Report | November 2025

HackOnChat

Unmasking the **WhatsApp Hacking Scam**

Analysis by CTM360

CTM360®

INDUSTRY	COUNTRY	REGION	DATE
All	All	All	19-11-2025

Overview

CTM360 has discovered a large-scale malicious campaign targeting WhatsApp users worldwide. This scam is designed to hijack WhatsApp accounts through deceptive phishing schemes that exploit user trust in the WhatsApp brand. Threat actors behind this campaign create fraudulent websites that closely imitate legitimate WhatsApp interfaces, using urgency-driven tactics to trick users into compromising their accounts. We have dubbed **WhatsApp Account Hacking scam** campaign as "**HackOnChat**".

This ongoing campaign leverages a variety of social engineering techniques to reach a global audience, often **deploying multilingual fake pages to maximize its impact** across different regions.

CTM360's Threat Intelligence Team continues to monitor the evolution of these campaigns, analyze their technical mechanisms, and take proactive measures to disrupt their spread. This report provides an in-depth look at the underlying attack infrastructure, outlines detection methodologies, and presents actionable strategies to mitigate the risks posed by HackOnChat.

Key Findings on HackOnChat Scam Campaign:

- Over **9000+** phishing URLs uncovered, spanning more than 3 distinct phishing templates.
- These sites are hosted on spoofed dedicated domains; these domains are frequently registered with low-cost or less regulated top-level domains such as .cc, .net, .icu, and .top, making them easier to set up and harder to trace.
- In addition, a significant portion of these sites are deployed using widely available website builders and hosting platforms, including Vercel, WIX, GitHub, and Netlify.
- The scam uses two primary techniques to compromise WhatsApp accounts: **Session hijacking** and **Account takeover**.
- Over the last 45 days (October–November 2025), **CTM360 recorded more than 450 incidents** tied to this campaign, an average of over **10 detections per day**.

  While victims have been identified globally, the activity shows a notable concentration in the Middle East and Asia, indicating these regions are of particular interest to the threat actors.

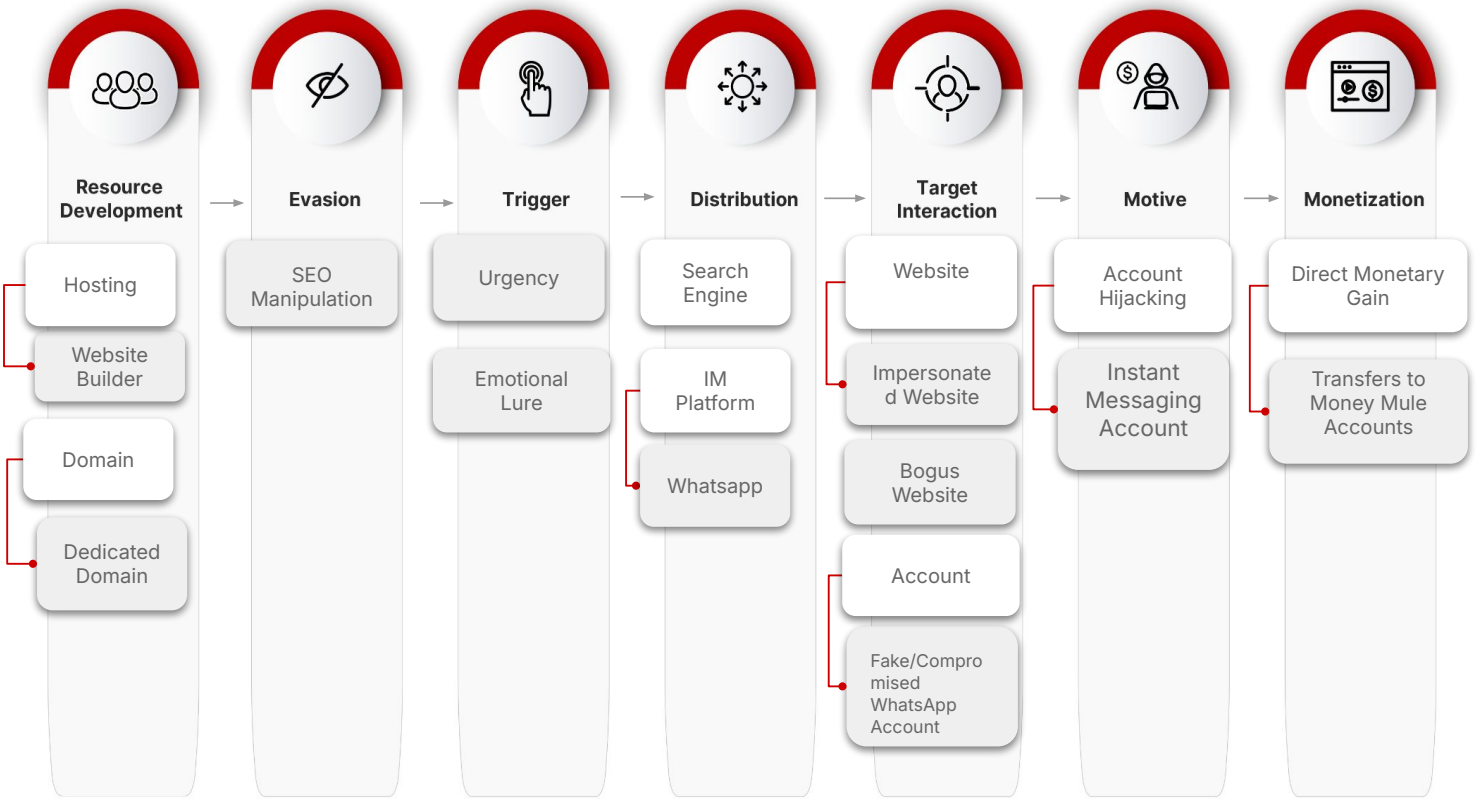
SCAM STAGES:

CTM360 Scam Navigator

CTM360 Scam Navigator, inspired by the MITRE framework, is an analysis of the observed scams showing how the scammers navigate through different stages of the scam. Scam Navigator is a tool that categorizes common techniques, providing insights into the 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 two phases in these scams, represented as Phase 1 (in white) and Phase 2 (in grey).

By breaking down the scam across its stages, the CTM360 scam navigator provides a clearer understanding of **WhatsApp Account Hacking techniques,** along with the underlying motives and monetization strategies.



*Scam Navigator - **HackOnChat***

CTM360 Observations

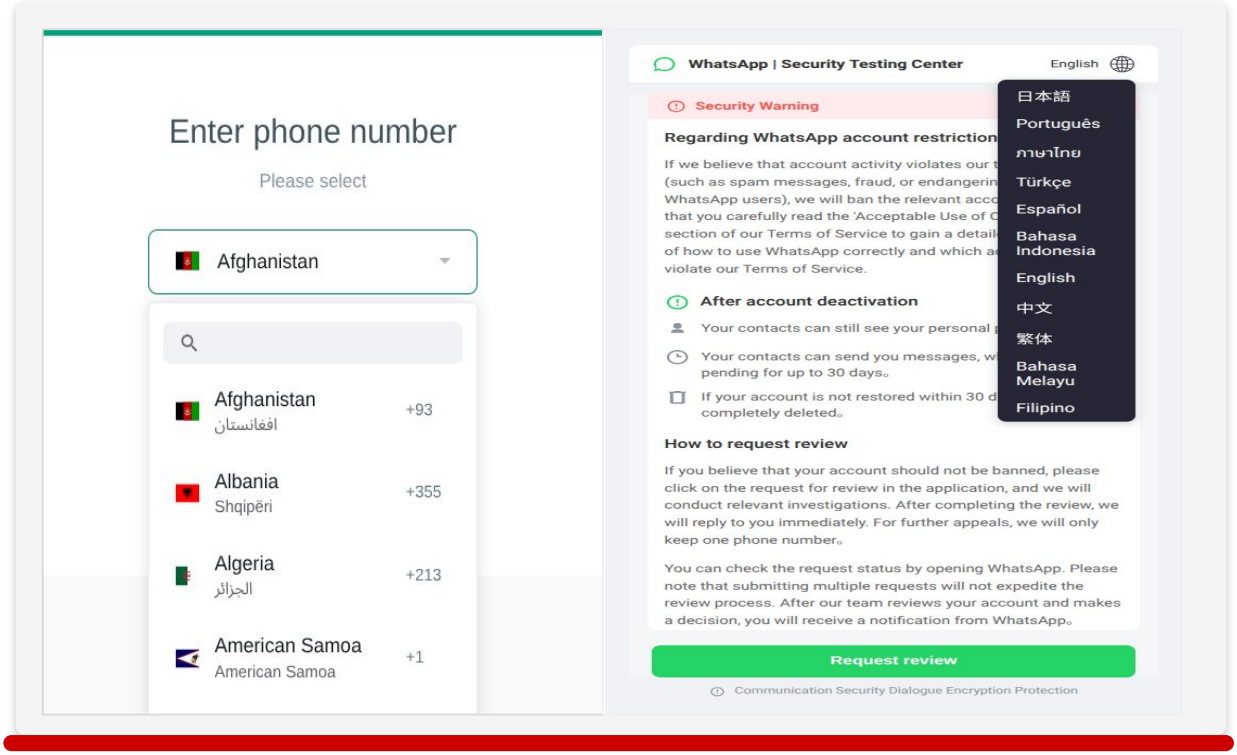
During the investigation of a HackOnChat campaign, CTM360 identified that scammers are deploying fraudulent websites that mimic the authentic WhatsApp interface with remarkable precision, copying its branding, colors, and overall layout to manipulate user trust.

The attackers rely on **two primary techniques**: **Session Hijacking**, where the WhatsApp linked device feature is exploited to hijack Whatsapp web sessions, and the **Account Takeover**, which involves tricking victims into revealing authentication key to seize full ownership of their accounts. Malicious links are using templates of fake security-alert verification, deceptive WhatsApp Web imitation pages, and spoofed group invitation messages, all designed to lure users into these traps and enable the hacking process.

TARGETED REGIONS DISTRIBUTION

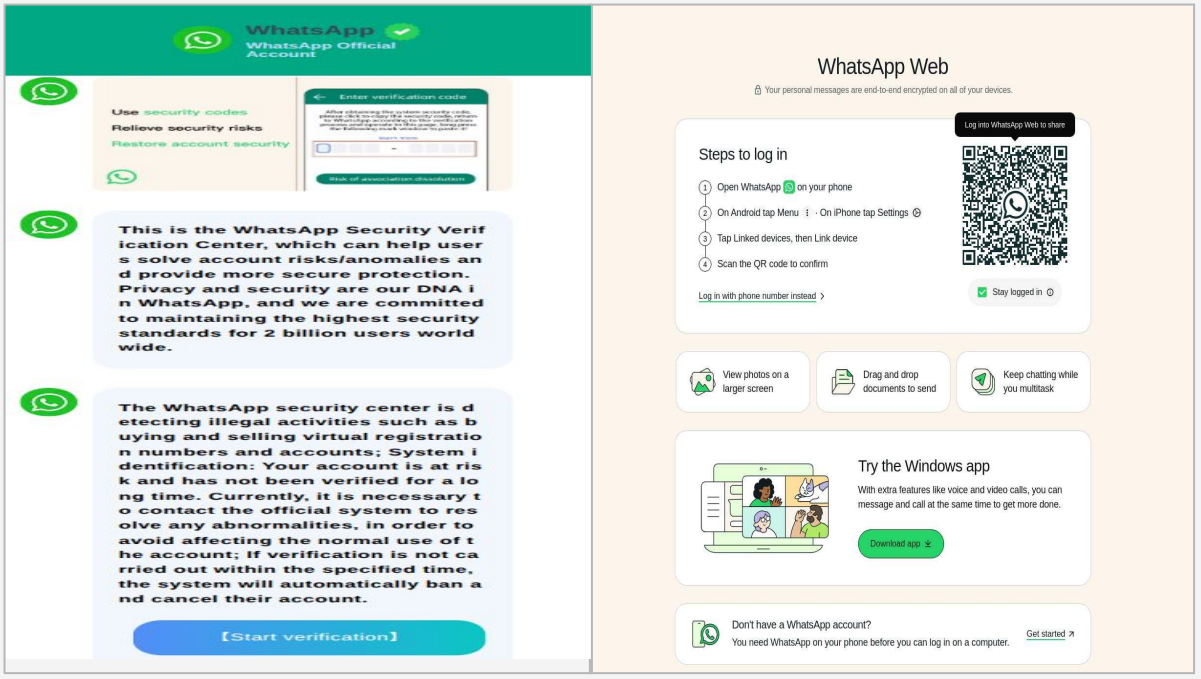
The sites are built to target multiple regions by using the methodology of multilingual sites and a prominent country selector that lets victims choose their country and automatically applies the corresponding international dialing code.

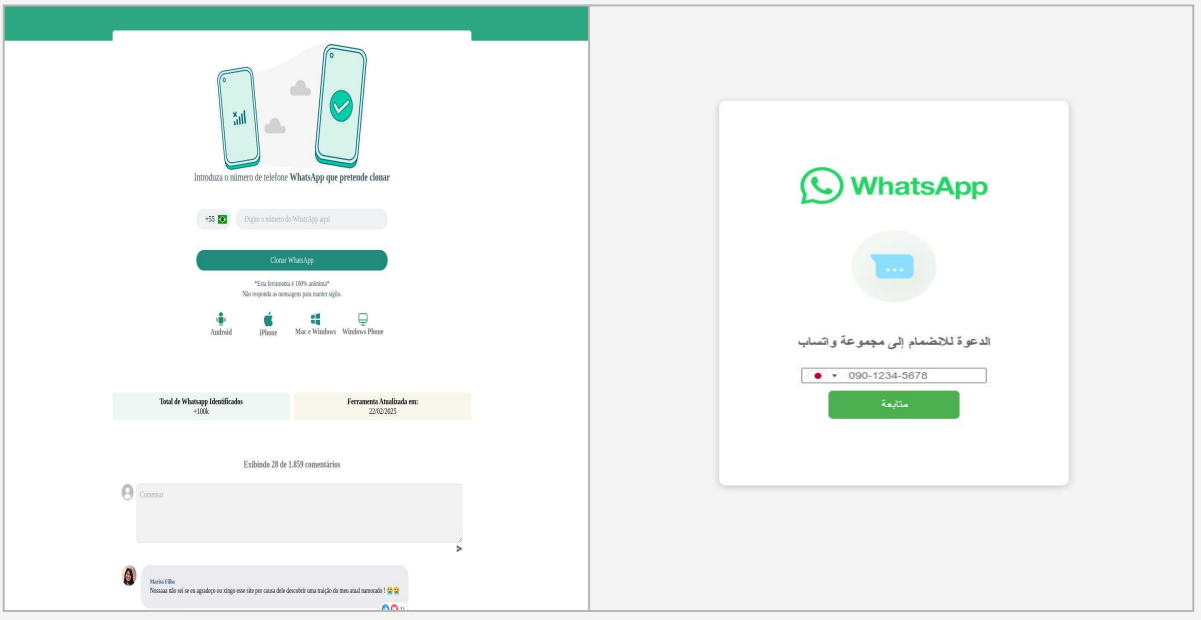
By supporting a wide range of country codes and a searchable country list, these sites broadens its geographic reach, simplifies localization, and makes it easy for attackers to target users across multiple regions globally.



Fraudulent WhatsApp Templates

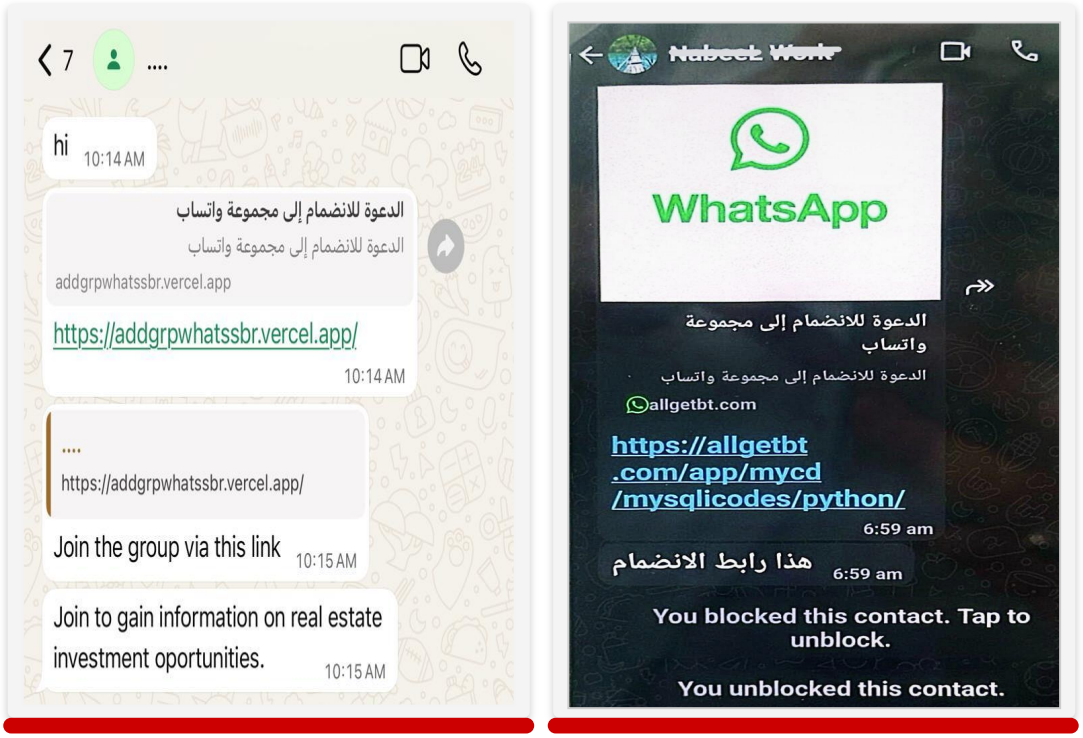
As CTM360 identified the HackOnChat campaign, multiple phishing templates were identified, these templates were crafted based on recurring keyword patterns identified within the associated phishing URLs, providing further insight into the structure and distribution of the campaign.



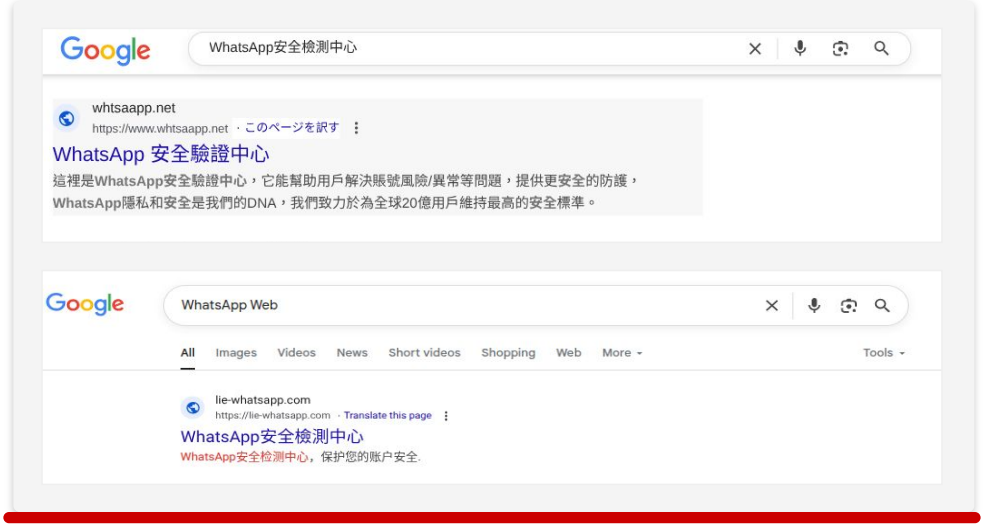


Trigger and Distribution

The WhatsApp account hacking campaign is typically propagated through messages delivered via WhatsApp. These messages may originate from spoofed or compromised accounts of the victim's existing contacts, or from anonymous accounts attempting to join random WhatsApp groups to distribute malicious links.



In some cases, these phishing URLs are also indexed by search engines and appear under misleading titles such as "WhatsApp Web," including within sponsored or promoted search results. This not only increases their visibility but also lends an additional layer of perceived legitimacy, enhancing the likelihood of user interaction.



In each case, the distribution approach is designed to create a false sense of trust and legitimacy, increasing the likelihood that the victim will engage with the malicious content. These messages contain phishing links that direct users to fraudulent websites designed to mimic the legitimate WhatsApp Web interface.

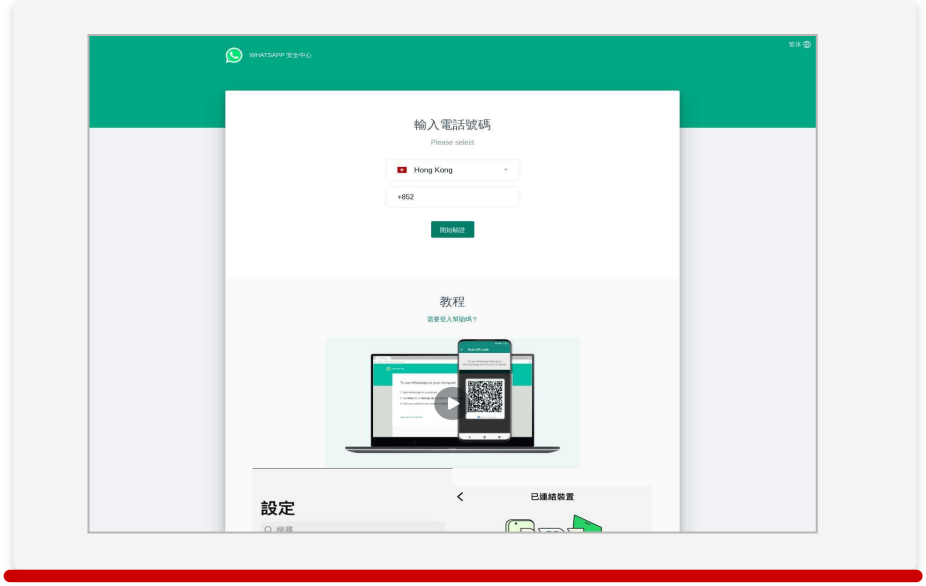
Technique 1: Session Hijacking

The attack is designed to hijack WhatsApp sessions by replicating the functionality and appearance of the legitimate WhatsApp Web login process. This technique mimics the legitimate WhatsApp Web theme to exploit the “Linked Devices” feature. Breaking down the attack, we observe that two primary methods have been utilized in this phishing vector.

- Evil QR Code Method
- Alphanumeric Code Method

CTM360 has observed that the scam unfolds in three stages:

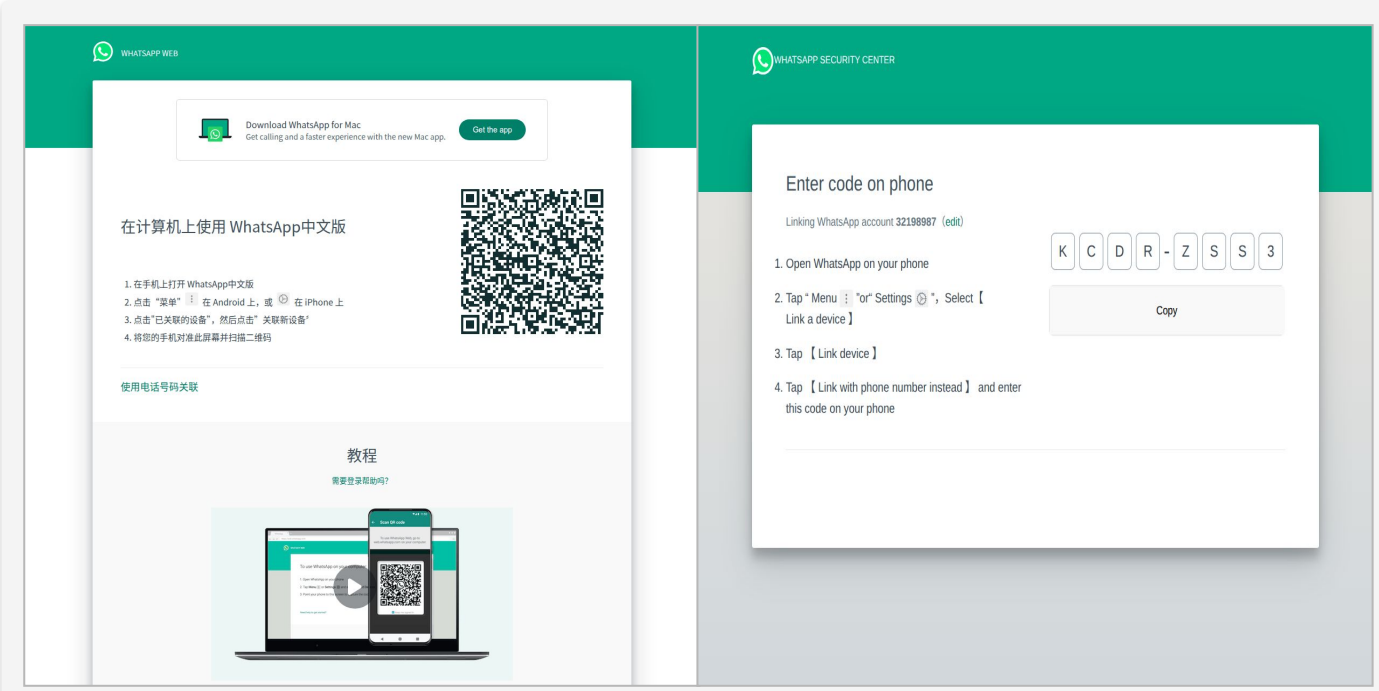
Stage 1: The victim is lured to a fake site impersonating the WhatsApp Web login, where the victim is asked to enter the account number.



Stage 2: At this stage, the threat actor exploits the “Linked Devices” feature, where the victim is presented with the pairing codes, such as QR Code or alphanumeric Code, to access the WhatsApp Web page.

This method involves proxying a legitimate WhatsApp Web QR code or alphanumeric code to a phishing site. The steps are as follows:

- The attacker accesses the official WhatsApp Web portal at https://web.whatsapp.com, where a unique QR code and an alphanumeric device-pairing code are displayed.
- The threat actor uses a malicious browser extension installed on the attacker's browser, specifically designed to monitor or manipulate the content of web pages accessed by the victim.
- Once the WhatsApp Web login page is loaded, the malicious extension automatically extracts the fresh, valid QR code and the alphanumeric code displayed on the legitimate site.
- These codes are then transmitted to an attacker-controlled server and embedded into a phishing webpage designed to mimic WhatsApp Web.



Stage 3: The unsuspecting victims are asked to scan the QR code or enter an alphanumeric code present on the phishing site and is instructed to scan or enter it within the WhatsApp application on their phone, specifically through the "Linked Devices" feature.

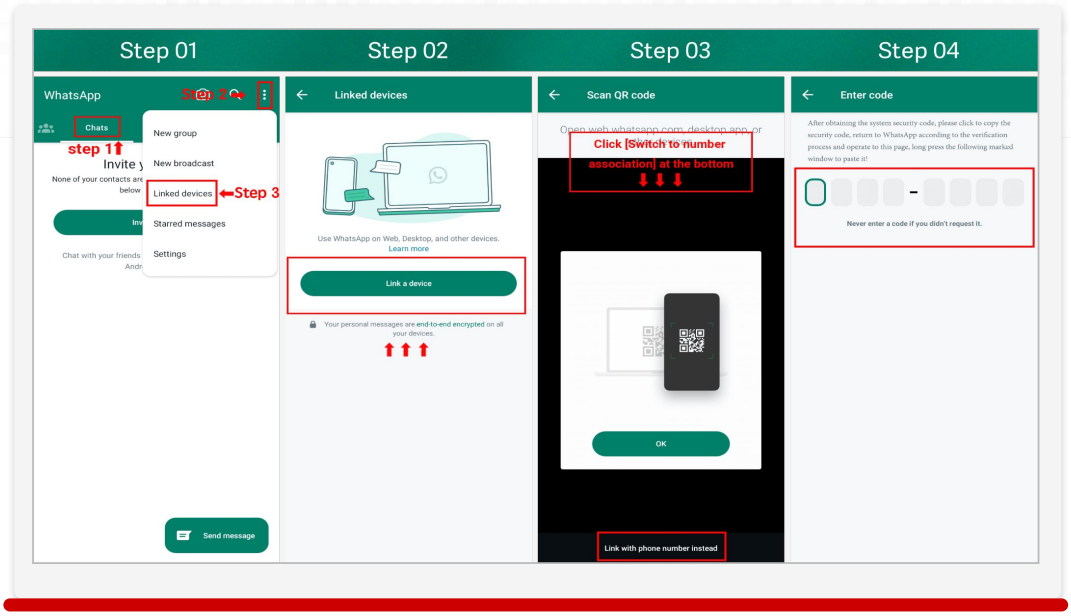


Figure A: Shows the operations of the Android "Linked Device" feature.

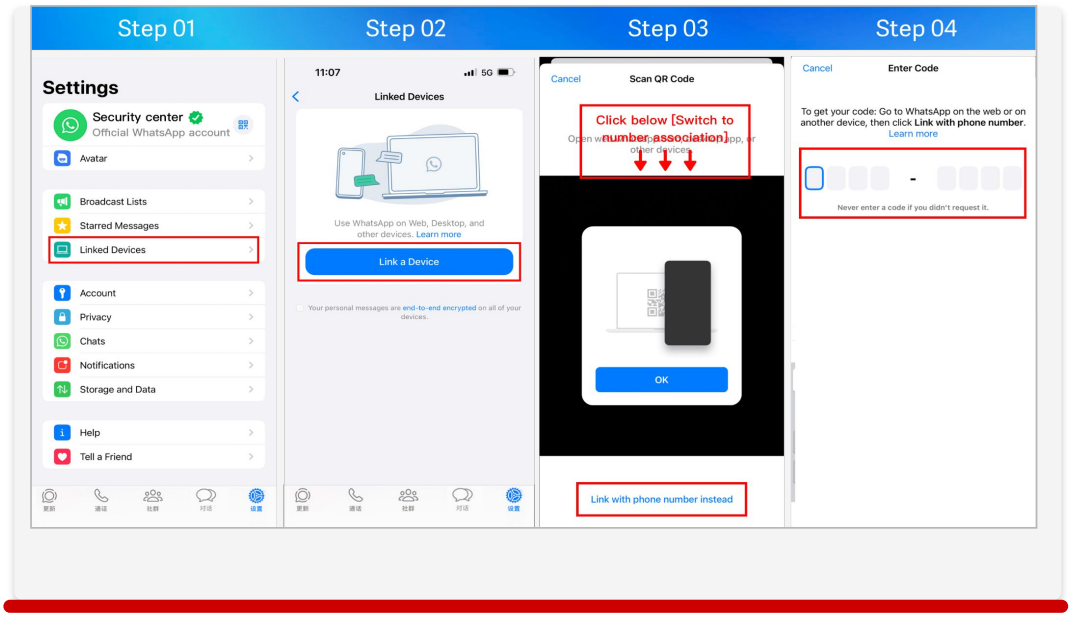


Figure B: Shows the operations of the Iphone "Linked Device" feature.

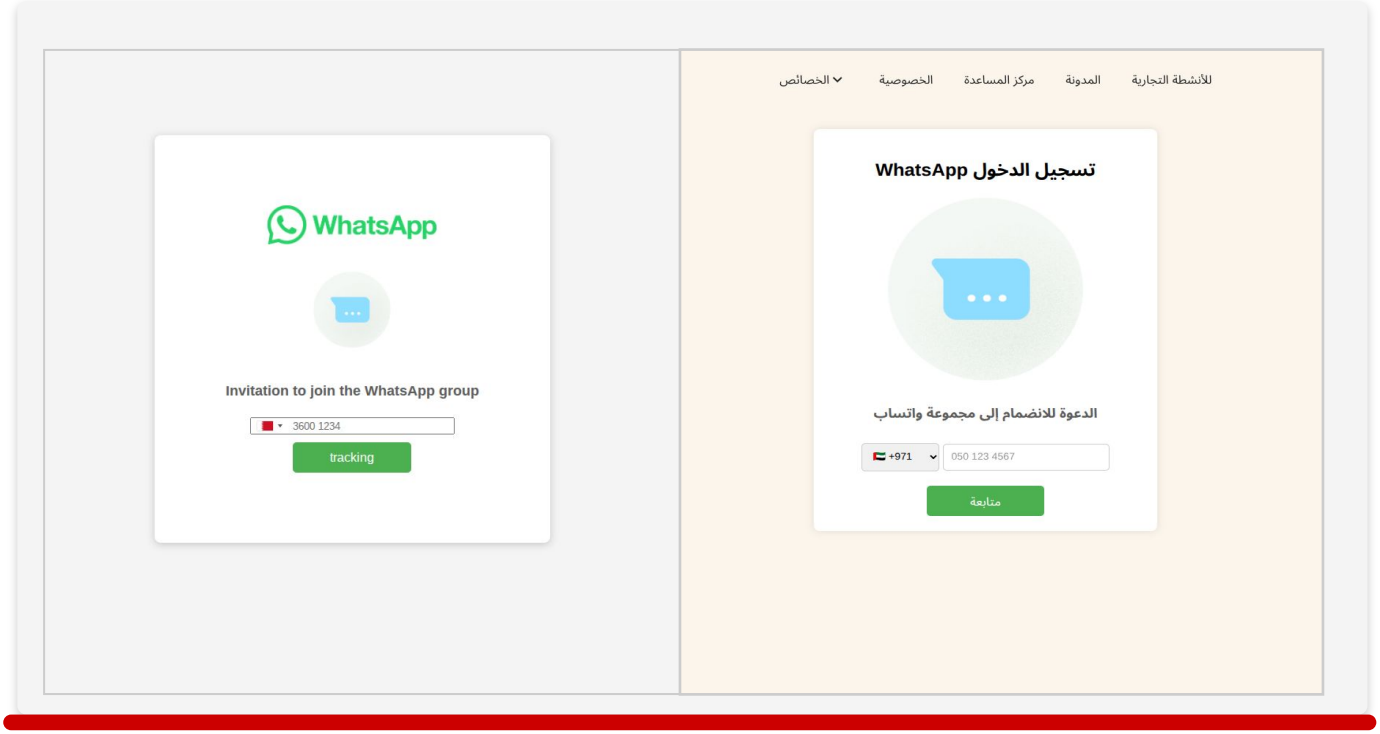
When this step is completed, WhatsApp interprets the action as a genuine request from the account owner to authorize a new web session. In reality, the QR code or alphanumeric code displayed on the phishing site has been generated by a WhatsApp Web session controlled by the threat actor.

This action links the victim's account to the WhatsApp web session controlled by a threat actor, effectively compromising the victim's account.

Technique 2: Account Takeover

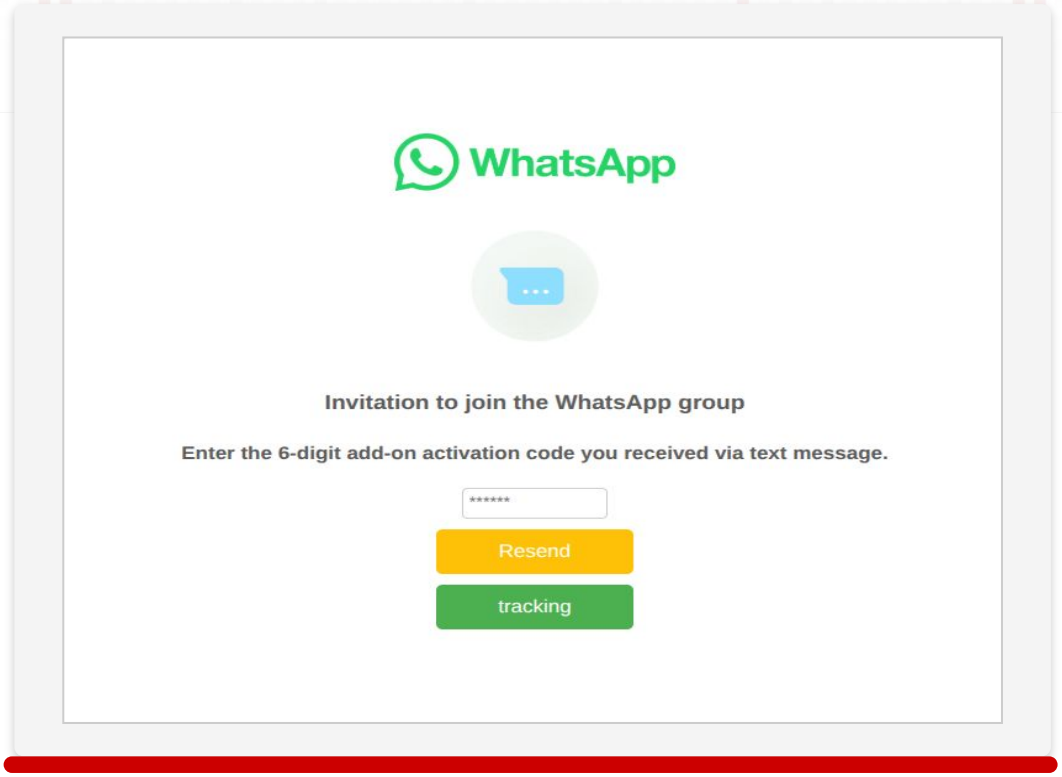
This technique uses phishing templates, mimicking the WhatsApp theme, with urgent hooks to prompt quick user actions. The goal is to gain unauthorized access to victims WhatsApp accounts by capturing their phone numbers and the One-Time Password (OTP) used for authentication. CTM360 has observed that the scam unfolds in two stages:

Stage 1. Victims receive an invitation that includes a link to join the WhatsApp group. Upon clicking the link, the victim is asked to enter their WhatsApp account number into the page.



Stage 2. Request for OTP: Once the phone number is submitted, the backend phishing system controlled by the threat actor immediately initiates an authentication request on the official WhatsApp platform, triggering the platform to send a legitimate six-digit One-Time Password (OTP) via SMS to the victim's device.

The victim is prompted to enter this OTP on the phishing site. Unbeknownst to the victim, this code is then immediately captured and forwarded to the threat actor in real time.



With both the phone number and the valid OTP in hand, the threat actor can now seamlessly complete the login process on the real WhatsApp platform. This allows them to take over the account by registering it on their device.

Motive & Monetization

Once scammers gain control of a victim's WhatsApp account, they exploit it for multiple malicious purposes, primarily driven by financial gain and social engineering opportunities. Their tactics often unfold in several phases:

Targeting Victim Contacts:

After compromising an existing WhatsApp account, malicious actors begin contacting the victim's close contacts to request fund transfers. They craft persuasive messages designed to lure their targets to transfer money and sometimes disclose sensitive personal information such as such as banking details or verification codes.
Because messages appear to come from a trusted source, recipients are more likely to comply without verifying authenticity.

Data Theft:

Scammers will rifle through your message history, documents, and media files to extract:

- Personally identifiable information (PII) such as names, addresses, or ID numbers.
- Financial or transactional details.
- Private content that may be used for further fraud, impersonation, or extortion.

Collected data may also be cross-referenced with other platforms to access linked services or escalate the compromise.

Spreading the Scam:

The attack often evolves into a chain of hijacks, exploiting trust relationships between contacts. New victims are targeted by phishing messages sent from the compromised account. They may trick your contacts into handing over their one-time passwords (OTPs), leading to a chain of attacks that spreads the scam.

Reference:

https://blog.darklab.hk/2023/10/26/watch-out-for-the-adversary-in-the-middle-whatsapp-qr-code-hijacking-targets-hong-kong-and-macau-consumers/
https://cyberfraudcentre.com/whatsapp-verification-code-scams-stay-safe-and-protect-your-account

ABOUT US

CTM360 provides a consolidated platform that includes external attack surface management, digital risk protection (brand protection & anti-phishing, data leakage protection, and unlimited managed 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®