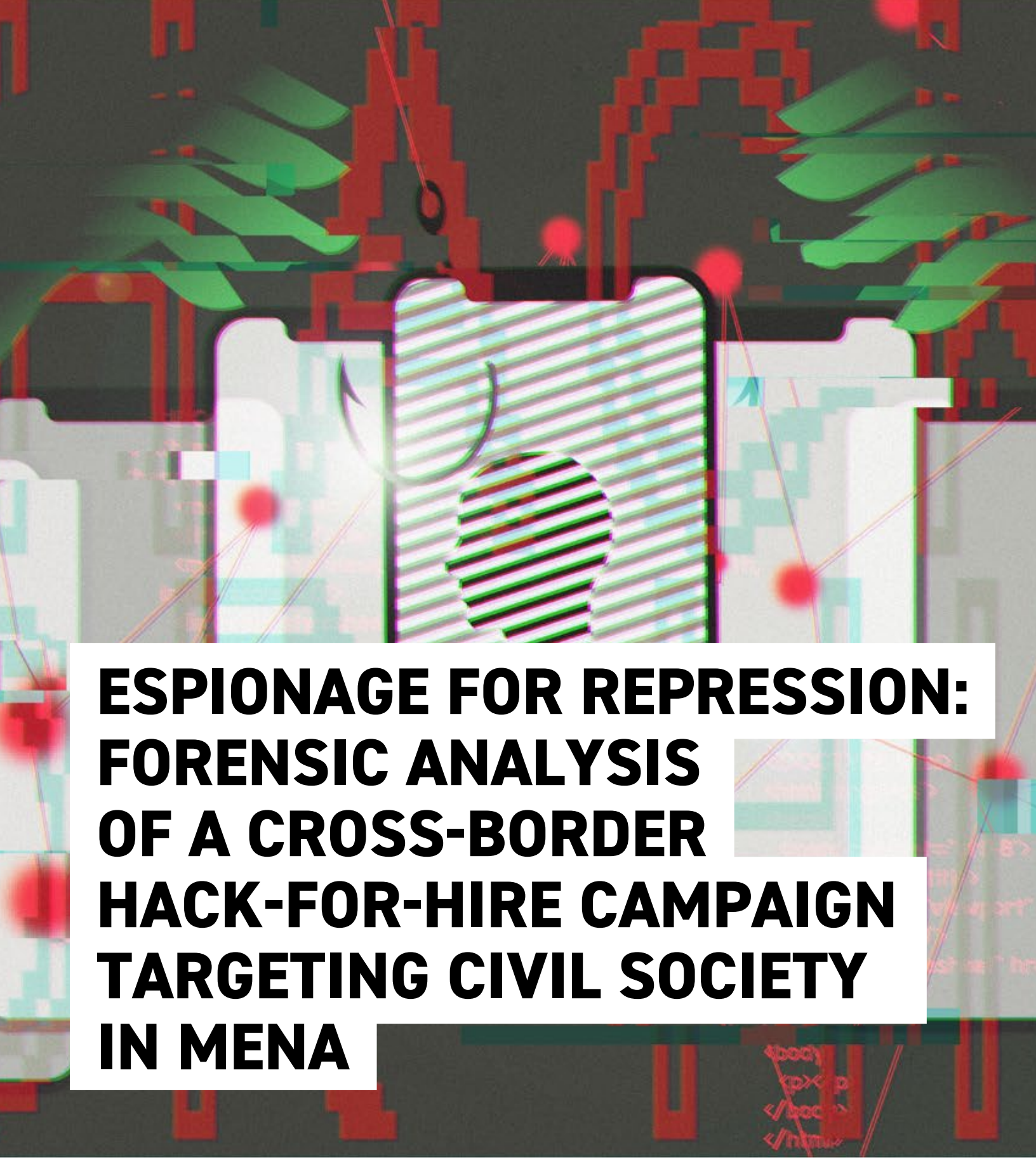

ESPIONAGE FOR REPRESSION: FORENSIC ANALYSIS OF A CROSS-BORDER HACK-FOR-HIRE CAMPAIGN TARGETING CIVIL SOCIETY IN MENA

accessnow

Access Now defends and extends the digital rights of people and communities at risk. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

ESPIONAGE FOR REPRESSION: FORENSIC ANALYSIS OF A CROSS-BORDER HACK-FOR-HIRE CAMPAIGN TARGETING CIVIL SOCIETY IN MENA

This is an Access Now publication, prepared by the **Digital Security Helpline** team. We would like to thank all colleagues and partners who provided support for this report.

For more information, please visit:
https://www.accessnow.org

Contact:
Hassen Selmi | Incident Response Lead
hassen@accessnow.org

Marilou Maala | Incident Response Analyst
marilou@accessnow.org

Jassem B. | Incident Response Analyst
jassem@accessnow.org

April 2026

Introduction

In this report, Access Now's Digital Security Helpline ("the Helpline") outlines our investigation into spear-phishing cases targeting Egyptian members of civil society in 2023 and 2024: Mostafa Al-A'sar, an independent journalist, and Ahmed Eltantawy, an independent journalist and editor who became a political opposition leader. We also collaborated with SMEX, the West Asia and North Africa (WANA) digital rights nonprofit, in their analysis of a similar attack against a Lebanese journalist, which took place in 2025.

The investigation led to the discovery of larger malicious infrastructure and activity of a likely Advanced Persistent Threat (APT); that is, a threat actor that is sophisticated, persistent, and well-resourced. This report characterizes the infrastructure used for the spear-phishing attacks; we find overlapping domains, hosting infrastructure, and code similarities across the attacks analyzed. It also reveals the wide range of tools used by the suspected APT, from basic harvesting pages to a sophisticated spyware delivery ecosystem capable of exfiltrating sensitive data from compromised Android devices.

The Helpline collaborated with the mobile security company Lookout on the technical analysis. Based on their review of the two phishing cases against Egyptian members of civil society investigated by the Helpline, Lookout independently assesses that the campaigns against these two individuals may be linked to a hack-for-hire threat group with ties to Asia. Based on the common patterns and infrastructure used in the attacks, Access Now believes that the case investigated by SMEX could be related to the same threat actor. While we have collaborated during the investigation, any assertions and representations, errors, or omissions in this report are our own.

The report aims to provide civil society with actionable intelligence to prevent and mitigate similar attacks. We also recommend exercising preventative measures, shared at the end of this document, as a necessary step for those at risk to reinforce their digital security.

Key findings

- A hack-for-hire group targeted several members of civil society in the Middle East and North Africa (MENA) region, through spear-phishing campaigns in 2023 and 2024, aimed at compromising their online accounts (Apple, Microsoft, and Google).
- The victims include two high-profile members of Egyptian civil society. We also supported SMEX's investigation of a similar case against a Lebanese journalist. Besides spear phishing, the threat actor used false Android Package Kit (APK) applications, disguised as legitimate services such as Signal.

- Based on analysis of the APK and malicious infrastructure connections we discovered in the two Egyptian cases, Lookout assesses that the hack-for-hire campaign in question is likely tied to an Asian threat actor. Specifically, they believe it is likely that unknown entities hired this threat actor or an organization with ties to the actor to conduct espionage against civil society targets in the MENA region. We believe that the same threat actor could be behind the case identified by SMEX, based on the use of similar impersonation tactics, a common fingerprint, and the repeated use of the same attack infrastructure.

Section I: Chronology of cases

The first section presents a chronology of the spear-phishing attacks against Mostafa Al-A'sar and Ahmed Eltantawy, which took place in October 2023 and January 2024. Spear phishing is a highly personalized type of phishing that targets specific individuals or organizations. We also include a summary of the findings from a similar investigation by SMEX on an attack that followed the same pattern, which targeted a Lebanese journalist and took place in 2025. We believe that the same threat actor could be behind the attacks targeting all three victims.

Mostafa Al-A'sar is an Egyptian multidisciplinary journalist, researcher, human rights defender, and former political prisoner who endured four years of detention in Egypt for his reporting work. After his release, he fled to Lebanon and later relocated to Canada.

Ahmed Eltantawy was a well-known journalist and a member of the Egyptian Syndicate of Journalists before becoming a politician. He was editor-in-chief of the political section of the *Al-Karama* newspaper and gained recognition for his work in print media, radio, and television. He became a Member of the Egyptian Parliament in 2015 and launched a presidential campaign in 2023, before he was imprisoned in 2024 for his peaceful political activism and barred from running for elections for five years.

Al-A'sar and Eltantawy collaborated during the former's stay in Lebanon due to common interests, including Egypt's politics. In May 2023, Eltantawy also published a video on Facebook of himself being interviewed by Al-A'sar, which was widely shared on social media.

A. Targeting of Al-A'sar's Apple account (October 2023)

The first identified case consists of multiple spear-phishing attempts aimed at compromising the Apple account of Mostafa Al-A'sar, which would have granted the attacker access to all his personal files, contacts, cloud storage, and store purchases. The attacker impersonated Apple.

The attack originated on October 18, 2023, when Al-A'sar was in Lebanon. He received a communication via iMessage from an account purporting to be linked to Apple (**secure[.]appleuser[at]icloud[.]com**). In it, the sender instructed the target to click on a malicious hyperlink in order to "verify" a phone number associated with their account. As shown on Image 1, the message indicates that the threat actor knew the phone number and email address associated with Al-A'sar's account.

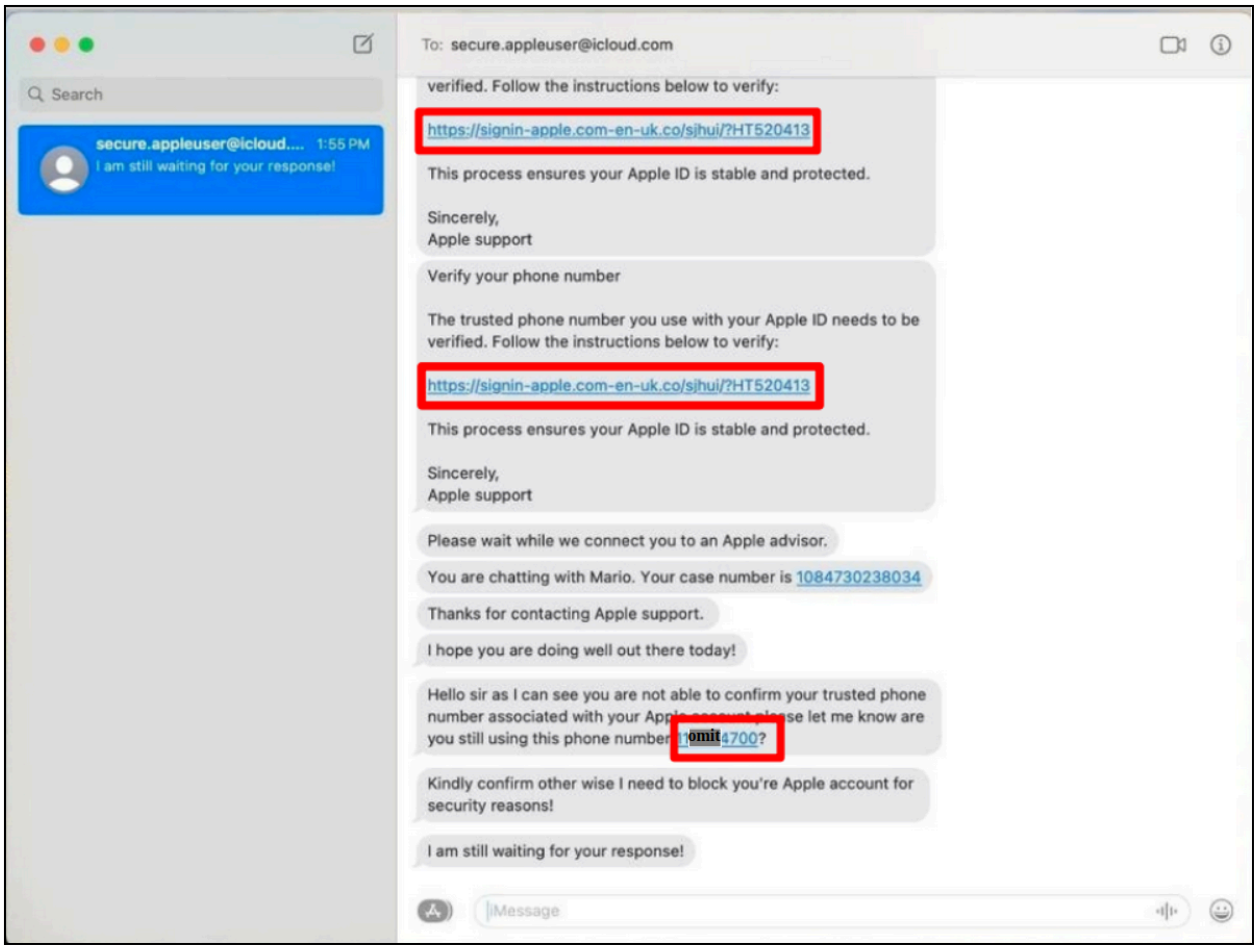

Image 1. Screenshot of the initial iMessage from the threat actor.

Despite the victim not engaging with the request at first, the threat actor persisted in their attempts to obtain the victim's credentials. This eventually led Al-A'sar to click on the link and submit his credentials. However, as the sign-in was attempted from a new device, Apple sent a notification to Al-A'sar's trusted devices asking for second-step verification. This type of notification shows the locations where the new sign-in is being attempted and prompts the user to allow or reject it from one of the devices where they are already logged in.

As shown in Image 2 below, the new, unauthorized sign-in was attempted from Cairo, Egypt, at a time when Al-A'sar was physically in Lebanon. While the location shown by Apple is based on the IP address or network that the device was using, rather than the exact location of the device, the disparity between Cairo and the victim's location at the time in Lebanon prompted the journalist to avoid engaging and seek support.

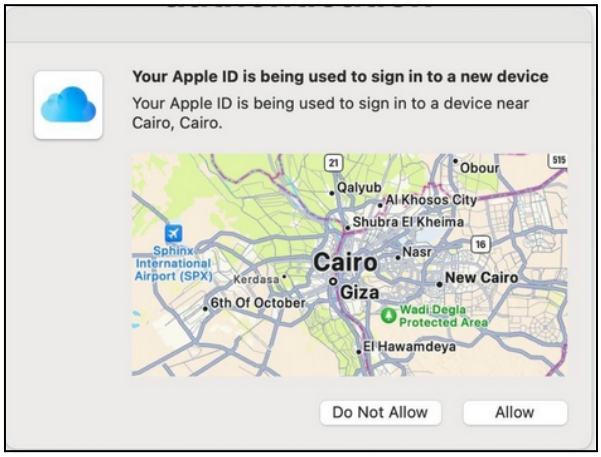

Image 2. Screenshot of the sign-in alert notification received by the victim.

The attacker made another attempt a few days later which also involved using a malicious link via iMessage. This time, the target was on a call with the Helpline discussing the first incident, so we were able to scan the active link in real time using URLscan.

The malicious link in the second attack was:

```
hxxps[://]signin-apple[.]com-en-uk[.]co/sjhui/?HT520413
```

This effectively resolved to the following URL:

```
hxxps[://]signin-apple[.]com-en-uk[.]co/2ci93ivnqovn.php?idvq=aEZzN04yaE51MEFmZDNkem5zVG
VLMmRSUncva3BKL2w1S2tlWGdOTWw5ST0=&rdle=&lsdg=RnBLSGU0WnhBZlIzRUtXdXZ4M2RJQT09
&adsw=&ctr=bUM1aFl1Q0cwbEkyS3FLb09sQzUyQT09
```

Through this initial verification, we found that the link in this second attempt directed to a page that asked for the target's code for two-factor authentication (2FA). The message on this phishing page indicated that the code had been sent to a phone number ending in **00** — which coincides with the last two digits of Al-A'sar's phone number. Since Al-A'sar had already entered a password in the previous attack, the attacker only needed to obtain the 2FA code to complete the earlier sign-in attempt and access the victim's Apple account.

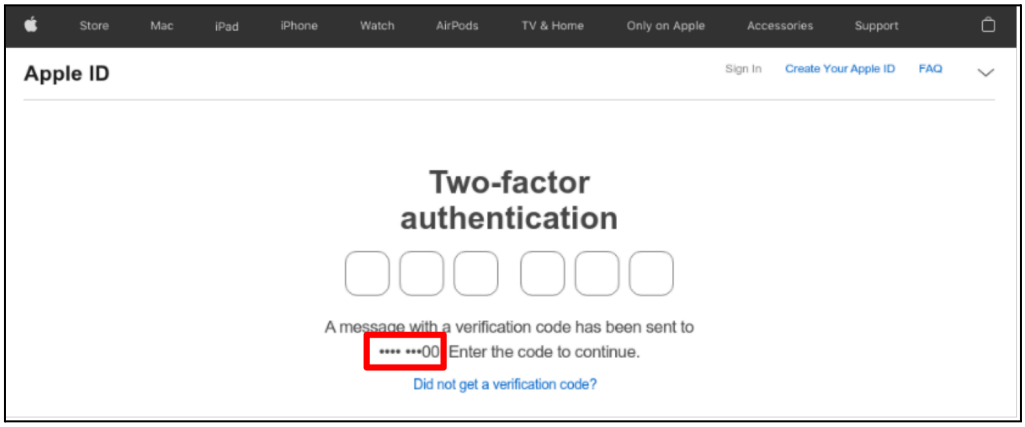

Image 3. Screenshot of the phishing page asking for the victim's second authentication factor.

WHOIS records show that the domain **com-en-uk[.]co** that is contained in the malicious hyperlink was created on July 26, 2023. However, passive DNS data show that the subdomain **signin-apple[.]com-en-uk[.]co** first resolved to the IP **45[.]144[.]155[.]158** on the day of the attack. This is a possible indicator that the attack was likely prepared specifically for Mostafa Al-A'sar.

When the Helpline checked the page code source via URLScan, we noticed that the HTML code uses randomly generated names for the variables and classes, a method often used to stop researchers from fingerprinting the page and searching for similar ones. In addition to the ambiguous variable names, a section of the JavaScript (JS) code was used to block access to the HTML source code. We found both the JS code and the choice of the variable names across other phishing pages that we discovered through our research.

B. Targeting of Al-A'sar's Google account (January 2024)

Four months after the first attempt, Mostafa Al-A'sar was targeted with another spear-phishing attack, this time aimed at compromising his Google account.

On January 6, 2024, an attacker using a Linkedin profile bearing the name "Haifa Kareem" reached out to Al-A'sar on the job-seeking and professional networking platform, under the pretense of offering him a job opportunity. The journalist provided his mobile number and email address to the LinkedIn user to continue the discussion about the job offer. Days later, on January 24, he received an email from the address **haifakareem657@gmail[.]com**, purporting to be from Haifa Kareem and offering a job interview. It included what looked like a Zoom video conferencing link for the journalist to join a call.

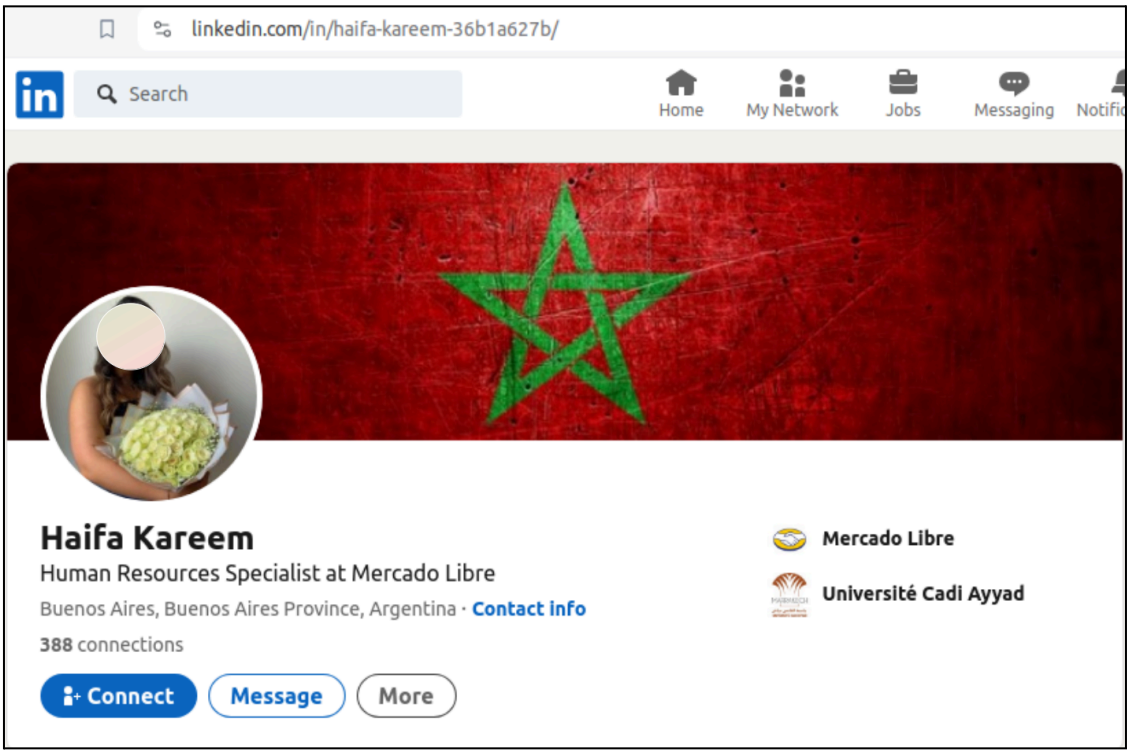

Image 5. LinkedIn profile used by the threat actor.

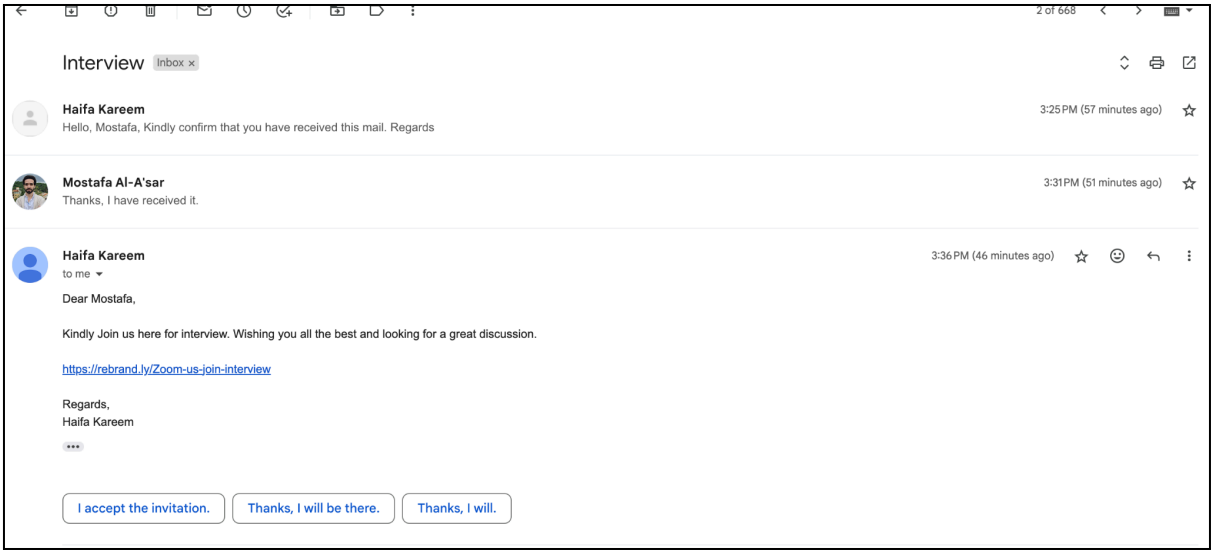

Image 6. Screenshot of email interaction between the threat actor and the victim.

Rather than engage with it, Al-A'sar asked the Helpline to examine the new link (**hxxps://rebrand[.]ly/Zoom-us-join-interview**).

Using URLScan, our analysis shows that this is a consent-based phishing attack leveraging Google OAuth 2.0, the company's protocol for authentication. Image 7 below explains the components of this attack.

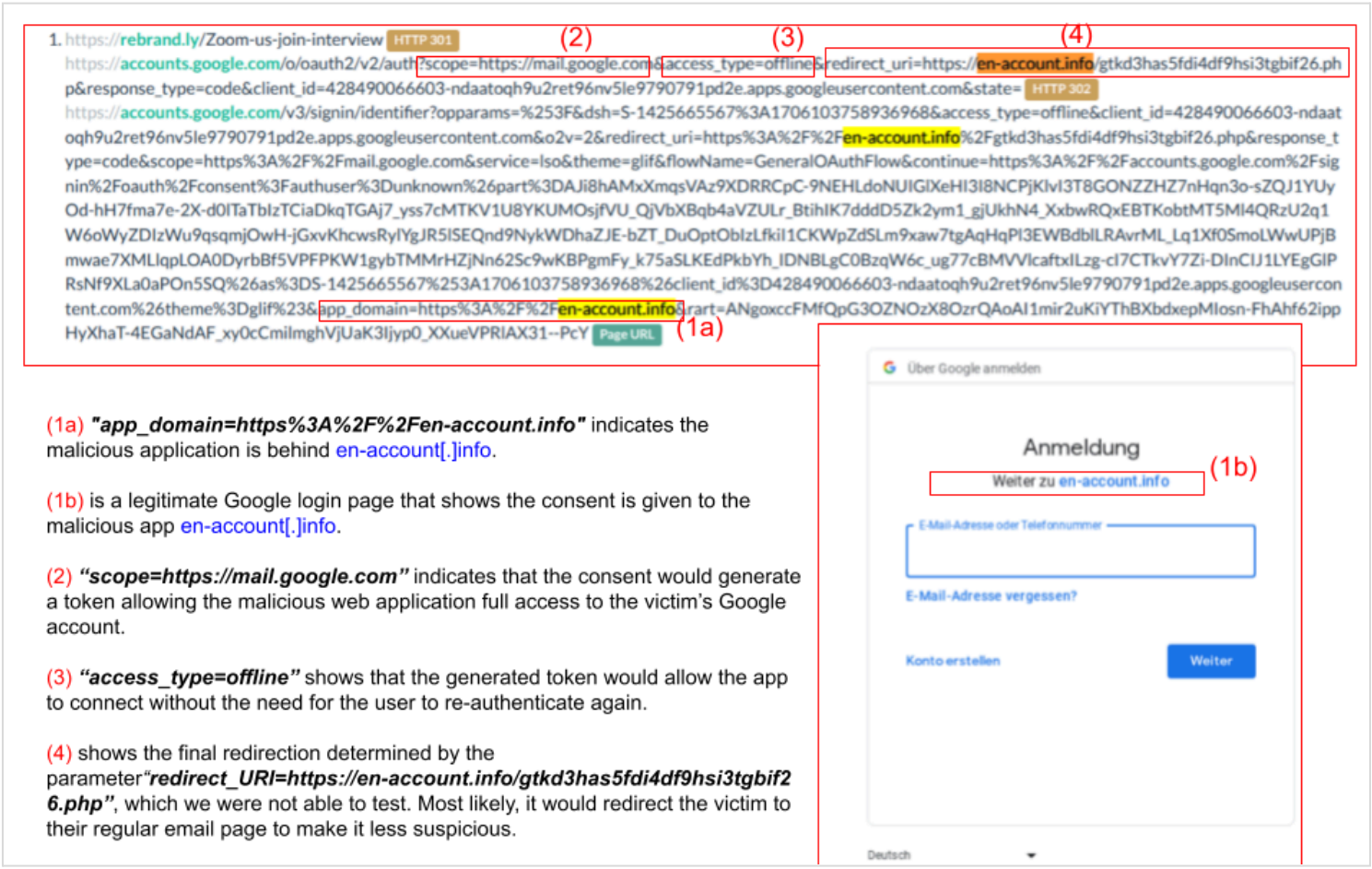

Image 7. OAuth consent phishing against Mostafa Al-A'sar.

Unlike the previous attack, where the attacker impersonated an Apple account login and used a fake domain, this attack employs OAuth consent to leverage legitimate Google assets to deceive targets into providing their credentials.

If the targeted user is not logged in to Google, they are prompted to enter their credentials (username and password). More commonly, if the user is already logged in, they are prompted to grant permission to an application that the attacker controls, using a third-party sign-in feature that is familiar to most Google users.

In both situations and after access is granted, an OAuth token is generated and communicated to the malicious server behind the domain **en-account[.]info**. This token would allow the attacker to access the victim's account data until the victim revokes access via Google account settings or changes the password.

The use of a URL shortener (rebrand.ly in this case) allows the attacker to create the illusion of legitimacy and hide the components analyzed in Image 7. It may also help the attacker avoid automated spam, phishing, or malware detection.

The link between October 2023 and January 2024 attempts

While the social engineering techniques used and platforms targeted in October 2023 and January 2024 attacks were different, we discovered that the two attacks share attack infrastructure. Concretely, domains **185.2.83[.]5** and **109.236.85[.]63** resolve to the IP address hosting **en-account[.]info.** The domain **review-ar[.]co**, also hosted in **185.2.83[.]5**, shares attributes with assets found on **com-en-uk[.]co**, specifically DNS records and JARM hash. These also fit the subdomain naming pattern that we explain in Section II below.

C. Targeting of Ahmed Eltantawy: multiple attacks targeting Apple account (October 2023 and January 2024)

We investigated two attacks against Ahmed Eltantawy aimed at compromising his Apple account. These follow the same time frame (October 2023 and January 2024) and pattern as those against Al-A'sar.

On October 18, 2023, the threat actor contacted Eltantawy via iMessage and asked him to verify his phone number. The sender used the following accounts to impersonate Apple's legitimate service: **review[.]support[at]icloud[.]com**, **appleid[.]review[at]messages.app**, and **secure[.]appleuser[at]icloud[.]com**. In the course of these attempts, the threat actor sent a phishing link that mimicked the Apple login page.

Both first attempts at compromising Mostafa Al-A'sar and Ahmed Eltantawy's Apple accounts occurred within hours of each other and used the same tactics. The malicious link itself was also very similar, with only a slight change in the last section:

https[://]signin-apple[.]com-en-uk[.]co/sjhui/**?HT213054**

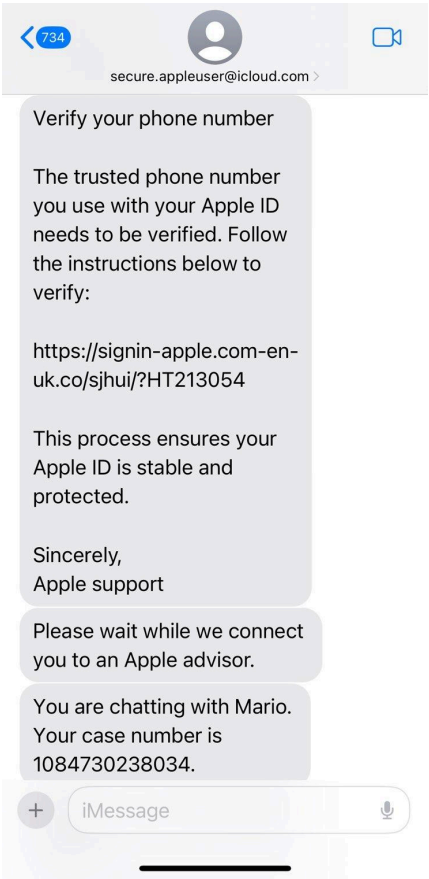

Image 8: Screenshots of the multiple phishing messages sent to Ahmed Eltantawy in October 2023.

A new round of attempts against Eltantawy took place in January 2024. This time, the impersonating account was different (**appleid[.]review[at]icloud[.]com**), but a similar malicious URL was used to try to lure the victim:

https[://]review-appleid[.]en-ae[.]io/GR0hGV/?HT125340

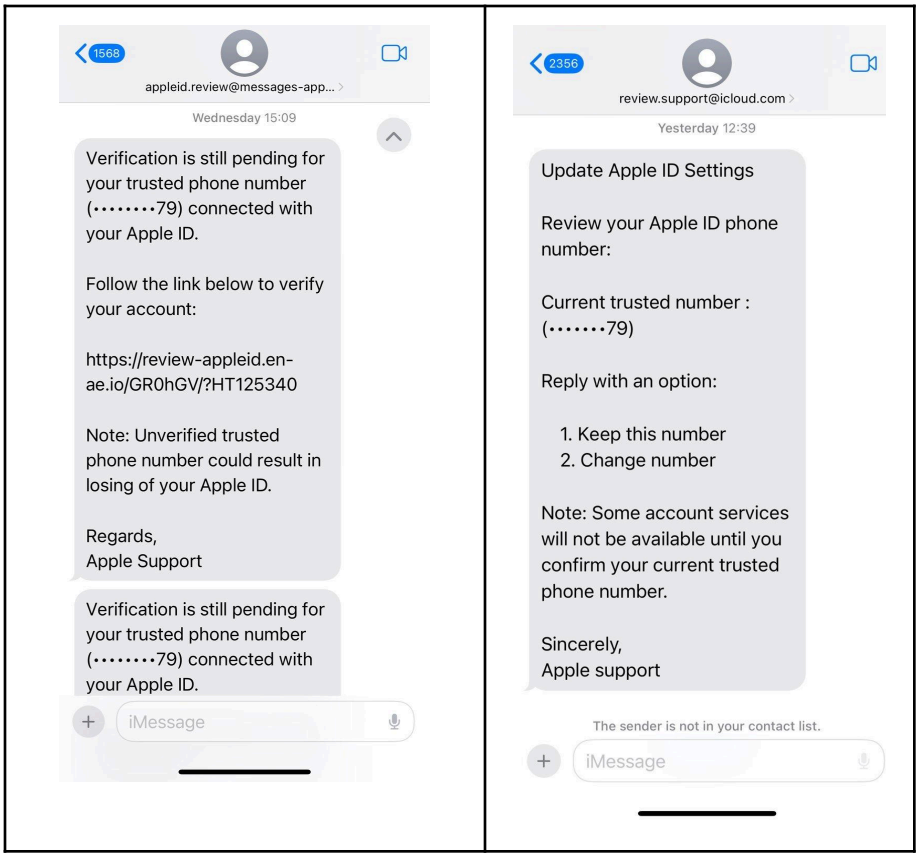

Image 8: Screenshots of the multiple phishing messages sent to Ahmed Eltantawy in January 2024.

These incidents were not reported to the Helpline immediately, so the URLs had been disabled by the time we investigated, limiting our findings. However, passive DNS records show that **review-appleid[.]en-ae[.]io** resolved to **93[.]174[.]90[.]20**. Additionally, **en-ae[.]io** follows the fingerprints of the attacks we documented across these different cases, and we assess with high confidence that the same attacker is behind all attempts.

In addition to these spear-phishing attacks, Eltantawy was previously targeted with Cytrox's Predator spyware in September 2021 and between May and September 2023, according to an investigation by The Citizen Lab at the Munk School of Global Affairs at the University of Toronto that attributes the attack to the Egyptian government. The first attempt to hack his Apple account, in October 2023, took place only a month after the publication of the Citizen Lab report and Apple issuing a software update aimed at closing the vulnerability that Predator spyware exploited. The attacks follow a broader set of repercussions that Eltantawy faced after announcing his intention to run for president, including his arrest and imprisonment and the arrests of several of his associates and family members. The International Commission of Jurists condemned Eltantawy's conviction for alleged electoral offenses, calling it politically motivated.

The timeline below summarizes the targeting of Eltantawy and Al-A'sar:

Timeline of attacks against Eltantawy and Al-A'sar in 2023 and 2024

D. SMEX investigation of multiple spear-phishing attacks against Lebanese journalist, targeting Apple account (May 2025)

SMEX, which promotes digital rights in the West Asia and North Africa (WANA) region, investigated a very similar case against a Lebanese journalist in early 2025, which we independently reviewed. The journalist's identity is not disclosed. Their report outlines a successful spear-phishing attempt using tactics similar to the ones we observed in the targeting of Al-A'sar and Eltantawy (legitimate service impersonation, similar patterns in malicious links and other attack infrastructure), which led us to conclude that the same threat actor is likely behind this attempt.

The malicious link used in the SMEX case is:

hxxps://id-apple[.]**com-en[.]io**/Txk62i/?HT584528

As we describe in Section II below, the domain **com-en[.]io** fits the fingerprint that we developed to uncover the infrastructure used by this threat actor in the campaigns against Al-A'sar and Eltantawy.

→ Read SMEX's technical note for further details about this attack.

Section II: Uncovering the malicious actor

This section presents further details about the infrastructure that the threat actor employed and provides information about Lookout's attribution of the attacks to the threat actor with ties to Asia.

To preserve ongoing monitoring capabilities, this section does not disclose the full fingerprint, complete indicator sets, or all detection logic used in our analysis. Instead, we highlight selected techniques that proved reliable for tracking the actor's infrastructure and activity over time.

Seeking legitimacy through meaningful subdomains

Two key aspects of the attackers' mode of action are the use of domains during a short period of time and diversifying subdomains.

The spear-phishing attacks against both Al-A'sar and Eltantawy show a common pattern, in which the attacker disables their domains shortly after using them, only making them available during the time of the attack. Additionally, they tend to keep one domain per IP — which they keep short and resembling a Top Level Domain (TLD) — relying instead on subdomain diversification to continue pointing to the same IP. All of the domains and subdomains are constructed to appear legitimate.

Below are the domains we observed in the spear-phishing attempts and the associated IPs and subdomains. The table shows a focus on attempts to compromise Apple accounts by using subdomains such as *id-apple*, *facetime*, *join-fts*, and *signin-apple*, but it also points to the targeting of other services like Signal and Telegram.

Domains	**Subdomains**	**IPs (and corresponding hosting provider)**
com-en-uk[.]co Targeting of Al-A'sar's Apple account (October 2023)	signin-apple[.]com-en-uk[.]co sign-in-user[.]com-en-uk[.]co signin-office[.]com-en-uk[.]co sign-in[.]com-en-uk[.]co login-office[.]com-en-uk[.]co	45.144.155[.]158 AS 9028 (OHOST LLC)
en-account[.]info Targeting of Al-A'sar's Google account (January 2024)	login-live[.]en-account[.]info login-live-online[.]en-account[.]info eblogin-live[.]en-account[.]info testid[.]en-account[.]info test-id[.]en-account[.]info	109.236.85[.]63 AS 49981 (WorldStream B.V.) 185.2.83[.]5 AS 49981 (WorldStream B.V.)

review-ar[.]co Targeting of Al-A'sar's Google account (January 2024)	signin-apple[.]review-ar[.]co signin-account[.]review-ar[.]co login-apple[.]review-ar[.]co login-live[.]review-ar[.]co number-appleid[.]review-ar[.]co id-appleid[.]review-ar[.]co	185.2.83[.]5 AS 49981 (WorldStream B.V.)
en-ae[.]io Targeting of Eltantawy's Apple account (October 2023 and January 2024)	signin-apple[.]en-ae[.]io review-appleid[.]en-ae[.]io login-apple[.]en-ae[.]io	93.174.90[.]20 AS 202425 (IP Volume Inc)
com-en[.]io SMEX investigation of multiple spear-phishing attacks against a Lebanese journalist, targeting Apple account (May 2025)	join-telegram[.]com-en[.]io telegram[.]com-en[.]io id-apple[.]com-en[.]io facetime[.]com-en[.]io numbers[.]com-en[.]io secure-signal[.]com-en[.]io join-fts[.]com-en[.]io	85.206.166[.]23 AS61272 (Informacines sistemos ir technologijos, UAB)

Table 1: Subdomains used by the threat actor attacking Mostafa Al-A'sar and Ahmed Eltantawy

During the investigation, we also observed the repeated reuse of domain infrastructure across different spear-phishing campaigns, as domains associated with earlier activity continued to be employed in subsequent attacks. This pattern suggests a level of operational continuity and may indicate that the threat actor considers this infrastructure sufficiently reliable or low risk to continue using over time.

Fingerprint based on unique URI patterns exposes MENA-wide operations

The analysis of URLs in the documented cases showed consistent structural patterns. For example, the threat actor reused URI variables (brief alphanumeric keys followed by an equal sign). This pattern is commonly seen in links generated by phishing kits, which are pre-packaged tools to facilitate and speed up the creation of convincing pages that impersonate trusted platforms and evade detection.

We developed a fingerprint based on these URI variables, the pattern used in domain and subdomain names, and used it to search for more connected domains across the URLScan and VirusTotal database. The resulting list is included in the Appendix section and shows the magnitude of this campaign and the activity of the threat actor. It also shows the diversity of services targeted and tools

impersonated, which in addition to Apple includes Microsoft, Zoom, Signal, and WhatsApp. The attackers also impersonate media outlets, like *The Guardian* and *Thomson Reuters*, and public agencies, like the Ministry of Foreign Affairs of Bahrain.

The origin of these indicators and submissions in the MENA countries is also relevant: the majority are from the United Arab Emirates, but they also come from Egypt, Jordan, and Bahrain.

Capacities range from spear phishing to Android spyware

During our investigation of the phishing attempts aimed at compromising online accounts, we also found URLs created by the attackers that lead to fake Android apps. One such app masquerades as the encrypted messaging app Signal. As we explain below, identifying these URLs allowed us to establish that the threat actor's wide-ranging toolkit includes Android spyware.

In the process of fingerprinting described in the previous section, we identified the following URL:

```
hxxps[://]sgnl-app[.]info/index[.]php?idjk=U2FVVWVCenVDOFluZ0ZJNDc5bWdPdz09&rdyu=&lsdt=
&adsp=bzdxYWg2TnoydmdCWFQ1bzN5M2p4UT09&cte=emNPM1VyQnJlemoxQ3dUdW84MGFNbkpq
bi82RnpVRS9zN1pWMU55VWIrZz0=
```

Passive DNS records showed that **sgnl-app[.]info** resolved to IP **185[.]225[.]114[.]70** on March 11, 2025, which later resolved to another domain **sgnlapp[.]info**. After looking for submissions of this domain, we found a URL (**hxxps://signal[.]ct[.]ws/?i=1**) that resolves to a landing page that impersonates the official **Signal** application download page, but which serves a malicious APK file named **signal_encyption_plugin.apk**.

Below is the full redirection chain:

```
hxxp[://]encryption[.]sgnlapp[.]info/
hxxps[://]signal[.]ct[.]ws/?i=1
hxxps[://]signal[.]ct[.]ws/?i=1/plugin/signal-encryption-plugin[.]apk
```

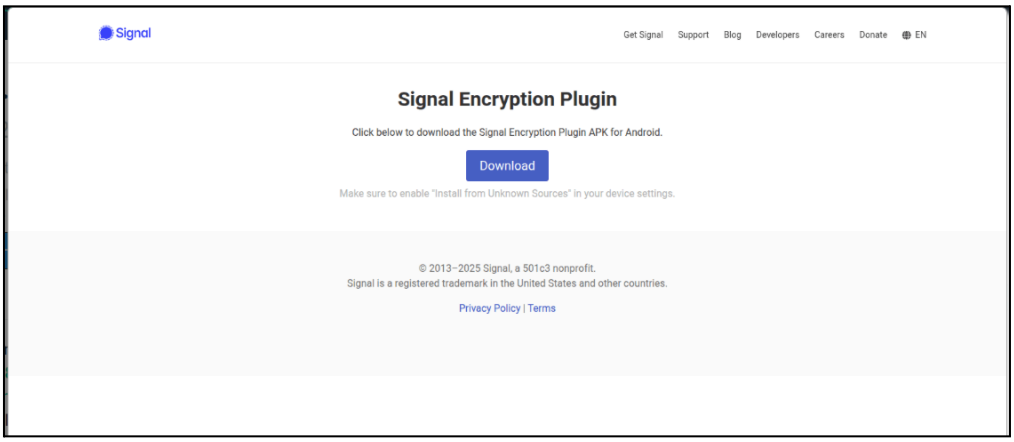

Image 9. Fake Signal download page.

```
<div style="margin-top: 80px;"></div>

<!-- Main content -->
<main class="section">
  <div class="container has-text-centered">
    <h2 class="title">Signal Encryption Plugin</h2>
    <p>Click below to download the Signal Encryption Plugin APK for Android.</p>
    <a href="plugin/signal-encryption-plugin.apk" class="button is-link is-medium mt-4">Download</a>
    <p class="has-text-grey-light mt-2">Make sure to enable "Install from Unknown Sources" in your device settings.</p>
  </div>
</main>
```

Image 10. Code to download the fake Signal APK .

URL	https[://]encryption-plug-in-signal.com-ae[.]net/signal_encyption_plugin.apk
SHA256	42f28501f3e6be38c0ce4ff2a5bfa2dfe3c56f99ed81804de54cba3bc26a5025
Filename	signal_encyption_plugin.apk

Table 2. Summary of APK impersonating Signal, its distribution URL, file hash, and Virustotal submission.

This represented a turning point in our investigation, as it was the first time we encountered a malicious APK distributed by this threat actor, and it provided relevant information for attribution. In August 2025, we began collaborating with Lookout, whose threat intelligence team identified more samples related to this APK. Their analysis shows that the APK has a set of spyware capabilities (summarized in Table 3 below), including the ability to search for a long list of files and exfiltrate them. Please refer to Lookout's report for more details about their code analysis.

Scan and exfiltrate document files
Check for recently modified files
Search for backup files
Search for archive files
Search for files not matching other specific MIME types
Search for image files
Search for audio files
Search for video files
Collect and exfiltrate SMS messages
Collect and exfiltrate phone contacts

Table 3. List of capabilities of malware samples analyzed by Lookout.

In October 2025, cybersecurity firm ESET published an independent analysis of the same APK sample we found and those Lookout found using criteria extracted from the APK. They call the spyware "ProSpy." According to ESET, attackers using the spyware appear to focus primarily on targets in the United Arab Emirates. Given the findings of our investigation, this suggests that the operation we identified may be part of a broader regional surveillance effort aimed at monitoring communications and harvesting personal data.

→ Please read Lookout's full analysis here.

Conclusion

The tactics and techniques described in this report range from spear phishing to the use of Android spyware. This suggests that the suspected threat actor can operate with different levels of skill and tools.

Our investigation has revealed targeted attacks attempting to compromise the Apple accounts of Mostafa Al-A'sar and Ahmed Eltantawy. If these attacks had been fully successful, all the data backed up to their iCloud accounts would have been breached. Since iCloud is used to back up and sync data across multiple Apple devices, this could have granted the threat actor and its customers access to a substantial amount of personal information, making it potentially a cheaper alternative to the use of more sophisticated and expensive iOS spyware.

Access Now and partners have published multiple reports on the use of targeted spyware against members of civil society. But while the use of spyware is rightfully alarming, investigations like this one demonstrate that phishing remains a significant threat. It is a widely used and effective tool for compromising the accounts of journalists and other members of civil society, and violates their human rights, putting their privacy and security at risk.

Hack-for-hire groups continue to grow in number and capability. It is important for researchers and the security community to keep investigating and sharing information about their activities to better protect current and future targets.

For civil society, the threat from phishing campaigns remains high. Staying alert and handling all unexpected messages with caution are key strategies to reduce the risk of compromise.

Phishing prevention measures and recommendations

Following are general tips for members of civil society to prevent and mitigate phishing attacks, as well as resources for learning more. While this kind of general guidance can be useful, we recommend that you consider your own circumstances, threats, and risk tolerance, and reach out to a trusted digital security practitioner for advice.

Start with prevention

Beware of social engineering: Hack-for-hire groups and others have built dedicated infrastructure and developed malicious applications to compromise their victims' accounts. However, in cases like the ones we have documented in this report, they still depend on the victim's participation to click on the malicious link, download the malicious files, and/or install the spyware. Techniques like social engineering — the psychological manipulation of people to do things like divulge confidential information — and attacks like phishing target human rather than technological vulnerabilities, and it's important to stay informed about the strategies attackers are using, as their techniques evolve quickly. In many cases, it helps to **trust your instincts**: If something feels off or you are being pressured or rushed to take action, take a step back and check in with your peers before moving forward.

Use two-factor authentication, correctly: Setting up two-factor authentication (2FA) is one of the most powerful ways to protect your account from getting hacked. However, hack-for-hire groups and other threat actors may try to trick you into revealing your second factor; we have seen attackers

successfully compromise the accounts of victims who enabled 2FA. **Never give out your 2FA codes to anyone**, and always make sure that you **input them only on the official website**.

We recommend that you use more advanced 2FA options such as security keys, or, if you are a Gmail user, Google Passkeys. Here are four guides for increasing the level of security for your account:

- Create a Passkey to log in to your Google account (Google)
- How to: Enable two-factor authentication (Electronic Frontier Foundation)
- Set up multifactor authentication (Consumer Reports)
- Use a security key (Consumer Reports)

Be aware that attackers may use familiar-looking, consent-based login pages for phishing attacks. As we have documented in this report with regard to Google OAuth, an attacker can use a legitimate-looking page or message to request your consent to authorize a new app or login using your existing accounts (such as your Google account or others). To avoid this, we recommend that you:

- Review third-party apps and services that are linked to your accounts, such as your Google account, and revoke access to any suspicious applications.
- If you are presented with a page to grant access permission to a new app, make sure to validate the origin carefully.
- If you are using an enterprise account, check with your system administrator before you grant access permission to a new app.
- System administrators can control which apps can access Google Workspace or Microsoft 365 data. Access to third-party apps should be restricted or require admin consent.

If you face a higher level of risk for digital attacks, enroll in programs and/or enable settings for high-risk users. Google and some other providers offer optional programs and settings for people who, because of who they are or what they do, may be targeted for attack. Some of these programs not only increase the security of your account, they also flag to companies that you could face sophisticated attacks. They include:

- Google Advanced Protection
- Microsoft AccountGuard
- Proton Sentinel high-security program
- Apple Lockdown Mode
- WhatsApp's Strict account settings

Received a message? Be a five-second detective

- **Step one: check the sender's username**. Ask yourself if you have received messages from this account before, and if this is an official account. Look carefully for anything out of place: threat

actors could use lookalike email addresses or user names to impersonate people you know or support teams from services that you use.

- **Step two: check with the sender using a different service**. If you have any concerns or are at all suspicious about a personal email or message, do not open any file attachment or click on any link in the email or message. Instead, check directly with the purported sender, via another service, to confirm whether they've reached out to you. If you don't already have a way to reach them directly using another service, consider asking someone you trust to inquire on your behalf. If you receive a message that purports to be from an online platform's security or service team, you may not be able to contact anyone directly to see if the message was legitimate. However, you can do a quick online search to verify whether the company in question, such as Signal, ever uses direct messages or chat bots to contact users.
- **Step three: double-check links before you click**. If you receive an email or chat message prompting you to make changes to your account, visit the official website manually rather than clicking on the link. If you have already clicked on a link and it sends you to a login page, that is a red flag. Stop and visit the official site to log in, to be sure that you are entering your credentials into the real page.

These recommendations address the kind of phishing attacks described in this report, but there are many other ways you could be targeted. Whatever your level of risk, you may find it helpful to use the *Consumer Reports* Security Planner to get personalized security recommendations, as well as access to a list of emergency resources and advanced security guides.

Think you are being targeted?

If you are part of an organization that is facing digital threats and you suspect that you have already been targeted in an attack, first reach out to a trusted digital security practitioner for advice. It is crucial to evaluate any damage to your organization and/or to other related organizations and individuals, such as journalistic sources, support organizations, and other partners, among others. If you determine that you have indeed been targeted, keep them informed about what has happened, whether and what information has been leaked, how this may impact them, and what steps you are taking to mitigate the impact.

In addition, Access Now's Digital Security Helpline is available to support members of civil society, including activists, media organizations, journalists, and human rights defenders, 24/7 in 10 languages. If your account has been compromised, we advise that you:

- **Change your password right away**. If you are using the same password for other accounts, you should change the password for those accounts too. Consider using a password manager to keep track of multiple passwords.

- **Review access logs on your accounts**, such as Proton Mail's activity monitor, Gmail's last account activity, or Microsoft's recent activity page, and review devices with account access. You may still have questions after reviewing these logs. If so, we encourage you to make a copy of the logs to share with an expert for review.

Appendix: Indicators of Compromise

APK Sample

42f28501f3e6be38c0ce4ff2a5bfa2dfe3c56f99ed81804de54cba3bc26a5025

Network

Domain	Subdomain	IP	ASN	Impersonated Service Provider
ac-im[.]cc	facpl[.]ac-im[.]cc	82[.]118[.]242[.]118	AS201133 (VERDINA, BZ)	Apple
ac-us[.]cc	appleid-verify[.]ac-us[.]cc	84[.]32[.]191[.]211	AS 59642 (UAB Cherry Servers)	Apple
acc-mn[.]info	hot-mail[.]acc-mn[.]info	91[.]206[.]228[.]22	AS58294 (CloudWall Cloud Wall Ltd., BG)	Microsoft
	sgnl-link-device[.]acc-mn[.]info	91[.]206[.]228[.]22	AS58294 (CloudWall Cloud Wall Ltd., BG)	Signal
ar-id[.]cc	num-blk[.]ar-id[.]cc	84[.]238[.]133[.]18	AS209625 (redcluster Redcluster LTD, CY)	Apple
ar-id[.]co	confirm-your-identity[.]ar-id[.]co	128[.]140[.]55[.]131	AS24940 (HETZNER-AS Hetzner Online GmbH, DE)	Apple
ar-info[.]co	auth-rev[.]ar-info[.]co connect[.]ar-info[.]co auth.rec[.]ar-info[.]co	176[.]123[.]6[.]86	AS 200019 (Alexhost Srl)	Microsoft
ar-me[.]cc	signin-guardian[.]ar-me[.]cc theguardian[.]ar-me[.]cc	94[.]156[.]104[.]163	AS 216194 ('Emrozian International Trading', AE)	The Guardian
	join-facetime[.]ar-me[.]cc review-apple[.]ar-me[.]cc	185[.]36[.]81[.]21	AS 209605 (UAB Host Baltic)	Apple

com-ae[.]org	checkdata[.]com-ae[.]org encryption-signal[.]com-ae[.]org	94[.]156[.]128[.]160	AS44901 (belcloud Belcloud LTD, BG)	Signal
com-ar[.]info	appleid-apple[.]com-ar[.]info	185[.]31[.]121[.]189	AS199364 (RAX-AS, BG)	Apple
com-ar[.]io	appleid-apple[.]com-ar[.]io appleid-number[.]com-ar[.]io review-appleid[.]com-ar[.]io	172[.]245[.]112[.]201 104[.]237[.]252[.]45 91[.]206[.]228[.]148	AS 36352 (AS-COLOCROSSING) AS 16628 (DEDICATED-FIBER-COMMUNICATIONS) AS 58294 (Cloud Wall Ltd.)	Apple
com-auth[.]cc	apple[.]com-auth[.]cc appleid-apple[.]com-auth[.]cc appleid-number[.]com-auth[.]cc id-appleid[.]com-auth[.]cc ids-appleid[.]com-auth[.]cc login-apple[.]com-auth[.]cc login-appleid[.]com-auth[.]cc number-appleid[.]com-auth[.]cc numbers-appleid[.]com-auth[.]cc review-appleid[.]com-auth[.]cc signin-appleid[.]com-auth[.]cc	172[.]245[.]112[.]201 104[.]237[.]252[.]46	AS 36352 (AS-COLOCROSSING) AS 16628 (DEDICATED-FIBER-COMMUNICATIONS)	Apple
com-ln[.]info	login-cloud[.]com-ln[.]info	104[.]237[.]234[.]31	AS 16628 (DEDICATED-FIBER-COMMUNICATIONS)	Apple
com-en[.]cc	appleid-apple[.]com-en[.]cc login-apple[.]com-en[.]cc	46[.]249[.]58[.]46	AS50673 (SERVERIUS-AS, NL)	Apple
com-en[.]io	id-apple[.]com-en[.]io appleid-apple[.]com-en[.]io join-facetime[.]com-en[.]io	85[.]206[.]166[.]23	AS61272 (IST-AS Informacines sistemos ir technologijos)	Apple
	secure-signal[.]com-en[.]io	85[.]206[.]166[.]23	AS61272 (IST-AS Informacines sistemos ir technologijos)	Signal
	join-telegram[.]com-en[.]io	85[.]206[.]166[.]23	AS61272 (IST-AS Informacines sistemos ir technologijos)	Telegram

com-en-uk[.]co	signin-apple[.]com-en-uk[.]co	45[.]144[.]155[.]158	AS9028 (OHOST LLC, BG)	Apple
com-en-us[.]info	join-facetime[.]com-en-us[.]info fc-blk[.]com-en-us[.]info fc-wid[.]com-en-us[.]info	185[.]123[.]53[.]102	AS 62005 (BlueVPS OU)	Apple
	login-live[.]com-en-us[.]info login-office[.]com-en-us[.]info	85[.]239[.]52[.]23	AS 62005 (BV-EU-AS, EE)	Microsoft
	join-zoom[.]com-en-us[.]info	185[.]123[.]53[.]102	AS 62005 (BlueVPS OU)	Zoom
	web-whatsapp[.]com-en-us[.]info	185[.]123[.]53[.]102	AS 62005 (BlueVPS OU)	Whatsapp
com-info[.]io	trusted-device-apple[.]com-info.io verify-apple[.]com-info.io ft-num-apl[.]com-info.io icloud-apple[.]com-info.io join-facetime[.]com-info.io	82[.]118[.]242[.]127	AS 201133 (VERDINA, BZ)	Apple
	zoom[.]com-info.io	82[.]118[.]242[.]127	AS 201133 (VERDINA, BZ)	Zoom
com-service[.]info	apple[.]com-service[.]info facetime-apple[.]com-service[.]info icloud[.]com-service[.]info	176[.]123[.]9[.]44 111[.]90[.]148[.]121	AS 200019 (Alexhost Srl) AS 45839 (Shinjiru Technology Sdn Bhd)	Apple
connect-signal[.]org	beta[.]connect-signal[.]org	176[.]123[.]8[.]154 141[.]98[.]11[.]48	AS 209605 (UAB Host Baltic) AS 200019 (Alexhost Srl)	Signal
en-account[.]info	login-live[.]en-account[.]info login-live-online[.]en-account[.]info	109.236.85[.]63 185.2.83[.]5	AS 49981 (WorldStream B.V.)	Microsoft

	eblogin-live[.]en-account[.]info			
en-ar[.]co	mail-auth[.]en-ar[.]co confirm-your-identity[.]en-ar[.]co	185[.]205[.]211[.]55	AS 44901 (Belcloud LTD)	Microsoft
en-id[.]cc	appleid-apple-com[.]en-id[.]cc auth-rev[.]en-id[.]cc auth-subb[.]en-id[.]cc facetime-apple[.]en-id[.]cc join-facetime[.]en-id[.]cc join-my-calls[.]en-id[.]cc join-the-call[.]en-id[.]cc join-the-calls[.]en-id[.]cc my-call-join[.]en-id[.]cc rev-id[.]en-id[.]cc log.rev[.]en-id[.]cc	185[.]246[.]188[.]133	AS 200651 (FlokiNET ehf)	Apple
	connect-signal[.]en-id[.]cc	185[.]246[.]188[.]133	AS 200651 (FlokiNET ehf)	Signal
	ms.connecting[.]en-id[.]cc info-team[.]en-id[.]cc join-teams[.]en-id[.]cc	185[.]246[.]188[.]133	AS 200651 (FlokiNET ehf)	Microsoft
en-id[.]net	confirm-your-identity[.]en-id[.]net	185[.]7[.]33[.]39 80[.]82[.]76[.]80	AS199968 (IWSNET IWS NETWORKS LLC, AM) AS202425 (INT-NETWORK IP Volume inc, SC)	Apple
en-me[.]cc	connect-signal[.]en-me[.]cc	185[.]246[.]188[.]120	AS 200651 (FlokiNET ehf)	Signal
	icloud[.]en-me[.]cc join-facetime[.]en-me[.]cc join-test[.]en-me[.]cc	185[.]246[.]188[.]120	AS 200651 (FlokiNET ehf)	Apple
en-uk[.]cc	appleid[.]en-uk[.]cc confirm-id[.]en-uk[.]cc manage-id[.]en-uk[.]cc number-appleid[.]en-uk[.]cc number-signin[.]en-uk[.]cc numbers-appleid[.]en-uk[.]cc review-appleid[.]en-uk[.]cc review-id[.]en-uk[.]cc review-ids[.]en-uk[.]cc	176[.]123[.]6[.]85	AS 200019 (Alexhost Srl)	Apple

final-restore[.]re	file-check[.]final-restore[.]re	23[.]106[.]39[.]154	AS205544 (LEASEWEB-UK-LON-11 Leaseweb UK Limited, GB)	Ministry of Bahrain Affairs
hm-en[.]cc	hot-acc-mail[.]hm-en[.]cc	185[.]100[.]87[.]244	AS200651 (FlokiNET FlokiNET ehf, IS)	Microsoft
id-ar[.]me	ft-join[.]id-ar[.]me ft-rev[.]id-ar[.]me join-facetime[.]id-ar[.]me num-rev[.]id-ar[.]me nums-rev[.]id-ar[.]me review-apple[.]id-ar[.]me	185[.]100[.]87[.]33	AS 200651 (FlokiNET ehf)	Apple
id-en[.]co	ft-join[.]id-en[.]co ft-rev[.]id-en[.]co ft-revs[.]id-en[.]co join-facetime[.]id-en[.]co num-rev[.]id-en[.]co num-revs[.]id-en[.]co review-apple[.]id-en[.]co	185[.]100[.]87[.]90	AS 200651 (FlokiNET ehf)	Apple
id-en[.]me	auth-manage[.]id-en[.]me auth-rev[.]id-en[.]me test.auth[.]id-en[.]me rec-auth[.]id-en[.]me	81[.]17[.]29[.]130 195[.]230[.]22[.]15	AS 51852 (Private Layer INC) AS 206383 (Voxlan Ltd.)	Apple
id-en[.]net	join-signal[.]id-en[.]net link-signal[.]id-en[.]net 2fa-signal[.]id-en[.]net number-signal[.]id-en[.]net	176[.]123[.]7[.]81	AS 200019 (Alexhost Srl)	Signal
	news-reuters-com[.]id-en[.]net	176[.]123[.]7[.]81	AS 200019 (Alexhost Srl)	Reuters
	news-jpost-com[.]id-en[.]net	176[.]123[.]7[.]81	AS 200019 (Alexhost Srl)	The Jerusalem Post
id-us[.]ca	review-apple[.]id-us[.]ca	149[.]3[.]170[.]37	AS 213373 (IP Connect Inc)	Apple

ilability[.]net	check-data-av[.]ilability[.]net	87[.]229[.]37[.]3	AS201670 (INFOTECH-GRUP S.C. INFOTECH-GRUP S.R.L., MD)	Apple
info-ar[.]cc	delivery-dhlr[.]info-arr[.]cc	176[.]123[.]4[.]36	AS 200019 (Alexhost Srl)	DHL
	num-apple[.]info-ar[.]cc nums-apple[.]info-ar[.]cc review-appler[.]info-arr[.]cc	176[.]123[.]4[.]36	AS 200019 (Alexhost Srl)	Apple
logs[.]re	imanage[.]logs[.]re rv-mn-en[.]logs[.]re	194[.]26[.]141[.]209	AS62005 (BV-EU-AS BlueVPS OU, EE)	Apple
mation-ae[.]re	idms-rec-infor[.]mation-ae[.]re join-facetime-call-infor[.]mation-ae[.]re	185[.]165[.]170[.]89	AS200651 (FlokiNET FlokiNET ehf, IS)	Apple
mation[.]re	encryption-sgnl-infor[.]mation[.]re	80[.]82[.]76[.]80	AS202425 (INT-NETWORK IP Volume inc, SC)	Signal
	idms-rec-infor[.]mation[.]re join-facetime-call-infor[.]mation[.]re	80[.]82[.]76[.]80	AS202425 (INT-NETWORK IP Volume inc, SC)	Apple
me-ar[.]io	appleid-number[.]me-ar[.]io	104[.]237[.]234[.]23	AS16628 (DEDICATED-FIBER-COMMUNICATIONS, US)	Apple
me-en[.]cc	mng-id-val[.]me-en[.]cc rev-number[.]me-id[.]cc review-appleid[.]me-en[.]cc number-appleid[.]me-en[.]cc 2fa-mange[.]me-en[.]cc mng-id-val[.]me-en[.]cc id-mana-ge[.]me-en[.]cc 2fa-manage[.]me-en[.]cc	176[.]123[.]5[.]221 146[.]19[.]254[.]137 103[.]145[.]13[.]82	AS200019 (ALEXHOST, MD) AS62005 (BV-EU-AS BlueVPS OU, EE) AS 60528 (Myweb Limited)	Apple

	join-facetime[.]me-en[.]cc mng-info[.]me-en[.]cc			
me-info[.]io	join-facetime[.]me-info[.]io num-blk[.]me-info[.]io	185[.]100[.]87[.]70	AS200651 FlokiNET FlokiNET ehf, IS)	Apple
org-ar[.]net	id-apples-mange[.]org-ar[.]net	185[.]225[.]114[.]26	AS204615 (ipfib-as IP Fiber Inc, SC)	Apple
privacy-ar[.]com	login-yahoo[.]privacy-ar[.]com	104[.]237[.]234[.]35	AS16628 (DEDICATED-FIBER-COMMUNICATIONS, US)	Yahoo
	signin-live[.]privacy-ar[.]com	104[.]237[.]234[.]35	AS16628 (DEDICATED-FIBER-COMMUNICATIONS, US)	Hotmail
	signin-ap[.]privacy-ar[.]com	104[.]237[.]234[.]35	AS16628 (DEDICATED-FIBER-COMMUNICATIONS, US)	Apple
re-ac[.]cc	loading-mng-blnk[.]re-ac[.]cc	185[.]225[.]114[.]26	AS204615 (ipfib-as IP Fiber Inc, SC)	Apple
review-ar[.]co	signin-apple[.]review-ar[.]co signin-account[.]review-ar[.]co login-apple[.]review-ar[.]co number-appleid[.]review-ar[.]co id-appleid[.]review-ar[.]co	185[.]2[.]83[.]5	AS 49981 (WorldStream B.V.)	Apple
	login-live[.]review-ar[.]co	185[.]2[.]83[.]5	AS 49981 (WorldStream B.V.)	Microsoft
sgnl-app[.]info	sgnl-app[.]info	185[.]225[.]114[.]70	AS204615 (ipfib-as IP Fiber Inc, SC)	Signal