Caso Revolut e dati sensibili sottratti indagine aperta a Reggio Calabria

Data: Invalid Date | Autore: Redazione

Gli hacker sostengono di possedere documenti riconducibili alle forze dell’ordine italiane e chiedono un riscatto da tre milioni di dollari mentre proseguono gli accertamenti sull’origine dell’attacco

La rivendicazione degli hacker e la richiesta di riscatto

Una presunta sottrazione di **dati sensibili appartenenti a clienti Revolut** è al centro di un’inchiesta avviata dalla Procura di Reggio Calabria. Il gruppo di hacker denominato **I Am Not A Villain** sostiene di aver ottenuto anche documenti e comunicazioni riconducibili alle **forze dell’ordine italiane**.

Secondo la rivendicazione, ancora sottoposta alle verifiche degli investigatori, l’operazione sarebbe proseguita per diversi mesi e avrebbe consentito ai pirati informatici di acquisire circa **147 gigabyte di informazioni**, tra documenti interni e conversazioni riservate.

Gli hacker avrebbero chiesto a Revolut un riscatto di **tre milioni di dollari**, minacciando di cedere il materiale ad altri gruppi criminali in caso di mancato pagamento entro il termine indicato.

Coinvolti centinaia di clienti internazionali

La violazione avrebbe interessato i dati di circa **680 clienti internazionali di Revolut**. Tra le informazioni potenzialmente finite nelle mani dei criminali informatici figurerebbero copie di passaporti e carte d'identità, coordinate bancarie e documentazione relativa a operazioni in criptovalute.

Gli investigatori stanno monitorando il **dark web**per individuare eventuali annunci di vendita o pubblicazioni del materiale sottratto. Al momento, tuttavia, l'effettiva quantità dei dati posseduti dal gruppo e la loro autenticità non risultano definitivamente accertate.

La vicenda presenta caratteristiche particolarmente delicate perché gli hacker affermano di essersi presentati alla banca come rappresentanti di un ente italiano incaricato di attività investigative. A sostegno della propria versione avrebbero mostrato alcune immagini di presunte comunicazioni elettroniche scambiate durante l'operazione.

L'indagine della Procura di Reggio Calabria

La **Procura di Reggio Calabria**ha aperto un fascicolo dopo aver ricevuto una prima informativa della Polizia postale. L'ipotesi investigativa riguarda un possibile **accesso abusivo a un sistema informatico di interesse pubblico**.

Gli accertamenti dovranno chiarire se sia stata compromessa la posta elettronica certificata della Prefettura di Reggio Calabria, se l'indirizzo istituzionale sia stato clonato oppure se siano state utilizzate altre tecniche capaci di riprodurre in modo credibile l'identità digitale dell'ente.

Non vi è ancora la certezza che siano stati violati direttamente i sistemi informatici della **Prefettura o del Ministero dell'Interno**. Secondo le prime ricostruzioni, però, l'operazione sarebbe stata pianificata con notevole attenzione e portata avanti attraverso richieste distribuite nell'arco di circa sei mesi.

Questo metodo avrebbe permesso agli autori dell'attacco di non destare immediatamente sospetti e di ottenere progressivamente informazioni riservate su alcuni correntisti.

Le rassicurazioni fornite da Revolut

Revolut ha precisato che **i propri sistemi informatici e i fondi dei clienti non sarebbero stati compromessi**. La ricostruzione al vaglio degli inquirenti indica infatti che i dati potrebbero essere stati consegnati in seguito a richieste fraudolente apparentemente provenienti da un'autorità italiana.

La distinzione è importante perché l'episodio potrebbe non derivare da una violazione diretta dell'infrastruttura tecnologica della banca. Potrebbe invece trattarsi di una sofisticata attività di **impersonificazione digitale**, realizzata sfruttando un indirizzo istituzionale autentico, compromesso o riprodotto artificialmente.

Gli investigatori dovranno quindi determinare il punto esatto della catena di comunicazione in cui si è verificata la falla e verificare se le procedure adottate per controllare l'identità dei richiedenti fossero adeguate.

Gli accertamenti della Procura nazionale antimafia

Sulla vicenda sono in corso approfondimenti anche da parte della **Procura nazionale antimafia e**

antiterrorismo, considerata la possibile violazione di sistemi o comunicazioni riconducibili a un ente governativo.

L'interesse degli investigatori non riguarda soltanto la sottrazione dei dati, ma anche il loro possibile utilizzo per ulteriori frodi, ricatti, furti d'identità o trasferimenti illeciti di denaro.

La disponibilità di documenti personali e informazioni finanziarie potrebbe infatti consentire ai criminali di costruire operazioni fraudolente particolarmente credibili, colpendo sia i singoli correntisti sia gli istituti coinvolti.

Il Garante della Privacy verifica i sistemi bancari

Anche il **Garante per la protezione dei dati personali**ha avviato verifiche per comprendere la portata dell'accaduto e accertare l'eventuale presenza di vulnerabilità nei sistemi utilizzati dagli istituti finanziari.

L'Autorità ha invitato i responsabili della protezione dei dati delle banche a effettuare controlli tempestivi sulle proprie procedure. In presenza di anomalie o falle di sicurezza, gli istituti sono stati sollecitati ad adottare immediatamente le misure necessarie e a informare il Garante.

L'obiettivo è verificare se episodi analoghi abbiano interessato altre banche e se le procedure adottate per rispondere alle richieste provenienti dalle autorità siano sufficientemente protette contro tentativi di falsificazione.

Collaborazione con l'Autorità lituana

Il Garante italiano ha inoltre coinvolto l'Autorità competente della **Lituania**, Paese nel quale si trova la principale sede legale europea di Revolut. Lo scambio di informazioni dovrebbe consentire di ricostruire con maggiore precisione la vicenda e coordinare le attività di controllo.

Sono stati avviati contatti anche con il Ministero dell'Interno per comprendere se siano state compromesse comunicazioni istituzionali e per accertare l'eventuale coinvolgimento di altri istituti finanziari.

Una vicenda ancora in fase di accertamento

Il **caso Revolut**evidenzia quanto le tecniche di ingegneria sociale possano essere pericolose anche quando non avviene una violazione diretta dei sistemi bancari. La capacità di presentarsi come un'autorità pubblica può indurre un'organizzazione a condividere informazioni che, in condizioni normali, sarebbero protette da rigide procedure di sicurezza.

Resta ora da verificare se i documenti mostrati dagli hacker siano autentici, quale sia stata l'origine dell'accesso e quanti clienti siano stati realmente coinvolti. Fino alla conclusione degli accertamenti, le dichiarazioni del gruppo responsabile della rivendicazione devono essere considerate affermazioni non ancora confermate dalle autorità.