Report | July 2026

The InsureTrap

Real-Time Phishing & Account Hijacking Through Fake Insurance Portals

Analysis by CTM360

CTM360®

CTM360®

INDUSTRY Insurance

COUNTRY All

REGION Global

DATE Jul, 2026

Threat Type Phishing Campaign

Threat Vector Google Ads

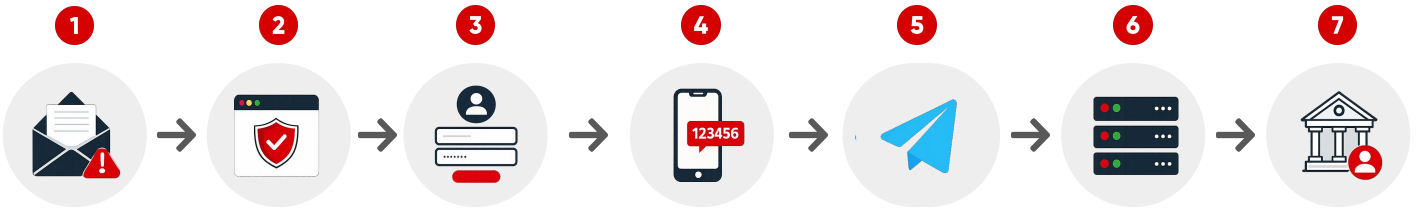
Key Techniques Credential Harvesting, OTP Interception

STIX Tool Phishing Kit

Overview

CTM360 identified a coordinated phishing campaign targeting customers of multiple insurance providers through fraudulent websites impersonating legitimate insurance brands and online service portals. The campaign abuses trusted insurance brands spanning various sectors, including motor, health, life, home, and travel insurance, among others, to lure victims into submitting personal information, policy details, account credentials, and authentication codes under the guise of account verification, policy updates, claim processing, or customer service requests.

Analysis of the campaign infrastructure indicates a real-time credential theft and account takeover workflow. During the investigation, CTM360 identified and named the phishing kit **InsureOTP Kit**, a previously undocumented phishing framework specifically designed to target insurance customers. The kit collects victim-submitted information through phishing portals and transmits it to attacker-controlled infrastructure, including Telegram bot integrations, local storage mechanisms, and built-in backend servers. The captured data enables threat actors to intercept one-time passwords (OTPs), gain unauthorized access to victim accounts, and facilitate account compromise.



1 Phishing Advertisement

Victim is presented with a sponsored Google advertisement leading to a fraudulent insurance quotation portal.

2 Redirection

Victim clicks the link and is redirected to a fraudulent insurance website impersonating a trusted brand.

3 Data Collection

Victim is prompted to enter personal information, policy details, and account credentials on the phishing portal.

4 OTP Interception

Victim enters the OTP/ authentication code received on their registered mobile/email for verification.

5 Data Transmission

Submitted data, including credentials and OTPS, is sent in real time to threat actors via Telegram bot integration.

6 Backend Processing

Data is stored and processed on the attacker's built-in backend server for monitoring and misuse.

7 Account Takeover

Threat actors use the stolen credentials and OTPs to gain unauthorized access and take over the victim's account.

Key Takeaway

This campaign represents a high-risk insurance-sector phishing operation that combines trusted brand impersonation, realistic phishing portals, exposed backend infrastructure, and real-time OTP interception to facilitate account compromise. The use of Telegram bot integrations, local data storage, and built-in backend servers provides threat actors with real-time visibility into victim submissions, enabling rapid account takeover and unauthorized access to sensitive customer information and insurance-related services.

CTM360®

FRAUD STAGES:

CTM360 Fraud Navigator

PHASE 1
Infrastructure & Delivery

PHASE 2
Victim Engagement & Fraud

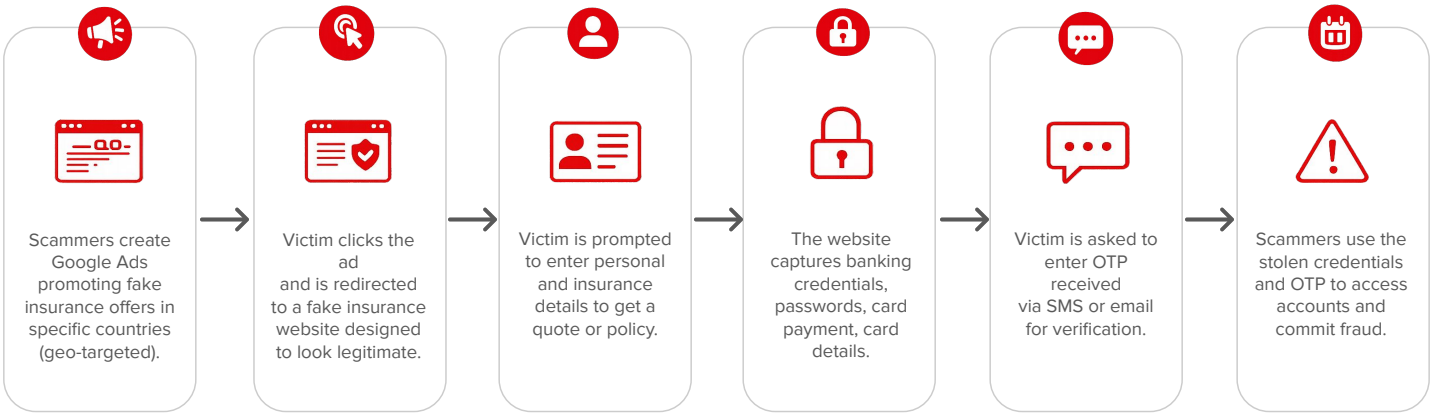
1. **Resource Development**
   - Hosting
     - Dedicated Hosting
     - Website Builder
     - Free Hosting
   - Domain
     - Lookalike Domain
     - Subdomain
     - Dedicated Domain
2. **Evasion**
   - Google Ads
     - Geo Targeted Content
     - User Agent Restricted
3. **Trigger**
   - Deceptive Incentives
     - Fake Offers
     - False Promise
4. **Distribution**
   - Ads
     - Google Ads
5. **Target Interaction**
   - Website
     - Impersonated website
6. **Motive**
   - PII harvesting
   - Credential Harvesting
7. **Monetization**
   - Credit/Debit Card charged
   - Sale of Stolen Digital Assets

Stage (Tactic/Category)
Category
Technique

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

Observed Attack Chain

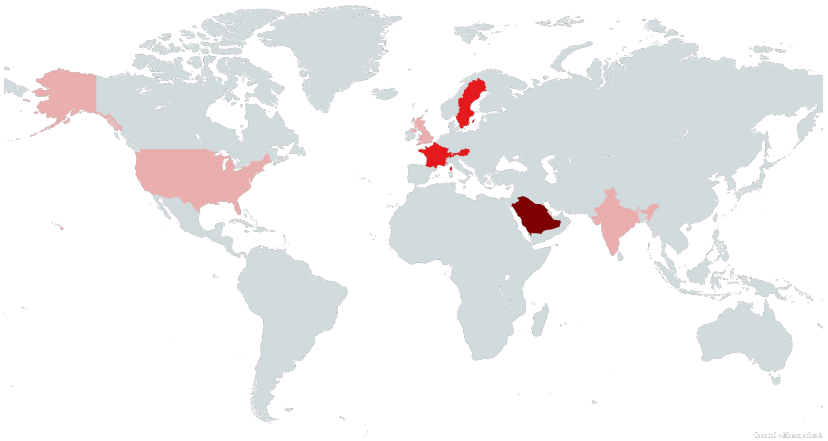
The simplified flow below illustrates what occurs when a user interacts with a fraudulent insurance advertisement distributed through Google Ads.



Each stage of this workflow has been observed across multiple insurance-themed sub-campaigns leveraging the same or closely related threat actor infrastructure, including operations targeting consumers across various regions and insurance sectors. The attack chain begins with public-facing Google Ads designed to establish legitimacy and impersonate trusted insurance providers, brokers, or policy management services. Victims are then redirected to fraudulent insurance portals tailored to their geographic location, where localized branding and content are used to increase credibility before any sensitive information is collected. The phishing portal subsequently harvests personal information, account credentials, and OTP values, which are captured in real time and may be leveraged to facilitate account compromise, identity theft, insurance fraud, or other unauthorized activities against the victim.

TARGETED REGIONS DISTRIBUTION

Displayed below is a summary of insurance-themed phishing activity observed across multiple regions. Campaigns are delivered through Google Ads and customized according to the target country's language, branding, and insurance market.



Top Targeted Countries

01 Saudi Arabia

Primary target: Multiple confirmed detections indicate that Saudi Arabia remains the campaign's primary area of focus, with sustained targeting of insurance providers.

02 European Countries

High activity: Several confirmed detections were observed across European insurance providers, indicating broad regional targeting through fraudulent insurance websites.

03 United States & India

Secondary targets: Additional detections were identified in the United States and India, showing wider campaign expansion beyond the primary target regions.

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
Google Sponsored Ads	Primary distribution
Typosquatted insurance-lookalike domains	Dedicated phishing landing pages
GitHub Pages / Hostinger / Wix etc	Free hosting for disposable phishing pages

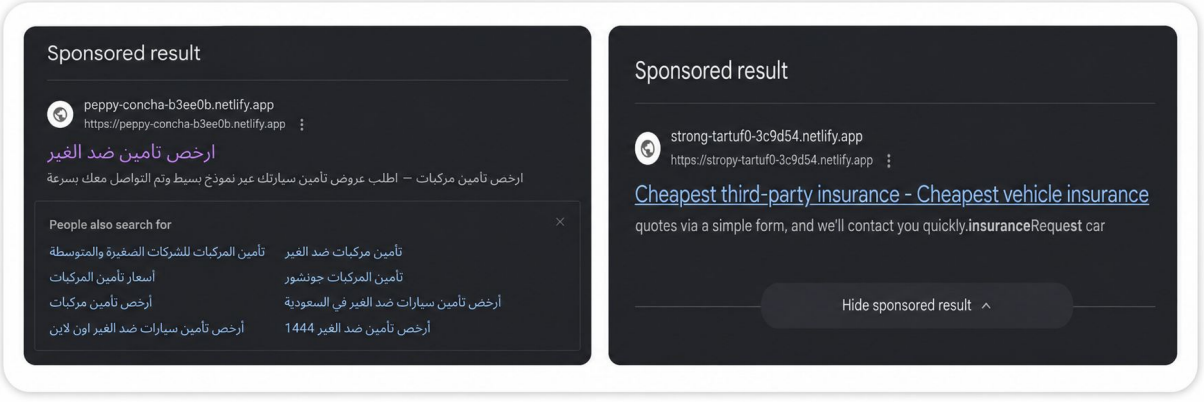
CTM360 OBSERVATIONS

Sponsored Google Ads

Sponsored Google Ads are used as the primary distribution vector, directing victims to fraudulent landing pages that extract personal information and capture account credentials. Campaigns operate across multiple regions and insurance brands, with ads served from disposable free-hosting infrastructure such as **Netlify, Lovable, etc.** using randomised domain names that carry no brand identifiers, a deliberate tactic to bypass insurer brand-monitoring systems.

Common Ad Characteristics Observed

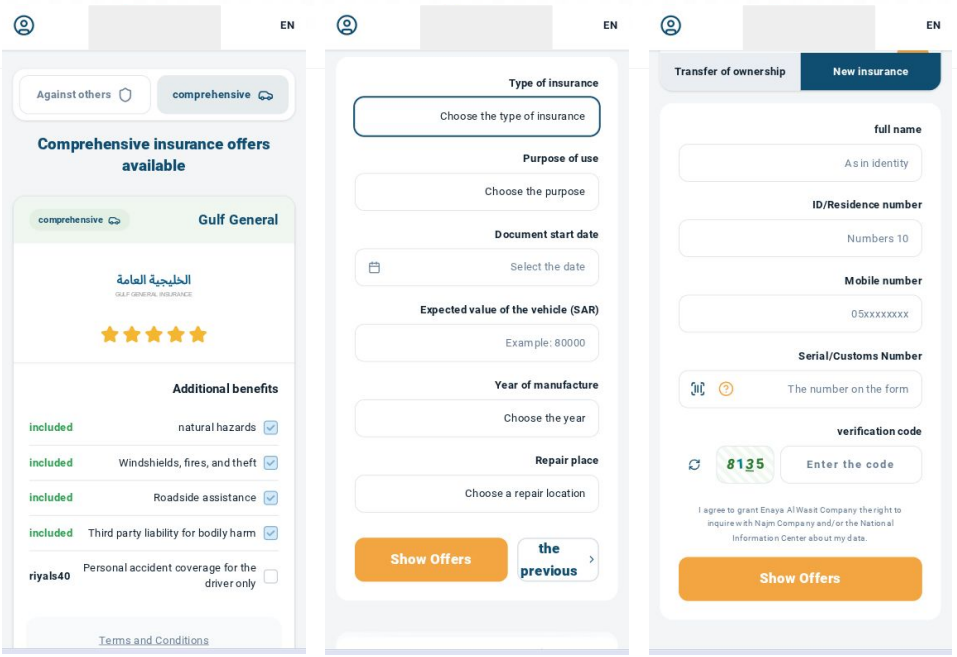
- Ads recirculate the same campaign template across multiple targeted regions and brands.
- Bilingual copy used across creatives, with Arabic-language ads promoting cheapest available quotes: "**أرخص تأمين ضد الغير**" (cheapest third-party insurance).
- Price-comparison and urgency-driven headlines: "**Compare car insurance offers**", "**Cheapest third-party insurance: request a quote via a simple form**"
- Landing pages vary by objective: quote-request forms capture PII such as **name, contact details, address**, while others serve spoofed portal login pages to steal account credentials.



Phishing Portal

The threat actor distributes sponsored Google Ads leading victims to fraudulent insurance quotation portals impersonating legitimate insurance providers.

Throughout the process, the phishing portal replicates the legitimate insurance provider's branding and user interface, harvesting personal information, payment card details, online banking credentials, and OTPs submitted during the insurance quotation workflow.



Landing-Page Hosting Patterns Observed (Sample)

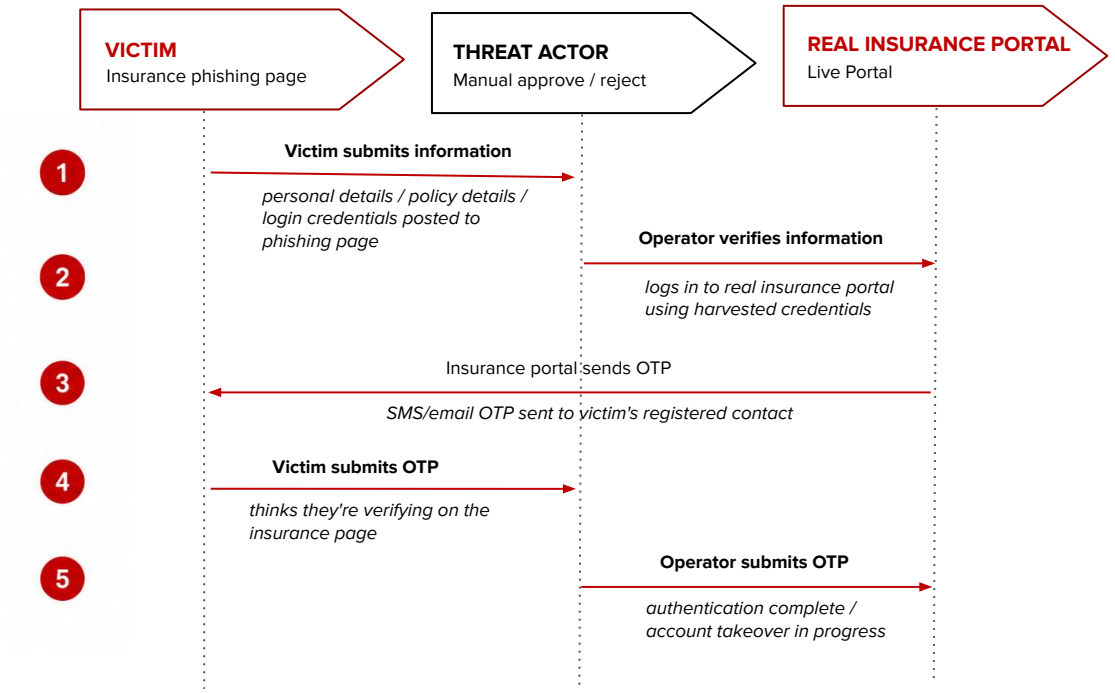
Category	Example	Number of Sites
.com domains	Most frequently observed TLD used across phishing sites	**2,141**
Website builders	editorx.io, wixstudio.com	**279**
Hostinger free hosting	hostingersite.com	**223**
Netlify free hosting	netlify.app	**205**
Lovable free hosting	lovable.app	**137**
EdgeOne free hosting	edgeone.app	**44**
Other domains & TLDs	manus.space, vercel.app, rf.gd, github.io, .net, .org, .online, and others	**1,345**

Data Captured on the Phishing Page

- Full Name
- National ID / Residence ID
- Mobile Number
- Vehicle Information
- Payment Card Details
- Verification Code / CAPTCHA
- SMS / OTP

Real Time Account Hijacking Flow

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

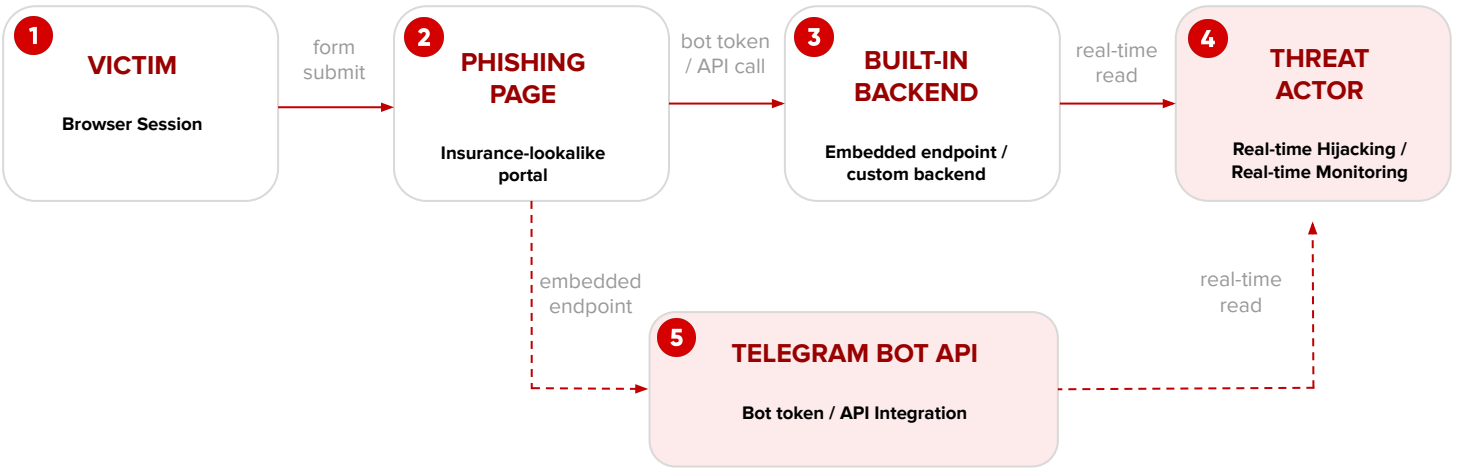


The phishing kit writes each victim submission to a database with a status field that cycles through a manual approval workflow. The Arabic-language status messages recovered from the backend confirm the threat actor's role at each step:

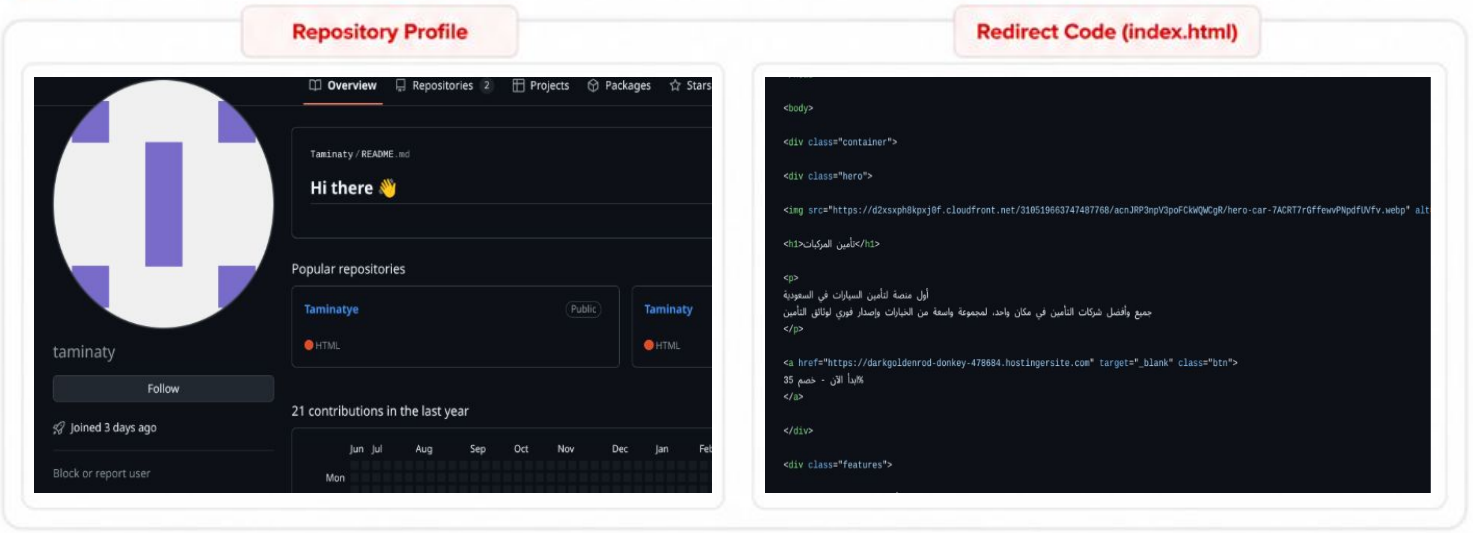
Stage	User-Facing Page / Label	What happens (high-level)	Security interpretation
1	صفحة معلومات التسجيل (Registration info page)	Victim is lured into entering basic identity or login-related information	Initial credential harvesting entry point
2	اسم المستخدم وكلمة المرور (Username & Password)	User submits banking or account credentials	Primary credential capture phase
3	رقم الجوال (Mobile number)	Phone number is collected for further targeting	Enables OTP interception / SMS targeting
4	صفحة البطاقة (Card page)	Payment or card details are requested	Financial data harvesting stage
6	رمز التوثيق / رمز سري (Verification / secret code)	Victim is prompted for authentication codes	2FA bypass attempt (OTP harvesting)
7	رمز التحقق / OTP input	One-time password is requested and captured	Multi-factor authentication compromise

Technical observation

Analysis of the campaign infrastructure indicates a real-time credential theft and account takeover workflow. Victim-submitted information is collected through phishing portals and transmitted to attacker-controlled infrastructure, including Telegram bot integrations, local storage mechanisms, and built-in backend servers. The captured data enables threat actors to intercept OTPs, gain unauthorized access to victim accounts, and facilitate account compromise.



Github Repository Hosting Phishing Redirect



The threat actor created a code repository account to manage multiple repositories, each hosting phishing redirect 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.

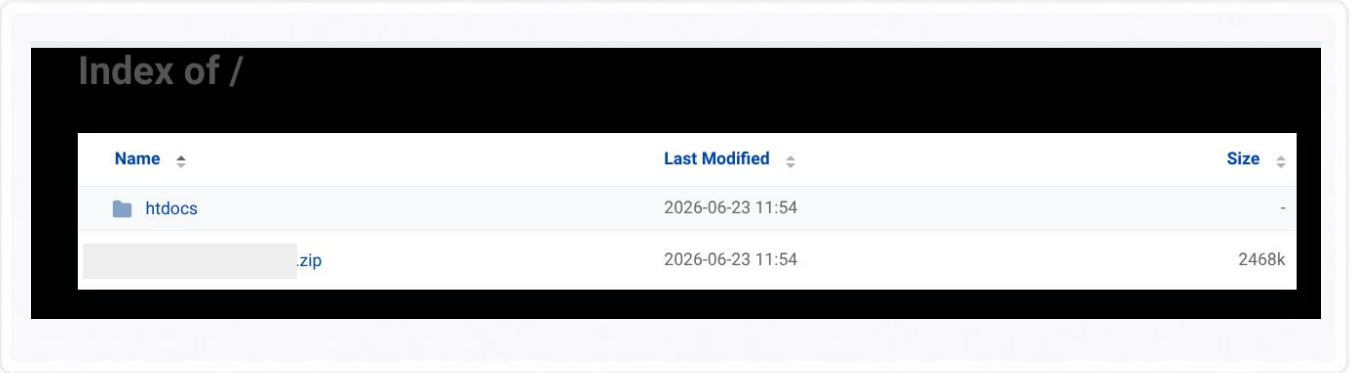
The phishing redirect sites were then deployed and made publicly accessible via GitHub Pages (github[.]io), eliminating the need for external hosting infrastructure and adding a layer of legitimacy to the malicious pages, increasing the likelihood of deceiving potential victims.

InsureOTP Kit - Backend Infrastructure

During the investigation, CTM360 uncovered the backend infrastructure of the **InsureOTP Kit**, we identified a publicly accessible directory path on the phishing page that exposed an index listing. The directory contained a ZIP archive file, which was successfully downloaded and analyzed. The archive held the backend source code and supporting data, which led to the discovery of the database and administrator credentials used to operate the phishing kit.

Exposed Directory Index

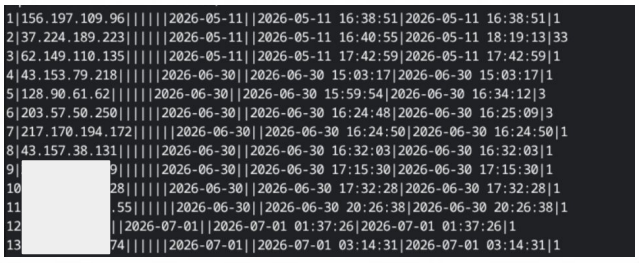
The phishing page contained a accessible directory path that exposed an index publicly accessible directory index that exposed an archive of the **InsureOTP Kit** backend, revealing the presence of a ZIP archive file.



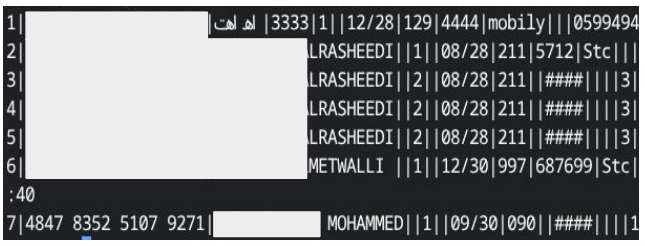
Archive Extraction & Data Discovery

Analysis of the downloaded archive revealed multiple SQLite database files containing victim information, session records, stored payment card details, user information, and administrator credentials associated with the phishing kit.

Visits Table (SQLite)



Card Table (SQLite)



Users Table (SQLite)

Administrator Credentials (SQLite)

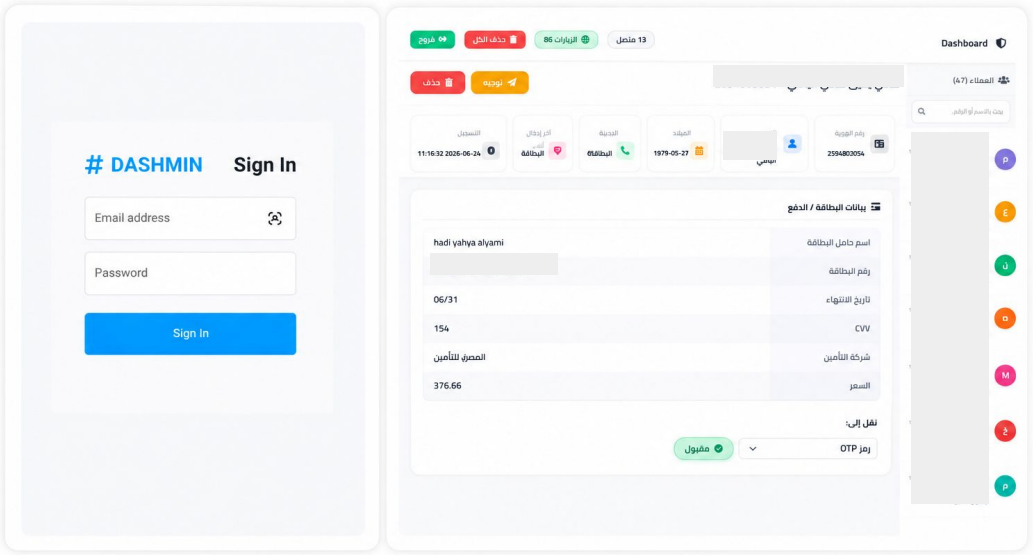
From the extracted **InsureOTP Kit** database, we obtained the administrator email and password used to access and manage the phishing kit backend. This access enabled full visibility into the threat actor's operations and the collected victim data.

InsureOTP Kit - Built-in backend

Analysis of the **InsureOTP Kit** identified a built-in backend infrastructure that enabled direct exfiltration of victim data to an attacker-controlled server. Unlike other variants that relied on third-party services such as Telegram bots, this version transmitted captured information directly to a proprietary backend endpoint integrated into the phishing framework.

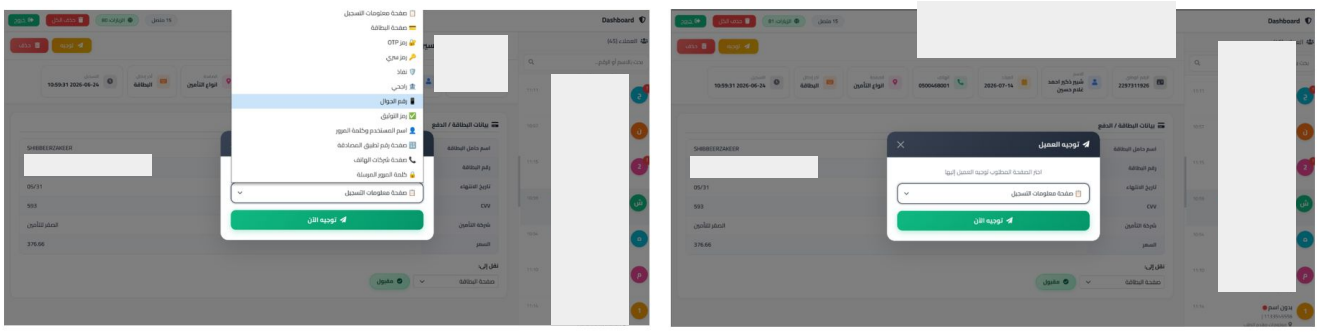
Backend Portal

A backend endpoint URL was identified during the analysis of the **InsureOTP Kit**. 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 **InsureOTP Kit** 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.



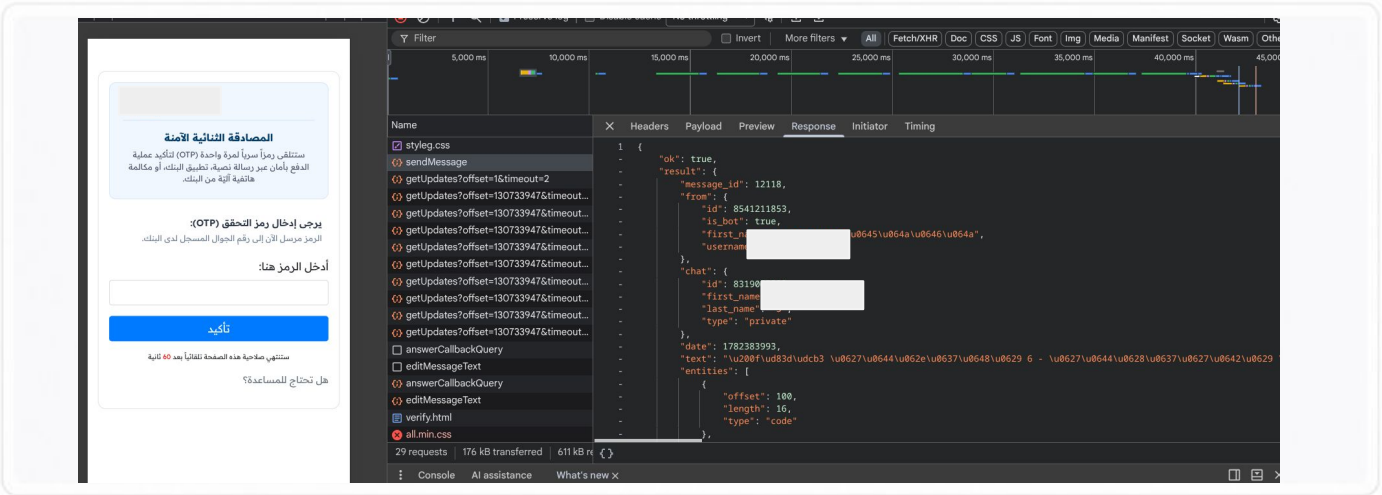
Records included full name, national ID, registered mobile number, online banking credentials, and OTP values captured across all sessions. The dashboard also revealed operational details of the campaign including submission timestamps and session metadata.

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.

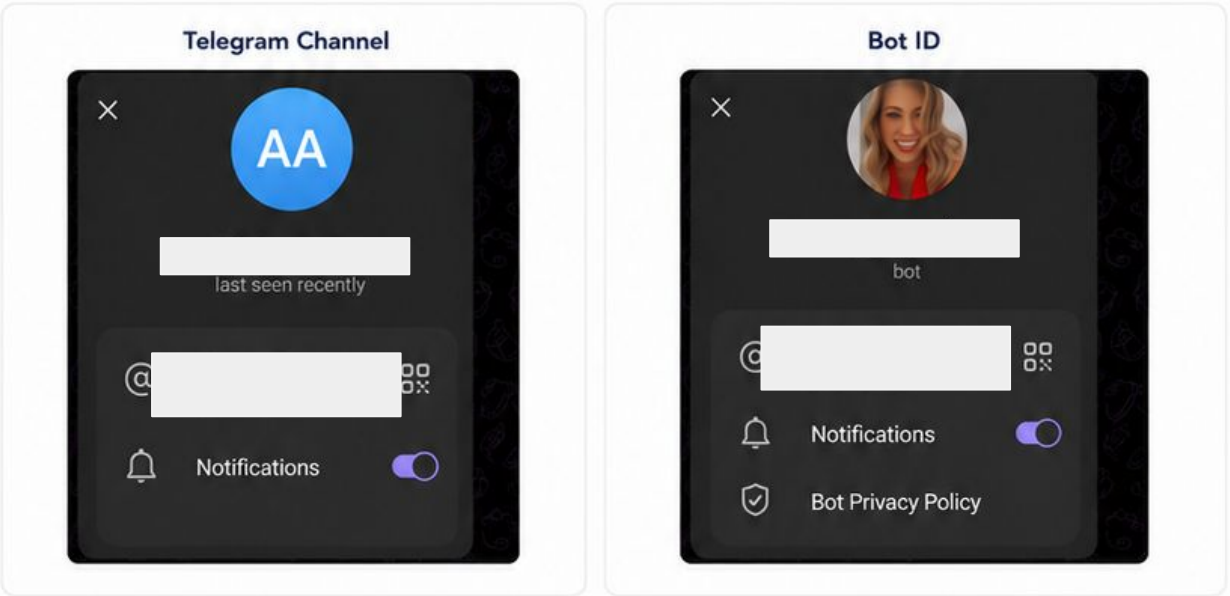
Bot API Requests (Source Code)

A Telegram bot token and associated chat ID were observed. These values were used by the phishing kit to transmit 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 observations indicate that the bot presents the structure of the transmitted data and how it is organized for the threat actor to conduct the real-time online insurance account hijacking workflow.



Based on the observed API communication and bot configuration, the Telegram bot is designed to deliver real-time victim submissions as structured text messages. The observed message structure indicates that each submission includes the victim's name, registered mobile number, online banking credentials, and OTP value, transmitted at each stage of the real-time online banking account hijacking workflow as the threat actor manually progresses the session.

Motive & Monetisation

The defining risk of this campaign is immediate, real-time account takeover. As the threat actor authenticates against the live insurance portal at the moment the victim submits their OTP, every successful submission corresponds to an active session within a genuine customer account. This enables unauthorized access to insurance accounts, policy information, and associated account management functions before the victim has left the phishing page.

The architecture of the operation compresses the conventional phishing kill chain into a single sitting. Credential capture, OTP interception, and resulting account compromise 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 sponsored Google Ads and rapid rotation of phishing infrastructure.
- **Manual validation of credentials and OTPs** as they are submitted, allowing the threat actor to authenticate each session against the legitimate insurance portal in real time.
- **Same-session account compromise,** eliminating the delay between credential capture and unauthorized access while enabling immediate exploitation of the authenticated session.

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®

Mapping the World's External Digital Risks

External | Consolidated | Technology, Data & Managed Services