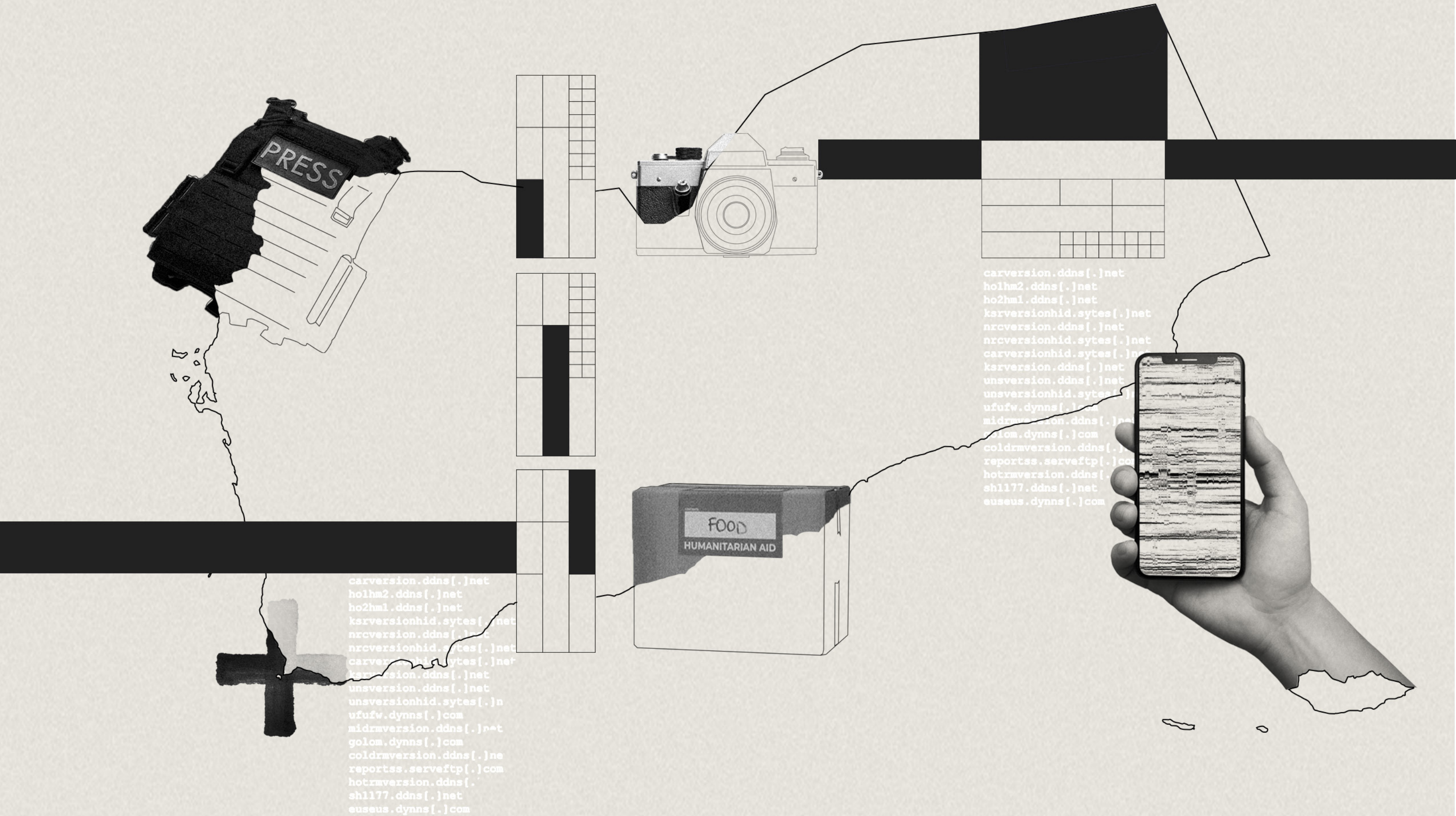
CYBER THREAT ANALYSIS

YEMEN

Recorded Future®

By Insikt Group®

July 9, 2024



OilAlpha Malicious Applications Target Humanitarian Aid Groups Operating in Yemen

One year after our first report, research indicates that OilAlpha is still highly likely focused on targeting humanitarian organizations operating in Yemen and potentially the broader Middle East.

A new cluster of malicious mobile applications and related infrastructure associated with OilAlpha has been uncovered and used to target at least three globally recognized humanitarian organizations.

Humanitarian and human rights organizations, NGOs, media and journalists, and government representatives operating in complex environments like Yemen face the threat of cyberattacks by OilAlpha.

Executive Summary

In May 2023, Insikt Group published its first report on likely pro-Houthi group OilAlpha depicting a campaign targeting humanitarian and human rights groups focused on development issues. At the time, we linked OilAlpha to a cluster of malicious Android applications and their supporting infrastructure, which were used to target humanitarian organizations with an operational mandate in Yemen.

Approximately a year after our report, we have identified a new cluster of malicious mobile applications and accompanying infrastructure almost certainly associated with the same threat group. The research indicates OilAlpha is still highly likely focused on targeting humanitarian organizations operating in Yemen and potentially the broader Middle East.

As of this writing, we have identified at least three globally recognized humanitarian organizations whose employees have likely been targeted by OilAlpha. These include CARE International, the Norwegian Refugee Council, and the Saudi Arabian King Salman Humanitarian Aid and Relief Centre. The latter two were already identified as targets in our research throughout 2023, while CARE International was uncovered during research for this report. Furthermore, we suspect malicious applications tied to OilAlpha also spoofed the United Nations or its World Food Programme.

Humanitarian and human rights organizations, other non-governmental organizations (NGOs), media and journalists, and government representatives operating in complex and challenging security environments like Yemen face the threat of cyberattacks by OilAlpha. OilAlpha's operations could provide logistical and targeting support to enable physical threats to humanitarian aid workers in Yemen and throughout the broader Middle East. Furthermore, as we have not identified a financial motive for this activity, we suspect OilAlpha's operations to be highly likely associated with pro-Houthi surveillance activity.

Key Findings

- The OilAlpha threat group is highly likely active and executing targeted activity against humanitarian and human rights organizations operating in Yemen, and potentially throughout the Middle East.
- OilAlpha infrastructure was highly likely used to conduct credential theft against human rights or humanitarian aid workers based in the Middle East. The threat group achieved this goal by establishing a fake web portal that spoofed a generic login capability.
- It is almost certain that the intended targets of the threat activity discussed in this report were Arabic-language speakers, which is indicative of the linguistic capabilities of the attackers.
- Social engineering and anti-phishing awareness exercises, coupled with using strong passwords and enabling multi-factor authentication (MFA), help detect and prevent attacks and the potential for compromise.

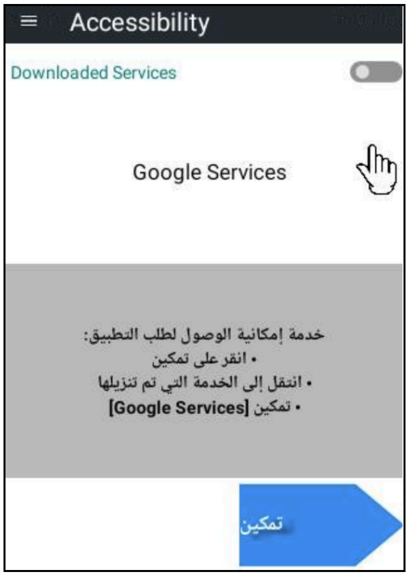
- There is little understanding about how OilAlpha executed the attacks discussed in this report. However, OilAlpha has been identified using encrypted chat messengers like WhatsApp to engage directly with its targets.
- OilAlpha threat actors are highly likely to continue targeted operations against humanitarian organizations throughout the Middle Eastern region.

Threat Analysis

Malicious Android Samples

In early June 2024, we identified an Android (`.apk`) file that was deemed suspicious based on our knowledge of OilAlpha threat activity and the name of the file — المساعدات النقديه.apk ("Cash Incentives.apk") [SHA256: `44cb9a9fe1ec9eb0ad20b2bbd6c4081d5c72f4bcad038077cecb4a1d13de46a6`]. A search for the Arabic term "المساعدات النقدية" in open-source databases yields results related to humanitarian cash-assistance programs. In fact, a quick glance at the top search result lists websites owned by the United Nations World Food Programme, the United Nations, and humanitarian aid groups like the International Federation of Red Cross and Red Crescent Societies (IFRC).

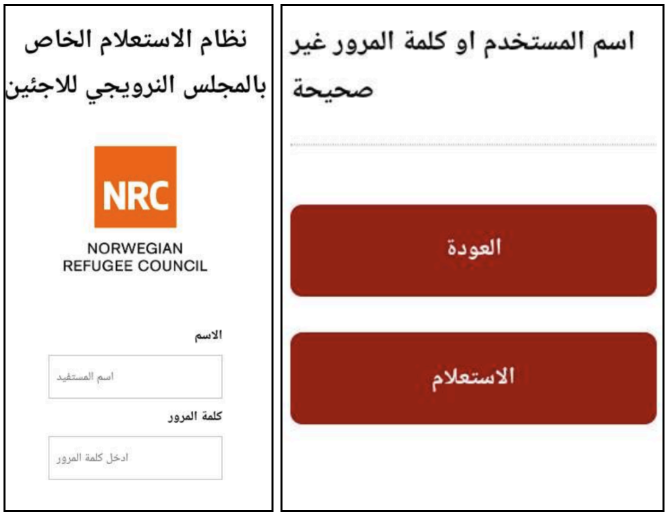
Using Recorded Future Malware Intelligence, we observed the malicious application attempting to contact a dynamic DNS (DDNS) domain — *ho1hm2.ddns[.]net* — on port 44414. At the time of analysis, the domain resolved to the IP address *206.189.98[.]34*. Our analysis suggested that the application makes excessive requests that are invasive of a user's privacy. This includes requesting access to a phone's camera, audio, SMS, contacts, internet, WiFi, external storage read and write permissions, and many other access permissions. The `.apk` file is listed by Recorded Future Malware Intelligence as a remote access trojan (RAT), which matches assessments by other public malware repositories. The sample is marked as SpyMax by some antivirus products. Both SpyMax and SpyNote are widely distributed RATs used by threat actors around the world, including OilAlpha.



خدمة إمكانية الوصول لطلب التطبيق:
• انقر على تمكين
• انتقل إلى الخدمة التي تم تنزيلها
• تمكين [Google Services]

Figure 1: *The fake Cash Incentives application requesting the user to enable "Google Services" during execution (Source: Recorded Future)*

We identified a second malicious sample named "NRC Business .apk" [SHA256: `bfc0226332978216a1a042c8422fb26073fca4d390c71502a5c505fab38ccb05`], which was reported to have also communicated with *ho1hm2.ddns[.]net*. Analysis of the sample revealed that throughout early 2024 the command-and-control (C2) server resolved to *141.255.145[.]221* and that the application was also configured to contact a second domain — *ho2hm1.ddns[.]net*. At the time, both domains were configured to communicate over port 44449. As depicted in **Figure 2,** this sample spoofs a login portal for the Norwegian Refugee Council (NRC).

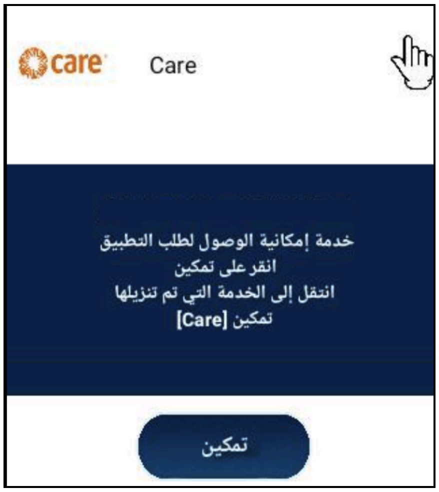


نظام الاستعلام الخاص بالمجلس النرويجي للاجئين

اسم المستخدم او كلمة المرور غير صحيحة

Figure 2: *The spoofed NRC application proved to be more interactive throughout the installation phase by enabling a registration process (Source: Recorded Future)*

The third sample [SHA256: 8f0bd17f682bdeb169ea0e1012c86a749a6bb466de3bed2feb2ee0e9ead1bcf9] we identified contacted another DDNS domain — *carversion.ddns[.]net* — according to our sandbox analysis. The third sample spoofed another humanitarian organization, CARE International. We observed throughout the installation process that the user was directed to input their username and password, just like the previous two malicious samples. If they failed, the application prompted the target to initiate a standard registration process. Much like the previous two examples, the application requests access to device permissions that are intrusive.



خدمة إمكانية الوصول لطلب التطبيق
انقر على تمكين
انتقل إلى الخدمة التي تم تنزيلها
تمكين [Care]

Figure 3: *The fake CARE International application follows similar installation procedures and contacts kssnew[.]online (Source: Recorded Future)*

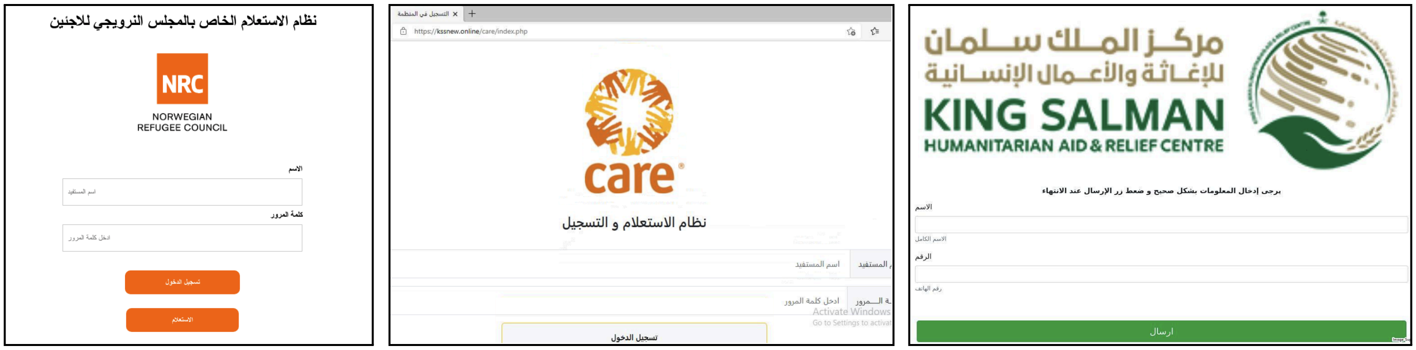
Credential Theft Portal

Analysis of the malicious `.apk` files led to the identification of a credential theft component that is hosted on the domain *kssnew[.]online*. The credential theft portal identified via submissions to urlscan.io and DomainTools was hosted on specific subdirectories entitled "`care`" and "`page`". We identified no additional subdirectories associated with victims.

```
kssnew[.]online/care/index.php
```

Figure 4: *URL path associated with the CARE International organization on kssnew[.]online (Source: Recorded Future)*

We also identified another spoofed portal associated with the King Salman Humanitarian Aid and Relief Centre (KSR) that was hosted on the landing page of *kssnew[.]online*. The spoofed login page was captured via DomainTools in February 2023, a month after the domain was registered (**Figure 5**).



نظام الاستعلام الخاص بالمجلس النرويجي للاجئين

نظام الاستعلام و التسجيل

يرجى إدخال المعلومات بشكل صحيح و ضغط زر الإرسال عند الانتهاء

Figure 5: *The fake NRC, CARE International, and KSR login portals hosted on the kssnew[.]online domain (Source: Recorded Future, urlscan.io, DomainTools)*

We observed the applications redirecting a target's internet browser on the infected mobile device to the credential theft page. This observation leads us to assess that the threat actors' likely goals are to initiate surveillance activity against the target and further their espionage efforts by accessing accounts associated with the affected organizations.

Mitigations

- Establish information security policies and carry out social engineering and anti-phishing awareness exercises to help detect and prevent attacks.
- To limit the potential damage of credential theft, use strong passwords and enable multi-factor authentication (MFA) where possible.
- "Cold-calling" is a common method social engineering operators use to engage with victims. This includes direct messaging on social media platforms and on encrypted chats. Be on the lookout for signs of inauthentic or reused material and attempt to directly verify with the source when possible.
- Recorded Future Third-Party Intelligence module users can identify activity involving OilAlpha — or the suspected targets of the group, including major organizations like the United Nations — in real time.
- Install the Recorded Future® Threat Intelligence Browser Extension to get instant access to threat intelligence from any web-based resource. This extension enables users to process alerts faster within their security information and event management (SIEM) process and to prioritize vulnerabilities for patching.
- When a suspicious file is identified, send it through the Recorded Future Malware Intelligence sandbox for detailed analysis. The sandbox environment will execute the file in a controlled setting, allowing for observation of its behavior, including network connections, system changes, and any attempts to contact GitHub repositories or other external services.

Outlook

Houthi militants have continually sought to restrict the movement and delivery of international humanitarian assistance and have profited from taxing and re-selling aid materials. One possible explanation for the observed cyber targeting is that it is intelligence-gathering to facilitate efforts to control who gets aid and how it is delivered. We also note the UN World Food Programme's decision to stop food distribution in Houthi-controlled regions, which will likely increase pressure on the group to control aid from other sources.

OilAlpha remains highly active throughout the Middle East. Despite increased attention since May 2023, the group remains focused on targeting humanitarian and human rights organizations active in Yemen. We anticipate this threat group will continue its operations against the aforementioned sectors, and we can't exclude the possibility that OilAlpha's remit is broader than the Yemeni cyber landscape.

Appendix A — Indicators of Compromise

Domains:
carversion.ddns[.]net
ho1hm2.ddns[.]net
ho2hm1.ddns[.]net
ksrversionhid.sytes[.]net
nrcversion.ddns[.]net
nrcversionhid.sytes[.]net
carversionhid.sytes[.]net
ksrversion.ddns[.]net
unsversion.ddns[.]net
unsversionhid.sytes[.]net
ufufw.dynns[.]com
midrmversion.ddns[.]net
golom.dynns[.]com
coldrmversion.ddns[.]net
reportss.serveftp[.]com
hotrmversion.ddns[.]net
sh1177.ddns[.]net
euseus.dynns[.]com

Credential Theft Domain:
kssnew[.]online

IP Addresses:
206.189.98[.]34
176.123.21[.]4
145.14.156[.]148
141.255.144[.]8
134.122.75[.]238
141.255.145[.]221

SHA256 Hash:
bfc0226332978216a1a042c8422fb26073fca4d390c71502a5c505fab38ccb05
8f0bd17f682bdeb169ea0e1012c86a749a6bb466de3bed2feb2ee0e9ead1bcf9
44cb9a9fe1ec9eb0ad20b2bbd6c4081d5c72f4bcad038077cecb4a1d13de46a6

File Name:
NRC Business .apk
المساعدات النقديه.apk(”Cash Incentives.apk“)

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com