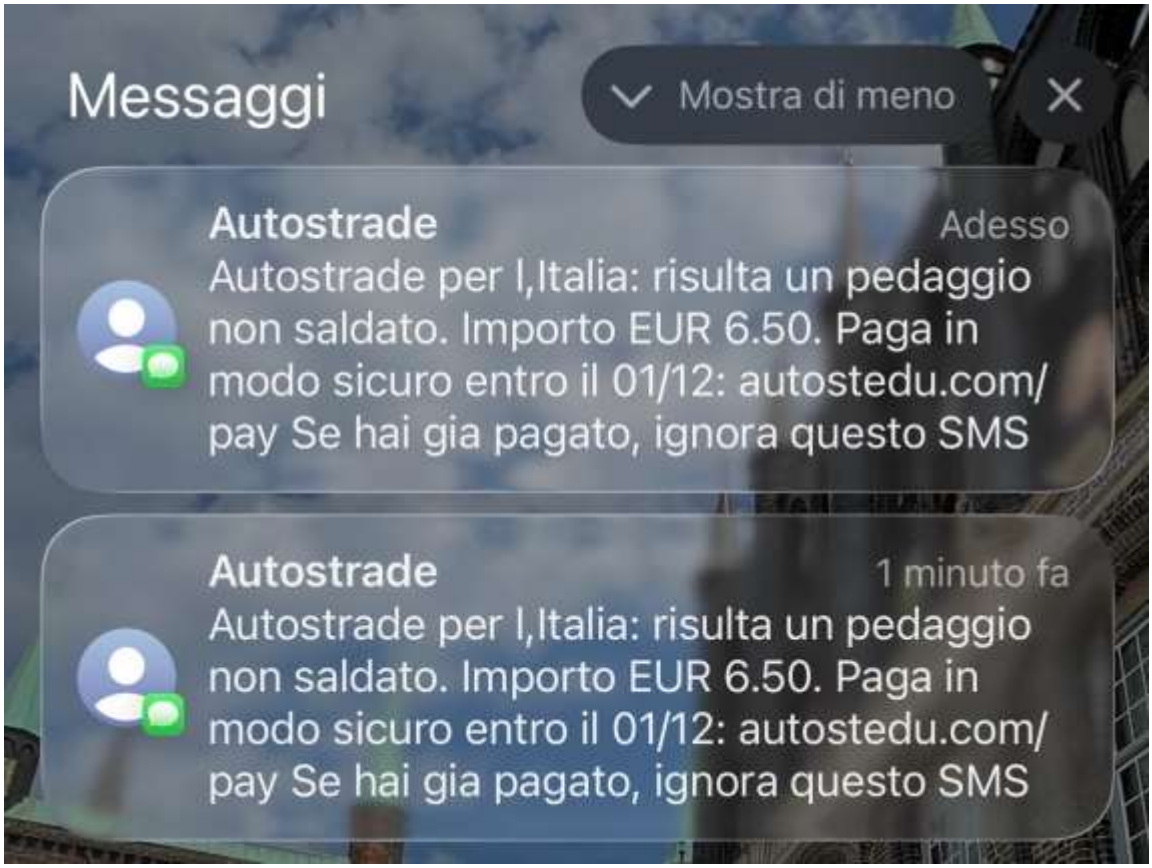
Allerta truffe, falsi sms di Autostrade per l'Italia segnalano il pagamento di pedaggi non saldati: come riconoscerli e che cosa fare

I truffatori riescono a raccogliere i dati sensibili degli utenti con sofisticate tecniche di phishing che portano al sito ufficiale o alla sua perfetta replicazione

(Fonte: https://www.corriere.it/ 8 dicembre 2025)



Negli ultimi giorni, molti utenti italiani potrebbero ricevere un messaggio via sms che afferma: «Autostrade per l'Italia, risulta un pedaggio non pagato». Questo è il preludio a una truffa altamente sofisticata, che si distingue dai tipici tentativi d**i phishing**.

La truffa avanzata

Il messaggio contiene un link che non è collegato ad Autostrade. Un aspetto preoccupante è che, se si visita il link da un computer, si viene reindirizzati al **sito ufficiale di Autostrade**. Tuttavia, se si accede tramite smartphone, appare una pagina che replica **perfettamente il sito ufficiale.** Questa pagina utilizza un codice complesso che, a differenza dei tradizionali siti di phishing, **non richiede l'inserimento dei dati tramite moduli standard**. Invece, i **dati vengono inviati in tempo reale** a un server controllato dai criminali attraverso un collegamento nascosto.

Il kit di phishing professionale

Questa truffa fa parte di un pacchetto di **phishing-as-a-service**, proveniente da mercati neri, che costa migliaia di euro al mese e viene venduto sui **marketplace illegali**. I criminali possono creare

pagine che imitano i sistemi di verifica delle principali banche italiane, riuscendo a rubare PIN, OTP (One Time Password), codici 3D Secure e credenziali di accesso. I documenti caricati dagli utenti vengono inviati a un secondo dominio fraudolento, dove i dati personali e biometrici possono essere abbinati alle credenziali già rubate.
Il kit consente anche d**i riconoscere la banca della vittima tramite il numero della carta**. Se l'utente inserisce un numero Visa, Mastercard o AmEx, il server identifica il circuito e reindirizza verso la schermata della banca corrispondente, replicando le interfacce di istituti come Intesa Sanpaolo, UniCredit e altri. Inoltre, i criminali possono monitorare in tempo reale ogni azione dell'utente, permettendo loro di modificare il flusso della truffa e richiedere ulteriori codici.

Misure di sicurezza
Il sito truffaldino è progettato per **ostacolare l'analisi tecnica**: blocca il tasto destro, disabilita la copia dei testi e cancella la console. La homepage è vuota, mentre solo la pagina per i pagamenti contiene l'app truffaldina. La registrazione del dominio è avvenuta il primo dicembre, coincidente con l'avvio della campagna, un comportamento tipico di kit generati automaticamente.
Abbiamo identificato il codice malevolo, che presenta riferimenti in cinese. Queste non sono frasi casuali, ma parole chiave utilizzate nei kit venduti nei forum asiatici **e nei marketplace Telegram**. Le strutture cinesi sono ulteriormente mascherate tramite Cloudflare Registrar, che oscura ogni informazione sul server.

Che cosa è possibile fare con i dati rubati
Ma cosa può fare chi ottiene questi dati? Potenzialmente tutto. I dati sottratti possono permettere ai criminali di **accedere a conti bancari, app di pagamento e di creare nuovi conti** senza che la vittima debba compiere ulteriori azioni. La truffa è stata costruita per sembrare credibile in ogni dettaglio. Quando l’utente inserisce tutte le informazioni richieste, viene reindirizzato sul sito reale di Autostrade, così da dare l’impressione che il pagamento sia andato a buon fine. Anche gli strumenti di analisi automatica vengono ingannati: il codice identifica alcuni scanner e li reindirizza verso il sito autentico, in modo che quello truffaldino non venga catalogato come malevolo dalle piattaforme di sicurezza.

Che cosa fare in caso di truffa
Se si sospetta di essere stati truffati, è fondamentale **bloccare le proprie carte e presentare denuncia.** È consigliabile cambiare immediatamente le password e informare il proprio istituto bancario.

Leggi anche

Perché all'improvviso riceviamo tante telefonate dall'estero? Telemarketing, spam e truffe: cosa sapere

Prima un (finto) messaggio dalla banca, poi una chiamata su WhatsApp: allarme della polizia per la nuova truffa

Black Friday, arriva un sms con un codice Amazon non richiesto? Si tratta di una truffa: come difendersi

Stop al telemarketing da finti cellulari italiani: dal 19 novembre arriva il secondo filtro. Sarà la volta buona?

«Meta con le truffe fa 16 miliardi l'anno, il 10% dei suoi ricavi totali»: cosa dicono i documenti scovati da Reuters