CTM360®

FreeWatch

Smartwatch Giveaway Scam Impersonating Retail Banks

Analysis by CTM360

INDUSTRY Financial Services / Banking

COUNTRY All

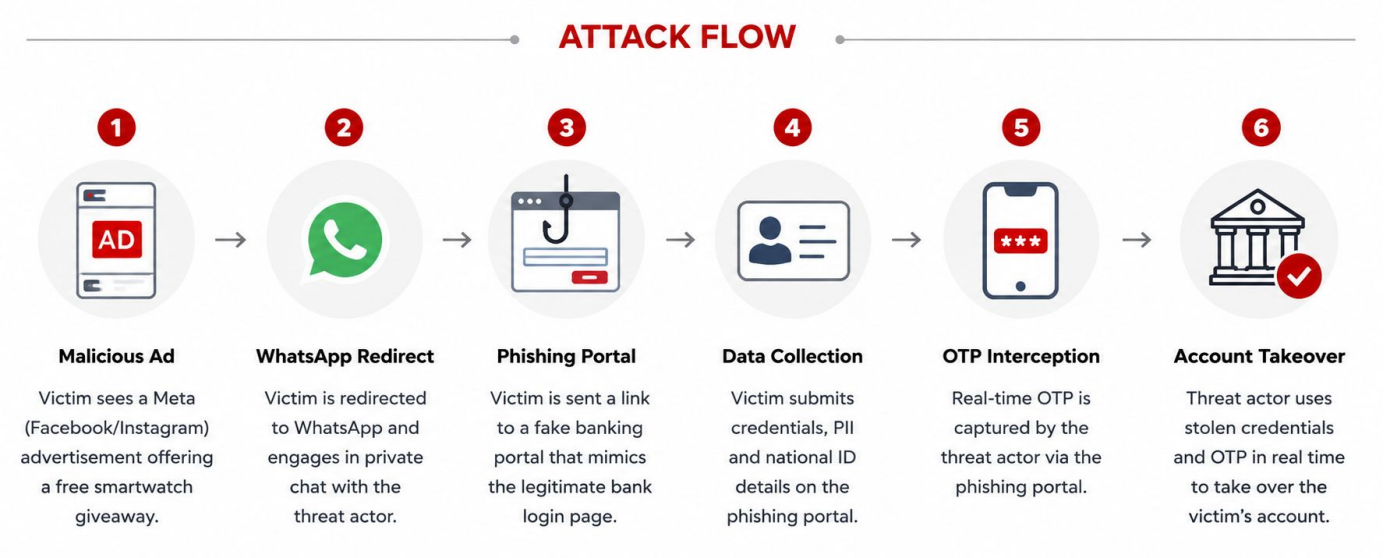
REGION MENA & GCC

DATE Jun, 2026

Overview

CTM360 identified a coordinated phishing campaign named **FreeWatch**, which targets retail banking customers across the MENA & GCC region through Meta (Facebook/Instagram) sponsored advertisements offering a **free smartwatch giveaway.** Victims are redirected to private messaging channels (Whatsapp) where threat actors collect PII and national identity data before delivering bank-lookalike phishing portals designed to harvest credentials and OTPs.

Static analysis of the campaign infrastructure confirms a real-time online banking account hijacking workflow. Captured data is transmitted to exposed cloud backends (Firebase, Telegram, Supabase, and Build-in Backend servers) in real time, where the threat actor manually approves submissions and replays the victim's OTP to authenticate against the legitimate banking portal and complete account takeover.



Key takeaway

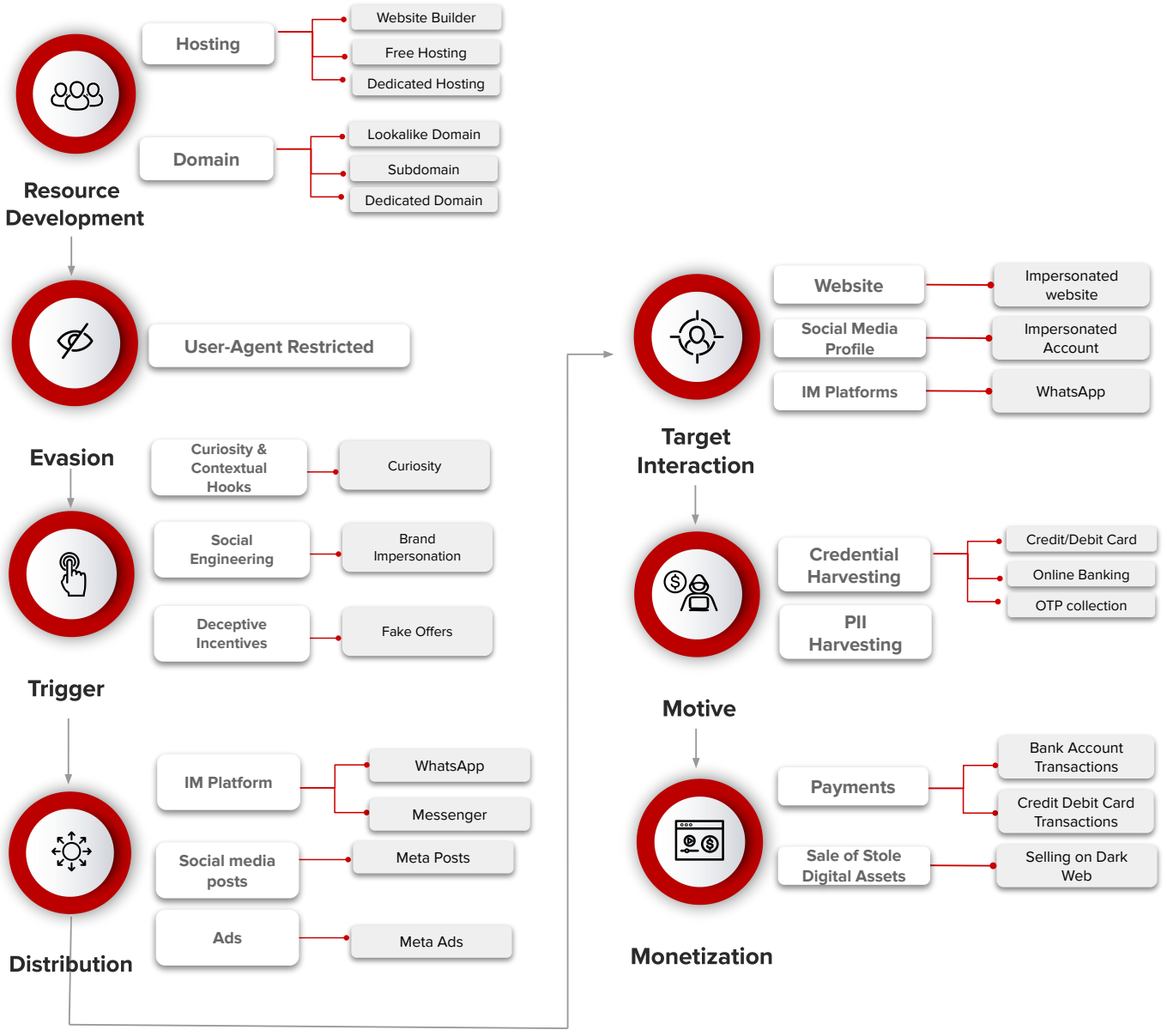
FreeWatch is a high-risk phishing campaign that leverages trusted brand impersonation, private-chat social engineering, and hackers exposed backend infrastructure to **hijack live online bank accounts.** The combination of paid social distribution, real-time threat actor involvement, and **OTP interception** enables threat actors to compromise accounts and perform unauthorised transactions in real time.

FRAUD STAGES:

CTM360 Fraud Navigator

CTM360 Fraud Navigator, inspired by the MITRE framework, is an analysis of the observed scams showing how the scammers navigate through different stages of the scam. Fraud Navigator is a tool that categorizes common scam techniques, providing insights into typical patterns of fraudulent activity. Built on the MITRE model, it identifies six key stages in a scam: resource development, trigger, distribution, target interaction, motive, and monetization.
There are commonly 2 phases in the scam, represented as Phase 1 (in white) & Phase 2 (in grey).

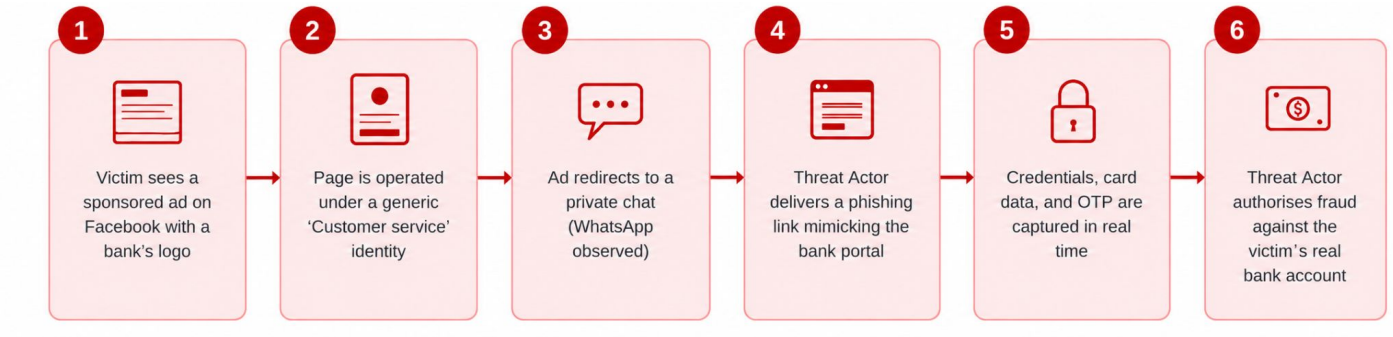
The Fraud Navigator framework has been mapped below to show how it aligns with each stage of the newly identified scam variants. This helps highlight how the scams evolve across both phases.



Fraud Navigator Framework - FreeWatch Campaign

Observed Attack Chain

The simplified flow below illustrates what occurs when a banking customer interacts with a FreeWatch sponsored advertisement.



Each stage of this workflow has been observed across multiple themed sub-campaigns leveraging the same or closely related threat actor infrastructure, including operations targeting other regional banking institutions. The attack chain begins with public-facing advertisements designed to establish legitimacy and impersonate trusted banking services. Victims are then redirected to WhatsApp conversations, effectively moving the interaction outside the visibility and moderation controls of the original platform before any sensitive information is collected. The phishing portal subsequently harvests banking credentials and OTP values, which are relayed in real time to facilitate real-time online banking account hijacking against the legitimate banking portal.

TARGETED REGIONS DISTRIBUTION

Displayed below is a summary of FreeWatch activity detected across regions. The campaign is concentrated in the MENA & GCC region, delivered in Arabic, and tailored to local banking brands.

Top Targeted Regions

REGION	DETECTION STATUS
Middle East & North Africa (MENA)	Primary target: Multiple confirmed detections across several banking brands indicate that MENA remains the campaign's primary area of focus. Activity was observed in Egypt, Jordan, Palestine, Tunisia, Iraq and Syria, reflecting a deliberate effort to target Arabic-speaking banking customers throughout the region.
Gulf Cooperation Council (GCC)	Secondary target: A limited number of confirmed detections were identified in Saudi Arabia, Kuwait, and Bahrain. While activity levels were lower than those observed across the broader MENA region, the detections confirm ongoing targeting of GCC banking users.

The findings are based on observations from the regions listed above. However, the campaign may extend to additional regions.

Distribution Channel Breakdown

CHANNEL	ROLE IN CAMPAIGN
Meta Sponsored Ads (Facebook & Instagram)	Primary distribution
Private chat (WhatsApp)	Handover from Meta ad; data harvesting
Typosquatted bank-lookalike domains	Dedicated phishing landing pages
GitHub Pages / Hostinger / Wix etc	Free hosting for disposable phishing pages

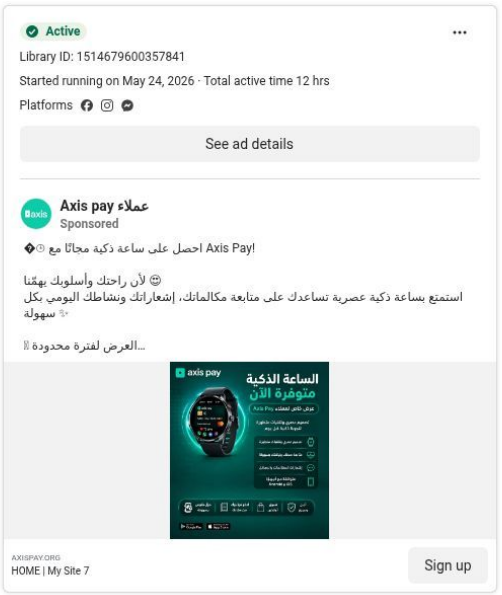
CTM360 OBSERVATIONS

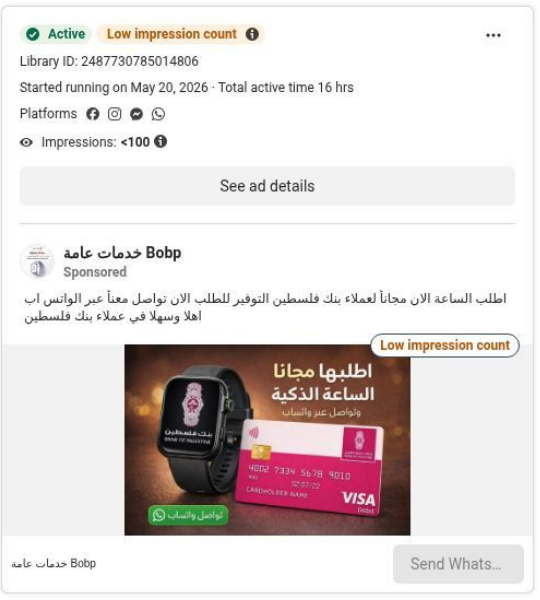
Sponsored Facebook Ads

Sponsored Facebook ads use the impersonated bank's logo, brand colours, and the templated free-smartwatch creative **"ساعة ذكية مجانية"** The advertisements are served from generically named pages that do not reference specific banks in their titles, likely to evade bank brand-protection detection and alerting systems.

Common Ad Characteristics Observed

- Each ad features the official logo of one specific targeted bank, with the same creative template recycled across different brands
- High-contrast Arabic call-to-action: **"ساعة ذكية مجانية"** (free smartwatch)
- Urgency-driven copy: **"Limited stock", "Exclusive for customers"**



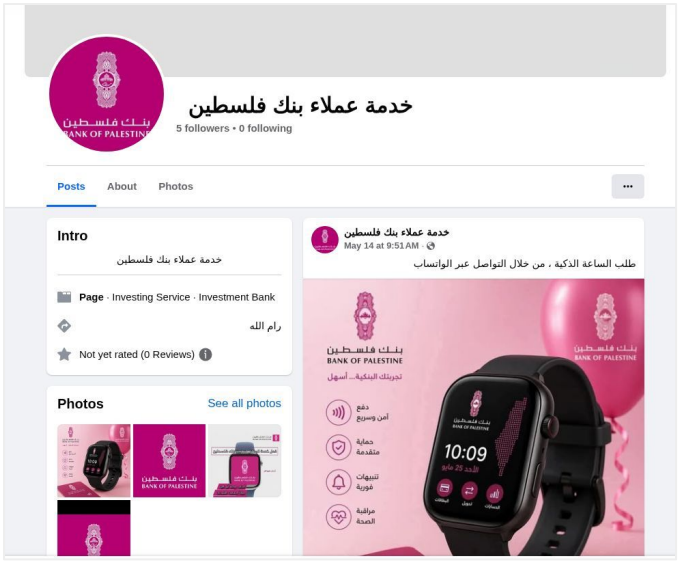


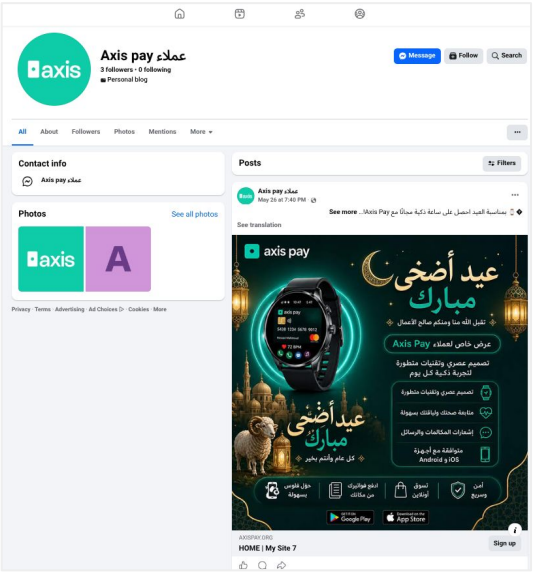
Threat Actor-Controlled Facebook Pages

The Threat actor-controlled Facebook pages are registered under generic, support themed names that offer bogus entity customer services. Each page is built specifically to host paid ad placements.

Page Characteristics

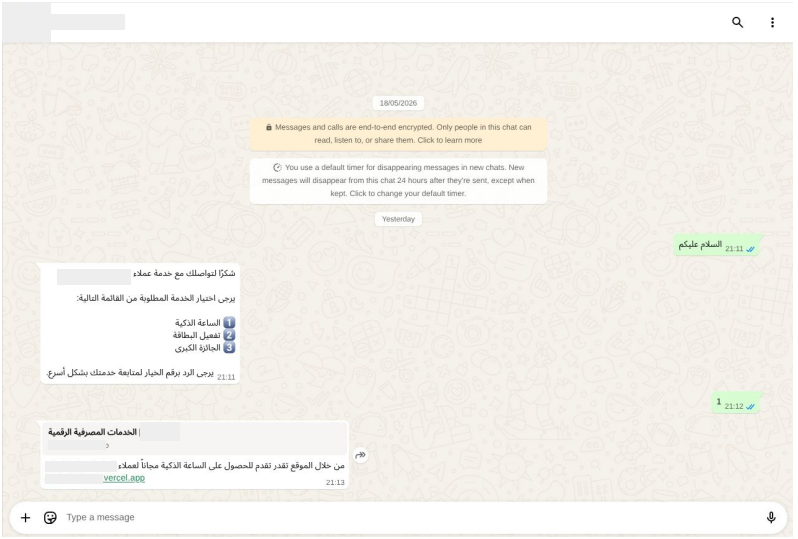
- Registered as a **“Financial services”** entity on Facebook
- Page name set to **“Customer service”** or **“خدمة العملاء”**
- Low follower count and minimal organic posting history
- Profile picture: direct bank logo, generic bank-style placeholder, or stylised logo from the targeted bank
- Same page often used to host ads impersonating multiple different banks in sequence





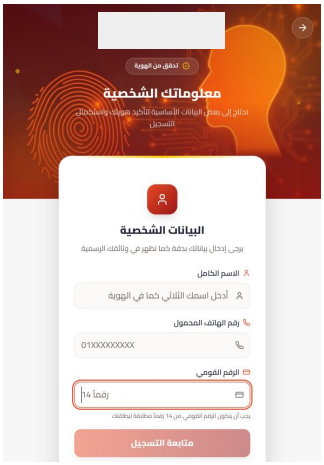
Private-Chat Handover

The Facebook ad's routes the victim out of the public ad surface into a private chat conversation controlled by the threat actor. WhatsApp is one observed delivery channel; the same flow works on other messaging platforms. The private chat serves a single purpose: the threat actor first confirms whether the victim is a bank customer and identifies what they are looking for, then shares the phishing link accordingly.



Phishing Portal

The threat actor delivers a phishing link styled as a “smartwatch request form”, as a request to get smarch watches. Within the process, the phishing page present an online banking webpage that replicates the bank’s visual identity and harvests credentials, card data, and OTPs.



Landing-Page Hosting Patterns Observed

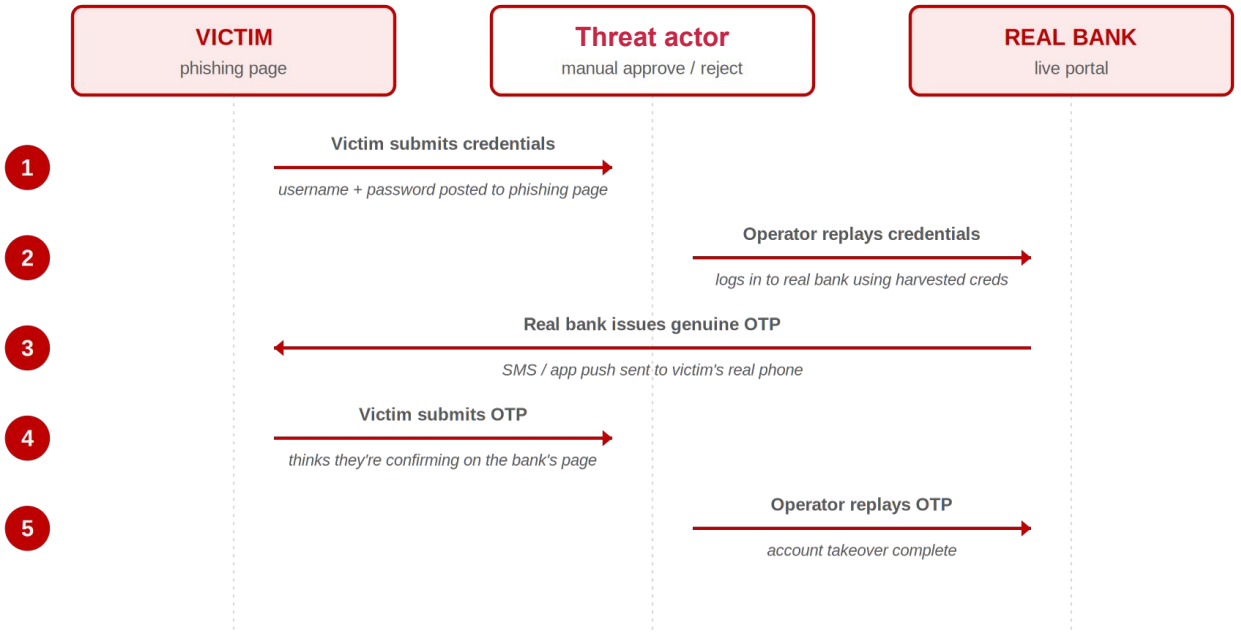
Host Type	Example	Number of Incident
Dedicated phishing domains	Typosquatted domains mimicking the target bank’s brand	**130+**
Wix free hosting	*.wixstudio.com, *.wixsite.com	**90+**
Lovable free hosting	*.lovable.app	**50+**
Hostinger free hosting	*.hostingersite.com	**60+**
Netlify free hosting	*.netlify.app	**25+**
Render free hosting	*.onrender.com	**15+**
Other free hosting	free[.]nf, ct[.]ws, rf[.]gd, web[.]app, manus.space, etc..	**45+**

Data Captured on the Phishing Page

- Full name
- National identifier
- Registered mobile number
- Online banking username and password
- OTP

Real Time Account Hijacking Flow

Analysis of the exfiltration backend reveals that this is not a passive harvest; a threat actor is actively interacting with each submission in real time, in the **online banking account hijacking** workflow. The diagram below illustrates how a single phishing session unfolds across three actors over five sequential steps.

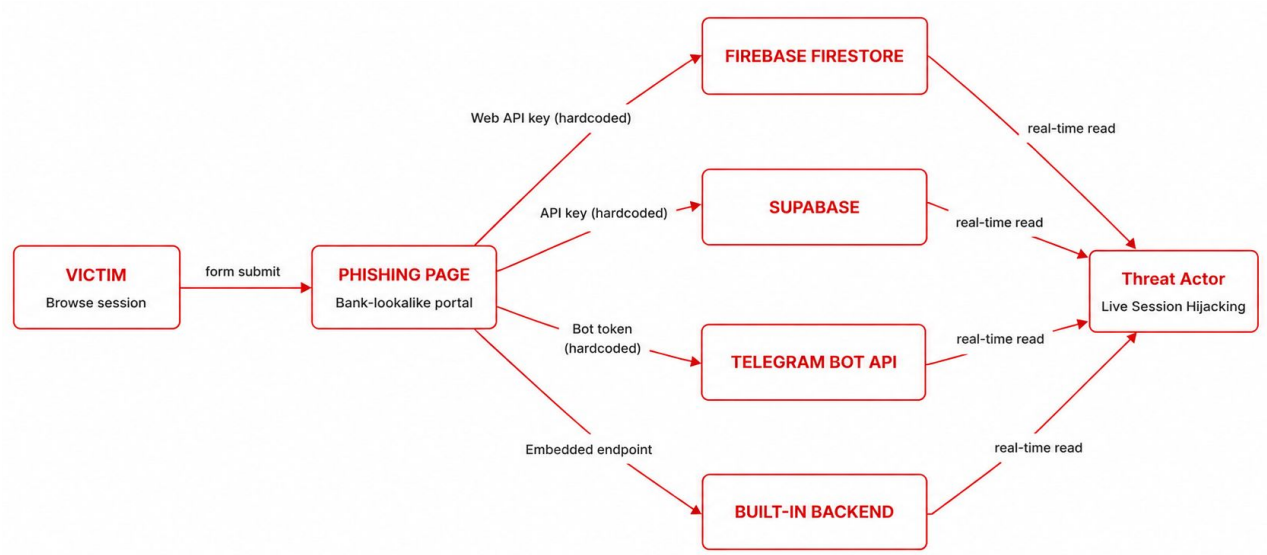


The phishing kit writes each victim submission to a database with a status field that cycles through a manual approval workflow. The Arabic-language status messages recovered from the backend confirm the threat actor's role at each step:

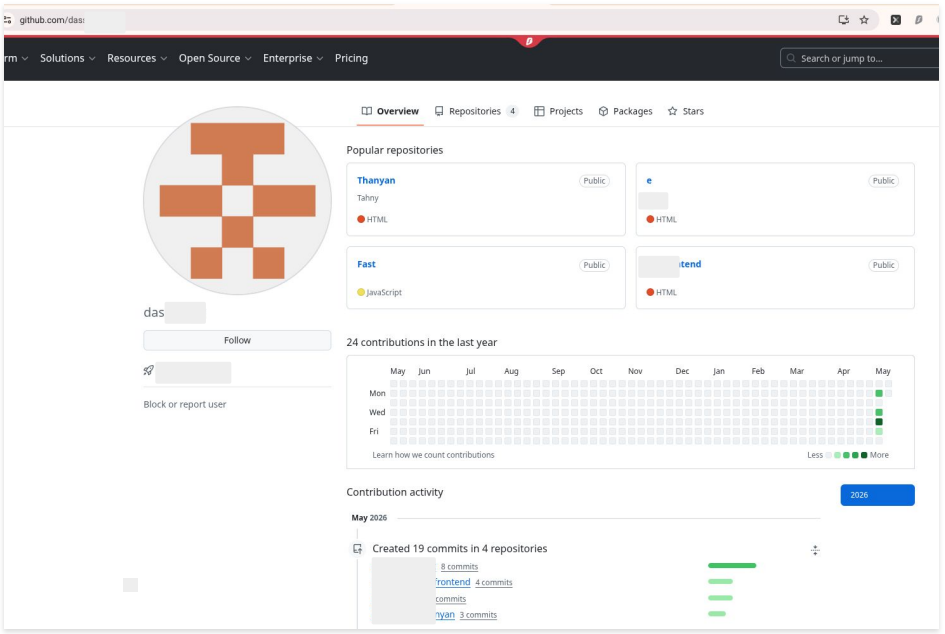
STEP	STATUS (AR)	THREAT ACTOR ACTION
1	تم تقديم بيانات الدخول - بانتظار الموافقة	Victim submits credentials; status set to "awaiting approval"
2	تمت الموافقة / تم رفض	Threat actor manually approves or rejects
3	أعاد المستخدم تقديم بيانات الدخول	If rejected, victim is forced to re-submit (harvesting fresh attempts)
4	تم تقديم رمز التحقق (XXXXXX)	Once credentials are approved, victim is prompted for OTP
5	تمت الموافقة على رمز التحقق	Threat actor approves the OTP and completes the real-bank login

Technical observation

Based on our review of the phishing kits used in this campaign, the observed kits employed exfiltration mechanisms that transmitted each victim's captured data to one or more of the following channels: **Firebase Firestore cloud database, Supabase cloud database, Telegram messaging bot, and built-in custom backend**. These channels are utilized through the phishing code to transmit/control the victim's data.



Github Repository Hosting Phishing Kits



The threat actor created a code repository account to manage multiple repositories, each hosting phishing content targeting different organizations. This approach allowed them to run several campaigns simultaneously while exploiting the platform's free hosting capabilities to minimize infrastructure costs.

The phishing sites were then deployed and made publicly accessible via GitHub Pages (github[.]io), eliminating the need for external hosting infrastructure and adding a layer of legitimacy to the malicious pages, increasing the likelihood of deceiving potential victims.

Threat Actor Infrastructure:

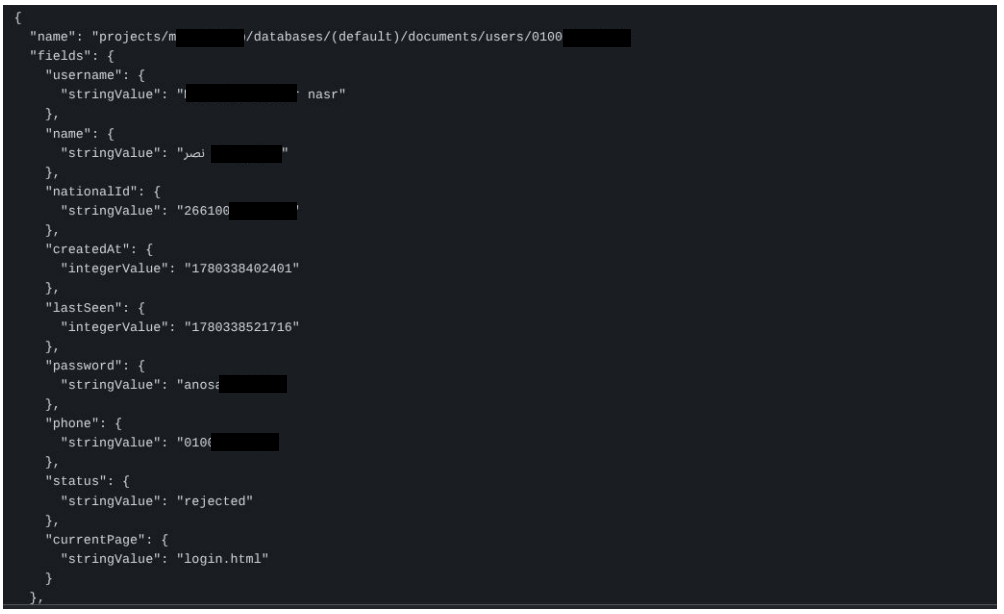
Firebase cloud database

One of the phishing kits employed Firebase as its primary data collection backend. Through analysis of the kit's code, we were able to observe all victim submissions that had been collected and stored in the database throughout the campaign.

Observations

The phishing kit utilized Firebase as its backend infrastructure. Victim data was passed to Firebase alongside the authentication flow, allowing us to observe the submissions as victims navigated through the malicious pages (Online banking page, OTP page, etc.).

Through our analysis, we observed that the collected records were structured to capture a comprehensive profile of each victim, including full name, national ID number, registered mobile number, online banking credentials, and OTP values harvested in real time confirming that the data was positioned for immediate exploitation, enabling the threat actor to perform account takeover and unauthorized financial transactions.

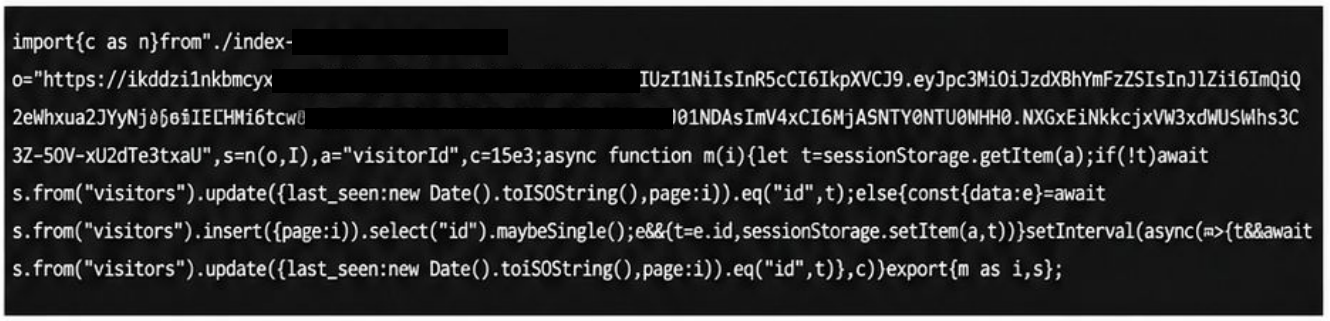


Supabase cloud database

A second cloud database backend was observed in a variant of the phishing kit, where Supabase was utilized as a structured data store, following the same exfiltration pattern observed throughout this campaign.

Observations

Further analysis of the phishing kit variants revealed Supabase as an additional cloud database backend, consistent with the exfiltration patterns identified across this campaign.



```
import{c as n}from"./index-[redacted]
o="https://ikddzi1nkbmcyx[redacted]IUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJzdXBhYmFzZSIsInJlZii6ImQiQ
2eWhxua2JYyNj[redacted]01NDAsImV4xCI6MjASNTY0NTU0WHH0.NXGxEiNkkcjxVW3xdWUSWhs3C
3Z-5OV-xU2dTe3txaU",s=n(o,I),a="visitorId",c=15e3;async function m(i){let t=sessionStorage.getItem(a);if(!t)await
s.from("visitors").update({last_seen:new Date().toISOString(),page:i)).eq("id",t);else{const{data:e}=await
s.from("visitors").insert({page:i)).select("id").maybeSingle();e&&(t=e.id,sessionStorage.setItem(a,t))}setInterval(async(m>{t&&await
s.from("visitors").update({last_seen:new Date().toiSOString(),page:i)).eq("id",t)},c))export{m as i,s};
```

Through our analysis of the Supabase backend, we observed the logs within the submissions table, where entries captured each victim's full name, phone number, email address, online banking username and password, and OTP codes - confirming active data collection targeting customers of the impersonated bank, with the harvested data positioned for real time utilization to hijack victims' online banking accounts.

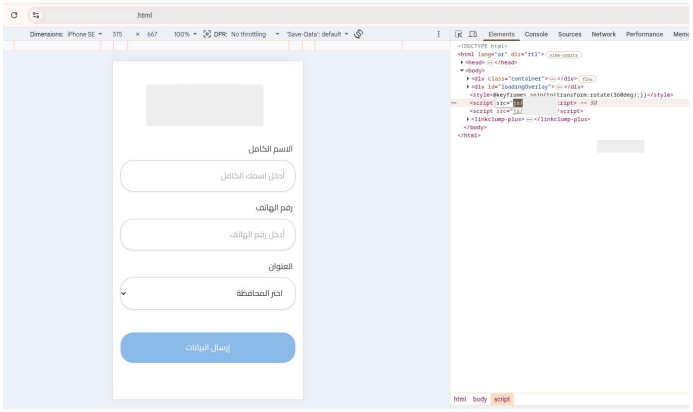

```
[{"id":"06853566-fc25-49e7-98f5-b29948c27515","created_at":"2026-06-
02T10:26:33.836344+00:00","full_name":"[redacted]","phone":"[redacted]","email":"ewfw
[redacted]f","request_type":"smart_watch","selected_watch":"watch4","status":"new","
page_source":"","username":"","login_password":"","login_status":"pending","redirec
t_page":"waitaccount.html","otp_code":""},
 {"id":"3649d273-300f-4650-9b2b-aea700af00da","created_at":"2026-05-
29T19:33:08.768185+00:00","full_name":"[redacted]","phone":"[redacted]","email":"bg[redacted]hg
h.com","request_type":"credit_card","selected_watch":"","status":"new","page_source
":"","username":"[redacted]","login_password":"[redacted]666","login_status":"pending","r
edirect_page":"waitaccount.html","otp_code":"550[redacted]"},
 {"id":"3a9b1f7b-b112-4788-92fd-eecd3cabdae7","created_at":"2026-05-
29T22:36:26.877297+00:00","full_name":"Test
User","phone":"[redacted]","email":"test@example.com","request_type":"credit_card",
"selected_watch[redacted]s":"new","page_source":"","username":"","login_password":
"","login_status[redacted]pending","redirect_page":"waitaccount.html","otp_code":""},
 {"id":"4b826337-9931-4a0f-8765-dfa0ddc7ae46","created_at":"2026-05-
29T22:39:45.363052+00:00","full_name":"Test
User","phone":"[redacted]","email":"test@example.com","request_type":"smart_watch"
,"selected_watch":"watch4","status":"new","page_source":"","username":"testuser","l
ogin_password":"password123","login_status":"login_pending","redirect_page":"waitac
count.html","otp_code":""},
```

Telegram Bot API

Another phishing kit used a Telegram bot as a real-time notification and exfiltration channel. A bot token and chat ID, enabling the threat actor to receive victim submissions as instant messages.

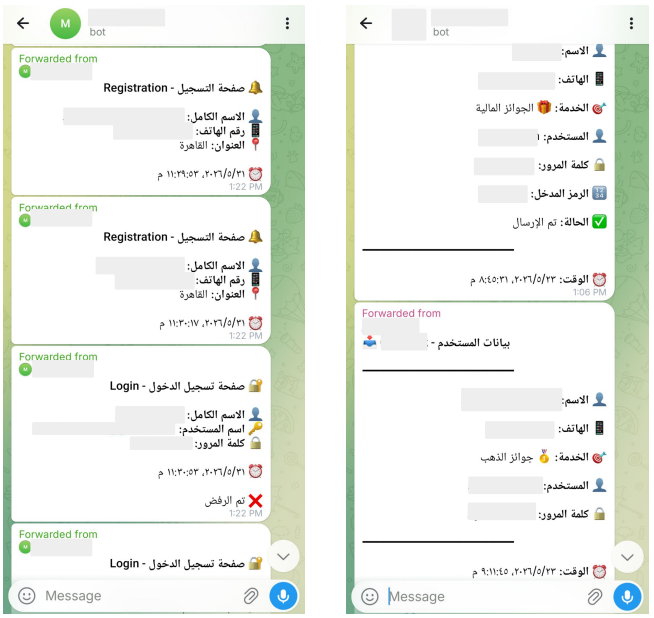
Credential Exposure

A Telegram bot token and associated chat ID were observed, These values were used by the kit to submit structured victim data to the Telegram Bot API following successful form submissions.



Threat Actor Exposure

Telegram bot tokens grant control over the bot, including the ability to read all messages it has [received.](#) Additional observation highlighted, that the bot presents the structure of the received data, and how the data being organized for the threat actor to conduct the online banking hijack.



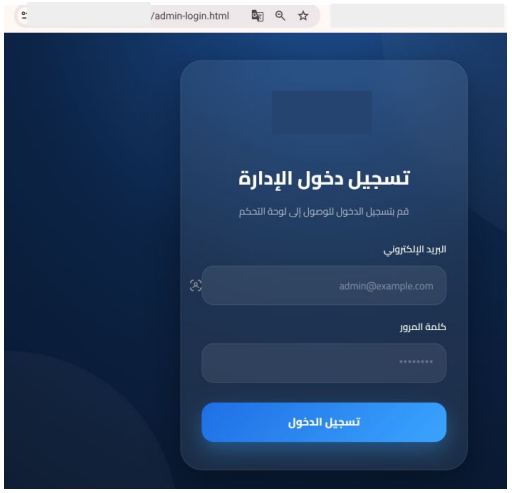
The bot's messages contained real-time victim submissions formatted as structured text messages. Each message included the victim's name, registered mobile number, online banking credentials, and OTP value, delivered by the phishing kit at each step of the real-time online banking account hijacking workflow as the threat actor manually progressed the session.

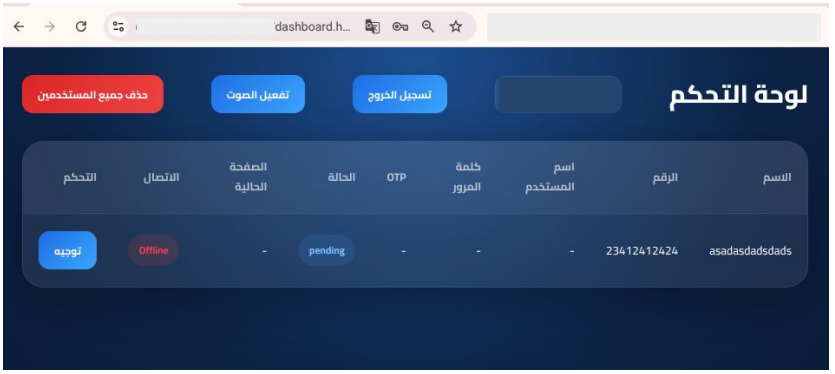
Built-in backend

A fourth exfiltration channel within an additional phishing kit variant that leveraged a backend endpoint. Unlike the other exfiltration methods, no third-party service was involved. The kit transmitted victim data directly to the proprietary endpoint.

Backend Portal

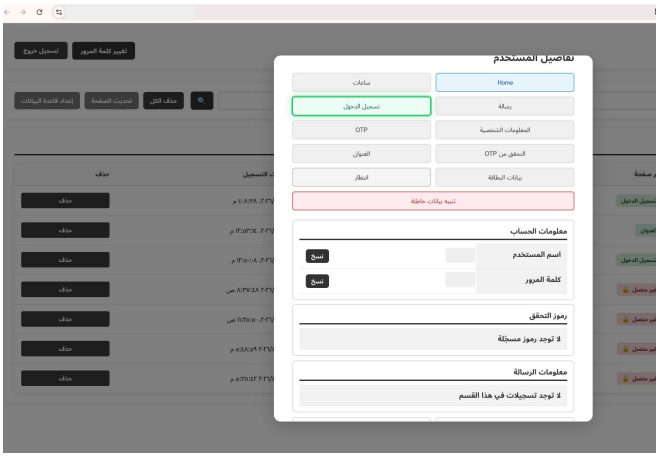
A backend endpoint URL was identified during the analysis. Further investigation observe that the associated domain functioned as both the phishing infrastructure and the administrative dashboard used by the threat actor to access and manage captured victim data.

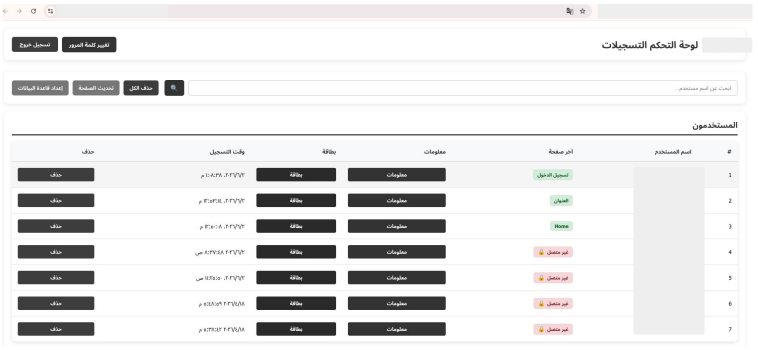




Threat Actor Exposure

The dashboard utilized by the threat actor to read a session flag from the browser and granted access if it was present. The admin panel allowed controlling victim's navigation to validate OTP, before disconnecting the victim from the phishing by presenting OTP failure and ask for another OTP, which from the threat actor's end will be another attempt to hijack the victim's account before OTP expires.





Records included full name, national ID, registered mobile number, online banking credentials, and OTP values captured across all sessions. The dashboard also revealed operational details of the campaign including submission timestamps and session metadata.

Motive & Monetisation

The defining risk of this campaign is **immediate, real-time account takeover.** As the threat actor authenticates against the live banking portal at the moment the victim submits their OTP, every successful submission corresponds to an active session within a genuine customer account. This enables **fund transfers, card purchases, and bill payment** authorisations to occur before the victim has left the phishing page.

The architecture of the operation compresses the conventional phishing kill chain into **a single sitting**. Data capture and resulting fraud constitute one event rather than two, removing the staging window typically exploited by post-compromise monitoring. Captured credentials retain limited residual value beyond the live session, as the operational model is built around immediate exploitation rather than subsequent resale.

The monetisation model depends on session-time conversion, defined by three operational characteristics:

- **High-volume victim throughput** driven by paid social media advertising and rapid rotation of phishing infrastructure.
- **Manual approval of credentials and OTPs** as they are submitted, allowing the threat actor to validate and act on each session in real time.
- **Same-session execution of fraudulent transactions** eliminating the delay between data capture and financial loss.

ABOUT US

CTM360 provides a consolidated platform that includes external attack surface management, digital risk protection (brand protection & anti-phishing, data leakage protection, and fully managed unlimited takedowns), security ratings, third party risk management, email intelligence (dmarc) and cyber threat intelligence.

CONTACT US:

+973 77 360 360

info@ctm360.com

www.ctm360.com

21st Floor, East Tower Bahrain Financial Harbour, Kingdom of Bahrain

CTM360®