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

recordedfuture.com/oilalpha-likely-pro-houthi-group-targeting-arabian-peninsula

Research (Insikt)

Posted: 16th May 2023

By: Insikt Group®

Since May 2022, Insikt Group has tracked an ongoing campaign by the threat group, OilAlpha,; which we are linking to threat actors that likely support a pro-Houthi movement agenda.

The group 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. 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). As of this writing, we suspect that the attackers targeted individuals the Houthis wanted direct access to.

وإعمار اليمن حسب بروتوكولات الامانه العامة
حيث وكما هو معلوم انه تم تخصيص مبلغ ٢٠٠
مليون دولار للجميع الهيئات الحكومية مع أفراد
وزارة الدفاع والامن للبداء في مشروع التنمية
وإعمار اليمن وسوف يتم تخصيص دعم مالي
للدوائر لهذا نرغب منكم الاطلاع على المشروع
عبر تطبيق الامانه العامة والنظر في سير توزيع
الميزانية المخصصة وطرح ملاحظاتكم في
البرنامج وسوف يتم الاتصال بكم خلال الأيام
القادمة للمعرفة سير عمل خطة التنمية
ونحن في انتظار ملاحظاتكم ومقترحاتكم لرفعها
قبل النشر .

ملاحظة : سيتم إرفاق إليكم ملف الخطة
والميزانية للإطلاع نرجو ابلغنا عند الاطلاع على
الملف

لجنة الدعم للجمهورية اليمنية
الأمانة العامة للمجلس التعاون الخليجي

٢:٢٤ م

APK برنامج الدعم للجمهوريه اليمنيه ل..

٧٨٧ كيلوبايت • APK ٢:٢٤ م

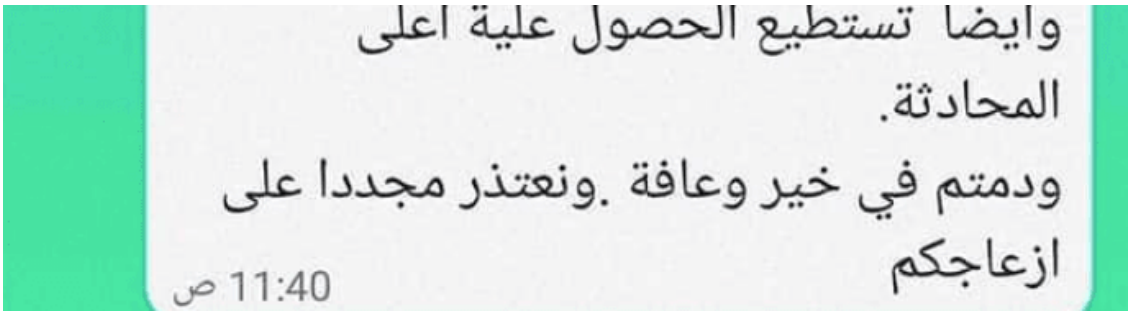
4:48 ص | 5.5ك.ب/ث 57

+966 59 022 6535

هيئة إدارية وسياسية تضم كل الدو..الخليج العربي"


إضافة
حظر
اليوم
الرسائل والمكالمات مشفرة تمامًا بين الطرفين، بحيث لا يستطيع أحد خارج هذه الدردشة، ولا حتى شركة واتساب نفسها، قراءتها أو الاستماع إليها. انقر هنا لمعرفة المزيد.
Hi محمد, how are you!
3:22 ص
YEMENOFKSA.apk
APK
815 كيلوبايت • APK
3:22 ص
+966 58 116 9165


ui Program for th...construction of Yemen
تستطيع الحصول على تطبيق "البرنامج
السعودي لتنمية واعمار اليمن من
" متجر ابلي او ابل ستور "او من خلال
الواتساب اسفل المحادثة
2:59 م
SDPRY signed.apk
APK
787 كيلوبايت • APK
2:59 م
18 مارس 2022
تطبيق البرنامج السعود...
APK
820 كيلوبايت • APK
11:40 ص
جمعتك مباركة ...
نعتذر عن وجود خلل فني بسيط في
التطبيق "السابق" حيث انه تم تعديله الان
تستطيع الحصول على التطبيق السليم من
خلال الرابط :
https://2u.pw/7Oxuw



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

OilAlpha has almost exclusively relied on infrastructure associated with the Public Telecommunication Corporation (PTC), a Yemeni government-owned enterprise reported to be under the direct control of the Houthi authorities. OilAlpha used encrypted chat messengers like WhatsApp to launch social engineering attacks against its targets. It has also used URL link shorteners. Per victimology assessment, it appears a majority of the targeted entities were Arabic-language speakers and operated Android devices.

OilAlpha threat actors are highly likely to be involved in espionage activity, as handheld devices were targeted with remote access tools (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.

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.

To read the entire analysis with endnotes, click here to download the report as a PDF.