Attacco a Revolut: quando una PEC compromessa diventa un’arma. E perché l’Italia è al centro della vicenda

Un gruppo di criminali informatici si è finto forza dell’ordine italiana usando una PEC istituzionale compromessa. Revolut ha consegnato dati sensibili di 680 clienti. Le rivendicazioni su presunti archivi delle forze dell’ordine restano da verificare.

Una truffa di impersonificazione, non un attacco ai server di Revolut (questa è una fintech britannica – tecnologia finanziaria) che offre servizi bancari digitali interamente tramite app**.**

Secondo le ricostruzioni di ANSA, Euronews e Financial Times, Revolut ha ricevuto per mesi richieste di dati da un indirizzo PEC appartenente al dominio **pec.interno.it**, riconducibile alla Prefettura di Reggio Calabria. La banca, come previsto dalle procedure di cooperazione con le autorità, ha risposto fornendo:

- nomi, indirizzi, date di nascita;
- numeri di telefono;
- copie di passaporti e carte d’identità;
- selfie e foto ;
- estratti conto e cronologie di transazioni, incluse quelle in criptovalute.

Non c’è stata alcuna violazione dei sistemi Revolut: i fondi e l’infrastruttura tecnica non sono stati toccati. Il punto debole è stato **il processo di verifica delle richieste provenienti da autorità europee**, che la banca ha considerato valide perché provenienti da un dominio governativo certificato.

Il gruppo “IAmNotAVillain”: rivendicazioni, fuga di notizie e richiesta di riscatto

Il gruppo (o individuo) che si firma **IAmNotAVillain / iamnotavillain** ha rivendicato l’operazione tramite Telegram, condividendo screenshot delle comunicazioni con Revolut. Dichiara di aver:

- selezionato i target tra “cripto valute”;
- operato per mesi fingendosi forze dell’ordine;
- ottenuto dati di circa **680 clienti**;
- sottratto **147 GB** di documenti, che includerebbero anche materiali interni delle forze dell’ordine italiane (non verificati).

Il gruppo chiede un riscatto di **3 milioni di dollari in Monero**, ((XMR, una criptovaluta molto difficile da tracciare) minacciando di vendere i dati se Revolut non paga.

La parte italiana: cosa è certo e cosa no

Cosa è confermato

- La PEC della Prefettura di Reggio Calabria è stata **compromessa**: non inganno, ma **accesso abusivo** alla casella, probabilmente tramite furto di credenziali.
- Le richieste fraudolente sono state inviate da un indirizzo reale appartenente a un dominio governativo.
- Polizia Postale, Procura di Reggio Calabria e DNA hanno aperto indagini.

Cosa non è confermato

La rivendicazione dei 147 GB di “dati interni delle forze dell’ordine italiane” — calendari, chat personali, documenti — **non ha al momento riscontri ufficiali**. Gli investigatori non hanno evidenze di una compromissione profonda dei sistemi del Ministero dell’Interno o della Prefettura.

È possibile che il gruppo stia **gonfiando le rivendicazioni** per aumentare la pressione, come spesso accade nelle estorsioni cyber.

Perché è successo: il punto debole della catena di fiducia

Social engineering di alto livello

La PEC istituzionale ha superato i controlli tecnici. Il problema non è stato tecnologico, ma **procedurale**: molte aziende tendono a soddisfare richieste apparentemente ufficiali senza verifiche secondarie, soprattutto quando arrivano da domini governativi.

Rischio sistemico sulla PEC

Se le credenziali di caselle istituzionali vengono rubate tramite malware, l’intero sistema di fiducia della PEC — pensato per garantire autenticità — diventa un vettore di attacco. Questo caso mostra come un singolo anello debole possa produrre un danno enorme.

Impatto sulle vittime: privacy, identità e sicurezza personale

Per i 680 clienti coinvolti, molti con grandi posizioni crypto, il rischio è elevato:

- furti d’identità;
- truffa fraudolenta mirata;
- estorsioni personalizzate;
- vendita dei dati a gruppi specializzati.

Revolut ha contattato direttamente le persone coinvolte, ma il potenziale danno resta significativo.

Il lato “teatrale” dell’operazione

Countdown, fughe di notizie, faide interne tra criminali, rivendicazioni amplificate: sono elementi tipici delle campagne di estorsione, pensati per:

- aumentare la pressione sulla vittima;
- generare confusione;
- attirare attenzione mediatica.

Non tutto ciò che viene dichiarato è necessariamente reale.

L’attacco a Revolut è un caso da manuale: **nessun server bucato**, nessuna falla tecnica nella banca, ma un anello debole nella catena di fiducia — la verifica delle richieste ufficiali e la sicurezza delle credenziali istituzionali.

Se le rivendicazioni sui 147 GB di dati delle forze dell’ordine italiane venissero confermate anche solo in parte,

sarebbe un tema di sicurezza nazionale. Ad oggi, però, restano **non verificate**.

Per i clienti Revolut: chi non ha ricevuto comunicazioni dalla banca **non è coinvolto**. Per tutti: nei prossimi mesi è prudente prestare attenzione alle truffe, richieste anomale e tentativi di contatto sospetti.

Chiusura

L'attacco a Revolut non è solo un incidente informatico: è un promemoria brutale del mondo in cui stiamo entrando. I criminali non cercano più di forzare porte blindate: cercano la porta lasciata socchiusa, la procedura non verificata, la password rubata a un dipendente distratto. Non hanno remore, non hanno etica, non hanno freni. Attaccano dove il sistema è debole, e il sistema — pubblico o privato — ha sempre un punto fragile.

Il guadagno facile è diventato un mestiere. Un mestiere senza fatica, senza responsabilità, senza conseguenze personali. E ogni volta che un'infrastruttura di fiducia viene compromessa, come una PEC istituzionale, il danno non è solo tecnico: è culturale. È la dimostrazione che la nostra società digitale può essere piegata da chi non ha alcun interesse a rispettarne le regole.

La domanda che resta sospesa è semplice e inquietante: cosa succederà quando questi gruppi useranno l'intelligenza artificiale non come strumento, ma come moltiplicatore? Perché il problema non è che l'IA diventi "cattiva". Il problema è che **diventi un alleato naturale di chi non ha scrupoli**.

E allora la vera sfida non è difendere i server, ma difendere la fiducia. Difendere la parte umana dei processi. Difendere la responsabilità, che è l'unica cosa che i criminali non possono rubare.

La delega tecnologica è nata per liberarci dalla fatica. Ma alcune fatiche sono necessarie: pensare, verificare, dubitare, controllare. Quando deleghiamo tutto, anche ciò che richiede coscienza e discernimento, la tecnologia non diventa un aiuto: diventa un sostituto. E ogni sostituto, se non è vigilato, diventa un rischio.

La tecnologia non ha intenzioni, ma amplifica quelle di chi la usa. Per questo la delega non è mai neutra: è un atto di fiducia. E la fiducia, nel mondo digitale, è fragile come una password rubata.

Data di pubblicazione: 20/09/2026

Salvato in PDF in data: 20/09/2026

Link all'articolo: https://civico20-news.it/cronaca/attacco-a-revolut-quando-una-pec-compromessa-diventa-unarma-e-perche-litalia-e-al-centro-della-vicenda/20/09/2026/