



# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:39:25 UTC

## APT group: OilAlpha

Names	OilAlpha ( <i>Recorded Future</i> ) TAG-41 ( <i>Recorded Future</i> ) TAG-62 ( <i>Recorded Future</i> )
Country	  <a href="#">Yemen</a>
Motivation	<a href="#">Information theft and espionage</a>
First seen	2022
Description	<a href="#">(Recorded Future)</a> Since May 2022, Insikt Group has tracked an ongoing campaign by a threat group which is highly likely to have targeted entities associated with the non-governmental, media, international humanitarian, and development sectors. It is almost certain that the entities targeted shared an interest in Yemen, security, humanitarian aid, and reconstruction matters. It is highly likely that OilAlpha threat actors were involved in espionage activity, as handheld devices were targeted with remote access tools (RATs) like SpyNote and SpyMax. Our assessment of the victimology suggests that the majority of the targeted entities were Arabic-language speakers and operated Android devices.
Observed	
Tools used	<a href="#">njRAT</a> , <a href="#">SpyMax</a> , <a href="#">SpyNote RAT</a> .
Information	< <a href="https://go.recordedfuture.com/hubfs/reports/cta-2023-0516.pdf">https://go.recordedfuture.com/hubfs/reports/cta-2023-0516.pdf</a> >

Last change to this card: 21 June 2023

Download this actor card in [PDF](#) or [JSON](#) format

---

Source: <https://apt.eta.da.or.th/cgi-bin/showcard.cgi?u=425b11e0-adbb-4d6f-a5e0-169df11b15bf>