's malicious apps provide GPS tracking, call interception, SMS exfiltration and camera and microphone access. Previous research by Recorded Future's Insikt Group identified the Norwegian Refugee Council, CARE International and KSrelief among the organisations impersonated, with the United Nations and World Food Programme also suspected.

The threat is not abstract. As of February 2026, 73 UN staff were in Houthi detention, many on espionage charges. The report warns that the people OilAlpha surveils are the same people being detained, and assesses with high confidence that the group is active as of August 2026 and highly likely to remain so.

"Every public exposure has changed OilAlpha's tooling, not its mission," said the FalconFeeds.io Threat Intelligence team. "After the 2024 reporting, the group abandoned its phishing portal within weeks, rebuilt its infrastructure and came back with new builds and the same humanitarian lures. Defenders should expect another rotation after this report and prioritise behaviour-based detection over static indicators."

The report includes 28 platform-tracked OilAlpha C2 domains with per-indicator confidence scoring, the full 2026 indicator set, a MITRE ATT&CK Mobile mapping and detection guidance for security teams, NGO security managers and end users. Immediate recommendations include:

Block or sinkhole all OilAlpha hostnames and both C2 servers across staff mobile fleets, and review DNS logs from December 2025 onward.

Block sideloading on managed devices and flag apps that request Accessibility and device-admin rights or hide their launcher icon.

Tell staff and beneficiaries that the organisation never distributes apps over WhatsApp, Telegram or SMS, and enforce multi-factor authentication on organisational accounts.

Never open APK or ZIP files received over WhatsApp, even when forwarded by a known contact.

FalconFeeds.io is a threat intelligence firm providing real-time monitoring of deep and dark web activity, from ransomware gangs to Telegram dumps and access marketplaces, along with threat actor profiles, indicators of compromise and threat-feed intelligence for security teams worldwide.

Nandakishore Harikumar

Technisanct

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/946063591>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable

in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.