TLP:CLEAR THREAT INTELLIGENCE REPORT

Parcel-Redelivery Smishing Impersonates UAE Couriers: J&T Express, Naqel Express, Aramex, Zajel, Quiqup and Jeebly

One "missing address" story, sent by iMessage under at least seven UAE delivery brands since September 2026, leads to rotating throwaway domains on a shared phishing system that also targets postal, courier and government services in many other countries.

Report	Published	Version	Sector	Region
AH-TR-2026-002	28 November 2026	1.1, updated 29 November	Logistics, parcel delivery	United Arab Emirates; also Jordan, Albania, Puerto Rico, Australia and others

Executive Summary

Ask Haris users in the UAE submitted SMS messages that impersonate the couriers J&T Express and Naqel Express. The messages say a parcel arrives today but the Emirate in the delivery address is missing, and send the reader to a look-alike site to "update" it.

The three messages analysed here are one script under two brands. All carry the same tracking digits, `JT7845120390AE` for J&T and `NQ7845120390` for Naqel, and word-for-word instructions to reply "Y" so that the link becomes clickable. The other sentences are reworded from message to message. They arrived by iMessage from foreign numbers, a US number for J&T and a Philippine number for Naqel, so they never passed through UAE telecom SMS filtering. Each link is a brand subdomain on a random six-letter `.cfd` domain, such as `jtexpress.zrkgyg[.]cfd` or `naqelexpress.vsjwmm[.]cfd`.

Registration records, public scans and a shared stylesheet tie these to 15 domains registered through one registrar, Aceville Pte. Ltd., between 3 and 27 November, in batches seconds or minutes apart. Naqel Express was targeted first, from 3 November, and J&T Express from 9 November; one batch on 9 November covers Naqel, J&T and Albanian Post within two minutes. The same set also impersonates Jordan Post and Islandwide, a courier in Puerto Rico, with the same "we could not verify your address" story.

The sites show their page only to a phone browser at the exact link sent; automated visitors get an empty "not found". The Jordan Post pages add a fake CAPTCHA, and the app code runs about 40 checks for automation tools before it connects. Decoded, the app is a live relay: card details reach an operator as they are typed, and the operator can then ask the victim for the code their bank sends, the card PIN or approval in the banking app. The gate value is shared at the same time with look-alikes in at least eight other countries, and with Aramex and Emirates Post look-alikes in the UAE. The pages carry no Google, Meta or other tracking tags and no site icon. Google Safe Browsing flags 11 of the 15 sites, mostly one to three weeks after registration, but still treated the link in SMS 1 as safe on 28 November. SMS 3 arrived on 10 November, the day after its domain was registered; the registry has since suspended five of the six early-November domains, including that one. The UAE lures moved from the Naqel Express brand (SMS on 10 November) to J&T Express (SMS in the week of 23 November).

Update, 29 November. A fourth lure, sent on 27 November from a Gmail address, used the name of **Jeebly** and the same "missing building or villa number" story. Its site was registered three hours earlier and sits behind Cloudflare's own human check; once past it, the app is the same kit, and our detection rule for the kit's engine matched the new build. Searching public scans from there found look-alikes of **Zajel** (six, from 28 October) and **Quiqup** (four, from 27 September) on the same registrar and, for Zajel, in the same registration batch as the Naqel and Aramex domains. The operator has therefore targeted at least seven UAE delivery brands since September. The live Zajel and Quiqup apps contain the same engine code, so the link rests on the code, not only on registration timing.

The behaviour and targets match the Lucid phishing-as-a-service platform described by PRODAFT in March 2025, which we assess with moderate confidence; a platform of this kind is rented to many criminal customers, so it says little about who sent these particular messages.

An ongoing risk. Because the messages travel over iMessage rather than the phone network, the protections UAE residents rely on for SMS do not apply to the message itself: operator spam filtering and the registered sender names that genuine businesses must use. Blocking a known bad website at the network still helps when the link is opened, but only once the site is known, and new sites appear every few days. Taking down a domain does not stop the next wave, which arrives from a new number under a new brand within days. Residents and authorities should treat delivery messages received by iMessage from unknown or foreign numbers as a standing threat, not a single campaign.

Ask Haris flags these messages as phishing with its rules alone: the look-alike domain (the real sites are `jtexpress[.]me` and `naqelexpress[.]com`), the throwaway domain ending, and the "reply to activate the link" instruction.

> **Assessment boundary.** Findings are based on three SMS messages submitted to Ask Haris: one received on 10 November 2026 and two during the week of 23 November, sender details as reported by the recipient, registration and DNS records collected on 2026-11-28, and saved public scan records from urlscan.io. On 28 November we requested the two J&T links and the related pages once as an automated visitor and once with an iPhone browser identity, from a UAE connection, and read the page and script files the server returned. We read and decoded the app's code without running it. We did not click the fake verification box, reply to the messages or enter any data, and we did not test from outside the UAE. On 29 November an analyst passed Cloudflare's human check on the Jeebly site by hand in a desktop browser; we read the files served and took screenshots without clicking or typing on the page. The Zajel and Quiqup app files were requested once each at their link paths with an iPhone identity and read as text, not run. The other Zajel and Quiqup sites come from public scans and registration records. The gate values come from saved pages in public urlscan.io scans. By 28 November the SMS 3 domain had been suspended and could not be requested. Lucid sites can be limited to visitors from chosen countries, so the J&T sites may show nothing to visitors outside the UAE; we did not test this. Google Safe Browsing status comes from Google's public Transparency Report. The Naqel Express and Islandwide pages come from public scans. We have no confirmed victims or losses. The total number of courier submissions to Ask Haris is not included in this version.

Key Judgments

ID	Judgment	Confidence	Basis
KJ1	One SMS script is sent under at least two courier brands, J&T Express and Naqel Express, with its wording varied on purpose, most likely to get past spam filters that look for repeated text.	**High**	The same tracking digits (7845120390) in all three SMS and on a fake Naqel page; word-for-word activation instructions; SMS 3 repeats SMS 2 sentence for sentence with the brand changed.
KJ2	The UAE courier sites belong to infrastructure that also impersonates postal services in Jordan, Albania and Puerto Rico, which points to one operator or one shared service.	**Moderate**	All 15 domains at one registrar; four registration batches, one of which covers Naqel, J&T and Albanian Post within two minutes; one Cloudflare name-server pair on six of the ten domains still active; the J&T page headers and the Jordan Post gate carried the same server value at the same moment; the same stylesheet on the Naqel, Albanian Post and Islandwide pages.
KJ3	The sites are built to hide from scanners and takedown teams, and this partly works: the link in SMS 1 is still not flagged by Google Safe Browsing, although 11 of the 15 sites are.	**High**	An automated visitor gets an empty 404 at every path; an iPhone browser gets the app. The app checks for automation tools; the Jordan Post pages sit behind a fake CAPTCHA.
KJ4	The end goal is payment-card theft through a small "redelivery" fee, with an operator steering each victim live through the bank's own security checks: one-time codes by SMS or email, the card PIN, or approval in the banking app.	**High**	Decoded app code: every form field is sent to the server as it is typed; the server can reject a card ("Use another card") or switch the victim to an SMS-code, email-code, card-PIN, bank-app approval or Amex security-code page; an unattended mode moves on by itself when no operator is watching. Read from the code; we did not see these screens live.
KJ5	The operator sends lures within about a day of registering a domain, then rotates to new domains and brands as old ones are suspended. New ones will keep appearing every few days.	**Moderate**	SMS 3 arrived on 10 November, the day after its domain was registered (9 November, 10:19 UTC). The Jeebly lure was sent on 27 November at about 08:07 UTC, about three hours after its domain was registered (04:59 UTC). UAE courier domains were registered from 27 September (Quiqup) to 27 November (Jeebly), moving from brand to brand; five of the six early-November Naqel and J&T domains are now suspended by the registry.
KJ6	The lures reach UAE phones by iMessage from foreign numbers, outside UAE telecom SMS filtering and sender registration. This is an ongoing risk: the same channel will carry the next brand and the next set of domains, and only Apple can stop the sending accounts.	**High**	The recipient reports iMessage delivery from a US (+1) number for J&T and a Philippine (+63) number for Naqel. Neither number appears in public scam reports; such accounts are often stolen or bought, so the numbers may not belong to the operator.
KJ7	The sites are consistent with Lucid, a phishing-as-a-service platform that PRODAFT attributes to Chinese-speaking operators.	**Moderate**	Matches PRODAFT's description of Lucid: iMessage delivery with "reply Y", per-site device filtering that hides pages from computers, an optional verification page, an empty icon setting, a redelivery fee and a live victim panel; Lucid's target list includes Jordan Post and Aramex UAE. Other platforms such as Darcula and Lighthouse share several of these traits, and we have not seen the operator panel.
KJ8	The sites run on a shared server system that, in the same weeks, also served look-alikes of postal, courier, tax and parking services in at least eight other countries, and of Aramex and Emirates Post in the UAE.	**Moderate**	The verification gate carries a server value that changes every one to two weeks and is the same, at the same time, across unrelated brands: 70 public scans from July to November 2026 show five values in turn, the last two shared by the Jordan Post sites with Australia Post, Canada's Intelcom and Polish-language lures. The J&T page header carries the current value. Shows a shared system, not a single customer.
KJ9	The same operator targets at least seven UAE delivery brands, J&T Express, Naqel Express, Aramex, Emirates Post, Zajel, Quiqup and Jeebly, and has done so since at least 27 September 2026. It now also hides sites behind Cloudflare's real human check.	**High**	On 3 November two Zajel domains, the first Naqel domain, the Aramex domain and a third Zajel domain were registered within 4 minutes 43 seconds at one registrar, the last 16 seconds after the Aramex one on the same name servers. The live Jeebly app (29 November) contains three of the six engine strings in our YARA rule, the same bot detector and the same live-link settings. On 29 November the live Zajel and Quiqup apps, requested at their link paths with a phone identity, contained the same three engine strings and the same visitor-ID and `shopHost` settings, and shared a code file. Quiqup domains were registered on 27 September and 8 October.

High: direct evidence with few plausible alternatives. **Moderate:** credible evidence with collection gaps. **Low:** limited or indirect evidence.

Attack Lifecycle

1. Register domains Random six-letter .cfd domains are registered in batches and put behind Cloudflare, with a brand name as the subdomain.	**2. Send the lure** An iMessage from a foreign number says a J&T Express or Naqel Express parcel arrives today but the Emirate in the address is missing.	**3. Activate the link** The text asks the person to reply "Y" and reopen the message, which makes a blocked link clickable, or to paste it into Safari.
4. Open the country path The link opens an exact path such as /ae, /ae.en or /com. The bare domain shows "not found", or a human check stands in front: a fake CAPTCHA, or since late November Cloudflare's real one.	**5. Update the address** A fake tracking page says delivery failed and asks for the address (seen on the Naqel Express and Islandwide sites).	**6. Take the card** A payment page asks for a small AED fee and the card details, which reach the operator as they are typed.
7. Pass the bank check While a fake "processing" screen runs, the operator can ask for the code the bank sends, the card PIN or approval in the banking app. Read from the code, not observed live.		

Technical Analysis

The lure

The three messages tell the same story. SMS 2, sent about two weeks after SMS 3, is the same text with the brand changed from Naqel Express to J&T Express, sentence for sentence. The fields that stay fixed are the most useful for detection.

Element	SMS 1 (J&T, week of 23 Nov)	SMS 2 (J&T, week of 23 Nov)	SMS 3 (Naqel, 10 Nov)
Brand and subject	`J&T Express – Parcel Delivery Information`	`J&T Express – Here's How Far Your Shipment Has Come`	`NAQEL Express – Parcel Tracking Progress Notification`
Tracking number	`JT7845120390AE`	`JT7845120390AE` (same)	`NQ7845120390` (same digits)
Pretext	Emirate missing from the delivery address	Same, reworded	Same as SMS 2, brand changed
Pressure	Parcel held at a collection point; collection code "expires in 5 minutes"	Parcel placed in a collection locker; redelivery "within 2 hours"	Same as SMS 2 ("NAQEL collection locker")
Link	`hxxps://jtexpress.zrkgyg[.]cfd/ae.en`	`hxxps://jtexpress.iwixbs[.]cfd/ae`	`hxxps://naqelexpress.vsjwmm[.]cfd/ae`
Delivered by	iMessage from `+1 (412) 296-07xx` (United States)	iMessage from the same number	iMessage from `+63 907 105 47xx` (Philippines)
Activation text	Reply "Y", close and reopen the SMS; else paste into Safari	Identical, word for word	Identical, word for word
Punctuation	Chinese full-width brackets （） in English text	Same	Same

Activating the link. iPhones disable links in messages from senders who are not in the contacts and have not been replied to. Asking the reader to reply "Y" and reopen the message gets around that protection; the fallback asks them to paste the link into Safari. This instruction appears word for word in all three messages and is the strongest single sign of this campaign.

Writing. All three messages use Chinese full-width brackets around an English sentence, which suggests a template prepared with Chinese input settings. On its own this is not evidence of who sends them.

SMS 1

```
J&T Express – Parcel Delivery Information

Your shipment, JT7845120390AE, is arranged for delivery
between 14:00 and 18:00 today. However, further
verification of the specified Emirate may be necessary.

Please check your delivery address and provide the missing
Emirate so we can proceed with your delivery.

Update your Emirate here:

hxxps://jtexpress.zrkgyg[.]cfd/ae.en

 (Simply reply with “Y”, then close the SMS and reopen it to
activate the link. If the link still does not work, please
copy it and paste it directly into Safari.)

• If you do not update your delivery address, your parcel
will be held at the designated J&T Express collection
point.

 •Your collection code is [code] and will expire in 5
minutes.

 •If you would prefer home delivery, please update your
delivery address.

J&T Express Delivery Team
```

SMS 2

```
J&T Express – Here’s How Far Your Shipment Has Come

Today between 14:00 and 18:00 marks the scheduled arrival
for JT7845120390AE, though supplementary details regarding
the Emirate may be needed.

Please check your delivery address and provide the missing
Emirate so we can proceed with your delivery.

Update your Emirate here:

hxxps://jtexpress.iwixbs[.]cfd/ae

 (Simply reply with “Y”, then close the SMS and reopen it to
activate the link. If the link still does not work, please
copy it and paste it directly into Safari.)

We identified missing Emirate information in your delivery
address, and your parcel has been placed in a designated
J&T Express  collection locker.

To request home delivery, please update your address.
Delivery will be rescheduled within 2 hours, subject to
confirmation.

J&T Express Delivery Team
```

SMS 3

```
NAQEL Express – Parcel Tracking Progress Notification

For package NQ7845120390, arrival at the destination is
expected today from 14:00 to 18:00, with additional Emirate
information potentially required.

Please check your delivery address and provide the missing
Emirate so we can proceed with your delivery.

Update your Emirate here:

hxxps://naqelexpress.vsjwmm[.]cfd/ae

 (Simply reply with “Y”, then close the SMS and reopen it to
activate the link. If the link still does not work, please
copy it and paste it directly into Safari.)

We identified missing Emirate information in your delivery
address, and your parcel has been placed in a designated
NAQEL collection locker.

To request home delivery, please update your address.
Delivery will be rescheduled within 2 hours, subject to
confirmation.

NAQEL EXPRESS Delivery Team
```

Access controls

The sites decide what to show based on who is asking. The same links returned different results to an automated visitor and to an iPhone browser, both from a UAE home connection:

Request	Automated visitor	iPhone browser
Bare domain	404, empty	404, empty
Link path (/ae, /ae.en)	302, then 404, empty	200: app loader, 2.7 KB
Jordan Post path (/jo/)	not tested	Fake "I am not a robot" box

The empty 404 comes from Cloudflare's edge rather than from a web server, which points to filtering rules running at Cloudflare before the page is served. Scanners, security tools and takedown teams that do not present a phone browser see nothing.

Inside the app

The page is a loader for a Vue application of about 1.3 MB whose text is hidden in scrambled lists. We recovered the text by decoding those lists with our own copy of the decoding routine and reading the code; none of the kit's code was run. The decoded scripts and lists are kept with the evidence.

Two layers. A brand layer holds the J&T texts, the fee and the screens; a shared engine underneath holds the page router, the live link, the bank-check pages and a bot detector. The engine names its pages in Chinese, for example `手机验证页` ("phone verification page") and `运通CVV验证页` ("Amex CVV verification page"), and its error messages are Chinese. It also carries fields for markets other than the UAE: US Social Security number, date of birth, bank account and branch number, province and postal code.

Reused templates. The J&T layer was copied from J&T Express Saudi Arabia: its footer gives the Riyadh head-office address, the Saudi customer-service number and `jtexpress.sa.com` e-mail addresses. The Arabic version still contains text for **Zajel**, a UAE courier ("Zajel branch or pickup point", Zajel customer service), and the language setting is stored as `ae_zajel_post_lang`. So the same people, or the same template seller, has built or holds a Zajel look-alike for the UAE. A sample delivery date, "Thu 24 Sept", suggests the layer was made in September 2026.

The screens. Tracking page with waybill `JT7845120390AE`, "Out for delivery, Dubai" and "We couldn't verify your building or apartment details"; an address form with the seven Emirates, area, building, flat and landmark; a date and a delivery window in UAE time; a payment page for a "redelivery fee" of AED 15.00; then a "processing" screen that steps through ten messages such as "Checking fraud risk..." and "Awaiting bank approval..." with "SSL encryption" and "PCI-DSS certified" badges. The success page carries a badge reading "Design preview · No transaction processed", in English and Arabic, shown only after the card details have been taken.

The live link. Unless the bot detector fires, the page opens a Socket.IO connection to the same site at the path `/console`, passing a visitor ID and a `shopHost` value, and reconnects without limit. Every message is encrypted with AES using a key written into the code. Each form field is sent as it is typed, in batches every 0.3 seconds, and the server is told the moment the victim starts typing a card number. The server sends the site settings and then commands that decide what the victim sees next:

Server status	What the victim sees
`rejected`	Card error; the victim goes back to the payment page or sees "Use another card"
`rejectedCode`	The code entered is wrong; ask again
`waitVerificationPhone`, `waitVerificationEmail`	Show a page asking for the one-time code the bank has just sent by SMS or email, with the last digits of the number
`waitVerificationPin`	Show a page asking for the card PIN
`waitVerificationApp`	Show "open your bank's app and approve the request", with "I've approved in app"
`waitVerificationExpressCvv`	Ask for the security code printed on the front of an American Express card
`waitVerificationCustomCode`	Show a page whose text, fields and images the operator writes on the spot
`completed`	Show "Payment successful"; the browser is marked as done and later visits go elsewhere

This is a live relay. While the victim waits on the "processing" screen, the operator can use the card at a real merchant or bank and, when the bank challenges, show the matching page so the victim hands over the code, PIN or app approval. If no one is watching, an **unattended mode** moves the victim on after a countdown (30 seconds by default). After "completed", the browser is marked as done and later visits are sent to another address, so the page cannot easily be opened again for checking.

The bot detector. A module named `HeadlessDetector` runs about 40 checks: automation-tool traces (WebDriver, Selenium, Puppeteer, Playwright, Chrome DevTools Protocol), software graphics renderers typical of virtual machines, canvas, audio, font and emoji fingerprints, a background-worker identity check, plugins, languages, cameras and microphones, battery and permissions. Above a score of 0.31 the visitor is treated as a spider: the page still draws, but the live link never opens, so a scanner never receives the site settings or reaches the operator. The phone-only display and the country allow-list are not in the page code; they run on the server or at Cloudflare.

Decoy labels. The page header carries tags claiming it is a high-security login page, and a 128-character hexadecimal value. At the time we requested them, the value was identical on all three live J&T sites and began with the same 16 characters as the Jordan Post gate value. Aramex look-alikes from October carry the same tags and a different value, so it changes over time.

The fake CAPTCHA. The Jordan Post pages show a box styled as hCaptcha with "I am not a robot" in Arabic. It loads nothing from hCaptcha and has no site key. Clicking it reloads the page with `?__eat=` and a 16-character value printed in the page itself; a comment in Chinese calls it the query value added "after verification passes". The server checks it: in public scans, links carrying the current value received the app, while links carrying an older value received the box again. Because the value is in the page, the box is no test at all for a person; it only stops scanners that do not click. We did not click it.

The fake tracking page. Public scans show the screen that follows on the Naqel Express sites: a copied Naqel tracking page for waybill `NQ7845120390`, the same number as in SMS 3, with Dubai on the map and the message "We couldn't verify your villa, building or apartment number" above an "Update delivery address" button (Figure 1). Islandwide pages show the same layout for Puerto Rico. By 28 November one of them, `islandwide.qavzqa[.]cfd`, showed Cloudflare's own "Suspected Phishing" warning instead.

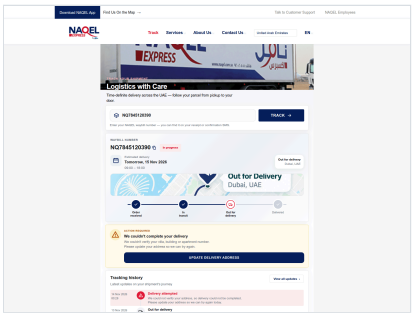

Figure 1. `naqelexpress.sdasjb[.]cfd/ae/` from a public urlscan.io scan on 13 November 2026, 21:00 UTC. The waybill matches the tracking digits in all three SMS. SHA-256 ec84f04a8fda0deb40f9e3ade8aab8c3278da60bf68643b6be95139213b3456a

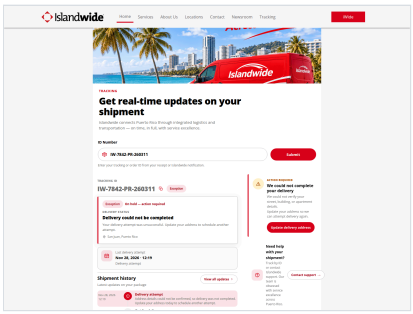

Figure 2. `islandwide.qavzqa[.]cfd/com/` from a public urlscan.io scan on 28 November 2026, 16:47 UTC: the same template for a Puerto Rico courier. SHA-256 7d42688d71eb431994a15e9b91689f1e7deb418388ef9422478a95e01b54e061

Why the delivery channel matters

Ordinary SMS to UAE numbers passes through the mobile operators, where spam filters, blocking of messages that carry known bad links, and the registration of business sender names apply. iMessage messages are carried over the internet by Apple between Apple devices, so none of those controls see them. The sender appears as a plain phone number or email address, here from the United States and the Philippines, and a reply turns on the links that iPhones otherwise disable for unknown senders. Phishing kits of this kind are built around that gap. Messages cost the sender nothing per message, and accounts and numbers are replaced as they are reported. The protections that remain are on the device and with Apple: the "Report Junk" option, the unknown-sender filter in Messages settings, Apple disabling the sending accounts, and the recipient recognising the lure.

No tracking tags or site icon. None of the pages or app files contain Google Tag Manager, Google Analytics or Google Ads identifiers, or Meta, TikTok or other trackers. The only analytics is Cloudflare's own, with a different token on each site. Every site leaves its icon empty and returns "not found" for `/favicon.ico`. The app carries copied J&T images, including one named `favicon-jt.png`, under scrambled file names. These sites therefore offer no advertising or analytics account to trace.

Infrastructure Analysis

All 15 domains below use the `.cfd` ending, were registered through Aceville Pte. Ltd. and used Cloudflare. Five have since been suspended by the registry and have no name servers.

Host	Impersonates	Registered (UTC)	Name servers	Source
`naqelexpress.hpgynn[.]cfd`	Naqel Express (UAE)	2026-11-03 08:40	kehlani / rommy	Public scan, 10 Nov (fake tracking page)
`naqelexpress.cvhhms[.]cfd`	Naqel Express (UAE)	2026-11-07 11:13	none: suspended by the registry	Public scan, 10 Nov (fake tracking page)
`naqelexpress.clcizn[.]cfd`	Naqel Express (UAE)	2026-11-07 11:13	none: suspended by the registry	Public scan, 11 Nov (fake tracking page)
`naqelexpress.sdasjb[.]cfd`	Naqel Express (UAE)	2026-11-09 10:17	none: suspended by the registry	Public scan, 13 Nov (fake tracking page)
`naqelexpress.vsjwmm[.]cfd`	Naqel Express (UAE)	2026-11-09 10:19	none: suspended by the registry	SMS 3, received 10 Nov, submitted to Ask Haris
`jtexpress.cozojm[.]cfd`	J&T Express (UAE)	2026-11-09 10:19	pedro / zara	Public scan, 24 Nov (root returns 404)
`postashqiptare.etpmie[.]cfd`	Albanian Post	2026-11-09 10:19	none: suspended by the registry	Public scan, 13 Nov (fake tracking page)
`jtexpress.zrkgyg[.]cfd`	J&T Express (UAE)	2026-11-13 05:06	pedro / zara	SMS 1, submitted by an Ask Haris user
`jordanpost.ddeviw[.]cfd`	Jordan Post	2026-11-23 11:50	pedro / zara	Public scan, 27 Nov (verification gate)
`jordanpost.miffyh[.]cfd`	Jordan Post	2026-11-23 11:51	pedro / zara	Public scan, 27 Nov (verification gate)
`jtexpress.iwixbs[.]cfd`	J&T Express (UAE)	2026-11-23 11:52	pedro / zara	SMS 2, submitted by an Ask Haris user
`jtexpress.ujvjzr[.]cfd`	J&T Express	2026-11-23 11:52	daphne / garrett	Public scan, 25 Nov (root returns 404)
`islandwide.qavzqa[.]cfd`	Islandwide (Puerto Rico courier)	2026-11-27 10:47	chance / jocelyn	Public scan, 28 Nov (fake tracking page)
`islandwide.nnzkwf[.]cfd`	Islandwide (Puerto Rico courier)	2026-11-27 10:48	chance / jocelyn	Public scan, 28 Nov (fake tracking page)
`jordanpost.zzmrtw[.]cfd`	Jordan Post	2026-11-27 10:48	pedro / zara	Public scan, 28 Nov (verification gate)

Four batches stand out:

- **7 November:** two Naqel Express domains 29 seconds apart (11:13:14 and 11:13:43 UTC).
- **9 November:** Naqel Express (10:17:46 and 10:19:37), J&T Express (10:19:47) and Albanian Post (10:19:51): four domains for three brands within 2 minutes 5 seconds.
- **23 November:** Jordan Post and J&T Express, four domains within 2 minutes 14 seconds (11:50:37 to 11:52:51).
- **27 November:** Islandwide and Jordan Post, three domains within 69 seconds.

Six of the ten domains still active share the name servers `pedro` and `zara`. Cloudflare gives each account a fixed pair, so this usually means one account, although unrelated accounts can receive the same pair. Batches span more than one pair, which suggests one operator using several Cloudflare accounts.

Shared stylesheet. The kit's base stylesheet (`BR8QKs6I-ayaf.css` , 48,826 bytes) is identical on the Naqel Express, Albanian Post and Islandwide pages. Public scan records show the same file on 90 numbered `*.eu.cc` sites imitating the EasyPark parking app, hosted on Tencent and Alibaba Cloud. That shows the same tooling, not the same operator, and those sites are not counted in this report.

One server system behind many countries

The value the gate expects is not tied to a site or a brand. We read it from 70 public urlscan.io scans of "Verification" gates between July and November 2026. We then confirmed it live: on 29 November five sites under three brands served the same new value in the same minute. At any one time the same value is served by unrelated brands in several countries, and it changes every one to two weeks. Two or more values were sometimes in use at once, so there may be several servers or customer groups. The values that touch this campaign:

Gate value	Seen	Scans	Brands served with it
`7836a9f8e94dbc4b`	10 to 21 Oct	4	Aramex UAE (page header), Lithuanian-language lures
`c89335ce213891f5`	23 Oct to 3 Nov	28	**Emirates Post EMX (UAE)**, Norway tax office, Mexico treasury, Canada Intelcom, Spain social security, Japanese-language sites
`2571bdeb534f3e20`	7 to 18 Nov	7	**Aramex (UAE)**, Canada Intelcom, Bulgaria interior ministry
`34f31b78f2ce7899`	18 to 28 Nov	21	**Jordan Post** (3 sites), Australia Post (4), Canada Intelcom, Polish-language lures
`84cc720ce2c8bd75`	28 Nov, from 19:48 UTC	ours	**Jordan Post** gate and **J&T Express** page header, requested by us
`43f172ad85757f52`	29 Nov, 05:19 UTC	ours	**Aramex** gate, two **Jordan Post** gates and both **J&T Express** SMS links, all in the same minute

This ties the J&T, Naqel and Jordan Post sites to a shared system that also served postal, courier, tax and government lures for Australia, Canada, Norway, Mexico, Spain and Bulgaria, and Lithuanian-, Polish- and Japanese-language lures. It is the strongest technical link in this report between the UAE lures and the wider operation. It shows a shared platform, not one customer.

More UAE brands. Two more UAE look-alikes use the same gate and the same `/ae.en/` path as SMS 1: `emx.kixkn[.]cfd` for Emirates Post (EMX), registered on 2 November, and `aramex.yaoixi[.]cfd` for Aramex, registered on 3 November at 08:43:55 UTC, 3 minutes 20 seconds after the first Naqel domain (08:40:35), at the same registrar. Google does not flag either. On 29 November at 05:19 UTC the Aramex site was live behind the same fake CAPTCHA, serving the same gate value as both Jordan Post sites and both J&T links at that minute; the EMX site returned an empty 404 at every path we tried. Earlier Aramex look-alikes, `aramex.enjoyy[.]ink` and `aramex.itself[.]ink` (live 9 September to 10 October, another registrar), carry the same decoy tags and, on 10 October, the header value that the gate served from 11 to 21 October. So the UAE campaign covers at least Aramex, Emirates Post, Naqel Express and J&T Express, with a Zajel template in the code, from September to November 2026. These sites are not in the 15 counted above.

Hosting and cash-out

Hosting. Every UAE site sits behind Cloudflare's proxy, on four name-server pairs, so only Cloudflare addresses are visible; the live link to the operator also runs through Cloudflare on the same domain. We did not try to uncover the server behind Cloudflare. Sites on the same gate system that do not use Cloudflare (Polish-language, Canadian and Danish lures) show their servers directly, all on Tencent Cloud in Germany, mainland China and Hong Kong, and the parking-app lures sharing the kit stylesheet were on Tencent and Alibaba Cloud. The UAE sites' servers are therefore likely, but not shown, to be on the same providers; Cloudflare can confirm it from its own records. The site settings can also point the live link at a separate server (`backUrl`), so the server that collects victims' details need not be the one that serves the page.

No payment gateway. We read every way the app sends data out. There is exactly one: the encrypted live link. The only other network requests load animation files and images. The code names no payment provider, card processor or outside address, posts no form and sends no tracking beacon. The "payment page" charges nothing: it collects the card details and passes them to the operator, and the "processing" screen only buys time. The money is taken elsewhere, by the operator using the card with the victim's one-time code, PIN or in-app approval relayed in real time. Where that happens is visible only to card issuers and card networks, which is why banks are the place to stop the loss.

The campaign widens: Zajel, Quiqup and Jeebly

Searching public scans for UAE courier names placed in front of throwaway domains found three more brands on the same infrastructure. All of them were registered through Aceville except the Jeebly domains.

Zajel. Six look-alikes such as `zajel.ccvqn[.]cfd`, registered in two batches, on 28 October (three in 1 minute 44 seconds) and on 3 November. The 3 November batch places Zajel, Naqel and Aramex in the same five minutes, with the last Zajel domain 16 seconds after the Aramex one and on the same Cloudflare name servers. The Zajel template we found in the J&T app code (above) was therefore put to use.

3 Nov (UTC)	Host	Name servers
08:39:28	`zajel.ctuvjv[.]cfd`	kehlani / rommy
08:39:57	`zajel.fixaci[.]cfd`	kehlani / rommy
08:40:35	`naqelexpress.hpgynn[.]cfd`	see table above
08:43:55	`aramex.yaoixi[.]cfd`	julio / nia
08:44:11	`zajel.zpxzdq[.]cfd`	julio / nia

Quiqup. Four look-alikes such as `quiqup.fzpfw[.]cfd`: three registered within 92 seconds on 27 September and one on 8 October, scanned in mid-November at `/ae.en`. These are the earliest UAE domains we have found, so the UAE activity began at least five weeks before the Naqel lures.

All ten Zajel and Quiqup domains still resolved on 29 November and returned an empty 404 to an automated visitor, the same hiding behaviour as the J&T sites. The bare domains returned 404 even to a phone identity, but the link paths did not: `zajel.ctuvjv[.]cfd/ae.en`, `zajel.zpxzdq[.]cfd/ae.en` and `quiqup.fzpfw[.]cfd/com` served the app. There was no human check in front of these older sites. We downloaded the files and read them as text without running them. Both apps use the same page shell and loading spinner as Jeebly and the same long hex value in a keywords header tag. The Quiqup page also carries decoy header tags that label it a secure login page. Both load one shared code file, `DeosFkVQ`, which holds the Socket.IO client. Both engine files carry the same three scrambled engine strings as Jeebly, with the same visitor-ID and `shopHost` settings, and contain the card-security-code fields, dirham amounts and the Emirates list. The Zajel stylesheet has the same base name as the Naqel kit stylesheet. So Zajel and Quiqup are tied to the operation by the code itself, not only by registration timing. `quiqup.dqrdb[.]cfd` no longer connected, and we did not request the other three Zajel or two Quiqup domains.

Jeebly. On 27 November an iMessage from a Gmail address, not a phone number, told an Ask Haris user that a "Jeebly Central Hub" could not deliver because the building name and apartment or villa number were missing, and linked to `jeebly.qrsx[.]top/com`. The text is longer and more formal than the J&T script and has no "reply Y" instruction, but tells the same story. Its domain, a four-letter `.top` name, was registered through Dominet (HK) about three hours before the message; a second one, `jeebly.mtkc[.]top`, followed 75 minutes later and was suspended within two days. Both sit behind **Cloudflare's own managed human check**, which scanners cannot pass, so no public scanner had captured the page. On 29 November an analyst passed the check by hand in a desktop browser; we then read the files the site served without clicking anything on the page or typing into it. The page is a fake Jeebly "Delivery Unsuccessful" screen with three steps, Failed, Address and Pay, a made-up tracking number and Jeebly's real support details (Figure 3). Its engine file carries three of the six scrambled strings in our engine rule, the same `HeadlessDetector` and the same Socket.IO settings with a visitor ID and `shopHost`, and the separate live-link file contains the Socket.IO client and AES code. Only the build ending (`-yzjz`) and the decoder's name differ. So the engine rule below, written from the J&T build, matched a new build of the kit for a new brand.

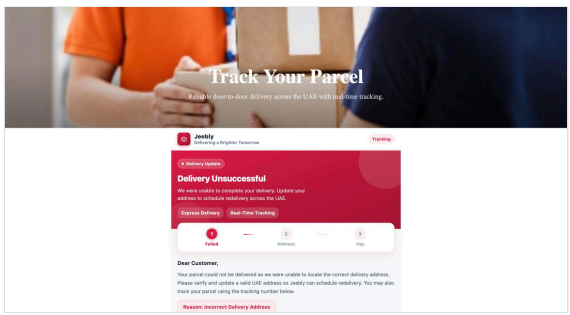

Figure 3. `jeebly.qrsx[.]top/com/` on 29 November 2026, after Cloudflare's human check was passed by hand. SHA-256 e6df11122c9cbdfa32464447b5d1e37c92e50c33466255c2cd5f0dfb74f32748

A real human check in front of the site is a shift. The fake CAPTCHA stopped scanners that do not click; Cloudflare's check stops almost all of them, and it is Cloudflare's own service. It also explains why browsers give no warning: Google Safe Browsing cannot see the page either.

A separate kit for Emirates Post. `www.emiratespost[.]co`, registered in April 2026 through another registrar, showed on 28 November a personalised "Action required: Delivery was unsuccessful" page whose only button is "Continue with Apple". It aims at Apple ID logins rather than card details. It shares the delivery theme and Cloudflare but nothing technical with the kit above. Stolen Apple IDs are one way to obtain the iMessage accounts that send these lures, but we have no evidence that links the two.

The international picture

For defenders outside the UAE, the UAE lures are one market of a larger operation. Three strands, from strongest to weakest:

- **The shared gate (strong).** The gate value rotates on one schedule across look-alikes of Jordan Post, Australia Post, Canada's Intelcom, the Norwegian tax office, the Mexican treasury, Spanish social security and the Bulgarian interior ministry, and Lithuanian-, Polish- and Japanese-language lures (table above). The same infrastructure also registered Albanian Post and Islandwide (Puerto Rico) domains in the UAE batches, and its stylesheet appears on 90 EasyPark parking look-alikes.
- **A different kit, the same method.** A separate kit imitating Aramex Australia, seen on about 30 sites in late November, also streams card details, the bank's one-time code and the card PIN to an operator in real time, with operator messages in Chinese. Its code shares nothing with the kit in this report, and we found no technical link to this operator. It shows that the live relay of bank checks has spread beyond one kit.
- **Same pattern, not linked.** In the same days public scans show DHL look-alikes on numbered `*.eu[.]cc` domains on Tencent Cloud and FedEx look-alikes on random `.shop` domains, several already behind Cloudflare's phishing warning. They use the brand-as-subdomain pattern but we found nothing technical tying them to this kit. By 29 November the FedEx host served only a default server page and the DHL host did not connect.

What carries across countries and kits is the method, not the domains or the code: a courier or government brand as the subdomain of a fresh cheap domain, a per-country path, an empty response to scanners, a human check in front, and a live relay of the bank's checks behind it. The detection patterns below are written for that method.

Each brand lives on its own subdomain and each country on its own path: `/ae` for the UAE, `/jo/` for Jordan, `/al/` for Albania, `/com/` for Puerto Rico. This is consistent with a phishing kit sold or shared as a service, in which case several customers may use the same tooling. The pattern is consistent with parcel-redelivery campaigns that UAE and international researchers have reported since 2023.

Platform assessment: Lucid

We assess with moderate confidence that these sites run on Lucid, a phishing-as-a-service platform described by PRODAFT (CATALYST report, 24 March 2025). PRODAFT attributes Lucid to Chinese-speaking operators who rent it to customers on weekly licences. The points of agreement:

- **Delivery:** PRODAFT describes delivery over iMessage and RCS to avoid SMS filtering, using a "please reply with Y" request to get around iMessage link restrictions. The lures here arrived by iMessage with the same request.
- **Site settings:** PRODAFT's sample Lucid site configuration has switches that block computers and allow iPhones and Android phones, a country allow-list, an optional verification page, a fee and card-rejection messages, and an empty icon field. Here, automated visitors get an empty 404 while an iPhone gets the app; the Jordan Post pages open behind a verification box; the app has an AED fee; and every site has an empty icon.
- **Live panel:** PRODAFT describes a real-time panel showing each victim's visit, a card that can be rejected and verification steps. The app here streams every field to the server as it is typed and takes commands to reject a card or ask for a bank code, PIN or app approval.
- **Scale:** PRODAFT describes one platform serving many brands in many countries. The gate value here is shared at the same time by look-alikes in at least eight other countries.
- **Targets:** PRODAFT's list of Lucid templates includes Jordan Post and Aramex in the UAE. J&T Express UAE, Naqel Express and Islandwide are not on that March 2025 list, which would make them newer templates.

The assessment is moderate rather than high because other Chinese-language platforms, such as Darcula and Lighthouse, share most of these traits, and we have not seen the operator panel or a Lucid-specific file. A rented platform also means the customer who sent these messages may differ from the platform's operators.

Google Safe Browsing

Google's public Transparency Report, checked on 28 and 29 November 2026, lists 11 of the 15 sites as deceptive. The early Naqel Express sites were flagged one to three weeks after registration. The link in SMS 1 is not among them: Google last checked it on 16 November and found nothing, consistent with the empty page served to automated visitors. "Last updated" is when Google last changed or checked a site's status, so for flagged sites it is close to, but not exactly, when Google started warning.

Host	Registered	Google status	Last updated (UTC)
`naqelexpress.hpgynn[.]cfd`	2026-11-03	Deceptive	2026-11-22 21:09
`naqelexpress.cvhhms[.]cfd`	2026-11-07	Deceptive	2026-11-21 13:16
`naqelexpress.clcizn[.]cfd`	2026-11-07	Deceptive	2026-11-27 11:34
`naqelexpress.sdasjb[.]cfd`	2026-11-09	Deceptive	2026-11-24 16:54
`naqelexpress.vsjwmm[.]cfd`	2026-11-09	Deceptive	2026-11-27 23:57
`jtexpress.cozojm[.]cfd`	2026-11-09	Deceptive	2026-11-27 01:41
`postashqiptare.etpmie[.]cfd`	2026-11-09	Deceptive	2026-11-27 05:38
`jtexpress.zrkgyg[.]cfd`	2026-11-13	Not flagged	2026-11-16 06:18
`jordanpost.ddeviw[.]cfd`	2026-11-23	Deceptive	2026-11-27 11:50
`jordanpost.miffyh[.]cfd`	2026-11-23	Not flagged	2026-11-27 17:54
`jtexpress.iwixbs[.]cfd`	2026-11-23	Deceptive	not given
`jtexpress.ujvjzr[.]cfd`	2026-11-23	Not flagged	2026-11-27 01:08
`islandwide.qavzqa[.]cfd`	2026-11-27	Not flagged	2026-11-28 18:06
`islandwide.nnzkwf[.]cfd`	2026-11-27	Deceptive	2026-11-28 16:54
`jordanpost.zzmrtw[.]cfd`	2026-11-27	Some pages deceptive	2026-11-28 02:59

MITRE ATT&CK Mapping

Tactic	Technique	ID	Evidence	Confidence
Resource Development	Acquire Infrastructure: Domains	T1583.001	Batch registrations at one registrar, seconds apart.	**High**
Resource Development	Obtain Capabilities: Tool	T1588.002	Phishing kit consistent with the Lucid phishing-as-a-service platform.	**Moderate**
Resource Development	Stage Capabilities: Link Target	T1608.005	Brand subdomains with per-country paths (/ae, /jo/, /com/).	**High**
Initial Access (Mobile)	Phishing	T1660	SMS lures impersonating J&T Express and Naqel Express sent to UAE phones.	**High**
Defense Evasion	Impersonation	T1656	J&T Express, Naqel Express, Aramex, Emirates Post, Zajel, Quiqup, Jeebly, Jordan Post, Albanian Post and Islandwide names and branding.	**High**
Defense Evasion	Hide Infrastructure	T1665	Cloudflare proxy; 404 on the root; verification gate before content; Cloudflare's managed human check on the Jeebly site.	**Moderate**
Defense Evasion	Virtualization/Sandbox Evasion	T1497	Checks for automation tools and mismatched browser identity; empty 404 for non-phone visitors; fake CAPTCHA gate.	**High**
Defense Evasion	Obfuscated Files or Information	T1027	String-array obfuscation of the app code; random value in the page header.	**High**
Execution	User Execution: Malicious Link	T1204.001	Victim is told to reply "Y" or paste the link into Safari.	**High**

Tactic	Technique	ID	Evidence	Confidence
Collection	Input Capture: Web Portal Capture	T1056.003	Each form field, including the card number, is sent to the server as it is typed.	**High**
Credential Access	Multi-Factor Authentication Interception	T1111	Operator-triggered pages ask for the bank's one-time code (SMS or email), the card PIN or approval in the banking app.	**High**

Indicators of Compromise

Indicators are defanged. Cloudflare addresses are excluded because they are shared with many unrelated sites.

Senders

Partly masked here, because these may be stolen accounts that belong to real people. Full details are in the TLP:AMBER annex for Apple, telecom regulators and other teams that can act on them.

Indicator	Type	Context
`+1 (412) 296-07xx`	Phone number (iMessage)	Sender of both J&T Express lures; may be a stolen or bought account
`+63 907 105 47xx`	Phone number (iMessage)	Sender of the Naqel Express lure (10 November); may be a stolen or bought account
`f********06@gmail[.]com`	Email address (iMessage)	Sender of the Jeebly lure (27 November); likely a throwaway or stolen Apple account

Network

Indicator	Type	Context
`naqelexpress.hpgynn[.]cfd`	Domain	Naqel Express (UAE); registered 2026-11-03
`naqelexpress.cvhhms[.]cfd`	Domain	Naqel Express (UAE); registered 2026-11-07
`naqelexpress.clcizn[.]cfd`	Domain	Naqel Express (UAE); registered 2026-11-07
`naqelexpress.sdasjb[.]cfd`	Domain	Naqel Express (UAE); registered 2026-11-09
`naqelexpress.vsjwmm[.]cfd`	Domain	Naqel Express (UAE); registered 2026-11-09
`jtexpress.cozojm[.]cfd`	Domain	J&T Express (UAE); registered 2026-11-09
`postashqiptare.etpmie[.]cfd`	Domain	Albanian Post; registered 2026-11-09
`jtexpress.zrkgyg[.]cfd`	Domain	J&T Express (UAE); registered 2026-11-13
`jordanpost.ddeviw[.]cfd`	Domain	Jordan Post; registered 2026-11-23
`jordanpost.miffyh[.]cfd`	Domain	Jordan Post; registered 2026-11-23
`jtexpress.iwixbs[.]cfd`	Domain	J&T Express (UAE); registered 2026-11-23
`jtexpress.ujvjzr[.]cfd`	Domain	J&T Express; registered 2026-11-23
`islandwide.qavzqa[.]cfd`	Domain	Islandwide (Puerto Rico courier); registered 2026-11-27
`islandwide.nnzkwf[.]cfd`	Domain	Islandwide (Puerto Rico courier); registered 2026-11-27
`jordanpost.zzmrtw[.]cfd`	Domain	Jordan Post; registered 2026-11-27
`hxxps://jtexpress.zrkgyg[.]cfd/ae.en`	URL	SMS 1 link
`hxxps://jtexpress.iwixbs[.]cfd/ae`	URL	SMS 2 link

Indicator	Type	Context
`hxxps://naqelexpress.vsjwmm[.]cfd/ae`	URL	SMS 3 link
`emx.kixkn[.]cfd`	Domain	Emirates Post (EMX) look-alike, path /ae.en/; registered 2026-11-02; same registrar and gate; empty 404 at every path on 29 Nov; not flagged by Google
`aramex.yaoixi[.]cfd`	Domain	Aramex look-alike, path /ae.en/; registered 2026-11-03, 3 min 20 s after the first Naqel domain; live behind the fake CAPTCHA on 29 Nov; not flagged by Google
`aramex.enjoyy[.]ink`, `aramex.itself[.]ink`	Domain	Aramex look-alikes, path /ae/, live 9 Sep to 10 Oct 2026; same decoy header tags and rotating header value
`hxxps://jeebly.qrsx[.]top/com`	URL	Jeebly lure link, 27 Nov; domain registered 2026-11-27 04:59 UTC (Dominet (HK)); live behind Cloudflare's human check on 29 Nov
`jeebly.mtkc[.]top`	Domain	Jeebly look-alike, path /com; registered 2026-11-27 06:14 UTC, same registrar; suspended by the registry by 29 Nov
`zajel.ccvqn[.]cfd`, `zajel.ffxbg[.]cfd`, `zajel.oofrq[.]cfd`	Domain	Zajel look-alikes registered 2026-10-28 09:15 to 09:17 UTC (Aceville); still resolving on 29 Nov, empty 404 to scanners
`zajel.ctuvjv[.]cfd`, `zajel.fixaci[.]cfd`, `zajel.zpxzdq[.]cfd`	Domain	Zajel look-alikes registered 2026-11-03 08:39 to 08:44 UTC, in one batch with the first Naqel domain and the Aramex domain
`quiqup.fzpfw[.]cfd`, `quiqup.rxmrf[.]cfd`, `quiqup.nqhnx[.]cfd`	Domain	Quiqup look-alikes registered 2026-09-27 10:12 to 10:14 UTC (Aceville), the earliest UAE domains found; still resolving on 29 Nov
`quiqup.dqrdb[.]cfd`	Domain	Quiqup look-alike, path /ae.en; registered 2026-10-08 (Aceville)
`www.emiratespost[.]co`	Domain	Separate kit: Emirates Post "delivery unsuccessful" page asking for an Apple ID login; registered 2026-04-05 (Gname)

Message artifacts

Artifact	Context
`?__eat=` followed by 16 hex characters	Added by the fake CAPTCHA; the server checks it and the value changes every one to two weeks (84cc720ce2c8bd75 on 28 Nov from 19:48 UTC; 34f31b78f2ce7899 from 18 to 28 Nov)
`验证通过后追加的 query 值，如 ?__eat=token`	Chinese comment in the gate page ("query value appended after verification passes")
`/console` with query `uuid` and `shopHost`	Socket.IO path for the live link to the operator (websocket, then polling)
`changleField`, `userSiteConfig`, `waitVerificationApp`	Event and status names in the live link (misspelling in the original)
`_SyyqA0IJJU`, `_8CxKQNqkdE`, `ae_zajel_post_lang`	Browser-storage names: "already completed" flag, saved form, language key from a Zajel template
`Design preview · No transaction processed`	Badge on the success page, shown after the card is taken
`assets/yde_Cy_h-dmsl.js` (SHA-256 069cae04968bf423f601466046520a4247503e6808b29a10cc131afba6aa35f5)	Main app file on both SMS links
`-dmsl.js`, `-ayaf.js`, `-yzjz.js`, `-sheq.js`	File-name endings of the app builds (J&T; Islandwide; Jeebly; Zajel). The Quiqup build has none
`DeosFkVQ` (SHA-256 3511c7416bc179848fdafd3cd22620d4a2e502abbf82067e4371a6951a586f18 as `DeosFkVQ-sheq.js` on Zajel; f7b817017c88ae6ebf054534e323dbc9d14fe46e6bb7b4c7a90f59896e381a89 as `DeosFkVQ.js` on Quiqup)	Shared code file, with the Socket.IO client, on the Zajel and Quiqup apps
`Bxu1vWPI-sheq.js` (SHA-256 660d6a4a11822dd8e9290426e54838b6d6f67259d9bc90c73ff70a73e630506a), `BSjQXFho.js` (SHA-256 7090ee574c41a0dc0970bbb318f74a6e656dc868a1b27d7cd4abef1160117cda)	Engine files of the Zajel and Quiqup apps on 29 Nov; both match the engine rule
`<meta name="keywords" content="` + a long hex value	Header tag on the Jeebly, Zajel and Quiqup pages; one 128-character value on both the Zajel and Quiqup sites on 29 Nov
`/apps/AU_PACK_05/`, `__verify_submit` + `verify_code`	A different kit, not this one: file path and check request of an Aramex Australia look-alike kit with the same live relay (see The international picture)
`<meta name="purpose" content="login">`	Decoy header tag on the J&T pages
`Simply reply with “Y”, then close the SMS and reopen it to activate the link`	Activation text, identical in all three SMS
`please copy it and paste it directly into Safari`	Targets iPhone users
`provide the missing Emirate`	UAE-specific pretext
`JT7845120390AE`, `NQ7845120390`	Fake tracking numbers: the same digits under each brand, in the SMS and on the fake pages
`BR8QKs6I-ayaf.css` (SHA-256 2d8add36af9ca956c1a1e2bc3879d83786271e70ade39551d9450303b269d1b3)	Kit stylesheet on the Naqel Express, Albanian Post and Islandwide pages; the same base name, `BR8QKs6I-sheq.css`, on the Zajel page

Artifact	Context
`（ ）` (U+FF08, U+FF09)	Full-width brackets inside English SMS text
`-yzjz.js`, `-yzjz.css` (`DujpD-ns-yzjz.js` engine, `8-wRPtlu-yzjz.js` live link)	File-name ending of the Jeebly build; the engine decoder is named `_yzjb` in place of `_dmsb`
`<meta name="keywords" content="` + 80 hex characters	Decoy header value on the Jeebly page
`Jeebly Central Hub | Delivery Exception Notice`	Opening of the Jeebly lure; fake tracking number `JB2024839174658203`

Detection and Hunting

- Block and hunt for hosts matching `^(jtexpress|naqelexpress|aramex|emx|zajel|quiqup|jeebly|jordanpost|postashqiptare|islandwide)\.[a-z]{4,6}\.(cfd|top)$`, and more generally any courier, postal or government brand as the only subdomain label of a domain registered in the last 30 days.
- The operator now also places sites behind Cloudflare's real human check. A scanner that cannot pass it sees only the challenge page; treat a brand subdomain on a fresh domain that serves only a challenge as suspicious, and ask Cloudflare to review it.
- Treat a checkbox branded as Cloudflare's on a server not behind Cloudflare as a phishing gate.
- Hunt for the tracking digits `7845120390` in SMS and in page content.
- In SMS filtering, match the activation text ("reply with “Y”, then close the SMS and reopen it to activate the link") and "paste it directly into Safari" rather than the reworded body.
- Flag English SMS containing full-width brackets (U+FF08, U+FF09) together with a link.
- Scan the exact paths `/ae` and `/ae.en` with a mobile browser profile, not the bare domain and not a desktop or bot profile: anything else gets an empty 404.
- Hunt for URLs with `?__eat=` and 16 hex characters, pages titled "Verification" that contain the Chinese comment above, and the decoy header tags. The gate value changes every one to two weeks, so match the pattern, not one value.
- On networks and in browser telemetry, look for Socket.IO traffic to `/console/?uuid=…&shopHost=…&EIO=4` on newly registered domains: it means a victim has the page open with the live link running.
- In script content, match the kit's event names listed in the indicators; they survive brand and domain changes. The kit's fixed encryption keys and an engine rule for its scrambled code are in a TLP:AMBER annex for defenders, available on request.
- Treat a page styled as hCaptcha that loads no hCaptcha script as a phishing gate.

```
rule AskHaris_UAE_Courier_Smishing_2026_11 {
  strings:
    $act = "reply with \u201cY\u201d, then close the SMS and reopen it to activate the link" nocase
    $saf = "paste it directly into Safari" nocase
    $emi = "missing Emirate" nocase
    $dom = /(jtexpress|naqelexpress)\.[a-z]{6}\.cfd/
  condition:
    $dom and ($act or $saf or $emi)
}

rule AskHaris_Courier_Kit_Gate_2026_11 {
  strings:
    $t = ""
    $c = "hcaptcha-container"
    $q = "__eat"
    $zh = { E9 AA 8C E8 AF 81 E9 80 9A E8 BF 87 E5 90 8E }  /* 验证通过后 */
  condition:
    $q and ($zh or ($t and $c))
}
```

A third rule, for the kit's scrambled engine code, matched the new Jeebly, Zajel and Quiqup builds. We share it, with the full sender details, in a TLP:AMBER annex with teams that can act on it, so that the operator cannot simply change those strings. For live traffic, use the network pattern above.

Mitigation Recommendations

Telecom operators and regulators

- These lures arrive by iMessage, which travels over the internet and bypasses operator SMS filtering and the UAE sender-ID rules. Raise the listed sender numbers and the message pattern with Apple, which can disable the accounts.
- Where the same text arrives as ordinary SMS, block messages containing the activation text and the listed domains; because the body is reworded, filter on the fixed instruction text and the domain pattern.
- Share the sender numbers with the US and Philippine telecom regulators (FCC, NTC) and carriers.

Apple

- Disable the listed iMessage senders and look for accounts sending the activation text to +971 numbers.
- Consider showing a warning on iMessage messages from unknown foreign senders that contain links and ask for a reply.

Regulators and public-awareness bodies

- Warn UAE residents that delivery messages received by iMessage from unknown or foreign numbers are not covered by operator spam filtering, and that genuine couriers do not ask them to reply to make a link work.
- Recommend the unknown-sender filter and the "Report Junk" option on iPhones.
- Raise the channel, not only the domains, with Apple: domain takedowns alone do not stop the next wave.

J&T Express, Naqel Express and other couriers

- Remind customers of the official sites, `jtexpress[.]me` and `naqelexpress[.]com`, and that the courier never asks them to reply to make a link work.
- Other UAE couriers should expect the same script under their name: the same system has already served Aramex, Emirates Post, Naqel Express, J&T Express, Zajel, Quiqup and Jeebly look-alikes.
- Watch for the brand as a subdomain on newly registered cheap domains, not only for look-alike domain names.

Banks and card issuers

- The kit relays the bank's own checks in real time: the one-time code sent by SMS or email, the card PIN and approval in the banking app. A small AED payment attempt followed within minutes by a larger payment, a new device or a request to add the card to a mobile wallet fits this pattern.
- Make one-time-code and in-app approval messages name the merchant and the action plainly, for example "to add your card to a wallet on a new device", so that a victim expecting a AED 15 delivery fee can see the mismatch.
- Tell customers that no delivery fee ever needs their card PIN, and that they should never approve a request in their banking app that they did not start themselves.

Registrars and hosting providers

- Suspend the listed domains, and review other registrations made by the same customer in the same minutes.
- Cloudflare: review the accounts behind the listed zones; scan the exact paths rather than the bare domains. The Jeebly zone uses Cloudflare's own human check to keep scanners out.
- Dominet (HK): the Jeebly domains.

Consumers

- Use "Report Junk" in Messages for these texts, and consider turning on the unknown-sender filter in Messages settings. Do not reply "Y" to a delivery message to make its link work. Track parcels only in the courier's own app or by typing its official address.
- If you entered card details, call your bank on the number on your card straight away.

Prepared by Ask Haris, a free UAE scam-checking service. Ask Haris is independent and does not act for J&T Express, Naqel Express, Aramex, Emirates Post, Zajel, Quiqup, Jeebly, DHL, FedEx, Jordan Post, Albanian Post, Islandwide or EasyPark. Those names appear because they were impersonated. TLP:CLEAR: disclosure is not limited. The indicators may be shared and reused freely.