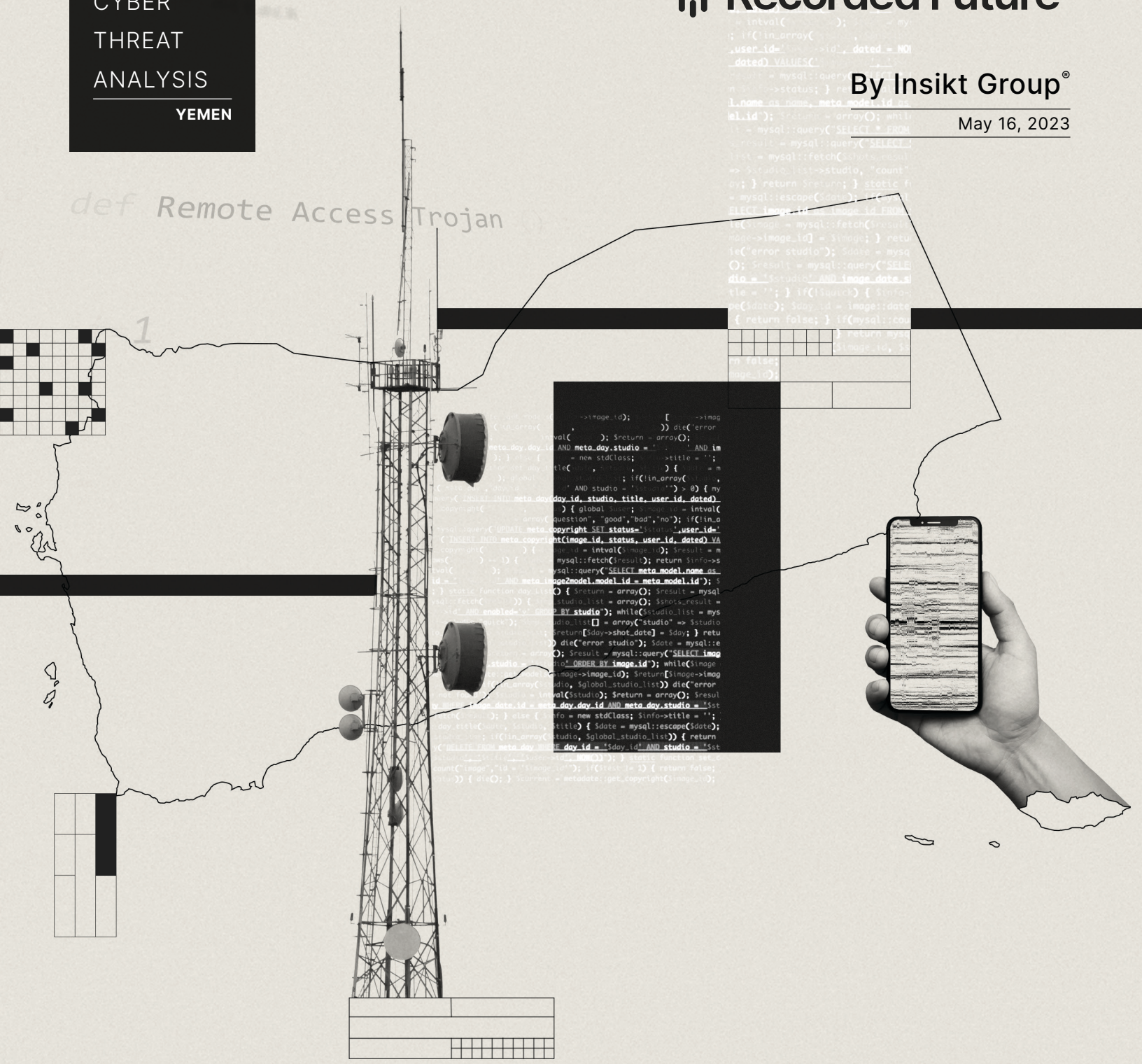
CYBER
THREAT
ANALYSIS
YEMEN

Recorded Future®

By Insikt Group®

May 16, 2023



OilAlpha:

A Likely Pro-Houthi Group Targeting Entities Across the Arabian Peninsula

Executive Summary

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.

The observed tactics, techniques, and procedures (TTPs) associated with this threat activity has included the almost exclusive use of Dynamic DNS (DDNS) for command and control (C2). Additionally, the threat actors used domain naming conventions associated with international, Saudi Arabian, and United Arab Emirates (UAE) humanitarian organizations, as well as media organizations, in addition to non-attributable entities; the threat actors also used encrypted chat messengers, like WhatsApp, to target victims.

We previously tracked this threat activity under the temporary designators TAG-41 and TAG-62. Insikt Group is combining these threat clusters under the cryptonym OilAlpha due to overlapping TTPs and our increased confidence that the activities we have observed are coordinated by a single entity. OilAlpha is predominantly engaged in espionage, and at the time of this writing, it is likely acting in the interest of the Houthi movement. The following factors have influenced our assessment:

1. OilAlpha has relied on infrastructure (PTC) reported to be under the direct control of the Houthi authorities.
2. The group's operations have reportedly included targeting persons attending Saudi Arabian government-led negotiations; coupled with the use of spoofed Android applications mimicking entities tied to the Saudi Arabian government, and a UAE humanitarian organization (among others), we suspect that the attackers are targeting individuals the Houthis want direct access to.

Key Findings

- OilAlpha is a threat activity group targeting political representatives, media, and journalists for espionage. The group spoofs various international humanitarian organizations, including entities in the Arabian Peninsula and a Norwegian non-governmental organization (NGO).
- OilAlpha has used Android remote access trojans (RATs) like SpyNote and SpyMax. We have also observed njRAT samples communicating with C2s associated with this group, making it likely that OilAlpha has used other malware for testing or attack operations.
- OilAlpha used encrypted chat messengers like WhatsApp to launch social engineering attacks against its targets. It has also used URL link shorteners.
- OilAlpha has almost exclusively relied on infrastructure associated with the Public Telecommunication Corporation (PTC), a Yemeni government-owned enterprise. All of the Dynamic DNS (DDNS) domains identified as part of our research resolved to IP addresses owned by the PTC.
- OilAlpha is likely from Yemen; while analysis of its political allegiance remains fluid, as of this writing, we are linking this activity to threat actors which support a pro-Houthi movement agenda.
- The activity Insikt Group is linking to OilAlpha is not unique throughout the Middle Eastern region. Various campaigns have been disclosed since 2018 highlighting espionage threats to smartphones and personnel from multiple sectors, including military and security, academia, the media, and international humanitarian groups. Many regional espionage groups conduct campaigns that solely target handheld devices. As handheld devices continue to fulfill a growing role in corporate and personal environments, attacks targeting them will continue in the medium to long term.

Initial Detection of Threat Activity

Background

On April 14, 2022, Yemen-based open sources revealed that malicious Android applications were disseminated to journalists and media representatives through lures associated with Yemeni development and security matters. The Android applications (APKs) were sent from WhatsApp accounts using Saudi Arabian telephone numbers to Yemeni nationals. For example, as depicted in **Figure 1**, an alleged communique from the Security Belt Forces, which is an armed wing of the Southern Movement (South Yemen Movement, and al-Hirak) is visible along with an app called "YEMENOFKSA.apk". The applications were created using other themes as well, such as "Saudi-Yemen Development App", and were reportedly accessible via Google Play and Apple's App Store. The application identified in open sources is listed as SpyNote in a public malware repository by a large number of antivirus engines. Network analysis associated with this application suggested it was configured to communicate via HTTP on port 5551.

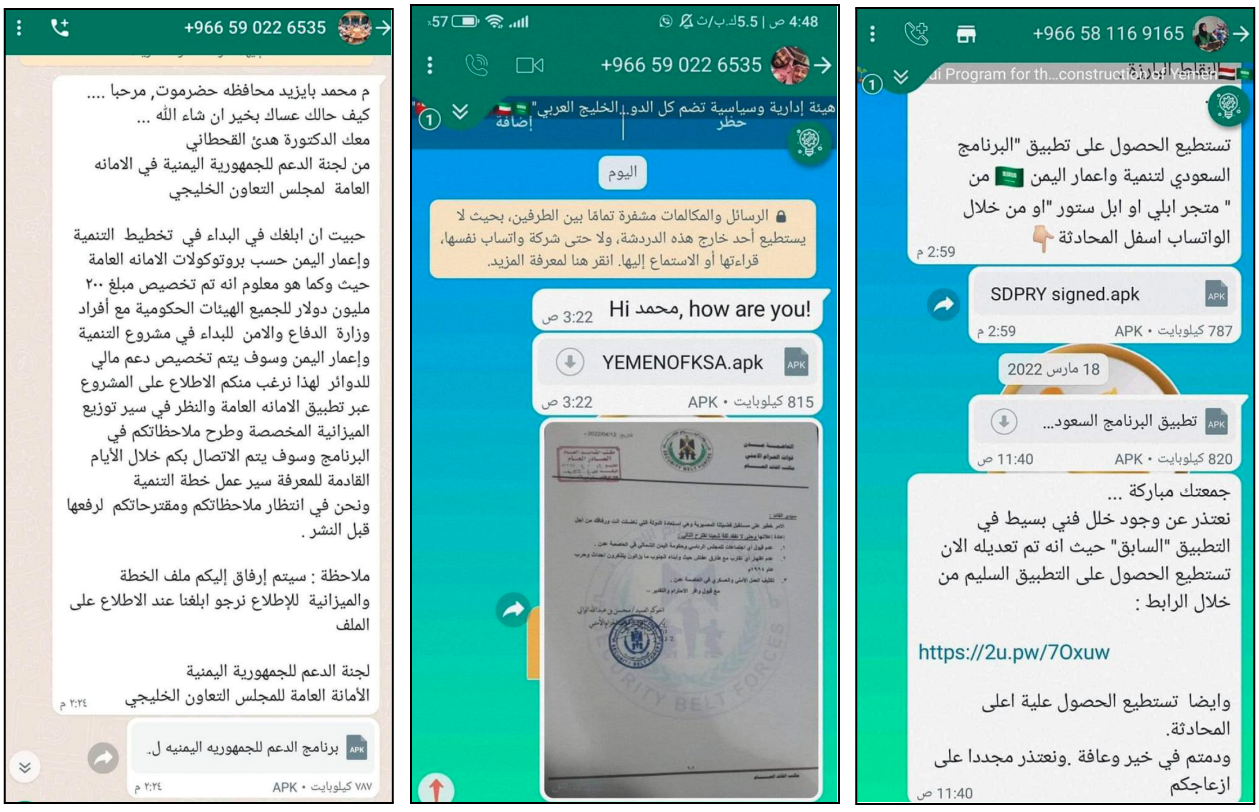


***Figure 1**: Messages reportedly sent to targets from Saudi Arabian telephone numbers (Source: Meta 1, 2, 3)*

The threat actors targeted their victims with social engineering techniques. Open source reports listed instances in which political representatives, media personalities, or journalists were reportedly sent messages around the time that negotiations were hosted in Saudi Arabia, in April 2022. The attacks transpired via encrypted chat messengers, like WhatsApp. While the first and only wave of social engineering attacks were detected and reported between April and May 2022, our tracking of DNS resolution changes for that attacker's domains suggests the threat actors are still active and are highly likely continuing their operations.

Insikt Research

TAG-41 and TAG-62: Graduating to OilAlpha

Insikt Group observed that the aforementioned applications were associated with at least 2 DDNS domain clusters that acted as C2 infrastructure (**Table 1**) for different applications. The DDNS clusters almost exclusively used infrastructure associated with Yemen's Public Telecommunication Corporation (PTC) (AS30873). Throughout March 2023, we also observed threat actors using infrastructure associated with the France-based dynamic infrastructure provider IELO-LIAZO Services SAS (AS29075).

The applications were developed using SpyNote or SpyMax, and the file names used similar international humanitarian, development and reconstruction, or security themes. Throughout 2022 and early 2023, we tracked these threat clusters with temporary designations as TAG-41 and TAG-62; however, due to their overlapping TTPs, we are graduating these threat clusters to "OilAlpha".

Malware, Lures, and Infrastructure

Analysis of the malware in sandbox environments (1, 2, 3, 4, 5, 6, 7, 8, 9, 10) depicted intrusive characteristics commonly associated with SpyNote and SpyMax; these included permissions to access call logs, SMS data, contact information, network information, access to the device's camera and audio, as well as GPS location data, among others.

C2 DDNS	IP Address	File Name	SHA256 Hash
87524uyre.ddns[.]net	134.35.15[.]220	استعلام واحصائيات المساعدات النقدية المقدة للنازحين.apk Inquiry and statistics of cash assistance provided to the displaced	1f1cdd9acd9e581f538bdefc1ec5f0aebcc57cfccf5a4a9389f35c8741242e32
mylab123321hm.ddns[.]net	134.35.130[.]126	WhatsApp.apk	8846b72ed2ecde60b805cfaf5d1f71e34742a18177ff3c4d8d5b9c3f250e153d
77112hilan.ddns[.]net	134.35.0[.]119	الخطة العامة المقترحة للدعم اليمن.apk Proposed general plan for Yemeni Support	2b7d2490bfc4eacd3e5870ae0de92fdb5c1f11a5e8fdc7c07773780c6db038d9
antahomaar2022.ddns[.]net	134.35.11[.]141	برنامج الدعم للجمهوريه اليمنيه لشهر ابريل 2022.apk The support program for the republic of Yemen for April	ad990791d595c149f6770d08be6411b88f9dab2ed56bf61fd274bea2327f17c3
manyouhomaar21.ddns[.]net	109.200.165[.]170	صندوق التنميه والاستثمار.apk Development and Investment Fund	2c2393a061901e13b9fc038bb25ba666fbff25d304c6dec51bac10a46dbd1fe6
Gomnd2873yemnenrc.ddns[.]net	134.35.11[.]130	نقاط الاستلام.apk Receipt Points	7d21d3dce90408ca530c5e2364495d4f0932cdd23d812e4714e3665c06bfc560
ndf236fgh4367h.ddns[.]net	134.35.2[.]7	اسماء المستفيدين من الحوالات النقدية لشهر فبراير.apk The names of the beneficiaries of cash transfers for February	92420eb9356e103864ba5edcffe98d6a5ecfe13f7580035202dea1a32739b256
Akjdaks54678sdas.ddns[.]net	134.35.1[.]116	unicef.apk	b0c54756dd5c53d13be190952fe63c1b9e1989f8673ab549d19035207f01d901
7687ytuyt78gfg.ddns[.]net	134.35.217[.]64	تواصل العمليات المشتركة.apk Continuation of Joint Operations	8bcc816a517ecdb72e6f97c53c4e40da8d96ebae239eb7f760c29bd943d1b722

***Table 1**: DDNS domain cluster and samples linked to OilAlpha (Source: Recorded Future)*

Additionally, file icons associated with the samples were dropped in the sandbox environment, providing insight about the possible victimology. The icons spoof regional political organizations such as the Gulf Cooperation Council (GCC), the United Nations, and regional non-governmental organizations (NGO) such as Project MASAM, a Saudi Arabian entity dedicated to landmine clearance efforts, and the UAE's Red Crescent Society, an international humanitarian organization. In a few instances the icons remained unidentifiable, although the imagery appeared to mimic emblems associated with the Saudi Arabian government, as depicted in **Figure 2** (far right).

***Figure 2**: File icons associated with the Android malware, in order of appearance (left to right); GCC, Project MASAM, Emirates Red Crescent, Yemeni Joint Forces, and a Saudi Arabian government emblem (Source: Recorded Future and Hybrid Analysis)*

A DDNS domain managed by OilAlpha acted as C2 for applications masquerading as WhatsApp, or as an adjunct application serving to "protect WhatsApp" (حماية واتساب) (**Figure 3**). In April 2021, a sample called "WhatsApp.apk" was first submitted to a public malware repository and was identified as SpyNote by a large number of antivirus engines. It shared similar intrusive requests and is detectable in the Applications Information directory of the Android emulator in the sandbox environment.

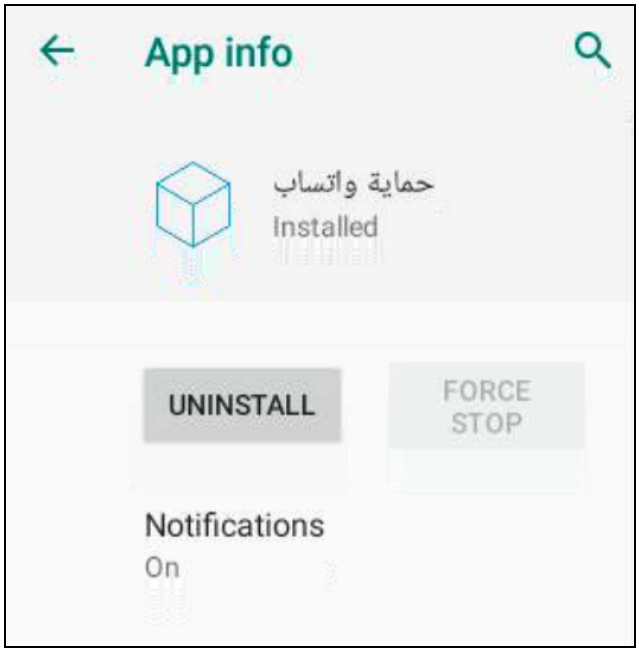


***Figure 3**: WhatsApp protection application linked to OilAlpha DDNS domain (Source: Recorded Future)*

As depicted in **Figure 1,** the threat actors also made use of a URL shortener, 2u[.]pw . The URL shortener claims to be a regional Arabic-language service, used throughout the Middle East, that offers its users analytics and marketing services, much like bit[.]ly.

In early 2023, Insikt Group identified 3 more malware samples associated with these threat clusters: "unjobs.apk", "KSA-YEMEN.apk", and "NRC ES.apk". The 3 samples used mylab123321hm.ddns[.]net for C2; as noted above, the domain was identified in early Insikt Group reporting affiliated with TAG-41 and the malware associated with these samples was classified in multiple repositories as SpyNote.

C2 DDNS	IP Address	ASN	File Name	SHA256 Hash
mylab123321hm.ddns[.]net	134.35.10[.]166	AS30873	unjobs.apk	8d07dc0745e57aeb40905a7426fb6515930a1fc7898db0ee93fda55ba085461b
mylab123321hm.ddns[.]net	134.35.2[.]3	AS30873	KSA-YEMEN.apk	7e6ec9df5e2218b5ad4111059f799e1348c06f98cb0f0742f86aae1875c6fd13
mylab123321hm.ddns[.]net	134.35.10[.]61	AS30873	NRC ES.apk	eb8edfd04c0d1e0b03f4629519800c8b043110dbe94a70406c60d5a009f723fe
goman239.ddns[.]net	134.35.11[.]92	AS30873	KSR HM.apk	f3f3764ee6a0e5b933e95040092e0b348f672aaab273cf8eaaeabca28be5da36

***Table 2**: SpyNote and SpyMax samples linked to OilAlpha DDNS domains (Source: Recorded Future)*

In March 2023, Insikt Group identified an additional malware sample called "KSR HM.apk". We executed it in Recorded Future's sandbox environment and revealed an icon linked to the Saudi Arabian King Salman Humanitarian Aid & Relief Centre (**Figure 4**). This is the same organization which was spoofed via OilAlpha's KSA-YEMEN application referenced in **Table 2**.

***Figure 4**: High-resolution version of the icon found in the KSR HM and KSA-YEMEN applications (Source: Recorded Future)*

OilAlpha has crafted applications with names associated with humanitarian and non-governmental organizations, including the United Nations and the Norwegian Refugee Council, as well as Saudi Arabian entities like the King Khalid Foundation, Project MASAM, and the aforementioned King Salman Humanitarian Aid & Relief Centre. All of these entities conduct or coordinate disaster response and humanitarian work in Yemen.

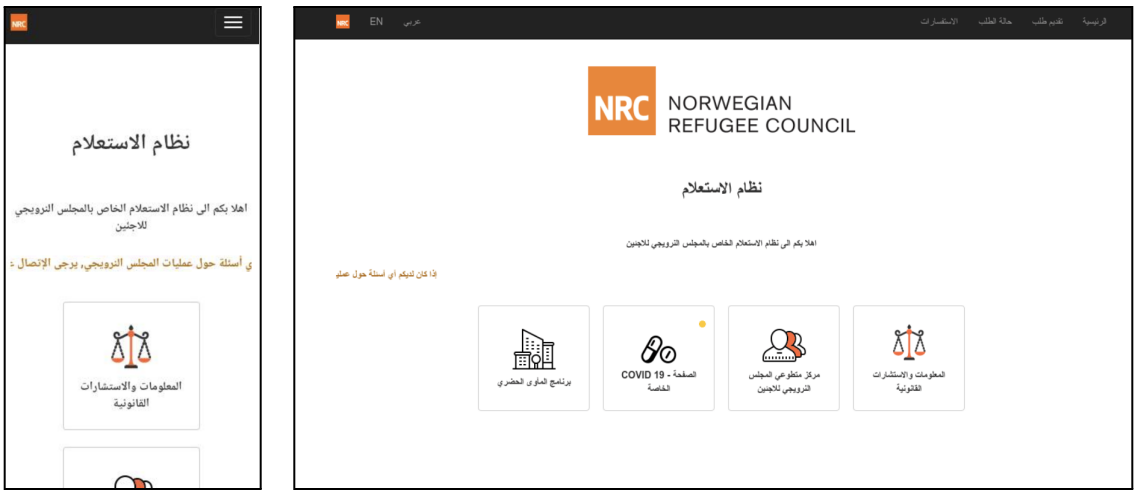


Figure 5: *The attacker's application "NCR ES.apk" executed in Recorded Future's sandbox revealing links to an NRC resource page (Left). Scanned NRC domain info.nrc[.]jo reveals identical page (Right) (Source: Recorded Future and urlscan)*

Another notable characteristic identified during the installation process included what appeared to be a permissions request (**Figure 6**). As the applications were executed, we observed a permission request load; however, clicking on "enable" (تمكين) appeared to serve no purpose, as all the permissions sought by the RATs administrator were already granted.

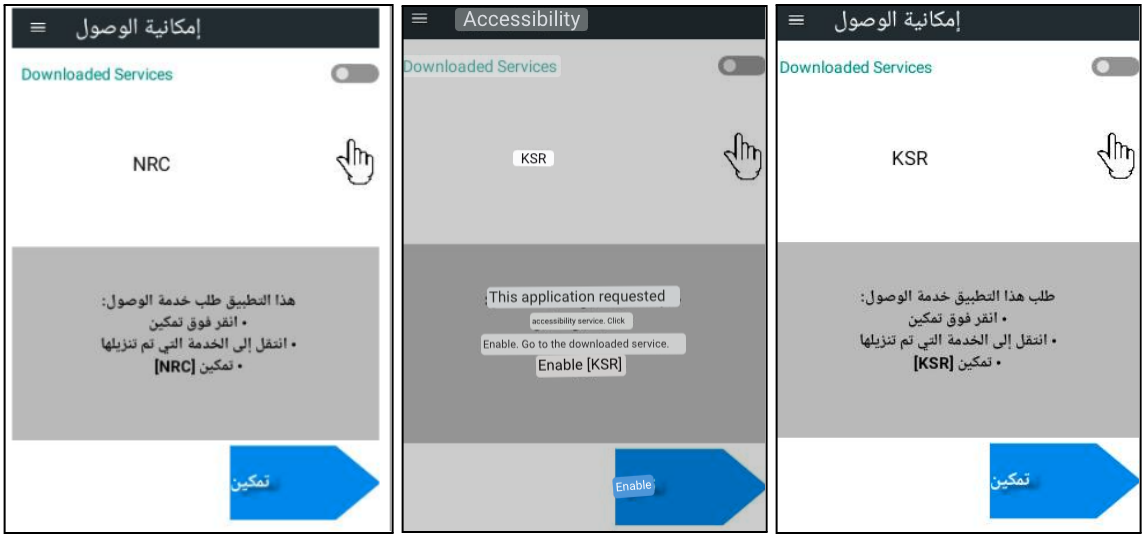


Figure 6: *A translation of the "enable" screen observed during the installation process (Source: Recorded Future and Google Translate)*

Android-Centric Threat Activity

OilAlpha's focus in targeting Android devices is not surprising due to the high saturation of Android devices in the Arabian Peninsula region (1, 2, 3, 4, 5, 6). According to the Statcounter website, in Yemen alone, between March 2022 and March 2023, Android devices accounted for more than 95% of total active devices.

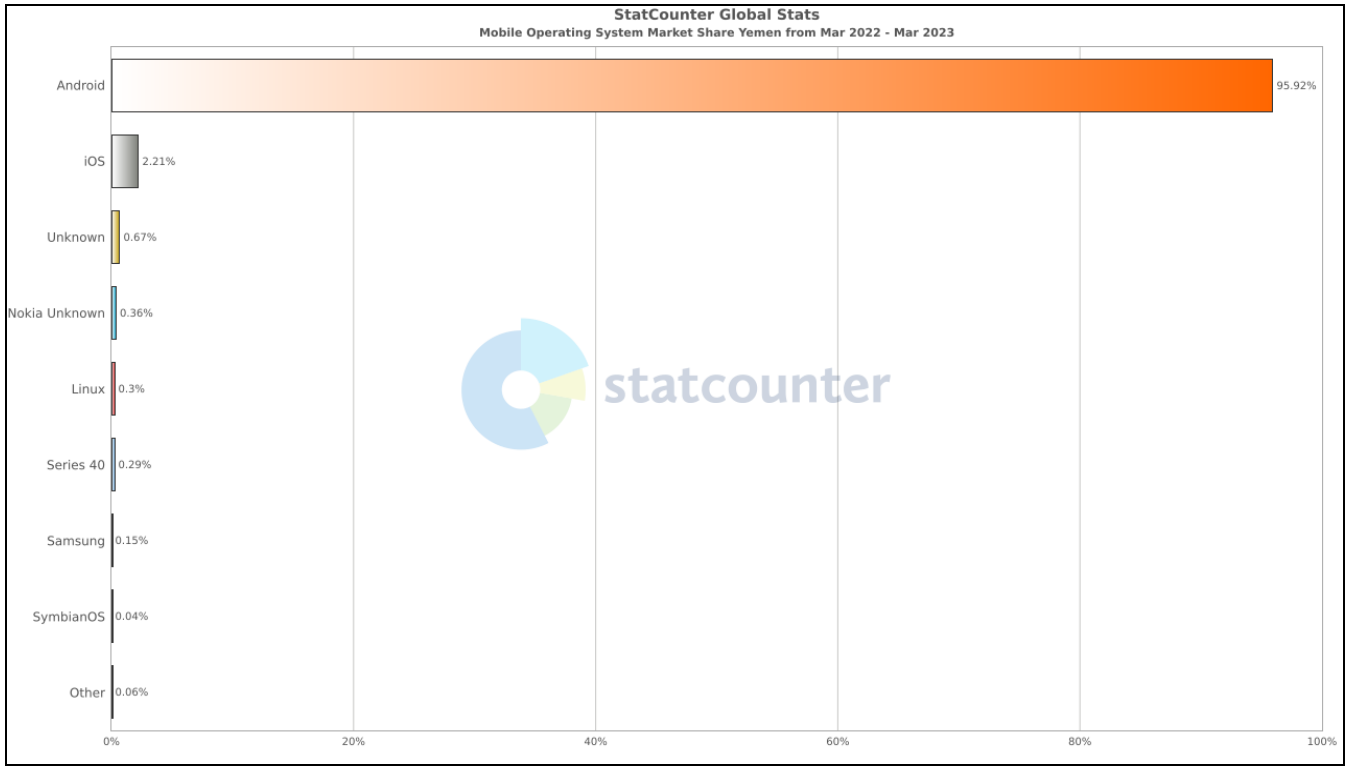


Figure 7: *Market share of Android devices in Yemen (Source: Statcounter)*

Submission Locations

Of the known Android samples linked to OilAlpha threat activity that were submitted to a popular malware repository, from April 2021 onwards we observed the first known sample, "WhatsApp.apk", noted in **Table 1**, being uploaded from Yemen. Other samples were uploaded from countries in the Arabian Peninsula, as well as North America and Turkey. While such information may only be an indicator of threat actor testing, this kind of geolocational information can help with comprehensive analysis, particularly with attribution and victimology.

Desktop Trojan Samples

Some of the DDNS domains associated with OilAlpha revealed that commodity trojans like njRAT communicated with attacker infrastructure throughout their operational lifespan. This trend was observed with C2 domains throughout 2021, and in early 2022. The identified files (**Table 3**) are generic

unlike the naming conventions of the Android applications discussed in this report. Insikt Group has not identified information to suggest that the files were used in an attack campaign.

File Name	SHA256 Hash	C2
yon.exe	0688dbd736e5a0e53024ee30cd2bcf205fcabc8d2a9800455572b1babe028fa2	ndf236fgh4367h.ddns[.]net
stupdate.exe	53e21aac7bf47d81342291d954d7a9cf51b446989b769cb6df3b187f8811f177	ndf236fgh4367h.ddns[.]net
New Client.exe	8cc2614d17b30355dc32a6466f80b64a72353c5c4aa5da8d0efe7c8d4b008fe7	ndf236fgh4367h.ddns[.]net
gi.exe	ca94223b97d9bb8049d24c506455bdaa4f853a68767885a6fecef362c01d2869	6386hgdsjg8172.ddns[.]net

***Table 3**: njRAT samples communicating with OilAlpha domains (Source: Recorded Future)*

Infrastructure Observations

Passive DNS analysis of OilAlpha infrastructure revealed that a C2 domain is typically associated with an IP address for approximately for 24 to 48 hours and is then rotated to another within the PTC autonomous system, AS30873; a sample listing of IP addresses seen in April 2023 associated with the mylab123321hm.ddns[.]net OilAlpha domain is available in **Table 4**.

IP Addresses	First Seen - Last Seen
134.35.6[.]69	April 9, 2023 - April 10, 2023
134.35.11[.]48	April 8, 2023 - April 9, 2023
134.35.14[.]204	April 8, 2023 - April 8, 2023
134.35.2[.]254	April 7, 2023 - April 8, 2023
134.35.6[.]170	April 6, 2023 - April 7, 2023

***Table 4**: Summary of mylab123321hm.ddn[.]net associated IP addresses (Source: Recorded Future Surface Browser)*

The threat activity has predominantly transpired over 3 CIDR ranges, all owned by the Yemeni PTC entity: 134.35.0.0/16 , 109.200.160.0/19 , and 175.110.0.0/18 . Additionally, OilAlpha C2 domains have increasingly been hosted on infrastructure associated with the IELO-LIAZO autonomous system, specifically on CIDR range 91.109.176.0/20 . While there is insufficient information to determine whether OilAlpha is shifting to the French-based infrastructure provider for operational security, or other reasons, reporting has revealed its popularity among Middle Eastern threat actors.

Geopolitical Influences

Who Controls The Telecommunications Sector in Yemen

In April 2022 a Human Rights Watch (HRW) report highlighted a case in which Saudi-backed Coalition airstrikes targeted a PTC facility in the Yemeni city of Hodeidah, which was reportedly occupied by Houthi (Ansar Allah) authorities. Public reporting (1, 2) also indicates that the telecommunications sector, in particular the administration of PTC and other government-owned telecommunication entities like TeleYemen, is controlled by Houthi authorities. Insikt Group research from November 2018 also revealed information about the power dynamics between the Houthis, the former government of Abd Rabbuh Mansur Hadi, and efforts to control the telecommunication sector in Yemen. This is notable as control of Yemen's telecommunication and infrastructure assets influence our attribution hypothesis discussed in the **Attribution** section.

The Iran-Saudi Deal, the UAE, and the link to OilAlpha

In March 2023, Iran and Saudi Arabia embarked on a new diplomatic rapprochement following negotiations mediated by China. This geostrategic development is likely to reduce tensions between Iran and Saudi Arabia, in addition to other Arabian Peninsula states, with renewed hope for reducing the conflict in Yemen. The dialogue reportedly led to Iran agreeing to cease its lethal aid support to the Houthis, and an Omani initiative is driving toward a permanent ceasefire between Saudi Arabia and the Houthi movement.

While the Houthis claimed they would not abandon their cause and asserted the new Iran-Saudi breakthrough would have little to no influence on their conflict against the Saudi-led coalition, Saudi Arabia and its partners held an official prisoner swap with the Houthis in mid-April, a potential sign of further de-escalation between the warring parties. Public analysis of the conflict suggests that a truce may be reached between the Houthis and Saudi Arabia; however, the potential for domestic conflict between the Houthis, the Southern Movement, and the internationally recognized government's forces is still elevated.

Other geopolitical influences have materialized in Yemen since the Houthi movement's takeover of Sana'a in 2014, and the Houthis have been engaged in conflict with and Saudi Arabia and its coalition partners since March 2015. Yemen deteriorated into a complex and fragmented state, with multiple internal and external parties pursuing their own security interests. For example, while the UAE is a partner in the Saudi Arabian coalition against the Houthis, it also supports its own political and military allies in the Southern Movement, including the Security Belt Forces. As depicted above, OilAlpha used documents depicting Security Belt Forces comuniques during its social engineering operations (**Figure 1**).

At least 3 major domestic political currents can affect Yemen's future: the Houthis (backed by Iran), the internationally recognized government (backed by Saudi Arabia), and the Southern Movement (backed by the UAE). OilAlpha's operations so far have depicted a clear attempt to spoof Saudi Arabian

organizations, as well as one from the UAE and another from Norway. The latter, the Norwegian Refugee Council, is the outlier, which raises the questions of why a threat group would spoof NGOs or target NGO-associated individuals in Yemen. Public sources suggest Houthi militia groups have abducted NGO workers and security. Houthi hardliners are wary of NGOs, which are viewed as tools of "Western influence" to enable foreign infiltration and espionage.

Attribution: OilAlpha For Whose Interests?

Insikt Group assesses that OilAlpha launched its attacks at the behest of a sponsoring entity, namely Yemen's Houthis. OilAlpha could be directly affiliated to its sponsoring entity, or could also be operating like a contracting party. Public reports have indicated that Houthi operatives have received training and cooperated in warfighting in operational theaters with Lebanese Hezbollah and Iran's Islamic Revolutionary Guard Corps' Quds Force (IRGC-QF). Under the banner of the "Axis of Resistance", the IRGC has helped Lebanese Hezbollah establish its own cyber capabilities, which Hezbollah has exported to aid Iraqi counterparts with cyber-enabled information operations capabilities. While OilAlpha's activity is pro-Houthi, there is insufficient evidence to suggest that Yemeni operatives are responsible for this threat activity. External threat actors like Lebanese or Iraqi Hezbollah, or even Iranian operators supporting the IRGC, may have led this threat activity.

The infrastructure used throughout OilAlpha's campaigns suggests it persistently uses Yemen's PTC assets. We recognize the potential for the PTC's infrastructure to be compromised by a foreign party. At the time of this writing, however, we have not identified information to support this hypothesis. Public reports ascertain that the PTC is under the control of Houthi authorities, and we take this information at face value.

Insikt Group has identified no evidence of activity such as spoofing Houthi communiques, or malicious APKs claiming to be, for example, a Houthi military app. While these may exist, they are not known to Insikt Group. The lack of spoofing against the Houthis is notable and moreover, reporting of Houthi distrust toward NGOs leads us to believe that such a factor likely acted as a driver for OilAlpha's operations.

The victimology (1, 2, 3) indicates that OilAlpha targeted victims in the media and journalism sectors, and also likely targeted delegates at a Saudi Arabian conference. Based on their social engineering attempts, which were written in fluent Arabic and did not include grammatical or idiomatic mistakes, the attackers are highly likely to be native Arabic-language speakers.

A WhatsApp account (**Figure 1**) adopted imagery of the current king of Saudi Arabia, Salman bin Abdulaziz Al Saud, as well as the crown prince, Mohammed bin Salman Al Saud, which was highly likely used to appear pro-Saudi to the target. If the targets represented Yemen's internationally recognized government, such profiles would likely serve to lower suspicions to enable the download of the malicious Android application.

Lastly, since May 2022, Insikt Group research revealed the continued spoofing of Saudi Arabian and UAE entities, and NGOs (**Table 5**). There is significant strategic and operational interest by the Houthis to target individuals from Saudi Arabia or representatives from Yemen's internationally recognized government. As noted above, specific counterintelligence elements within the Houthi movement could have also influenced OilAlpha's targeting requirements.

Other Attribution Considerations

An attribution hypothesis developed by a China-based security vendor suggests that a threat cluster linked to OilAlpha is associated with an intelligence ministry from a neighboring state in the Arabian Peninsula. No additional information was provided to ascertain how this assessment was made.

If the assessment is correct, OilAlpha's operators spoofed Saudi Arabian organizations and used Saudi Arabian telephone numbers to target victims with social engineering attempts while obfuscating their origins by using Yemeni infrastructure. This is an unlikely scenario, however, as it would defeat the purpose of creating a false flag by obfuscating attacker-controlled infrastructure, only to then use Saudi Arabian phone numbers and pro-Saudi Arabian WhatsApp accounts to disseminate the aforementioned applications.

Organization Name	Sector	Country of Origin
United Nations Children's Emergency Fund (UNICEF)	Humanitarian	International
King Khalid Foundation	Government/ Humanitarian	Saudi Arabia
King Salman Humanitarian Aid & Relief Centre	Government/ Humanitarian	Saudi Arabia
Emirates Red Crescent	Government/ Humanitarian	United Arab Emirates
Saudi Tourism Development Fund	Government/ Tourism	Saudi Arabia
Project MASAM	NGO	Saudi Arabia
Norwegian Refugee Council	NGO	Norway
National Commercial Bank (Saudi National Bank)	Finance	Saudi Arabia

***Table 5**: Entities spoofed based on APK file names or identified application icons (Source: Recorded Future)*

Mitigations

- Establish robust policies and carry out social engineering and anti-phishing awareness exercises to help detect and prevent attacks.
- Use strong passwords and enable multi-factor authentication (MFA) where possible to limit the potential damage of credential theft.
- "Cold-calling" is a common method social engineering operators use to engage with victims. This includes direct messaging on social media platforms as well as on encrypted chats. Be on the lookout for signs of inauthentic or reused material and attempt to directly verify with the source when possible.

Outlook

We do not foresee a reduction in attack operations led by OilAlpha. The group has continued to use the same TTPs with minor tradecraft shifts, such as the adoption of infrastructure associated with the IELO-LIAZO autonomous system throughout late March and early April 2023. The use of DDNS infrastructure and Android-specific malware are the more pertinent aspects of OilAlpha's TTPs; as noted in this report, the increased popularity of Android devices throughout the Arabian Peninsula is highly likely to have factored in the threat actors' decision-making.

Barring the discovery of new information or broader geostrategic shifts, OilAlpha is likely to continue to use malicious Android-based applications to target entities that share an interest in Yemen's political and security developments and the humanitarian and NGO sectors that operate in Yemen.

Appendix A

DDNS Domains:
hilan77112.ddns[.]net
87524uyre.ddns[.]net
mylab123321hm.ddns[.]net
musicmatrix.access[.]ly
magtimego.servegame[.]com
77112hilan.ddns[.]net
antahomaar2022.ddns[.]net
djhgurjhwdskh72532.ddns[.]me
ndf236fgh4367h.ddns[.]net
6386hgdsjg8172.ddns[.]net
akjdaks54678sdas.ddns[.]net
7687ytuyt78gfg.ddns[.]net
dhgrshghjrsg0092102.ddns[.]net
hsdg763276jgkjx.ddns[.]net
hm712175206zh.ddns[.]net
yemenofoneofline.ddns[.]net
712175206totot.ddns[.]net
fackyouman123456789.ddns[.]net
2020anekafkark2020.ddns[.]net
ncbyemen2008.ddns[.]net
you7788mtnq.ddns[.]net
saudigazette2022yemen.ddns[.]net
bobkkfoundationyemen2022.ddns[.]net
moonname2022.ddns[.]net
saaoff33993homhl.ddns[.]net
hsgdjh78632.mypsx[.]net
bobm1jgjahsg81.ddns[.]net
manyouhomaar21.ddns[.]net
hjsdg2368gskambv.ddns[.]net
gomnd2873yemnenrc.ddns[.]net
goman239.ddns[.]net
abas1.ddns[.]net

IPs:
134.35.217[.]64
134.35.1[.]116
134.35.2[.]7
134.35.11[.]130
109.200.165[.]170
134.35.11[.]141
134.35.0[.]119

134.35.15[.]220
134.35.130[.]126
134.35.11[.]92
134.35.10[.]61
134.35.2[.]3
134.35.10[.]166

Malware Hashes:
ad990791d595c149f6770d08be6411b88f9dab2ed56bf61fd274bea2327f17c3
fb6b8cdca2b35c5c0174e1e44b562f73194d9e0e79181fe4e312503b2ce801ec
b0653d049b3e0cadf4a198e3063b0025dd1fdaee70ac3a03b34c248a7dd89890
1f1cdd9acd9e581f538bdefc1ec5f0aebcc57cfccf5a4a9389f35c8741242e32
92420eb9356e103864ba5edcffe98d6a5ecfe13f7580035202dea1a32739b256
8bcc816a517ecdb72e6f97c53c4e40da8d96ebae239eb7f760c29bd943d1b722
B0c54756dd5c53d13be190952fe63c1b9e1989f8673ab549d19035207f01d901
8846b72ed2ecde60b805cfaf5d1f71e34742a18177ff3c4d8d5b9c3f250e153d
2b7d2490bfc4eacd3e5870ae0de92fdb5c1f11a5e8fdc7c07773780c6db038d9
8d07dc0745e57aeb40905a7426fb6515930a1fc7898db0ee93fda55ba085461b
7e6ec9df5e2218b5ad4111059f799e1348c06f98cb0f0742f86aae1875c6fd13
Eb8edfd04c0d1e0b03f4629519800c8b043110dbe94a70406c60d5a009f723fe
105d0533e48a7cdda29111f20818958f2d07e7ea0d7d323e59739703e61186c2
f3f3764ee6a0e5b933e95040092e0b348f672aaab273cf8eaaeabca28be5da36
7d21d3dce90408ca530c5e2364495d4f0932cdd23d812e4714e3665c06bfc560
2c2393a061901e13b9fc038bb25ba666fbff25d304c6dec51bac10a46dbd1fe6
48e4533ff3e121fd5e3a514206d3bfdde621d800d319dc7d157041aba06b8399
2028ede216c0cbf803d2d2e07415d0dd44c9d495ed9a3c63ec6645a770ad5443
fbd8551a74d6a7674dcea72fc8eea717c8cb932a22a715360554a91490bdfd6f
41d76e2a672d2815f1dc1ca43f2a716dd4c3f51afad7da1718deadddd52ad5a1
7959471cc0e0e4d7799e2544cd5db455d6bc892e9c2cb680c8a09879a4177222

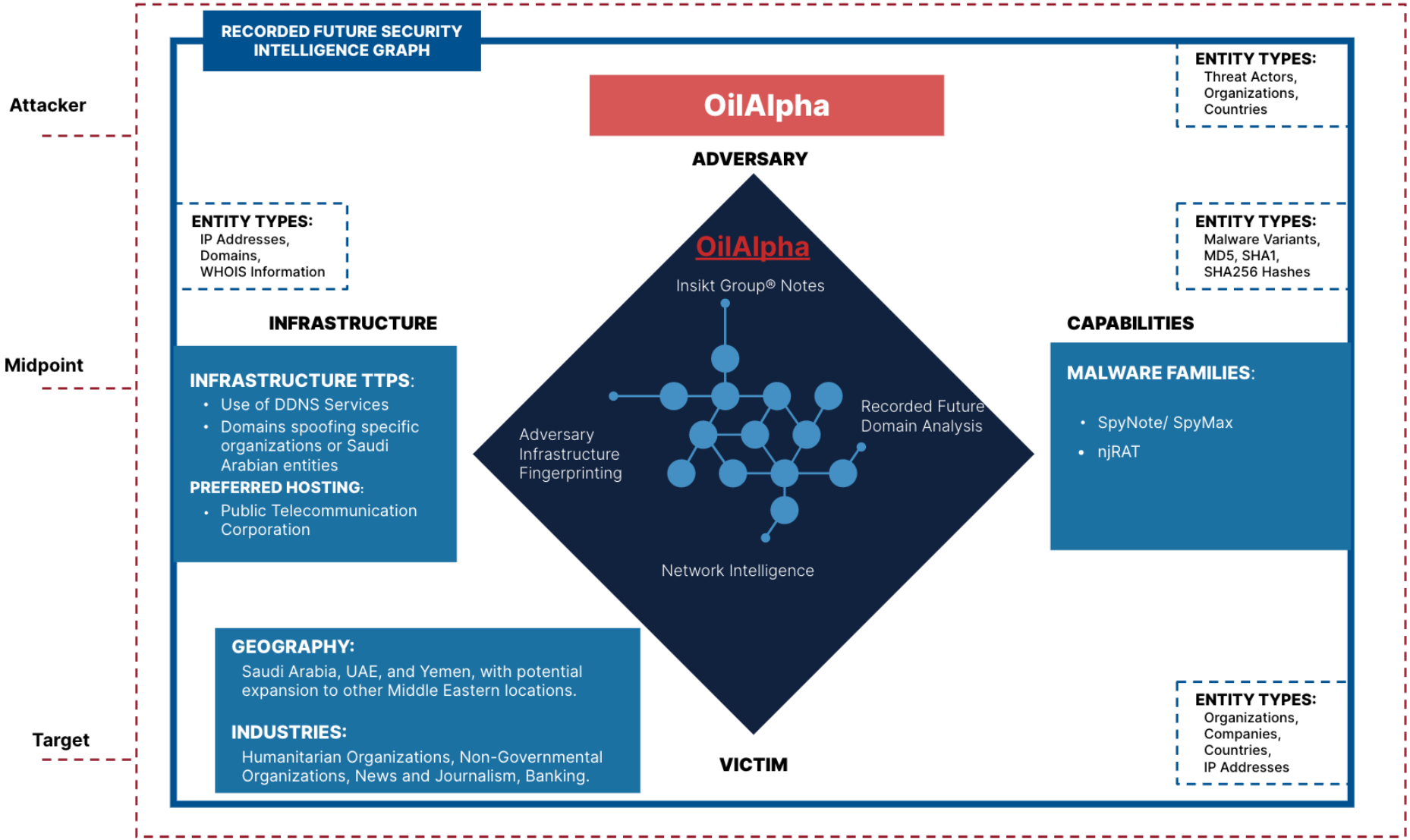
File Names:
unjobs.apk
unicef.apk
KSA-YEMEN.apk
NRC ES.apk
KSR HM.apk
WhatsApp.apk
gi.exe
yon.exe
stupdate.exe
New Client.exe
نقاط الاستلام.apk
خطة تنمية واعمار اليمن.apk
مساعدات مالية الهلال الأحمر الاماراتي.apk
تطبيق استلام ارقام الحوالات الماليه.apk
الخطة العامة المقترحة للدعم اليمن.apk

تواصل العمليات المشتركة.apk
اسماء المستفيدين من الحوالات النقدية لشهر فبراير.apk
صندوق التنميه والاستثمار.apk
استعلام واحصائيات المساعدات النقدية المقدة للنازحين.apk
برنامج الدعم للجمهوريه اليمنيه لشهر ابريل 2022.apk

Appendix B — Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Initial Access: Phishing	T1566
Execution, Persistence: Broadcast Receivers	T1402
Defense Evasion, Impact: Delete Device Data	T1447
Credential Access, Collection: Capture SMS Messages	T1412
Discovery, Collection: Location Tracking	T1430
Discovery: File and Directory Discovery	T1420
Discovery: System Network Connections Discovery	T1421
Discovery: System Network Configuration Discovery	T1422
Collection: Email Collection	T1114
Collection: Audio Capture	T1429
Collection: Access Call Log	T1433
Command and Control: Encrypted Channel	T1573
Command and Control: Ingress Tool Transfer	T1105

Appendix C — Diamond Model



Recorded Future®

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,600 businesses and government organizations across more than 70 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture