Scamdemic outbreak

blog.group-ib.com/middle-east-scam

17.09.2021

Scammers attack users in Middle Eastern countries

Yakov Kravtsov

Head of Digital Risk Research team

Evgeny Egorov

Lead Digital Risk Protection analyst

Introduction

In spring 2021, Group-IB Digital Risk Protection (DRP) analysts identified a fraud scheme targeting users in Arabic-speaking countries. As part of their attacks, the threat actors abused more than **130** well-known brands worldwide from sectors such as telecommunications, retail, entertainment, and etc.

In total, Group-IB analysts discovered more than **4,300** fraudulent pages created on **Blogspot**, a popular blogging service. The webpages were all registered by a group that included more than 100 accounts.

The scammers used a tried-and-tested scheme involving giveaways supposedly by popular brands, lottery games purporting to be recommended by celebrities, and fake job offers from the government. The threat actors used such lures to steal personal data or attract traffic to other fraudulent websites. More than **500,000** people per month visit the end websites involved in the scheme.

How the scheme works

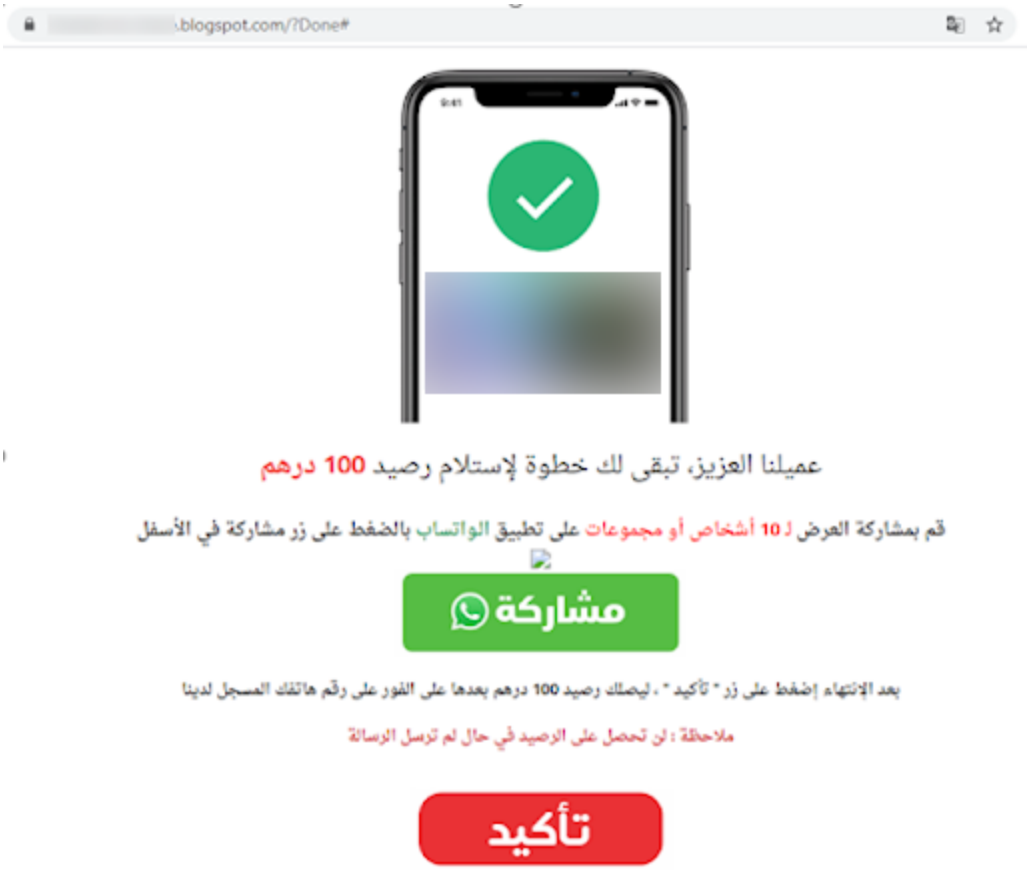
Users fall victim to the schemes by agreeing to take part in a promotion supposedly organized by a famous brand, a government organization, or a celebrity. Victims are promised they could win a prize or money, play the "wheel of fortune", or get a job by completing a survey.

A WhatsApp message with links to fraudulent blogs

Victims may be asked to enter their full names, phone numbers, places of residence, education details, and desired place of work.

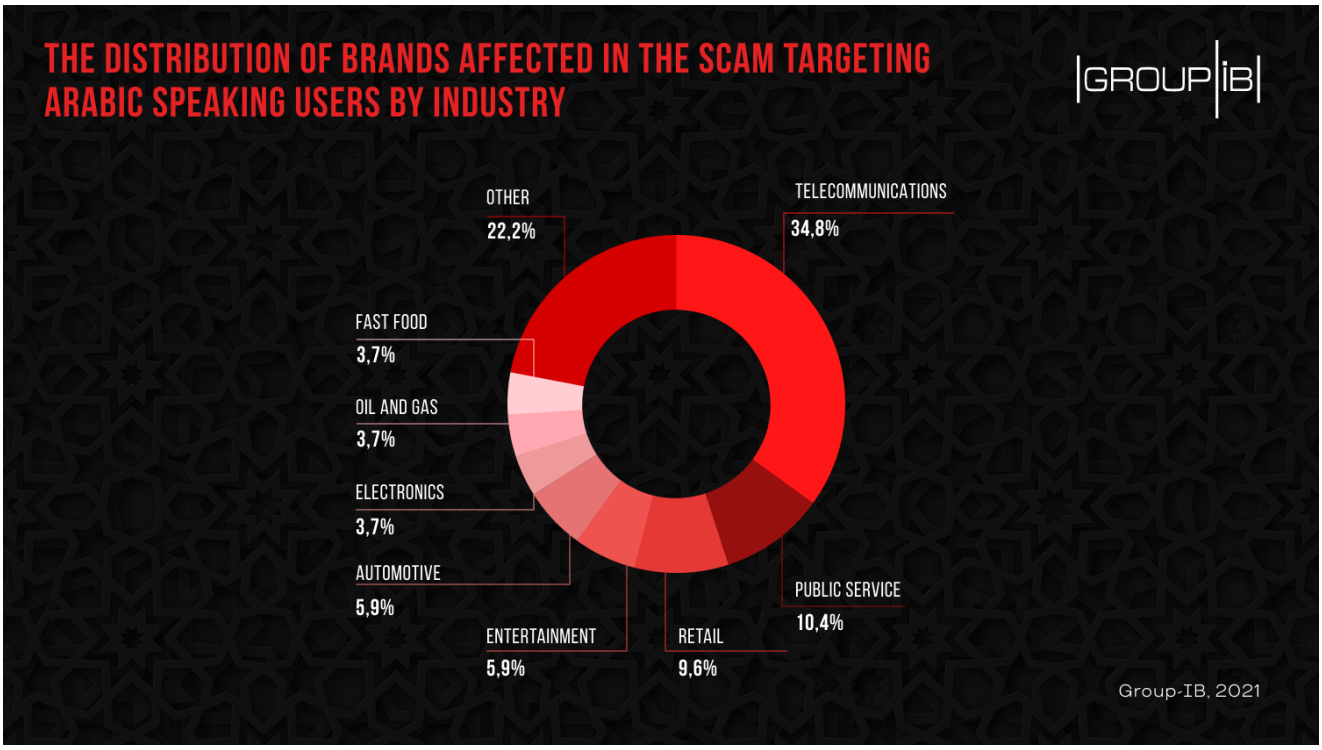
Regardless of the answers or where the wheel of fortune stops, victims become "winners." After completing the survey or playing the wheel of fortune, victims are asked to share the link to the website or a similar one with a lottery game with 5-20 WhatsApp contacts. The scammers do so to widen the pool of their potential victims.

After the victim sends the required number of messages, they are redirected to another fraudulent resource: other lottery games, scam dating websites, and websites with fake browser extension installations. In the worst-case scenario, victims may end up on a malicious or phishing website.



Fraudulent Blogspot page where the victim is asked to share the lottery game with their WhatsApp contacts

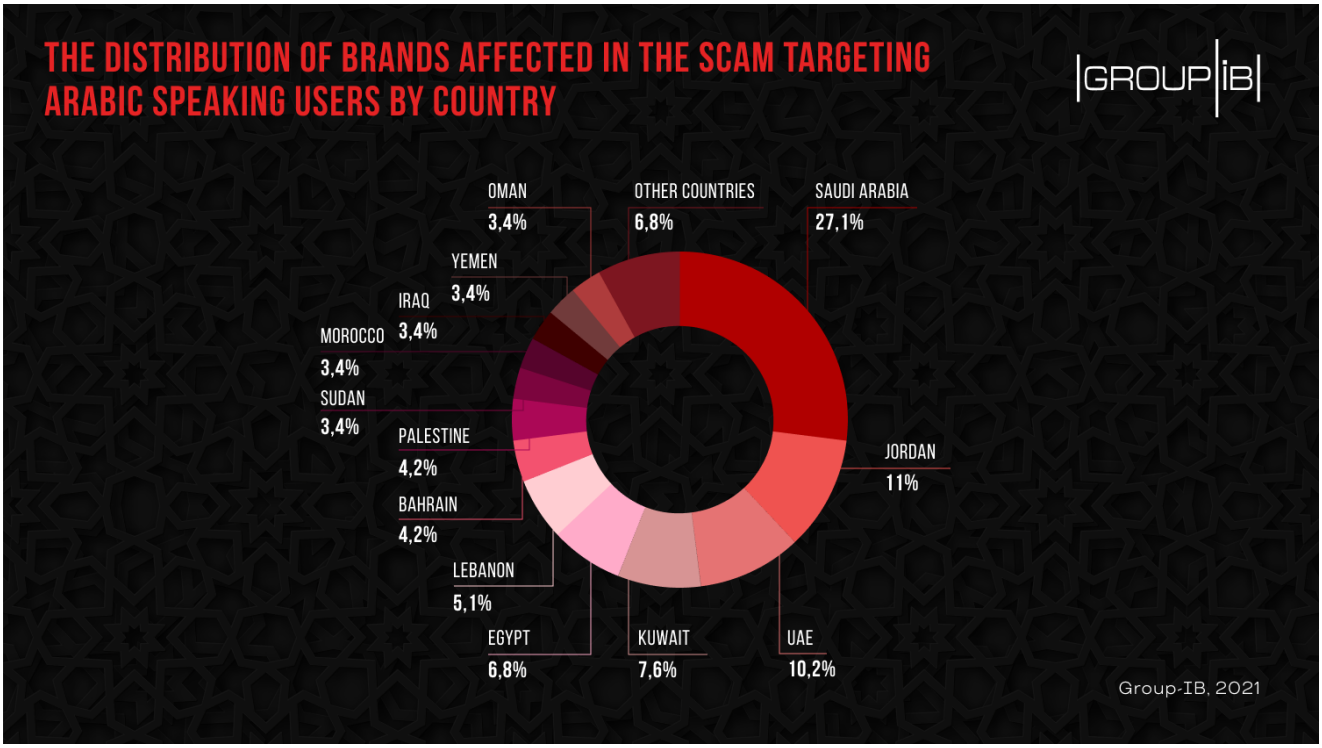
Telecommunications companies have been the main target for threat actors. Fraudsters have abused at least **47** telecom brands as part of their scheme. In addition to the telecommunications sector, brands in the retail, entertainment and automotive sectors have been affected.



Affected industries

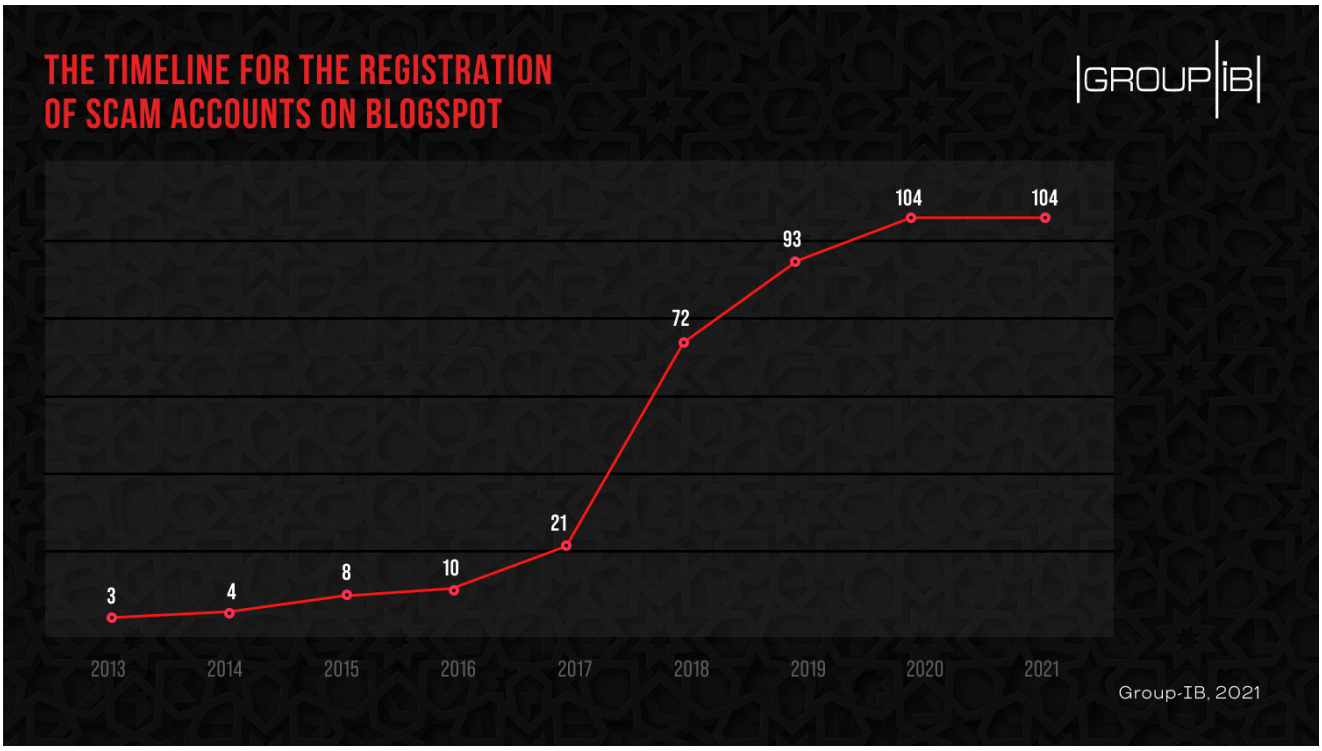
In addition to company brands, scammers abused personal brands of public figures, especially the Saudi royal family.

The fraudulent campaign targeted 16 Arabic-speaking countries: **Saudi Arabia**, **Kuwait**, **Jordan**, **Sudan**, **Morocco**, **Egypt**, **Bahrain**, **Iraq**, **Yemen**, **Palestine**, **the United Arab Emirates (UAE)**, **Algeria**, **Lebanon**, **Qatar**, **Syria**, and **Oman**. The attack also targeted English-speaking users from Turkey and Nigeria.



The fraudsters did not always use popular brands or celebrities on their websites. Group-IB DRP specialists also discovered fake dating websites and fake lottery games.

To lure users to scam websites, the fraudsters sent bulk WhatsApp messages and used pop-up windows and Google Ads. The first Blogspot account related to the fraudster group was registered in August 2013. Account registrations peaked in 2018 and the threat actors continued creating new accounts in 2019 and 2020. To this day, on some of the accounts the fraudsters continue to create fraudulent pages that abuse many brands.



How the threat group operates

Using Blogspot service as part of their schemes is typical for the threat group in question.

منصة التوظيف الإلكتروني

تم قبول توظيفك
سيتم التواصل معك
لتحديد موعد إستلام الوظيفة

تبقى خطوة للحصول على وظيفتك

أخي المواطن / أختي المواطنة

قال تعالى (وتعاونوا على البر والتقوى)

نرجو تكرما التعاون مع الباحثين
والعاطلين بنشرك اعلان التوظيف
للقروبات والحسابات لتعم الفائدة.

قم بمشاركة الرسالة لـ 10 أشخاص أو مجموعات على تطبيق الواتساب بالضغط على زر مشاركة في الأسفل

مشاركة

عند الإنتهاء إضغط على " تأكيد " ستصلك رسالة على جوالك بكافة معلومات الوظيفة وموعد المقابلة

تأكيد

ملاحظة : سيتم التواصل معك خلال 24 ساعة من موعد التقديم

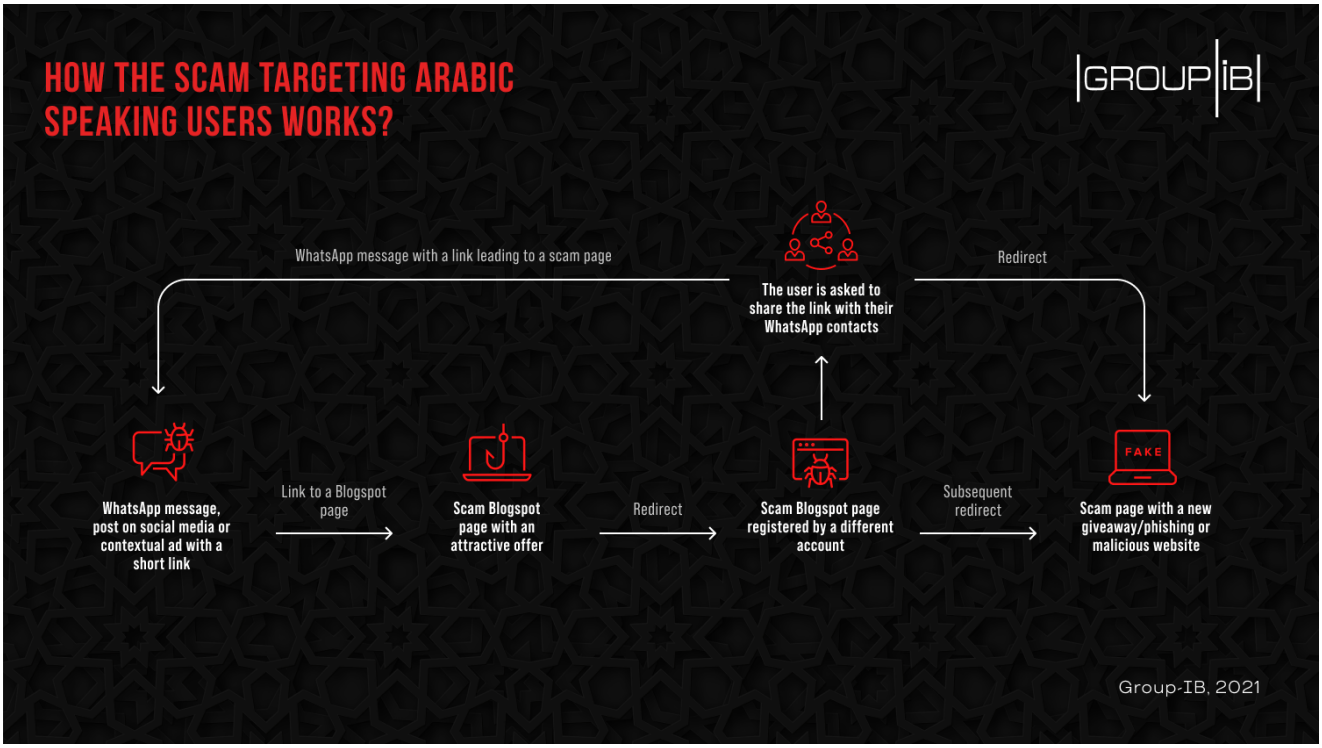
تعليقات الحاصلين على وظائف

Fraudulent Blogspot page where victims are asked to share a link to the survey with their WhatsApp contacts

In addition to registering fake pages that mimic the websites of well-known brands, the scammers use Blogspot as a data storage space or a content delivery network (**CDN**) to store media content and webpage code. In some cases, such data is uploaded to individual domains, which allows the fraudsters to save on hosting services.

The scammers can also use Blogspot as a link shortening service and redirect users to fraudulent domains. Search engines consider such links safe and do not show any warnings about the website being potentially dangerous.

It is difficult to detect the page from which visitors are redirected, especially when it comes to regular users, because the redirection is instant and users simply do not notice that they have been redirected.

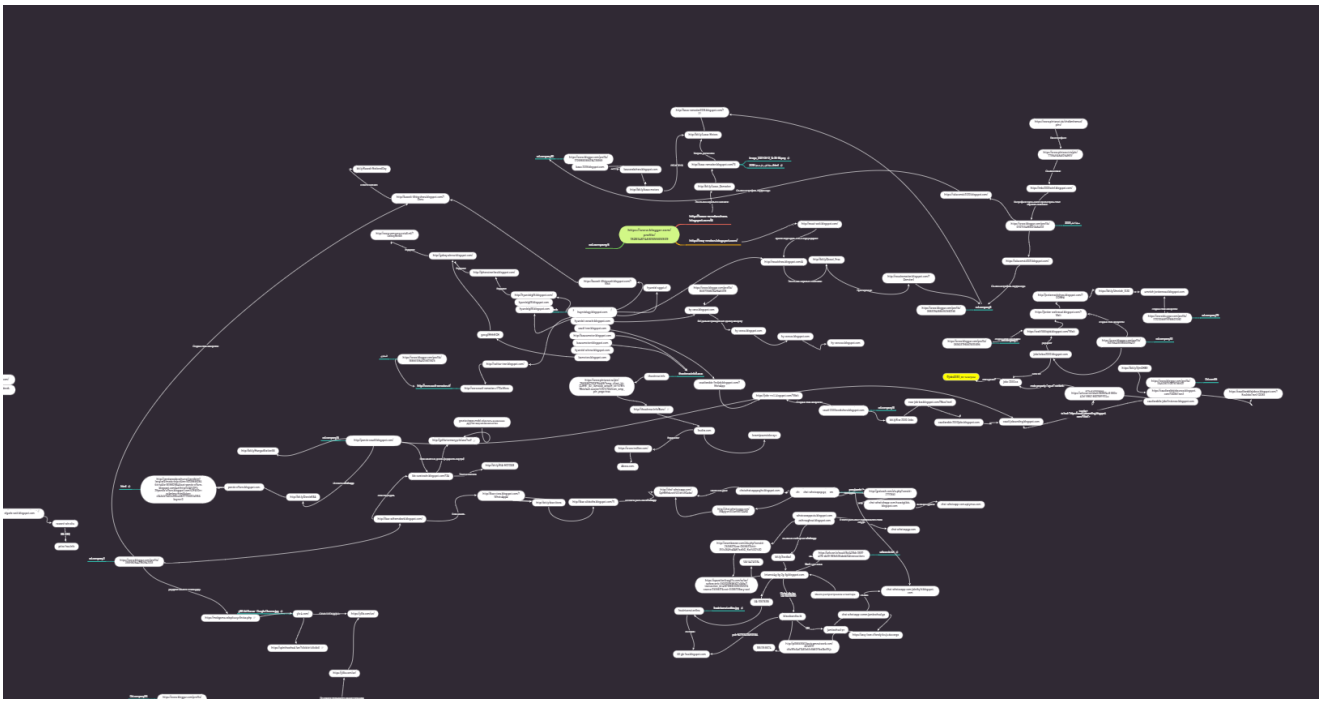


How fraudulent Blogspot pages work

Attack attribution

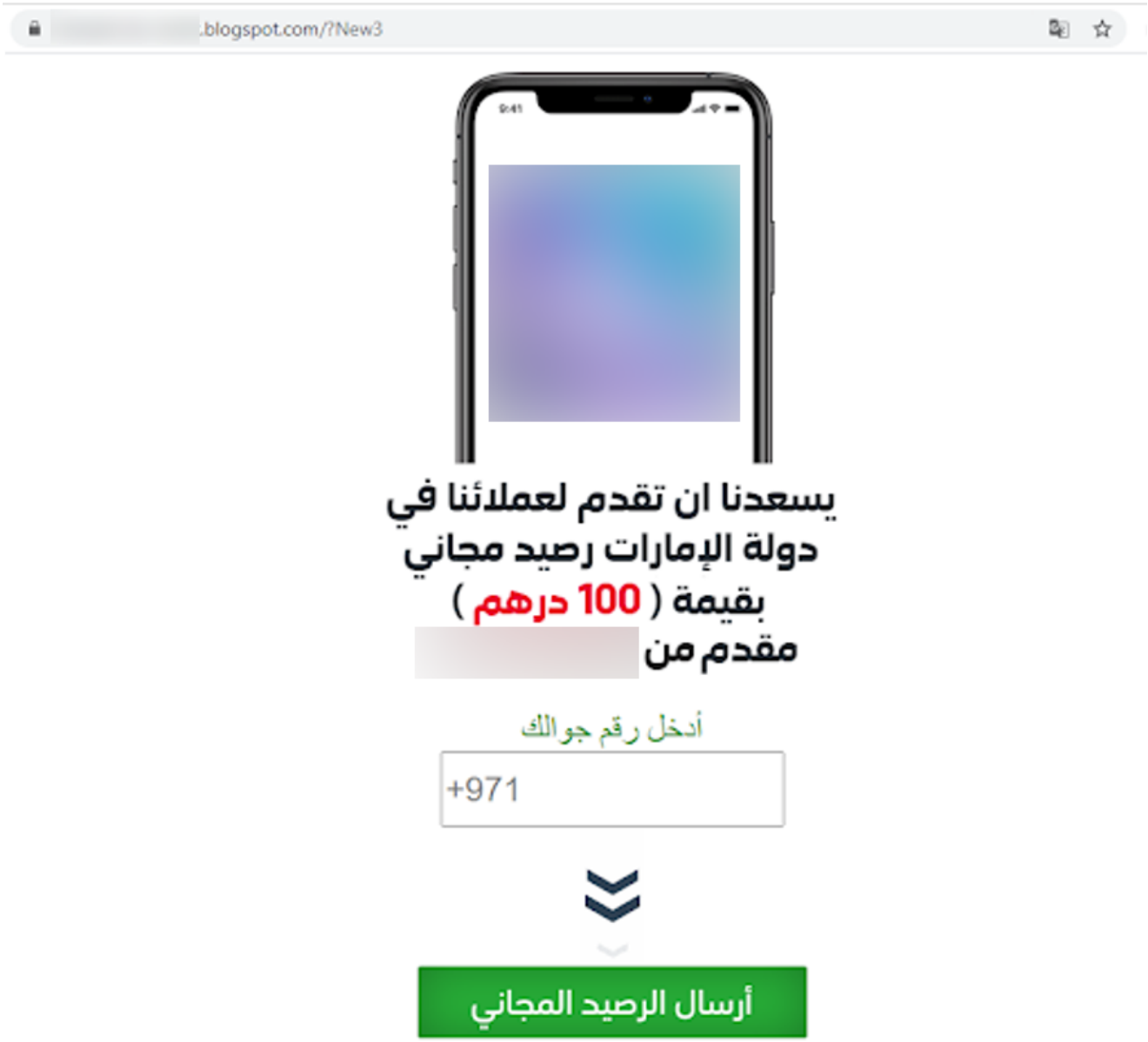
Finding links between elements of the fraudster group's infrastructure is relatively easy. In addition to identical names (**51.9%** of the profiles had "**od.company**" in their names), the registered accounts interlink each other and use the same servers, groups of domains, and links for sharing on WhatsApp. All the above factors mean that it is highly likely that the profiles belong to a single threat group.

The diagram below shows a high-level example of grouping these accounts by traffic source, Google statistics, and connections between domains.



The threat group uses more than **100** accounts, and that number keeps growing. For instance, over the first six months of this year, we have observed a 54% surge in the number of pages on these accounts. The earliest accounts related to the threat group were registered in 2013, which is surprising because fraudulent pages are usually active for no longer than a few months. Yet this group has been operating for at least six years.

In addition to Blogspot, the threat group uses many other tools, including social media ads and mass messaging in messaging apps.



How to avoid falling victim to fraud

1. Be cautious while following links that allegedly lead to the website of a specific company, a celebrity or a state agency and trust links from the official resources only — verified accounts on social media or messengers.
2. Enter confidential data and bank card details on trusted websites only.
3. When visiting links relating to offers by companies shared in messaging apps or on social media, check the domain names. Fraudsters usually use domain names that sound similar to brand names.
4. Verify the information about promotions and giveaways on the official accounts of brands, state agencies or celebrities.

Recommendation for rightsholders

1. Monitor and analyze complaints of the company's customers who fell victim to scammers.
2. Monitor online resources to promptly detect the illegal use of the company's name or trademark.
3. To prevent the illegal use of your intellectual property assets, use Digital Risk Protection (DRP) solutions that help promptly detect threats to a specific brand in the online space and then send them for blockage.