

Revolut, i dati dei clienti consegnati agli hacker: «La richiesta è partita da una Pec compromessa prefettura di Reggio Calabria» di Roberto Cosentino

Secondo fonti del Corriere, Revolut ha ricevuto una «finta e-mail» dalla prefettura di Reggio Calabria e ha poi trasmesso documenti d'identità, Iban, selfie di verifica e cronologia delle transazioni a un gruppo di hacker che si è spacciato per l'autorità pubblica. Circa 680 i clienti avvisati (Fonte: <https://www.corriere.it/> 15 settembre 2026)



La compagnia fintech britannica **Revolut**, ha consegnato dati personali e finanziari di alcuni suoi clienti ad un gruppo di criminali informatici. **Nessun hacking**, il caso è diverso dai precedenti in cui un'istituzione o un'azienda viene «bucata» da un attacco. **L'elemento nuovo di questo episodio è che la fintech ha consegnato dati sensibili dietro ad una apparentemente legittima richiesta inoltrata tramite una pec compromessa della prefettura di Reggio Calabria con la quale i criminali hanno scritto a nome della polizia postale.** Il gruppo di hacker è riuscito infatti a spacciarsi per l'autorità pubblica italiana.

La fintech non ha subito alcuna intrusione, dal momento che la richiesta è stata inoltrata dalla casella di posta elettronica certificata «compromessa» (una Pec) della prefettura. **Motivo per cui ha superato i controlli di autenticazione prima e trattata come una richiesta autentica poi**, come un normale adempimento di legge. Inizialmente i messaggi non hanno insospettito Revolut che ha inviato i dati richiesti. Le e-mail sarebbero poi proseguite finché l'azienda non ha voluto vederci chiaro e si è rivolta direttamente all'istituzione italiana che ha negato di essere la fonte dei messaggi.

Sull'episodio sta indagando la polizia postale: **l'ipotesi di reato è accesso abusivo a sistema informatico e frode informatica.**

La società, che con oltre **80 milioni di clienti** (5 milioni di Italiani, secondo i dati dello scorso maggio pubblicati da [Milano Finanza](#)) è la maggiore fintech europea, ha confermato l'incidente il 12 settembre. In una nota lo ha definito una «sostituita truffa di impersonificazione esterna» e parlato di un numero «molto limitato» di persone coinvolte. «Una terza parte non autorizzata - si legge nella nota - ha utilizzato un'email di dominio legittima di un'agenzia governativa per inviare richieste fraudolente di informazioni. Al momento del rilevamento, abbiamo immediatamente bloccato l'indirizzo e avvisato l'agenzia governativa competente, così come le agenzie di applicazione della legge, la protezione dei dati e i regolatori finanziari. I sistemi Revolut e i fondi dei clienti non sono stati toccati. Abbiamo contattato direttamente il numero limitato di persone coinvolte per informarle e fornire supporto».

Il [Financial Times](#), citando fonti a conoscenza dell'indagine interna, riferisce che i **clienti contattati dall'azienda sarebbero circa 680**: una cifra che Revolut non ha confermato pubblicamente. Il 15 settembre l'**Information Commissioner's Office**, l'autorità britannica per la protezione dei dati, ha reso noto di aver avviato un'indagine sull'incidente, dopo che la fintech si era autodenunciata all'organismo di controllo alcuni giorni prima.

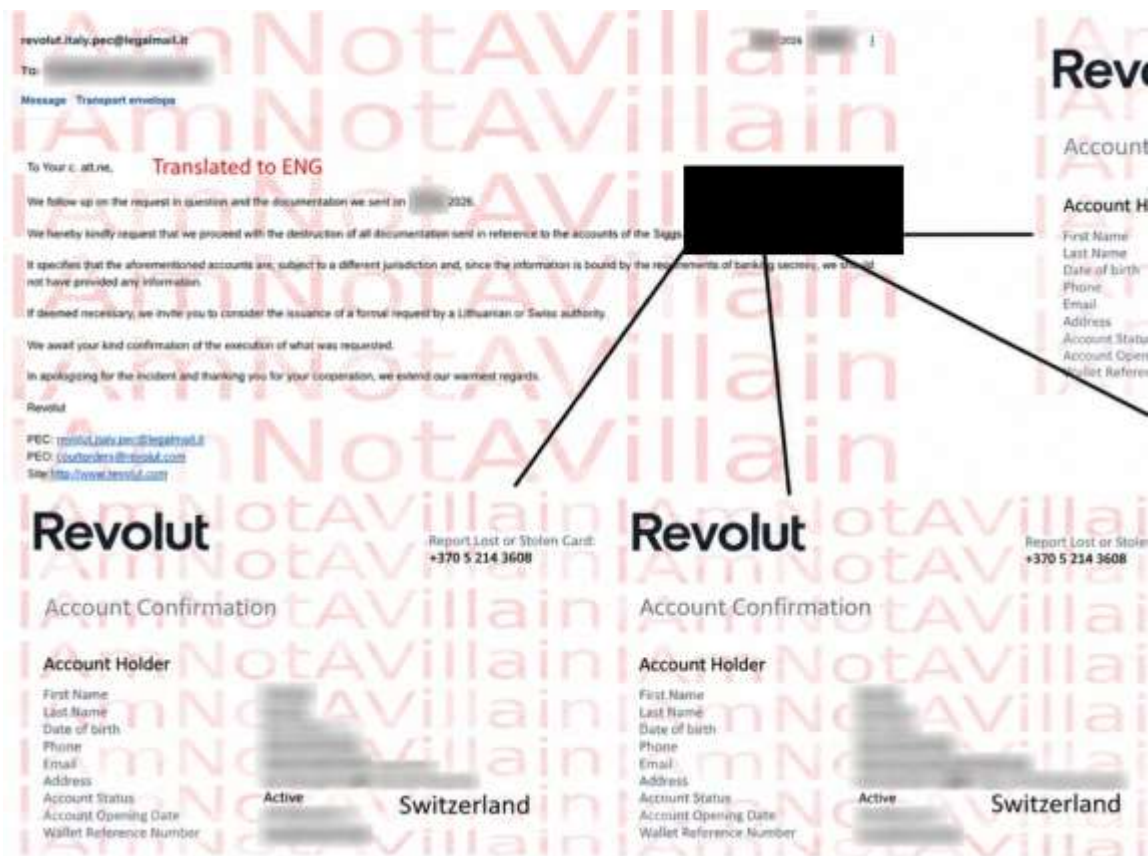
Il meccanismo utilizzato è quello che gli specialisti chiamano **impersonificazione di autorità**: una richiesta di informazioni su un cliente, formalmente identica a quelle che banche e istituti finanziari ricevono ogni giorno da procure e forze di polizia, inviata però un gruppo di criminali informatici. **A rendere l'inganno efficace è stato il canale.** La posta elettronica certificata attribuisce **valore legale alla trasmissione di un messaggio**: certifica che un documento è partito da un determinato indirizzo, che è stato consegnato e in quale momento. È il motivo per cui viene usata per le comunicazioni giudiziarie, ed è il motivo per cui una richiesta che arriva da una Pec istituzionale **viene considerata attendibile senza ulteriori controlli.**

Come più nello specifico afferma sui propri social **Paolo del Checco, consulente informatico forense**, l'attacco in sé viene definito «Man in the Mail». L'attaccante si sarebbe insediato all'interno della Pec dell'Istituzione italiana attraverso un **infostealer**, ovvero un software in grado di infettare un Pc per recuperare informazioni che gli hacker possono sfruttare a proprio piacimento. Così facendo, gli hacker non avrebbero falsificato un messaggio, ma avrebbero preso il controllo di una casella vera. **Ogni loro richiesta è partita davvero dall'indirizzo di un ufficio pubblico**, con tutte le certificazioni in regola, e nessun controllo automatico poteva accorgersene.

La violazione dei dati personali

Il materiale trasmesso è quello che un istituto finanziario raccoglie in fase di apertura del conto e conserva per obblighi antiriciclaggio. Secondo quanto riferito dal *Financial Times* e da [Reuters](#), e in base al materiale pubblicato dagli stessi attaccanti, comprende dati anagrafici e professionali, indirizzi di residenza, recapiti telefonici ed e-mail, copie di passaporti e patenti, le fotografie

inviata per la verifica facciale in fase di registrazione, coordinate bancarie, estratti conto, storico dei prelievi e cronologia delle transazioni, comprese quelle in Bitcoin. Tra i clienti che hanno subito il data breach, anche nomi illustri, come il tennista **Schevchenko** e **Mark Robert Karpelès**, imprenditore francese ed ex Ceo della piattaforma di scambio di bitcoin **Mt. Go**. A Karpelès la notifica di Revolut è arrivata alle 5.25 del 12 settembre e lì per lì l'ha scambiata per l'ennesimo tentativo di truffa; anche **Marc Zeller**, altro nome noto del settore, ha reso pubblico su X di essere tra i coinvolti: documenti d'identità, Iban, estratto conto, storico delle operazioni

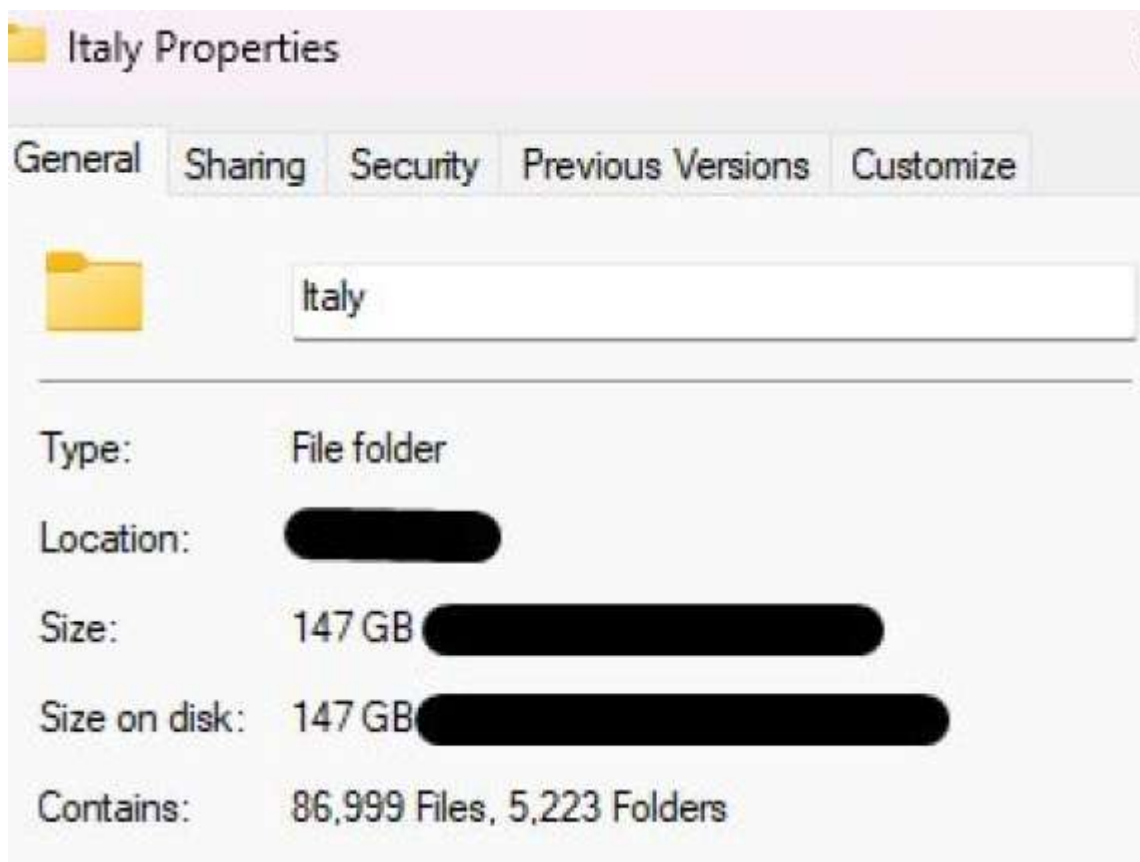


Fin qui siamo nel territorio delle informazioni confermate. Nelle ultime ore, però, è emersa una seconda parte della storia, per il momento basata esclusivamente sulle dichiarazioni dell'attaccante, con il quale abbiamo preso contatto, **e quindi da prendere con la necessaria cautela.**

Il gruppo: come agisce

Il gruppo, che si presenta con lo pseudonimo **iamnotavillain**, sostiene di essere rimasto a lungo all'interno dei sistemi delle forze dell'ordine italiane: **«Abbiamo registrato oltre 87 mila file, per un valore di 147 GB di documenti, e-mail, file personali»**. Alla richiesta di indicare quali strutture siano state colpite, la risposta è stata negativa: **«Non possiamo rivelare quale dipartimento sia stato violato per arrivare a Revolut (ma al Corriere risulta appunto che sia la polizia postale),** ma possiamo dire che nell'attacco in Italia sono stati coinvolti molti dipartimenti». Sollecitati sull'adeguatezza delle difese informatiche delle forze di polizia italiane, hanno risposto che andrebbero profondamente riviste: **«Conosciamo diverse persone che hanno ottenuto molto**

facilmente l'accesso alle e-mail delle forze dell'ordine italiane; ogni casella, se attiva, può contenere decine di gigabyte di messaggi, ciascuno con documenti allegati». Un account di intelligence informale, **International Cyber Digest**, ha riferito che l'operazione sarebbe durata circa sei mesi e avrebbe coinvolto più sistemi delle forze dell'ordine.



Il materiale presumibilmente sottratto alle forze dell'ordine

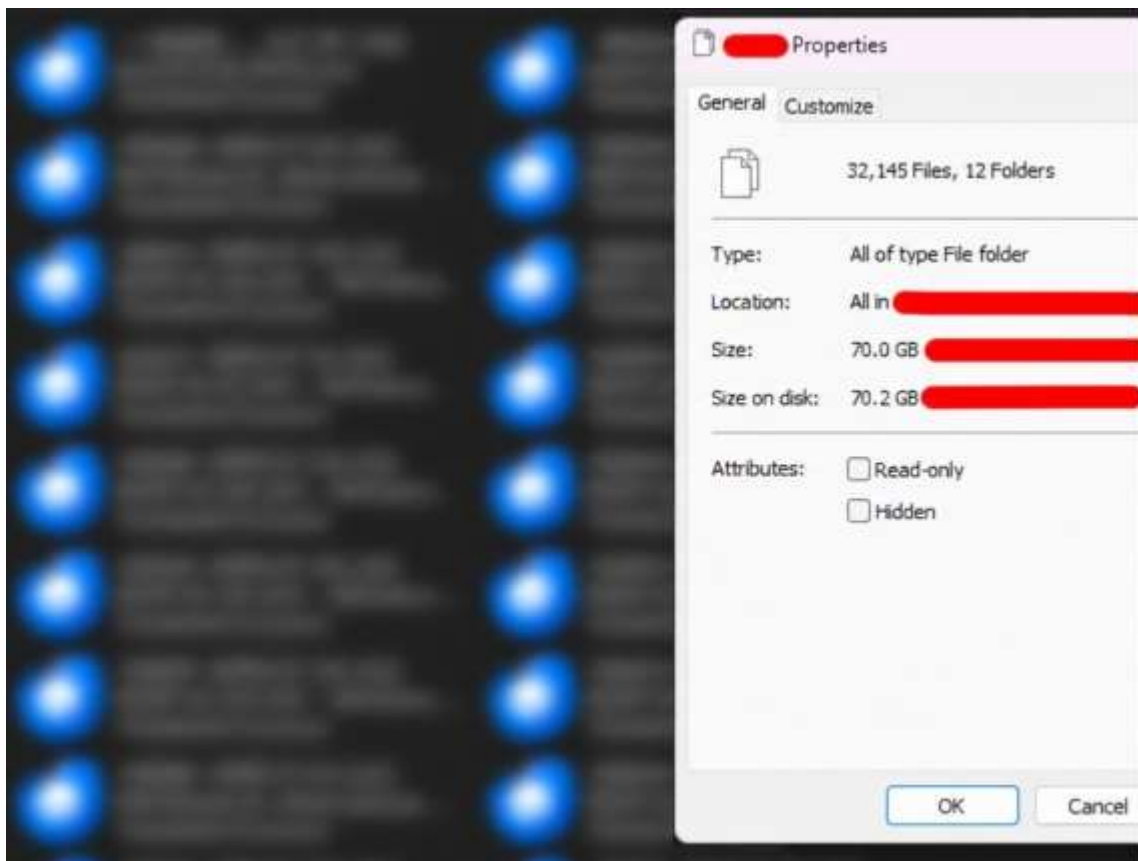
Sul sito del collettivo si possono leggere i motivi per cui hanno attaccato l'azienda a colpi di ingegneria sociale e sembra quasi un manifesto: «Revolut ha ricevuto una segnalazione riguardante un database di utenti. L'hanno ignorata, quindi li stiamo smascherando per non aver protetto adeguatamente le informazioni degli utenti e per aver inviato dati da una giurisdizione diversa». Il [Financial Times](#) riporta che gli hacker minacciano di voler rendere pubbliche le informazioni rubate se Revolut non pagherà il riscatto, ma su questo aspetto c'è ancora poca chiarezza. L'azione portata avanti dagli attaccanti sembra più una «sorta di denuncia» nel modo di gestire la piattaforma. Gli hacker hanno risposto così: «Siamo solo all'inizio. Siamo contrari alle ingiuste normative KYC (Know Your Customer), che Revolut stava applicando. Abbiamo anche scoperto che stavano inviando dati al di fuori della loro giurisdizione, il che costituisce una chiara violazione delle leggi internazionali sui dati».

Cosa sono i «KYC»

KYC ovvero Know Your Customer (conosci il tuo cliente) è un sistema attraverso il quale chi eroga un servizio come ad esempio una banca, deve obbligatoriamente verificare l'identità di un utente. Come ad esempio un selfie, un documento e così via. Per quanto riguarda l'affermazione degli

hacker, è bene precisare che non trova riscontro nella informativa sulla policy per i clienti svizzeri di Revolut. La stessa prevede infatti che **i dati possano essere condivisi con le autorità governative o le forze dell'ordine per ragioni legali, indagini o antifrode** e contempla anche trasferimenti al di fuori della Svizzera e dello Spazio economico europeo per adempiere a obblighi legali e normativi.

Tuttavia, nel presunto materiale attribuito a Revolut condiviso dal gruppo hacker, compare una comunicazione di cui l'autenticità non è stata confermata. La società avrebbe infatti chiesto all'interlocutore, di **distruggere tutta la documentazione trasmessa relativa a quattro clienti**. Questo perché i conti erano soggetti a una diversa giurisdizione e che, per i vincoli legati al segreto bancario, **quelle informazioni non avrebbero dovuto essere fornite**.



Per la sensibilità dei documenti abbiamo dovuto sfocare tutto, ma i dati corrispondono a modelli, istituzioni, etc.

Tra i file mostrati a chi scrive compaiono migliaia di messaggi in formato **.eml**, alcuni dei quali presentano denominazioni caratteristiche delle comunicazioni giudiziarie italiane. Nei nomi dei file ricorrono sigle come **RGPM-NT** e **RGIP-NT**, accompagnate dal numero e dall'anno del procedimento, oltre a riferimenti a procedimenti penali, pubblici ministeri e al cosiddetto «mod. 44», il registro utilizzato per le **notizie di reato contro ignoti**.

Abbiamo confrontato queste nomenclature con documentazione pubblicamente disponibile: **la struttura dei codici corrisponde a quella utilizzata dagli uffici giudiziari italiani**. Altri campioni mostrano indirizzi appartenenti a domini istituzionali della Polizia di Stato e dell'amministrazione giudiziaria; diversi indirizzi verificati trovano corrispondenza nei recapiti pubblicati dalle stesse

amministrazioni. Abbiamo contattato le forze di polizia e le istituzioni coinvolte, **che abbiamo contattato per un commento.**

L'interrogazione parlamentare

Intanto, l'onorevole. **Giulia Pastorella** di Azione ha affermato: «Quante altre mail sono state inviate da quella Pec governativa? Quante altre aziende sono finite vittime di questa truffa? Se le notizie dovessero essere confermate, nessuno dei nostri dati potrebbe dirsi al sicuro. Il Ministero deve immediatamente chiarire quanto accaduto. Porterò il caso in Parlamento con un'interrogazione urgente»