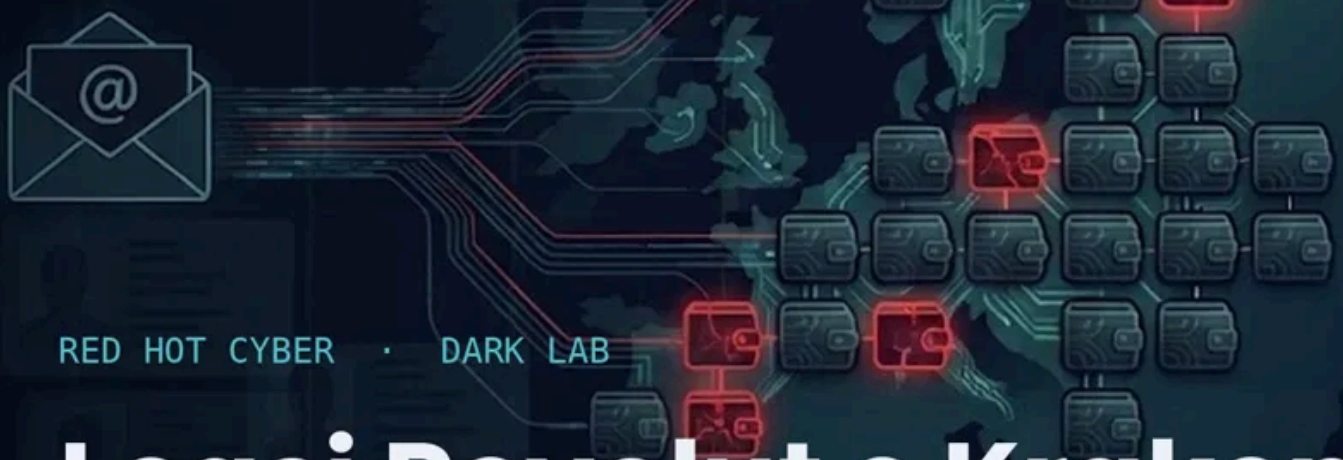
TLP:CLEAR



RED HOT CYBER · DARK LAB

I casi Revolut e Kraken

27 wallet, 27 superfici d'attacco

Report di Cyber Threat Intelligence
Analisi di caso e raccomandazioni operative

Settembre 2026 · v1.0

Olivia Terragni · Edoardo Faccioli · Luca Stivali · Raffaela Crisci

Introduzione

«27 wallets d'identité = 27 surfaces d'attaque.
La fuite Revolut me le confirme :
la souveraineté se joue dans l'exploitation.»
— Dear Vincent (@StarryCook), X, 16/09/2026.

Questo fascicolo ricostruisce due casi concreti — l'incidente Revolut (2026) e il precedente Kraken (2025) — allo scopo di trasformare l'analisi dell'attacco in uno strumento operativo di difesa.

In entrambi gli scenari, i dati sensibili dei clienti sono diventati una leva di attacco senza alcuna violazione diretta dei sistemi informatici. Nel caso Revolut, la compromissione è avvenuta tramite richieste falsificate inviate da una casella PEC istituzionale; nel caso Kraken (2026), tramite l'abuso di accessi interni ai sistemi di supporto. Al centro di questo report vi è un paradosso normativo: le informazioni che gli obblighi KYC/AML (direttive antiriciclaggio) impongono di raccogliere per tutelare il sistema (identità, documenti, transazioni) sono le stesse che, se consegnate alla parte sbagliata, espongono l'utente. Da qui la doppia natura del documento: un'analisi fattuale degli eventi e un framework di riferimento per gli operatori finanziari.

Il vettore d'attacco primario è l'abuso del canale fiduciario. Le richieste malevole sfruttano l'implicita fiducia riposta nel mittente ufficiale (PEC, email di enti governativi, o spoofing telefonico). Tra la ricezione della richiesta e l'invio dei dati si apre una falla critica di processo. Verificare una **richiesta proveniente dalle autorità** è complesso, stretto tra l'obbligo normativo di collaborazione rapida e la mancanza di strumenti per un'autenticazione certa. A ciò si somma l'errore umano: in almeno un passaggio documentato, i dati sono stati trasmessi rispondendo direttamente all'indirizzo compromesso, senza l'attivazione di canali di verifica indipendenti (es. *out-of-band*). Si tratta di fallimenti procedurali.

In una catena di fiducia tra autorità pubbliche e istituti finanziari, quali controlli spettavano a ciascun anello — l'ente titolare del canale, la banca che divulga i dati, il quadro normativo che regola le richieste — e quali sono venuti meno?" Sebbene la compromissione tecnica riguardi il mittente, le normative (a partire dal GDPR) pongono in capo all'istituto finanziario, in quanto titolare del trattamento, una responsabilità qualificata sui dati dei clienti — pur senza escludere quella degli altri anelli della catena.

Questo impone alle banche l'obbligo di implementare verifiche procedurali indipendenti: in almeno un passaggio documentato, invece, i dati sono stati trasmessi rispondendo direttamente all'indirizzo compromesso, senza attivare protocolli di autenticazione out-of-band (come una verifica telefonica tramite contatti ufficiali). Questo limite dei controlli tradizionali di fronte ad attacchi basati su credenziali istituzionali rubate (es. via infostealer) sta forzando un cambio di paradigma nel settore. Un caso emblematico è l'integrazione della Dark Web Intelligence nei processi di Anti-Financial Crime: la recente partnership strategica tra Nasdaq Verafin e Q6 Cyber evidenzia la necessità sistemica di monitorare l'underground criminale per intercettare le fughe di dati in via preventiva, colmando quella "zona grigia" procedurale sfruttata nei casi qui analizzati.

L'ultimo anello della catena è l'impatto reputazionale. Il dato sottratto viene impiegato non solo come merce nel mercato *underground*, ma come leva estorsiva: richieste di riscatto pubbliche e pressioni mediatiche su istituti esposti sui mercati dei capitali (quotazioni, *listing*, fiducia degli investitori). Poiché l'esecutore tecnico dell'attacco, l'estorsore e l'amplificatore mediatico non coincidono necessariamente, il report mantiene separati questi livelli, lasciando aperta l'attribuzione del movente.

Il perimetro metodologico si basa esclusivamente su fonti aperte (OSINT/CTI). Ogni affermazione è accompagnata da un livello di confidenza analitica (Alta, Media, Bassa), separando i fatti comprovati dalle dichiarazioni degli attori di minaccia, che sono trattate come fonti di parte e non come prove. Nessun dato personale delle vittime è riprodotto.

Infine, l'analisi solleva un interrogativo strategico di fondo: *cui prodest?* Il bersaglio reale di queste campagne è il database dell'istituto finanziario — per la mera monetizzazione dei dati — o la catena di fiducia stessa tra autorità pubbliche e soggetti privati? La distinzione non è secondaria: **se** l'obiettivo fosse il canale, e non il singolo record, il danno andrebbe letto su un piano sistemico — dubbio strutturale, collaborazione più lenta tra law enforcement e banche, l'obbligo di compliance che si ribalta in superficie di vulnerabilità — una dinamica che eccederebbe la semplice estorsione. È un'ipotesi da tenere aperta, non una conclusione: i reperti disponibili non permettono di stabilire se si tratti di monetizzazione opportunistica o di un bersaglio deliberato del canale fiduciario. Il documento non ha finalità accusatorie né stabilisce responsabilità legali; laddove i fatti non risultino accertati, lo dichiara esplicitamente. Trattandosi di un panorama di minaccia dinamico, il presente lavoro è da considerarsi in continua evoluzione.

Olivia Terragni

Indice

1. Sintesi esecutiva

Il caso Revolut non è soltanto un "data breach" nel senso classico: è un caso di **social engineering tramite abuso di un canale istituzionale e possibile fallimento dei controlli di verifica delle richieste**. Revolut ha dichiarato che i fondi dei clienti e i propri sistemi non risultavano compromessi, ma che dati sensibili sono stati consegnati a una parte non autorizzata dopo richieste fraudolente apparentemente provenienti da un dominio governativo legittimo (Reuters, 12/09/2026). Lo schema non é isolato e trova un forte parallelismo nel precedente incidente di Kraken (2025). In quell'occasione, l'esfiltrazione dei dati non è passata per la violazione del perimetro di sicurezza primario, ma per l'abuso di accessi interni ai sistemi di supporto. Entrambi gli scenari confermano un preciso trend: gli attaccanti aggirano le difese tecnologiche *core* per colpire direttamente i processi fiduciari e le procedure di assistenza.

Scala di confidenza

Livello	Significato
Alta	Più fonti indipendenti concordanti o fonte primaria (dichiarazione dell'azienda, atto giudiziario, dati tecnici verificabili)
Media	Fonte credibile ma singola, oppure più fonti che derivano dallo stesso materiale (screenshot, dichiarazioni di terzi) senza conferma ufficiale
Bassa	Rivendicazione dell'attaccante o di intermediari interessati, non verificata; oppure deduzione con elementi contrari

- **[Confidenza alta]** L’attacco ha sfruttato il processo di risposta alle richieste delle autorità, non una compromissione dei sistemi core o dei fondi di Revolut. *— Base: dichiarazione di Revolut; Reuters; PEC pubblicate*
- **[Confidenza media]** Le richieste ‘sarebbero’ partite da una casella PEC istituzionale italiana (riconducibile all’Ufficio Enti Locali della Prefettura di Reggio Calabria) e avrebbero incluso falsi Ordini europei di indagine intestati alla Procura di Milano, nel periodo marzo–luglio 2026. L’attaccante dichiara inoltre di aver ottenuto dati relativi a 680 clienti probabilmente selezionati previa analisi della blockchain e transazioni; questo numero e il metodo di selezione non sono stati confermati ufficialmente da Revolut. *— Base: screenshot PEC; StrettoWeb; Silere non possum; dichiarazioni dell'attaccante*
- **[Confidenza alta]** Lo schema non è isolato: nel 2025 Kraken avrebbe consegnato dati relativi a un cliente dopo aver ricevuto richieste false da un indirizzo @interno.it, seguite da minacce fisiche. *— Base: atto CGC-26-634771, San Francisco Superior Court.* La confidenza alta riguarda l’esistenza e il contenuto dell’episodio documentato nell’atto; non implica che l’episodio Kraken e quello Revolut siano stati condotti dallo stesso gruppo.
- **[Confidenza media]** Gli attori mostrano indicatori di disciplina operativa limitata — infrastruttura trascurata, conflitto pubblico tra gruppi e sito web basato su un modello — ma il successo dell’operazione dipende soprattutto dal canale istituzionale sfruttato e non dimostra necessariamente una capacità tecnica complessivamente bassa. *— Base: KELA; Duel; codice del sito; WHOIS*
- **[Confidenza media]** Il rischio è replicabile verso altri istituti che ricevono richieste delle autorità via PEC o email, incluse le banche italiane. La **circolazione di credenziali istituzionali in log di infostealer e combolist è indicata da fonti di threat intelligence** e da precedenti avvisi, ma il collegamento diretto con la PEC del caso Revolut non è pubblicamente dimostrato. *— Base: CERT-AGID; fonte TI di settore; FBI 2024*

2. Cronologia dell'incidente

Data	Evento	Confidenza
maggio–luglio 2025	Kraken riceve una richiesta falsa da "@interno.it"; consegna dati; minacce fisiche al cliente; ad agosto finto ordine irlandese	Alta (atto giudiziario, versione dell'attore)
06/03/2026	Causa Doe v. Kraken depositata: lo schema diventa pubblico (comunicato 16/03)	Alta
24/03/2026	PEC tra Revolut e @pec.interno.it: Revolut indica di reintestare la richiesta alla società crypto cipriota	Media (screenshot)
04–05/05/2026	Falso Ordine europeo di indagine "Procura di Milano" verso Revolut Bank UAB; circa 40 messaggi	Media
24/07/2026	Revolut invia dati cifrati a entilocali.prefrc@pec.interno.it; distinzione per giurisdizione (169 hash Revolut Ltd, 29 entità svizzera)	Media (screenshot)
12/09/2026	Revolut conferma la consegna dei dati e blocca l'indirizzo	Alta
13/09/2026	Prime pubblicazioni su Telegram ("Example 1"); creazione del canale di "smile"	Alta
14/09/2026	Sito di estorsione; imnotavillain.xyz registrato; Revolut Smilik contatta City AM; richiesta di rimozione Telegram da 8 aziende; ICO segnalazione ricevuta: *"We can confirm we have received a report and are assessing the information provided."* Euronews (16/09)	Alta
15/09/2026	iamnotavillain.com registrato; stampa italiana identifica la PEC della Prefettura; Polizia Postale indaga	Alta
16/09/2026	Riscatto di 6.000 XMR / 3 milioni di dollari con countdown; video del materiale; chiusura di GitHub, di canali Telegram e del sito del gruppo; nuovo dominio con dati di 12 clienti. In parallelo compare il sito informativo di terzi iamnotavillain[.]info, con countdown proprio verso il 21/09.	Media
17/09/2026	Scaduta alle 18:30 la deadline di 24 ore del sito di estorsione del gruppo; il sito va offline. Revolut dichiara di non aver ricevuto contatti diretti né richieste dal gruppo (FT/CoinDesk; Reuters).	Media
18/09/2026	Fonti investigative riferite dalla stampa: la Polizia Postale non ha riscontrato falle nei sistemi del Viminale e i primi accertamenti non confermano la sottrazione dei 147 GB; da stabilire se la casella sia stata	Media

Data	Evento	Confidenza
	compromessa o clonata. Il Garante privacy avvia verifiche sugli accessi delle banche italiane, invia una comunicazione ai DPO bancari, apre uno scambio con l'autorità lituana e un'interlocuzione con il Ministero dell'Interno	
19/09/2026	Risposta parlamentare: la sottosegretaria all'Interno Wanda Ferro riferisce (interrogazione Pastorella, Azione) che sono in corso i primi approfondimenti delle strutture di sicurezza cibernetica del Ministero, sotto riserbo, e che l'ACN ha interlocuzioni con Revolut e collabora con il Ministero, avendo informato Polizia Postale e DNAA. Il sito informativo iamnotavillain[.]info mostra un countdown ancora attivo (≈40 h) verso il 21/09.	Media

Secondo le ricostruzioni pubbliche, il caso Revolut potrebbe inserirsi in uno s**chema più ampio di abuso delle caselle istituzionali** e dei processi con cui banche, exchange e fintech rispondono alle richieste delle autorità. Alcune ricostruzioni collegano precedenti richieste rivolte a piattaforme crypto all'uso di indirizzi appartenenti a domini istituzionali; **questi collegamenti devono però essere verificati caso per caso e non possono essere presentati automaticamente come parte di un'unica campagna.**

Nel 2025, secondo la ricostruzione disponibile, **Kraken** avrebbe ricevuto una richiesta proveniente da un indirizzo del dominio **interno.it** e avrebbe trasmesso dati relativi a un cliente, che successivamente avrebbe ricevuto minacce fisiche. Nel 2026, lo schema sarebbe proseguito attraverso una PEC istituzionale sul dominio **`pec.interno.it`** e documenti presentati come Ordini europei di indagine. Nel caso Revolut, le ricostruzioni giornalistiche indicano che richieste fraudolente sarebbero state utilizzate per ottenere, anche per un **periodo prolungato**, fascicoli KYC di clienti ad alto patrimonio selezionati attraverso informazioni pubbliche sulla blockchain. Questi elementi suggeriscono una **possibile continuità operativa,** ma il collegamento tra i diversi episodi resta un'ipotesi da verificare. A settembre il caso è esploso: gli attori (IAmNotAVillain, Revolut Smilik) passano all'estorsione e alla pubblicazione dei dati, un casinò crypto (Duel) ottiene il contatto privilegiato con l'hacker e fornitori, media e account terzi amplificano l'incidente. Le rivendicazioni sul numero delle vittime, sulla selezione dei clienti tramite blockchain e sull'eventuale compromissione di altri sistemi devono essere classificate separatamente come dichiarazioni dell'attaccante, reporting giornalistico o elementi ancora non confermati.

Il punto di arrivo è politico-normativo: **Lyudmyla Kozlovska, attivista ucraina per i diritti umani** e **fondatrice e presidente della Open Dialogue Foundation (ODF)** usa il caso come prova che la verifica delle richieste statali è impossibile e che le regole FATF, antiriciclaggio e DAC8 vanno cambiate. Questo passaggio deve essere presentato come una lettura o una posizione nel dibattito pubblico, non come prova che le norme siano causalmente responsabili dell'incidente. *Lyudmyla Kozlovska, fornisce una lettura politico-normativa del caso.* ***Le sue dichiarazioni sono rilevanti per il dibattito su verifica delle richieste statali, cooperazione giudiziaria e repressione finanziaria transnazionale.***

Il punto analitico centrale è il **possibile abuso della catena di fiducia tra autorità pubbliche e operatori finanziari**. Se una richiesta viene considerata autentica soltanto perché proviene da un dominio o da una casella istituzionale, la verifica tecnica del mittente può diventare insufficiente. Le connessioni tra i diversi episodi restano ipotesi di analisi; i singoli elementi sono documentati nelle sezioni successive.

Aggiornato al 20 settembre 2026. Materiale raccolto da fonti aperte, documenti giudiziari, dati DNS e di rete, post social, screenshot e messaggi ricevuti.

Il punto critico (ipotesi)

La PEC certifica invio, consegna, integrità del messaggio e riconducibilità della trasmissione all'indirizzo PEC del mittente, ma non identifica automaticamente la persona che ha redatto il contenuto né garantisce che fosse autorizzata a farlo. L'identificazione dell'autore del documento richiede un elemento ulteriore,

normalmente una firma digitale qualificata o un diverso meccanismo verificabile. Nel caso Revolut, lo screenshot disponibile di un presunto ordine di esibizione informazioni (OEI) non mostra firma digitale né timbro chiaramente identificabile ed è redatto in inglese; allo stato delle informazioni pubbliche, non è noto se le richieste effettivamente ricevute da Revolut contenessero allegati firmati digitalmente. La trasmissione diretta alla PEC italiana di Revolut, anziché all'autorità di esecuzione competente dello Stato indicato (Lituania), appare incompatibile con il normale meccanismo di riconoscimento ed esecuzione dell'EIO (dir. 2014/41/UE, art. 9) e avrebbe dovuto richiedere verifiche supplementari. Da sola, tuttavia, non dimostra che il documento fosse falso: occorre verificare il mittente, la firma, il modulo standard (Allegato A), l'autorità emittente e gli eventuali contatti ufficiali tra le autorità.

REPUBBLICA ITALIANA

EUROPEAN INVESTIGATION ORDER (EIO)

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014
regarding the European Investigation Order in criminal matters

Issuing Authority: Public Prosecutor's Office at the Court of Milan
(competent pursuant to Legislative Decree 108/2017)
Address: Via Freguglia 1, 20122 Milano, Italy
Reference / Protocol: Prot. n. [redacted]/2026
Date: 4 May 2026

Issuing State: Italian Republic
Executing State: Republic of Lithuania
Recipient Executing Authority: General Prosecutor's Office of Lithuania or the competent Lithuanian authority for financial investigations / Revolut Bank UAB
Revolut Bank UAB registered address: Konstitucijos pr. 21B, Vilnius, LT-08130, Lithuania

Subject

Request for the acquisition of banking and financial information relating to the following deposit addresses associated with accounts held with Revolut Bank UAB (an entity registered in Lithuania).

Deposit Addresses (wallets):	[redacted]

PEC: cosa certifica e cosa no

A differenza della posta elettronica ordinaria, il campo mittente di un messaggio PEC non è falsificabile dall'esterno (*spoofing*). Un messaggio risulta valido solo se parte effettivamente da una casella PEC reale ed è processato dal suo gestore accreditato, il quale lo firma digitalmente e genera le ricevute di accettazione e

consegna. Non è quindi tecnicamente possibile contraffare il mittente entilocali.prefrc@pec.interno.it senza avere accesso diretto a quella specifica casella o all'infrastruttura che la ospita.

La PEC, per sua natura, certifica l'invio, la consegna, l'integrità del contenuto e la validità della casella mittente. **Tuttavia, non certifica l'identità fisica della persona che digita il testo, né la sua legittimazione a formulare la richiesta**. È la distinzione fondamentale tra *autenticità del canale* (tecnicamente ineccepibile) e *legittimazione del mittente* (in questo caso, fraudolenta). Ne consegue che, se i messaggi ricevuti da Revolut erano PEC autentiche, la casella governativa era realmente sotto il controllo degli attori di minaccia (ipotesi di *Account Takeover*); il *come* vi abbiano avuto accesso resta oggetto di indagine. Va infine precisato che la verifica tecnica di questa compromissione si può effettuare solo analizzando le intestazioni complete (*header*) e la busta di trasporto firmata dal gestore: elementi attualmente non presenti nel materiale disponibile su fonti aperte. **[Confidenza alta]** — *Base normativa: DPR 68/2005 e Regole Tecniche (DM 2/11/2005).*

Nota — autenticità dell'indirizzo mittente. Sul sito del gruppo l'indirizzo della casella è oscurato; l'indirizzo completo (entilocali.prefrc@pec.interno.it) è circolato tramite uno screenshot attribuito a Korra/Duel e la stampa italiana, non è stato "indovinato". Poiché quelle immagini sono curate e marchiate dagli attori, l'indirizzo non può essere considerato autentico sulla sola base degli screenshot: in linea di principio la casella mostrata potrebbe non coincidere con quella realmente usata.

Depongono però a favore della sua realtà tre elementi indipendenti dalle immagini: una PEC valida parte solo da una casella realmente esistente (un indirizzo inventato non genererebbe messaggi PEC validi); l'indirizzo segue la convenzione effettiva delle Prefetture (entilocali.pref<sigla>, cfr. Cosenza) su interno.it, gestito da InfoCert; gli investigatori trattano la casella come reale, valutando come vi si sia avuto accesso, non se esista.

Conclusione operativa: l'indirizzo va considerato reale ed esistente per validità PEC, convenzione e riscontro di terzi, non sulla base delle immagini del gruppo. La certezza sul fatto che la casella mostrata sia esattamente quella usata può venire solo dalla busta di trasporto/log del gestore PEC. [Confidenza media-alta sull'esistenza della casella; bassa sull'identità esatta ricavabile dagli screenshot] — Base: screenshot attribuito a Korra/Duel; stampa; convenzione PEC delle Prefetture; disciplina PEC

Confronto Kraken / Revolut

Kraken e Revolut mostrano due applicazioni successive e potenzialmente correlate dell'abuso di richieste apparentemente istituzionali contro operatori crypto. Il caso Revolut presenta un canale più evoluto — PEC, documento giudiziario formale e targeting su larga scala — ma il materiale disponibile non dimostra che i due episodi siano stati condotti dallo stesso attore,
A conferma della fase di mercato sensibile, all'epoca delle richieste contestate (maggio–agosto 2025) la traiettoria IPO di Kraken era già pubblica: obiettivo dichiarato per il primo trimestre 2026 (marzo 2025) e un round da 500 milioni di dollari a una valutazione di 15 miliardi nel settembre 2025. Il 3 febbraio 2026 Kraken ha inoltre pubblicato, pur restando privata, rendicontazioni in stile societario quotato — ricavi rettificati 2025 per 2,2 miliardi di dollari (+33% su base annua) ed EBITDA rettificato di 531 milioni — prima della pausa dell'IPO a marzo 2026.

[Confidenza alta sui dati IPO e finanziari di Kraken] — Base: Bloomberg (07/03/2025); Fortune (25/09/2025); comunicato Kraken (03/02/2026).

Aspetto	Kraken (2025)	Revolut (2026)
Tipo di azienda	Exchange crypto	Fintech con licenze bancarie (Regno Unito, Lituania, Francia) e società crypto a Cipro
Fase di mercato	In preparazione dell'IPO: traiettoria pubblica da marzo	In preparazione di una possibile doppia quotazione (Londra + Wall Street), orizzonte indicato al 2028

prima dell'attacco	2025, obiettivo dichiarato Q1 2026	
Periodo e sequenza dell'attacco	Email spoofate maggio–agosto 2025 → estorsione/sorveglianza (2025); filing IPO confidenziale annunciato ad aprile 2026, poi rinvio verso il 2027	Richieste da PEC (rif. 24/03 e 24/07 2026), campagna di raccolta dati durata ~5–6 mesi secondo il claim dell'attore → breach e richiesta di riscatto (settembre 2026)
Tipo di incidente	Consegna di dati a email che sembravano provenire da un'agenzia di law enforcement italiana	Consegna di dati a richieste inviate da una PEC autentica su dominio istituzionale italiano (Prefettura di Reggio Calabria)
Vettore tecnico	Spoofing del mittente: email contraffatte con branding di law enforcement, mittente falsificato	Abuso di canale certificato: PEC reale (entilocali.prefrc@pec.interno.it); l'autenticazione risulta allineata perché la posta passa dal canale genuino
Casella della falsa autorità	Indirizzo ordinario @interno.it	24/03: @pec.interno.it (oscurato) con copia a @interno.it; 24/07: entilocali[.]prefrc[@]pec.interno.it
Casella dell'azienda	lawenforcement[@]kraken[.]com	revolut[.]italy[.]pec[@]legalmail[.]it
Documento presentato	"Information request", seguito da un presunto ordine irlandese	Presunti Ordini europei di indagine intestati alla Procura di Milano
Metodo della richiesta	Singolo cliente	Centinaia di ID di transazione e indirizzi di deposito usati come chiavi di ricerca ("spray and pray")
Bersaglio	Cliente con conto di valore elevato	Detentori di crypto ("whale") tra i clienti, con saldi elevati
Dati esposti	Nome, data di nascita, indirizzo, telefono, informazioni sul conto	Dati KYC e finanziari di ~680 clienti europei: passaporti, selfie KYC, IBAN, storico transazioni
Claim aggiuntivi dell'attore [non confermati]	Nessun claim pubblico su larga scala; la vicenda emerge tramite la causa civile del cliente	147 GB sottratti a sistemi delle forze dell'ordine italiane e uso di un RAT; campagna durata ~6 mesi
Conferme ufficiali	Causa pubblica; Kraken non ha smentito la dinamica di base (email spoofate, disclosure di dati)	Revolut ha confermato il breach e la consegna a richieste fraudolente da dominio governativo autentico; nessuna conferma ufficiale sui 147 GB
Estorsione successiva	Dati usati per estorsione/sorveglianza: minacce, sorveglianza, tentato ingresso in abitazione	Richiesta di 3 milioni di dollari (indicati come ~6.000 XMR), ultimatum 24h scaduto il 17/09/2026; sito degli attaccanti poi offline

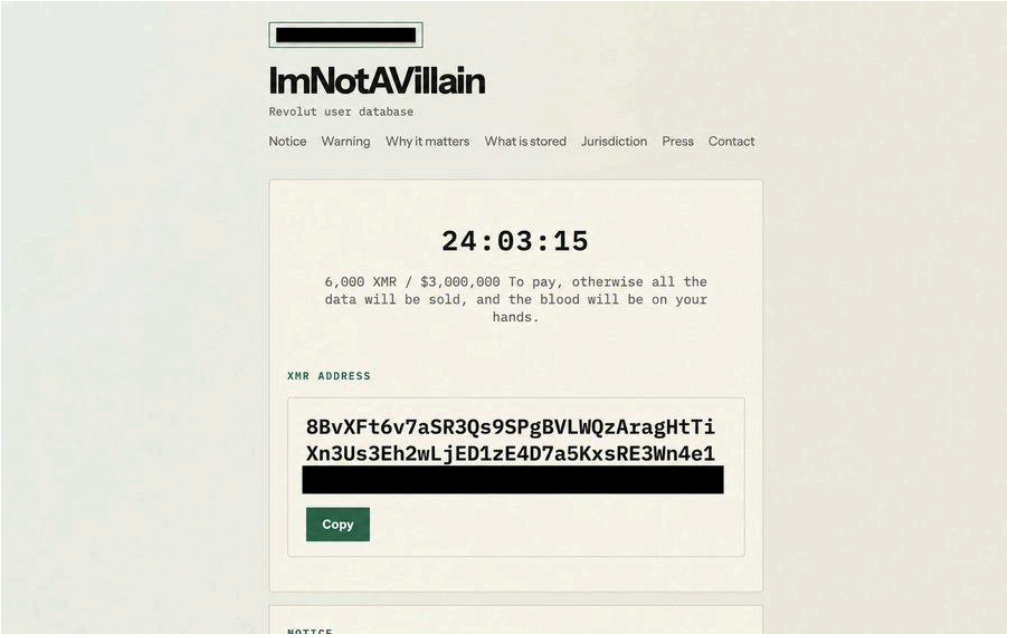
Coinvolgimento autorità italiane	Nessuna indagine italiana pubblica nota sulla mail spoofata; la causa è negli USA	Inchiesta della Procura di Reggio Calabria per intrusione in sistema informatico di pubblico interesse; accertamenti di ACN, Polizia Postale, DNA
Dimensione reputazionale / pre-quotazione	Incidente in fase pre-IPO; impatto potenziale sulla fiducia	Incidente in fase pre-quotazione; impatto potenziale su reputazione e valutazione. Nesso con la quotazione non dimostrato; effetto reputazionale reale a prescindere dall'intenzione
Threat actor identificato	Nessuno pseudonimo pubblico noto (gestita come causa civile, non come claim di gruppo)	Pseudonimo IAmNotAVillain, con siti (iamnotavillain[.]xyz, iamnotavillain[.]com) e canali Telegram
Secondo incidente Kraken (da non confondere)	Aprile 2026: accesso interno non autorizzato di due addetti al supporto a ~2.000 account; nessun legame con law enforcement italiano o PEC	Non applicabile

Confidenza alta sui fatti confermati; i claim su 147 GB, RAT e durata di sei mesi restano dichiarazioni non verificate dell'attore; "allegazioni" per la dinamica Kraken, da atto di parte] — Base: atto Doe v. Payward (Kraken); Bloomberg (07/03/2025), Fortune (25/09/2025), comunicato Kraken (03/02/2026); Il Post, Adnkronos, SecurityWeek, Cybernews (Revolut); Procura di Reggio Calabria, ACN, Polizia Postale (accertamenti).

3. Fatti confermati

- Revolut ha confermato la divulgazione di dati di clienti a una parte non autorizzata dopo la ricezione di richieste fraudolente inviate utilizzando un indirizzo appartenente a un dominio governativo legittimo. L'azienda ha dichiarato che i fondi dei clienti e i propri sistemi non risultavano compromessi, che gli utenti interessati erano stati contattati, che l'indirizzo era stato bloccato e che le autorità competenti erano state informate (Reuters, 12/09).
- Le informazioni potenzialmente coinvolte comprendono dati anagrafici e di contatto, copie di documenti d'identità e, secondo alcune ricostruzioni, selfie di verifica, estratti conto e dati transazionali. Revolut non ha pubblicato un conteggio ufficiale delle persone coinvolte; la cifra di 680 clienti proviene da fonti giornalistiche e da dichiarazioni attribuite agli attaccanti.
- Un precedente comparativo è documentato nell'atto di denuncia relativo a Kraken: nel 2025 l'azienda avrebbe ricevuto richieste provenienti dal dominio ufficiale interno.it di un'agenzia italiana di law enforcement e avrebbe divulgato dati senza un decreto dell'autorità giudiziaria. Questo elemento sostiene l'ipotesi di un **rischio ricorrente associato all'abuso dei canali istituzionali**, ma non dimostra da solo che i due episodi siano stati condotti dagli stessi attori.
- **Polizia Postale:** indaga sul caso Revolut per le ipotesi di accesso abusivo a sistema informatico e frode informatica.
- Accertamenti tecnici: secondo ricostruzioni giornalistiche del 18/09 gli accertamenti sono condotti dalla Polizia Postale e dal Cnaipic. Le ricostruzioni disponibili divergono però sul punto d'ingresso: Il Sole 24 Ore riferisce che gli investigatori non hanno la certezza che sia stato compromesso un computer della Prefettura o del Viminale e che si sta stabilendo se la casella sia stata "bucata" oppure clonata; altre ricostruzioni pubbliche riportano invece che la compromissione sarebbe limitata alle credenziali della casella dell'ufficio Enti Locali, senza accesso ai database delle forze dell'ordine né allo SDI. Non risulta una nota ufficiale del Ministero che chiarisca il punto. [Confidenza media sull'attività di accertamento; bassa sul punto d'ingresso]

- **ICO britannico:** ha ricevuto una segnalazione da Revolut, alcune testate hanno parlato di indagine, ma l'ICO non l'ha ancora confermato.
- **Kraken, 2025**: dati consegnati in risposta a richieste da "the official domain (interno.it) of an Italian law enforcement agency" (atto, par. 98), senza decreto dell'autorità giudiziaria.
- **Domini dell'attore registrati:** il 14/09 (imnotavillain.xyz) e il 15/09 (iamnotavillain.com).
- **Estorsione:** sono state pubblicate schede KYC con watermark ed è stata formulata una richiesta di riscatto in Monero. Questi elementi documentano l'attività osservata dell'attore, ma non provano da soli l'autenticità integrale di ogni scheda pubblicata. Nel pomeriggio del 17 settembre il countdown si è azzerato.



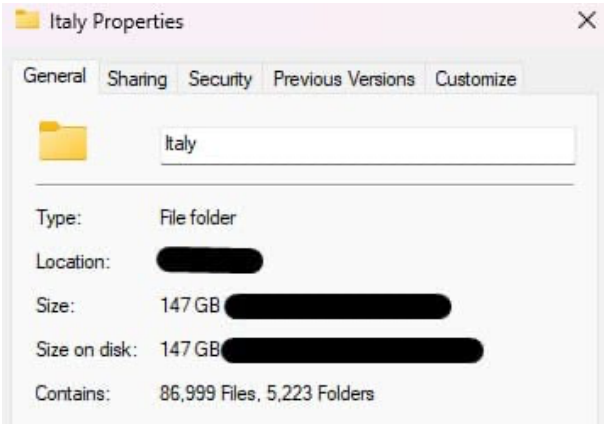
- e-Evidence: il regolamento (UE) 2023/1543 si applica dal 18 agosto 2026. Al 18 settembre 2026 non risultano dichiarazioni pubbliche specifiche del Ministero dell'Interno o dell'ACN sul caso; secondo la stampa, ACN, Banca d'Italia e Polizia Postale risultano al lavoro sul caso, e la Procura di Reggio Calabria ha aperto un'indagine.
- Garante privacy: secondo la stampa (18/09) ha avviato una verifica sugli accessi ai dati nelle banche italiane e sull'eventuale presenza di altri tentativi, ha inviato alla rete dei responsabili della protezione dei dati degli istituti bancari un invito a una "solerte verifica" con segnalazione immediata di eventuali falle, ha promosso uno scambio informativo con l'autorità di protezione dei dati lituana e ha aperto un'interlocuzione con il Ministero dell'Interno per accertare il coinvolgimento di altri istituti.

4. Dichiarazioni dell'attaccante non verificate

Le dichiarazioni vanno separate dai fatti confermati da Revolut e dalle evidenze tecniche indipendenti. La tabella seguente mantiene le qualifiche di confidenza e rende più precise le basi documentali.

Affermazione	Fonte	Confidenza
Dati di 680 clienti Revolut, selezionati tramite blockchain analysis sulla base delle disponibilità crypto	IAmNotAVillain; ripreso da fonti giornalistiche	Bassa.Il numero e il metodo di selezione non risultano confermati da Revolut. La consegna di dati a un soggetto non autorizzato è invece confermata, senza conferma pubblica del numero di clienti o del criterio blockchain.

Affermazione	Fonte	Confidenza
Accesso per sei mesi a più uffici delle forze dell'ordine italiane; 147 GB (cartella "Italy": 86.999 file, 5.223 cartelle), rivendicazione distinta dai dati Revolut	IAmNotAVillain via International Cyber Digest; screenshot delle proprietà della cartella	Bassa (lo screenshot mostra solo nome e dimensioni) I primi accertamenti della Polizia Postale, riferiti dalla stampa il 18/09, non confermano la sottrazione dei 147 GB.
Accesso alla casella tramite infostealer / RAT; indirizzo di recupero aggiunto; cancellazione dei messaggi	Duel (Korra); TA	Bassa. La sequenza è tecnicamente plausibile e compatibile con una compromissione di account, ma non è stata verificata tramite log, telemetria dell'ente o analisi forense indipendente.
Metodo "spray and pray": centinaia di ID di transazioni e indirizzi di deposito inviati come chiavi di ricerca	Duel (dichiara di aver verificato file .eml)	Media (coerente con elenco wallet-KYC e PEC)
Revolut avvisata prima della pubblicazione e rimasta in silenzio	sito del gruppo; FrenchBreaches	Bassa.Non risulta conferma pubblica indipendente della ricezione, del contenuto o dei tempi delle notifiche.
Riscatto di 10.000 BTC	IT-Connect, The Register, post social	Bassa. La richiesta è riportata da alcune fonti, ma non risulta documentata come richiesta autentica ricevuta direttamente da Revolut. Va mantenuta come rivendicazione non confermata e distinta dalla successiva richiesta in XMR.
Riscatto di 6.000 XMR / 3 milioni con scadenza 24 ore	sito ImNotAVillain; Duel	Media. La richiesta di 6.000 XMR, pari a circa 3 milioni di dollari, è la richiesta pubblica più documentata, ma resta una comunicazione degli attori e non una cifra confermata da Revolut. Eventuali riferimenti a 10.000 BTC devono essere trattati come rivendicazioni precedenti o non confermate e non vanno fusi con la richiesta in Monero.
"Revolut Smilik" identità separata e non correlata	IAmNotAVillain via KELA; Duel	Media, Bassa..È documentata l'esistenza di una rivendicazione separata associata al nome "Revolut Smilik", ma non è verificato che si tratti di un ex collaboratore, né che disponga di un sottoinsieme autentico dei file. International Cyber Digest riferisce di aver parlato con un soggetto che usava quel nome, ma ciò non prova l'identità dichiarata



Proprietà della cartella "Italy" diffuse come prova dei 147 GB (screenshot ricevuto)

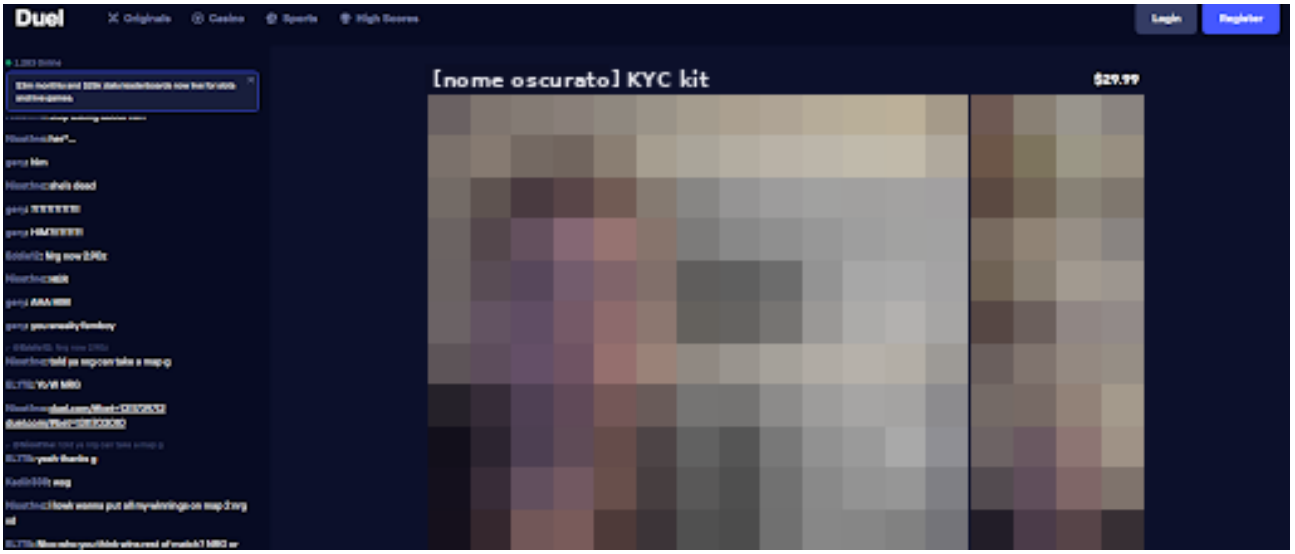
4-bis. Attori e infrastruttura

L'attribuzione primaria resta provvisoriamente associata a IAmNotAVillain, con confidenza media, sulla base della continuità delle rivendicazioni e delle informazioni pubblicate da Duel e KELA. Revolut Smilik è trattato come identità operativa separata: un collegamento con IAmNotAVillain è possibile ma non dimostrato, e l'ipotesi di un ex collaboratore con accesso parziale ai file rimane non verificata. Duel/Korra **non risulta coinvolto nell'intrusione**.

Ruolo di Duel/Korra. Il casinó crypto Duel (Duelbits/duel.com) ha pubblicato nella sezione merch del proprio sito una pagina "KYC kit" (29,99 dollari) con il documento d'identità e il selfie di verifica di una persona; l'esistenza della pagina è verificata (acquisizione diretta; urlscan, 17/09/2026).

[Confidenza alta] Secondo International Cyber Digest, i dati proverrebbero dagli attori della minaccia e sarebbero stati ottenuti da un dipendente di Duel, in un contesto in cui Duel/Korra dichiarano contatti diretti con IAmNotAVillain.

[Confidenza media-bassa affermazione non documentata pubblicamente] Se confermato, ciò configurerebbe un ruolo attivo nella diffusione e nella monetizzazione del materiale, distinto dall'intrusione iniziale, per la quale non emergono a oggi evidenze di coinvolgimento. Una parte rilevante delle comunicazioni attribuite a IAmNotAVillain proviene inoltre da materiale diffuso da Duel, soggetto con interesse diretto nella vicenda: tali contenuti non risultano validati in modo indipendente e potrebbero essere parziali o selezionati.



[Confidenza media] Va inoltre pesato l'effetto di concentrazione della fonte: gran parte di ciò che è pubblicamente noto sul metodo dell'attacco — durata, "spray and pray", tradecraft — è stata diffusa da Duel/Korra, che dichiara contatti diretti con l'attaccante e ha richiesto l'esclusiva sulle informazioni. Un canale unico e interessato può selezionare e amplificare la versione dell'attaccante: le affermazioni che poggiano solo su Duel vanno perciò trattate come racconto di parte e salgono di confidenza solo dove sono corroborate in modo indipendente (Hudson Rock, autorità). Ciò non implica un coinvolgimento di Duel nell'operazione, che non risulta. — Base: thread di Korra/Duel (X); Hudson Rock.

Contesto sul soggetto (non probatorio ai fini dell'attribuzione). Duel è una piattaforma di scommesse crypto controversa. Nel maggio 2026 International Cyber Digest ha documentato l'imitazione, durante una diretta, dell'autore della sparatoria alla moschea di San Diego; lo stesso account attribuisce a Duel contenuti che esaltano autori di stragi scolastiche e il nazismo e contenuti antisemiti e razzisti. Il 16/09/2026 Duel si è scusata pubblicamente per un video generato con AI. Questi elementi non costituiscono evidenza di partecipazione all'intrusione; sono riportati per inquadrare l'ambiente in cui è avvenuto il contatto con l'attaccante e la propensione della piattaforma alla provocazione pubblica.

Attore	Infrastruttura	Valutazione
IAmNotAVillain ("Villain")	- **iamnotavillain[.]xyz**, registrato il 13/09/2026 presso GoDaddy, con nameserver domaincontrol.com; **imnotavillain[.]xyz**, registrato il 14/09/2026 presso NICENIC, con nameserver my-ndns.com e registrante indicato a Dubai; **iamnotavillain[.]com**, registrato il 15/09/2026 presso Tucows, con aggiornamento WHOIS il 16/09/2026 e nameserver Njalla. Il passaggio da Cloudflare/Njalla va mantenuto come elemento da ricostruire sullo storico DNS/WHOIS, non come dato definitivo se non supportato dal record originale o da snapshot archiviati. Al 15/09/2026 i record WHOIS dei due domini .xyz riportano lo stato *server hold*; canale Telegram "I Am Not A Villain" (t.me/iamnotavillain1), risultato non raggiungibile al 19/09/2026; canale privato recuperato t.me/+gchoNXafnZRiMzg0; account GitHub indicato come sospeso/non più accessibile, stato da distinguere da account vuoto o rimosso.	Ritenuto autore originale da Duel, parte coinvolta nella vicenda, e da KELA, fonte di threat intelligence. Confidenza media. Le fonti collegano il nome alle rivendicazioni principali e all'infrastruttura pubblicata, ma non dimostrano da sole il controllo effettivo di ogni dominio, account o repository; ogni indicatore deve quindi essere classificato separatamente come confermato tecnicamente, riportato da terzi o dichiarato dall'attaccante.
Revolut Smilik ("smile")	revoloot[.]lol; account @revolutsmilik; canale di riserva backupsmile1231; ID di sessione parziale 05a6f11c…805f	Confidenza media-bassa. L'esistenza di una rivendicazione separata è documentata; non sono verificati l'identità, lo status di ex collaboratore né l'autenticità dei file. IAmNotAVillain lo definisce uno scammer; un

Attore	Infrastruttura	Valutazione
		collegamento tra i due non è dimostrato.
Duel (casinò crypto) / Korra	Account X `@korraflow`; canali e infrastruttura propri di Duel	Duel/Korra non risulta coinvolto nell'intrusione, ma ha avuto un ruolo attivo nella diffusione pubblica di dati personali.Duel dchiara di aver avuto contatti con l'attore e di aver analizzato il materiale ricevuto, e che ha pubblicato sul proprio sito una pagina "KYC kit" in vendita con il documento e il selfie di una persona (pagina verificata). [Confidenza alta sulla pubblicazione] Dal materiale disponibile non risulta coinvolto nell'intrusione. Le informazioni pubblicate da Korra sono intelligence di fonte umana, provengono da un soggetto con interesse diretto e non equivalgono a una conferma forense indipendente.
Siti informativi con il nome del gruppo (gestore non identificato)	**iamnotavillain[.]net** e **iamnotavillain[.]info**, entrambi registrati il 16/09/2026 presso Cloudflare, con la stessa coppia di nameserver (chip/dawn) e registrante indicato a Kyiv (UA).il .net raccoglie articoli di stampa sul caso; il .info ricostruisce la timeline dell'estorsione e dichiara di non riportare indirizzo XMR e contatti del gruppo. Entrambi si dichiarano indipendenti; il .info afferma di non essere affiliato a iamnotavillain[.]com. Il .info contiene link precompilati che invitano gli assistenti AI a "ricordare il dominio". I due siti “press” (.net e .info) e la pagina del gruppo (iamnotavillain[.]com) condividono lo stesso impianto grafico e la stessa struttura a schede (JURISDICTION, PRESS): elemento a favore di una paternità comune tra i tre siti, distinta dalla loro presentazione come “outlet indipendenti”. La scheda CONTACT del sito del gruppo dichiara inoltre “Same place for staff, press, and users”, con un unico contatto Telegram/Session: elemento che collega direttamente i canali “press” al contatto del gruppo. Il countdown del .info è vivo e punta al 21/09 (≈102 h al 16/09, ≈63 h al 18/09, ≈40 h al 19/09), scadenza distinta dalle 24 ore del sito del gruppo (deadline 17/09 ore 18:30). Non è determinabile la paternità né la finalità: la funzione osservabile è mantenere pubblica la narrazione del caso, con riscatto e contatti oscurati.	Confidenza bassa sull'identità del gestore. Non risultano elementi che li colleghino al gruppo; lo stesso nome e la stessa data non bastano a stabilire un rapporto. **Fonti:** record WHOIS; contenuto dei siti (16/09/2026)

- **[Confidenza media]** Gli attori mostrano una disciplina operativa limitata. Gli elementi citati — commenti di modello rimasti nel sito, come “replace proof.jpg with the screenshot”, file cancellati ma potenzialmente recuperabili, esposizione pubblica di metadati e password degli archivi, registrazione

dei domini dopo la scoperta dell'incidente e comunicazioni caratterizzate da conflitti pubblici e tono informale — indicano carenze di sicurezza operativa e gestione delle informazioni. Questi segnali possono facilitare la raccolta di intelligence, ma non provano da soli inesperienza tecnica né invalidano l'accesso dichiarato ai dati. La valutazione si basa su materiali attribuiti a KELA, codice sorgente pubblicato da Dark Web Informer, dati WHOIS e messaggi Telegram.— *Base: KELA; codice sorgente pubblicato da Dark Web Informer; WHOIS; messaggi Telegram*

- **[Confidenza bassa]** Non emergono elementi sufficienti per collegare gli attori a gruppi criminali già identificati o ad attori statali. La rivendicazione pubblica, la richiesta di riscatto, la pubblicazione dei dati e il conflitto tra soggetti sono compatibili con un'attività criminale a scopo di lucro, ma non costituiscono indicatori attributivi conclusivi. L'assenza di un collegamento tecnico, linguistico o infrastrutturale verificato impedisce di andare oltre questa classificazione.— *Base: assenza di indicatori di attribuzione*
- **[Confidenza media]** Smile e IAmNotAVillain devono essere trattati come identità operative non attribuite, potenzialmente collegate ma non ancora correlate. L'uso di canali distinti e la minaccia riferita a Duelbits il 17 settembre 2026 non dimostrano né collaborazione né identità comune. La frase deve quindi essere registrata come una rivendicazione di targeting, non come prova di compromissione di Duelbits o di appartenenza a una struttura condivisa.

Le altre aziende e il contesto del canale

Il canale backupsmile1231 è stato contestato per violazione del copyright da otto aziende: Coinbase, Kraken, LayerZero, Tools for Humanity, Phantom, Galxe, Backpack Exchange e Tripadvisor. Revolut non è tra queste. Il materiale disponibile non indica quali contenuti fossero oggetto delle contestazioni, e la presenza nell'elenco non prova che le aziende siano state violate. Coinbase (incidente 2025 legato a dipendenti del supporto corrotti, circa 69.461 persone, estorsione da 20 milioni di dollari respinta) e Kraken (false richieste da @interno.it tra maggio e luglio 2025) hanno precedenti documentati. Il collegamento con Revolut resta però tematico, non attributivo. Per LayerZero, l'incidente KelpDAO del 18/04/2026, attribuito a Lazarus, è di natura diversa e non collegato al caso.

Il sito di estorsione e la frattura Villain/Smilik

Secondo KELA, il sito attribuito a IAmNotAVillain conteneva contatti Telegram e Session, l'invito a "get Revolut on record" e 19 archivi "Document Revolut" per circa 326 MB e 688 file. Era ospitato su hosting gratuito, con cronologia delle versioni accessibile e metadati dei commit che includevano almeno un indirizzo e-mail: elementi compatibili con una disciplina operativa limitata, ma non sufficienti da soli a smentire l'autenticità del materiale. La valutazione resta quindi di threat intelligence e deve essere distinta da una verifica forense indipendente dei file. Sempre secondo KELA, IAmNotAVillain definisce Revolut Smilik "an impersonator and scammer who had previously worked with them" con accesso a un piccolo campione dei dati; anche questa è una dichiarazione dell'attore principale e non è verificata.

Negozio onion "Revolut Accounts"

Un sito onion (accountmwyi…[.]onion), attivo al 16/09/2026, dichiara di vendere accessi a conti Revolut compromessi, con proxy SOCKS e istruzioni per l'incasso. La pagina elenca 51 account riferiti a Stati Uniti, Norvegia, Germania, Austria e Svizzera, con prezzi pari a circa il 5–6% del saldo dichiarato. Il rapporto prezzo/saldo, il linguaggio promozionale e la struttura ricorrente di questi negozi fanno ritenere probabile una truffa ai danni dei compratori, ma non è stato possibile verificarlo. Nel contenuto non emergono riferimenti ai dati KYC, all'Italia o agli attori del caso. **Non è considerato un indicatore di compromissione.** [**Confidenza bassa** sulla natura del sito; media sull'assenza di collegamento con il caso] — *Base: acquisizione della pagina (16/09/2026)*

Contesto: offerte a marchio Revolut precedenti al caso. Il 27 luglio 2026 un annuncio su un forum criminale proponeva 75 milioni di record Revolut a 500 dollari. I ricercatori di Cybernews, esaminando oltre 100 record campione (ultime quattro cifre e scadenza della carta, password con hash, email, nomi, telefoni, indirizzi, dati dei dispositivi, stato KYC, numeri di conto e codici SWIFT), hanno valutato il materiale come "compiled from multiple sources rather than the result of a newly discovered breach"; Revolut ha dichiarato

“We see no indications of any breach”, precisando che nessuno degli identificativi corrispondeva a identificativi validi e che la verifica era in corso. L’episodio non risulta collegato al caso in esame e indica che un’offerta criminale a marchio Revolut preesisteva all’incidente. [Confidenza alta sull’esistenza dell’annuncio; media sulla natura dei dati] *— Base: Cybernews, 27/07/2026*

Titolo	Descrizione	Indirizzo	Età indicata
Revolut Accounts	"Buy hacked Revolut accounts. SOCKS and cashing instruction included."	accountmwyiilytqztx……[.]onion	1 week, 6 days
Revolut Accounts	"No description provided"	accounhyzgxmfo6wb5ctu……..[.]onion	1 week, 6 days

Accesso: casella PEC istituzionale reale, compromessa, clonata o creata ex novo

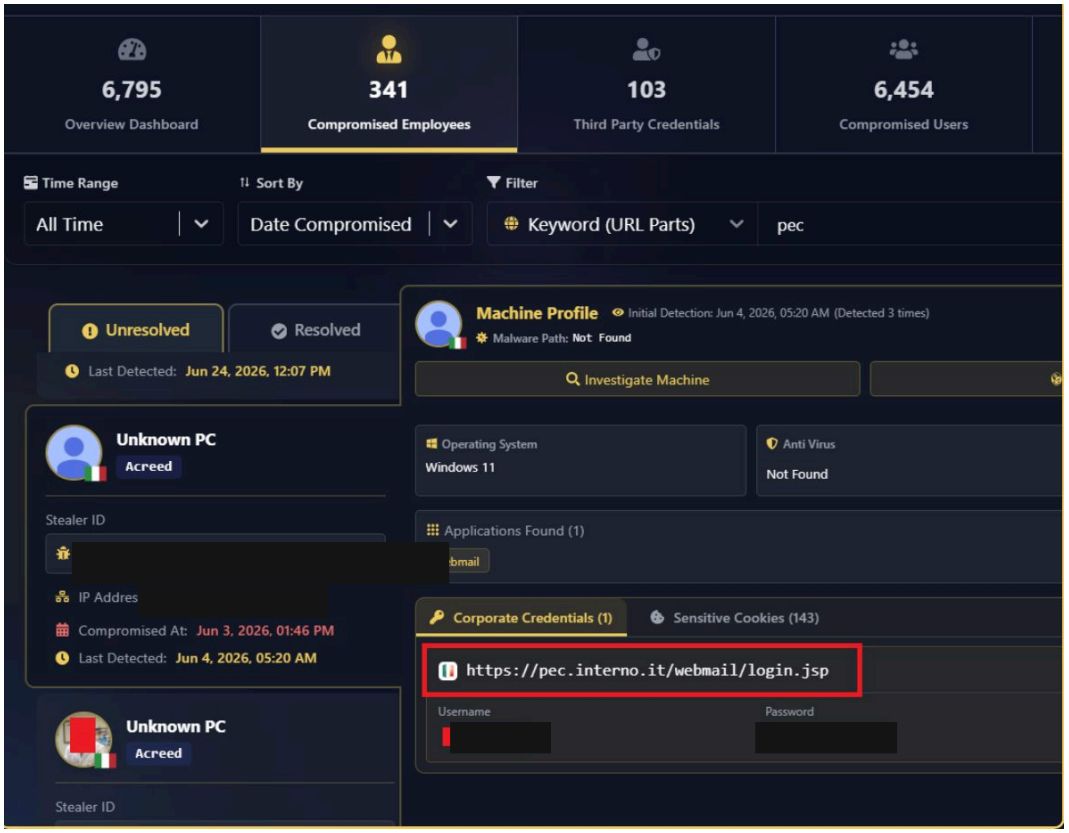
[Confidenza media-bassa] Le richieste sono partite da una casella del dominio @pec.interno.it che la stampa riferisce all’ufficio Enti Locali della Prefettura di Reggio Calabria. Restano aperte due alternative: la compromissione della casella, ipotesi sostenuta dal gruppo e da Duel che parlano di credenziali sottratte tramite infostealer, oppure la clonazione dell’indirizzo. Secondo Il Sole 24 Ore (18/09) gli investigatori non hanno la certezza che sia stato compromesso un computer della Prefettura o del Viminale e stanno stabilendo se la casella sia stata “bucata” oppure clonata; la Polizia Postale non avrebbe finora riscontrato falle nei sistemi del Ministero.
Una terza alternativa emerge da The CyberSec Guru (12/09, aggiornato il 15/09), secondo cui l’attacco avrebbe sfruttato un account di posta non autorizzato creato all’interno dell’infrastruttura dell’agenzia governativa; l’articolo la presenta come elemento confermato da Revolut, ma non ne cita il testo: va verificata sulla notifica o sulla dichiarazione ufficiale dell’azienda.

[IPOTESI, confidenza bassa] Abuso di privilegi amministrativi. L’attivazione o l’uso della casella sarebbe avvenuto tramite un’utenza dotata di privilegi sul dominio di posta, per compromissione dell’account amministrativo o per condotta di un soggetto interno. L’ipotesi è coerente con l’assenza di falle riscontrate nei sistemi, con la mancata pubblicazione e il mancato censimento dell’indirizzo e con la durata prolungata dell’operazione; non trova però riscontri nel materiale disponibile e non spiega, da sola, la rivendicazione di dati provenienti da più uffici delle forze dell’ordine.
Elementi dirimenti: data di creazione della casella, richiesta di attivazione e primi accessi presso il gestore PEC. In alternativa, un infostealer che abbia colpito l’utenza amministrativa anziché quella d’ufficio produrrebbe lo stesso esito. *— Base: dichiarazioni dell'attore e del team Duel (infostealer); indagine della Procura di Reggio Calabria riportata dalla stampa; pattern CERT-AGID 2025–2026 sulle caselle PEC legittime compromesse.*

[Confidenza media-alta] Un elemento indipendente rafforza l’ipotesi della compromissione via credenziali. Secondo Hudson Rock (15/09/2026), società specializzata in intelligence sugli infostealer, nel proprio database figurano circa 300 credenziali di accesso alla webmail pec.interno.it provenienti da macchine già infettate da infostealer. Su questa base Hudson Rock valuta improbabile che l’attaccante abbia infettato attivamente quei dipendenti: più verosimilmente ha acquistato o riutilizzato log di infostealer già esistenti, mascherando il vero metodo di accesso iniziale e ridimensionando il claim del “RAT”. Il tradecraft riferito — accesso alla casella con credenziali rubate, aggiunta di una recovery email controllata dall’attaccante, monitoraggio continuo della posta e cancellazione dei messaggi inviati e ricevuti per non allertare il titolare, con individuazione di Revolut Bank UAB (Lituania) come soggetto tenuto a rispondere a un Ordine europeo di indagine — è coerente con un abuso di credenziali, non con un’intrusione nei sistemi del Ministero. — *Base: Hudson Rock (15/09/2026); Duel.*

[Confidenza media-alta sul dato negativo] Una verifica indipendente restringe il quadro. La ricerca della casella specifica — ***entilocali.prefrc@pec.interno.it*** — su quattro piattaforme di threat intelligence che catalogano miliardi di credenziali sottratte da infostealer non produce alcun riscontro (zero occorrenze su tutte e quattro), mentre risultano presenti altre credenziali PEC della stessa Prefettura di Reggio Calabria. Il

dato non contraddice Hudson Rock: al livello di dominio (pec.interno.it) esistono circa 300 credenziali webmail compromesse, ma la casella effettivamente usata non compare nei feed monitorati. Le letture compatibili sono due: un log infostealer privato, sfruttato prima di entrare nel circuito underground tracciato dalle piattaforme; oppure un accesso non riconducibile a un infostealer catalogato — per esempio la clonazione dell'indirizzo, ipotesi che il fascicolo tiene aperta. In entrambi i casi, il metodo di accesso alla casella specifica resta non determinato dai dati pubblici. *— Base: verifica su quattro piattaforme TI; Hudson Rock.*



Screenshot Hudson Rock (dati personali oscurati): il dominio pec.interno.it figura tra le credenziali corporate raccolte da infostealer; i contatori mostrano le identità compromesse del dominio interno.it. La casella specifica del caso non compare invece nei feed TI verificati.

[Confidenza media] Due elementi rafforzano l'anomalia della casella. La funzione: **gli indirizzi del tipo entilocali.pref<sigla>@pec.interno.it sono in genere riferibili agli uffici prefettizi per la comunicazione con gli enti locali (comuni, province)** — ad esempio nelle tornate elettorali — non a un canale deputato a ordini europei di indagine o a richieste di dati ultrasensibili. Il video diffuso dall'attore, inoltre, mostra la creazione di una cartella nascosta e di filtri per occultare lo scambio al legittimo proprietario e — nell'archiviazione automatica — una cartella "Luglio" 2026 che conterrebbe quasi soltanto corrispondenza con Revolut, indizio di una casella poco usata per il traffico ordinario. Il video è materiale di parte, non verificato in modo indipendente. — Base: elenchi PEC del Ministero; video attribuito all'attore.

[Confidenza media] Questo scioglie l'apparente tensione con la dichiarazione secondo cui non risulterebbero falle nei sistemi del Viminale: l'uso di credenziali sottratte da endpoint tramite infostealer non richiede né implica una compromissione dell'infrastruttura del Ministero. "Nessuna falla nei sistemi" e "casella usata per mesi" sono compatibili proprio perché il vettore è il furto di credenziali, non l'intrusione. Resta invece una verifica tecnica distinta e dirimente sul piano investigativo: accedendo ai log di trasporto del gestore PEC (conservati per legge), le autorità possono stabilire se e quando quella casella ha contattato domini Revolut, con quale frequenza e volume. Che tale incrocio sia già stato effettuato, o che le email verso Revolut siano state a lungo classificate come legittime, incide sullo stato delle indagini, non sull'esistenza del vettore.

— **Limiti:** il metodo di accesso non è confermato ufficialmente; la rivendicazione di 147 GB "dal lato italiano" non è verificata e, secondo i primi accertamenti della Polizia Postale riferiti dalla stampa il 18/09, non risulta confermata

Operazione: richieste ripetute, costruite su dati blockchain pubblici

[Confidenza media] Per diversi mesi gli attaccanti avrebbero inviato a Revolut Bank UAB richieste presentate come OEI italiani. Come chiavi di ricerca avrebbero usato hash di transazioni e indirizzi di wallet, per selezionare clienti ad alto valore. Revolut avrebbe applicato un filtro giurisdizionale, rifiutando le richieste per le entità UK e svizzera, ma non una verifica sull'autenticità del mittente. Ha quindi restituito i dati dei conti UAB. *— Base: post di Kozlovska del 15 e 16/09, che citano documenti e file .eml ricevuti da Duel.*

— **Limiti:** i file .eml non sono verificati in modo indipendente; le fonti divergono sulla durata precisa, quindi è preferibile indicare che le richieste si sarebbero protratte “per diversi mesi” anziché fissare cinque o sei mesi come dato certo. Sul comportamento di Revolut, le informazioni disponibili vanno lette distinguendo tra richieste evase, richieste respinte per ragioni giurisdizionali e richieste non verificabili.

Monetizzazione: estorsione e frattura interna

[Confidenza media-bassa] Dopo la raccolta, i dati sarebbero stati usati per un'estorsione con pubblicazione progressiva di documenti e selfie KYC. La richiesta pubblica più documentata è pari a 6.000 XMR, circa 3 milioni di dollari; eventuali riferimenti a 10.000 BTC restano non confermati e devono essere trattati come messaggi o fasi distinte, non come importo coerente con la richiesta in Monero. Nel frattempo si sarebbe formata una frattura interna: IAmNotAVillain, Revolut Smilik e un presunto ex membro gestiscono canali e rivendicazioni in concorrenza tra loro, e i domini di IAmNotAVillain sono stati bloccati.*— Base: canali Telegram, revoloot[.]lol, messaggi ricevuti, record WHOIS (server hold sui .xyz), stampa.*
— **Limiti:** identità, rapporti tra i soggetti e autenticità dei file non sono verificati.

Amplificazione: soggetti terzi con interessi propri

[Confidenza media sui fatti -bassa sulle motivazioni] Il caso è stato amplificato da soggetti esterni con agende diverse. Duel, piattaforma crypto a KYC minimo, fa da intermediario con l'attore e pubblica sul proprio sito documenti d'identità di una persona. Kozlovska e l'Open Dialogue Foundation usano il caso nel dibattito su AML/CFT e "transnational financial repression".
— Base: post X di Korra e Kozlovska; pagina duel.com/merch verificata.
— Limiti: le motivazioni di Duel non sono dichiarate; la provenienza dei documenti pubblicati da Duel non è verificata.

5. Kill chain e TTP

Alcune tecniche sono **dichiarate o inferite**, non osservate direttamente. Inoltre, la consegna dei dati da parte della compliance di Revolut non è una normale esfiltrazione tecnica dell'attore: è una divulgazione ottenuta tramite il processo legittimo della vittima. La kill chain osservata combina ricognizione open source su wallet e transazioni, possibile compromissione di account istituzionali, uso di credenziali valide, manipolazione della casella, impersonificazione di autorità giudiziarie e abuso del processo di risposta alle richieste legali. La divulgazione dei dati Revolut non risulta ottenuta tramite esfiltrazione tecnica dai sistemi della banca, ma mediante social engineering e uso fraudolento di un canale istituzionale apparentemente legittimo. Le fasi relative a infostealer/RAT, persistenza, cancellazione dei messaggi e selezione delle vittime restano dichiarate o inferite e non verificate indipendentemente.

Fase	Azione osservata o dichiarata	MITRE ATT&CK	Stato
Ricognizione	Individuazione di clienti ad alto valore tramite indirizzi wallet e ID di transazione pubblici su blockchain	T1589 — Gather Victim Identity Information; T1593 — Search Open Websites/Domains	Riportato da terzi, soprattutto Duel; coerente con l'elenco wallet–KYC, ma non confermato da Revolut
Sviluppo risorse	Acquisizione o compromissione di credenziali di caselle istituzionali italiane	T1586.002 — Compromise Accounts: Email Accounts	Riportato da terzi; il coinvolgimento di una casella istituzionale è compatibile con il caso, ma il metodo di acquisizione non è verificato
Accesso	Uso di credenziali valide per la webmail PEC; infostealer o RAT come strumento dichiarato	T1078 — Valid Accounts; T1555 — Credentials from Password Stores; T1219 — Remote Access Software	Dichiarato, non verificato da log o analisi forense
Persistenza ed evasione	Aggiunta di un indirizzo di recupero e cancellazione dei messaggi inviati o ricevuti	T1098 — Account Manipulation; T1070.008 — Clear Mailbox Data	Dichiarato, non verificato. T1070.008 è coerente con la cancellazione o manipolazione dei dati della casella.
Impersonificazione	Presunti OEI intestati alla Procura di Milano, firma "Polizia postale" e invio da una PEC riconducibile a una Prefettura	T1656 Impersonation	Supportato da screenshot e fonti di stampa; autenticità, completezza e provenienza dei documenti non completamente verificate
Raccolta e divulgazione	Consegna dei dati KYC da parte della compliance di Revolut, tramite archivi cifrati e password trasmessa separatamente	Non è una tecnica ATT&CK di esfiltrazione tecnica; descrivere come abuso del processo legittimo della vittima	Divulgazione a soggetto non autorizzato confermata da Revolut; dettagli su archivi e 33 cartelle riportati da Duel
Infrastruttura di pressione	Domini registrati il 14–15 settembre, Cloudflare, canali Telegram, canali di riserva e identificativi di sessione	T1583.001 — Acquire Infrastructure: Domains	Domini e nameserver supportati da WHOIS quando verificati sul record originale; lo storico DNS/WHOIS e gli eventuali snapshot

Fase	Azione osservata o dichiarata	MITRE ATT&CK	Stato
			archiviati sono necessari per confermare cambi di provider, blocchi o aggiornamenti successivi. Il collegamento operativo tra tutti gli elementi resta parzialmente non verificato.
Impatto	Pubblicazione di schede KYC, richiesta di riscatto in XMR e minaccia di vendita dei dati	T1657 — Financial Theft; possibile estorsione come impatto operativo	Pubblicazione e minacce riportate; autenticità e completezza dei dati pubblicati devono essere valutate separatamente. T1657 include furto finanziario ottenuto tramite estorsione o social engineering.

Distinzione centrale. Non emergono elementi pubblici che indichino una compromissione dell'infrastruttura core di Revolut. La kill chain tecnica si sviluppa presumibilmente sul lato della casella istituzionale. Sul lato della banca, l'attacco appare principalmente procedurale e non risulta, dalle evidenze pubbliche, una compromissione dei sistemi core.

5-bis. Precedenti e schema di settore

Caso	Canale sfruttato	Esito
Twitter, 2020	Spear phishing telefonico su dipendenti, escalation su strumenti di supporto	130 account compromessi, truffa bitcoin
Coinbase, dic. 2024–mag. 2025	Addetti del supporto corrotti	69.461 clienti; estorsione da 20 milioni di dollari respinta
Kraken, 2025	Richieste false da @interno.it, poi finto ordine irlandese	Dati consegnati, minacce fisiche e tentativo di intrusione; dettaglio documentato nell'atto giudiziario verificato.
Hardware wallet, gen. 2026	Social engineering dopo fuga di dati associata a Ledger	Circa 282 milioni di dollari in criptovalute sottratti tramite social engineering su hardware wallet e successivamente convertiti o riciclati anche tramite Monero; il riferimento a KelpDAO non va mantenuto se non supportato da una fonte specifica.
Kraken, apr. 2026	Accessi abusivi del supporto	Tentativo di estorsione relativo a circa 2.000 account; Kraken ha dichiarato che non erano stati compromessi i sistemi core né i fondi.
Revolut, 2026	PEC istituzionale e falsi Ordini europei di indagine	Circa 680 clienti secondo fonti giornalistiche e dichiarazioni attribuite all'attaccante, dato non confermato ufficialmente da Revolut; estorsione e pubblicazione di dati.

Valutazioni

- **[Confidenza alta]** Nei casi esaminati del settore finanziario e crypto ricorre lo sfruttamento di canali fiduciari umani o procedurali — supporto clienti, compliance, personale e richieste delle autorità — più che una vulnerabilità tecnica direttamente dimostrata nell'infrastruttura core. — *Base: casi documentati sopra; FBI 2024; Security4Web3 2026*
- **[Confidenza alta]** Lo schema della "falsa autorità italiana" risulta documentato in almeno due episodi distinti nell'arco di due anni: il caso Kraken del 2025, basato su richieste provenienti da @interno.it, e il caso Revolut del 2026, associato a una PEC istituzionale italiana e a documenti presentati come ordini giudiziari europei. Il passaggio da email ordinaria a PEC e da richiesta semplice a documento giudiziario aumenta la credibilità apparente del canale, ma non dimostra che i due episodi siano stati condotti dallo stesso gruppo. — *Base: atto Kraken; PEC Revolut*
- **[Confidenza bassa]**Non ci sono elementi sufficienti per attribuire i casi Kraken 2025 e Revolut 2026 allo stesso attore. La possibile circolazione di credenziali relative a caselle istituzionali rende plausibile che soggetti diversi abbiano sfruttato lo stesso tipo di accesso o la stessa opportunità criminale.— *Base: assenza di elementi di collegamento*

Social engineering nel settore crypto: precedenti

Il social engineering nel settore crypto colpisce spesso le persone che dispongono di accesso o potere autorizzativo, come addetti al supporto clienti, sviluppatori, compliance officer e amministratori di account, ma anche singoli possessori di patrimoni digitali.

Un precedente significativo è l'attacco a Twitter del 15 luglio 2020, analizzato da HKCERT: 130 account di alto profilo furono compromessi per promuovere una truffa Bitcoin presentata come raccolta per il "COVID-19 relief", con un ricavo di 12,83 BTC. Gli aggressori iniziarono con spear phishing telefonico rivolto a un numero ristretto di dipendenti, consultarono poi la messaggistica interna per individuare chi disponeva di privilegi sugli strumenti di gestione degli account e infine aumentarono i propri privilegi. Il 31 luglio 2020 furono arrestati tre sospetti. HKCERT indicò come contromisure l'autenticazione multifattore, la formazione con simulazioni di phishing, il principio need-to-know, il monitoraggio del comportamento degli utenti e la revisione periodica degli account privilegiati.

Un altro quadro utile è fornito dall'analisi di Security4Web3 del 9 giugno 2026 sugli attacchi di social engineering contro le società crypto.

Tra gli episodi richiamati figurano il furto da 1,5 miliardi di dollari subito da Bybit nel febbraio 2025, ottenuto attraverso l'ingegneria sociale rivolta agli sviluppatori e l'inserimento di JavaScript malevolo nell'interfaccia Safe{Wallet}; il furto da 308 milioni di dollari subito da DMM Bitcoin nel maggio 2024, attribuito da FBI e autorità giapponesi a Lazarus; il falso dipendente nordcoreano assunto da KnowBe4 nel luglio 2024 mediante identità rubata e immagini generate con IA; i casi di SIM swap rilevati dall'FBI nel 2023 e le oltre 1.800 candidature di presunti operatori nordcoreani bloccate da Amazon nel 2025.

Le tecniche ricorrenti includono spear phishing, vishing con clonazione vocale o deepfake, SIM swap, impersonificazione su Discord e Telegram, falsi investitori e falsi candidati. Nel modello Lazarus/TraderTraitor, l'attacco procede attraverso l'individuazione dei bersagli su LinkedIn e GitHub, la costruzione della fiducia mediante falsi recruiter, la consegna del malware e la sua esecuzione. Le difese raccomandate comprendono chiavi hardware FIDO2, verifica out-of-band per le operazioni di alto valore, multifirma e gestione degli accessi privilegiati con registrazione delle sessioni.

Il 10 gennaio 2026, secondo Yahoo Finance e il ricercatore ZachXBT, un attacco di social engineering rivolto al possessore di un hardware wallet avrebbe causato la sottrazione di circa 282 milioni di dollari in Litecoin e

Bitcoin. La vittima non è stata identificata pubblicamente come persona o società. I fondi sarebbero stati convertiti rapidamente in Monero tramite exchange istantanei, mentre parte dei Bitcoin sarebbe stata trasferita verso Ethereum, Ripple e Litecoin tramite THORChain. L'episodio è stato collegato alla fuga di dati personali dei clienti Ledger del 5 gennaio 2026, ma ZachXBT non avrebbe rilevato indicazioni sufficienti per attribuirlo a hacker nordcoreani. Questi precedenti sostengono l'ipotesi che, **nel settore crypto, il bersaglio principale sia spesso il fattore umano dotato di accesso o potere di autorizzazione, non la tecnologia in astratto.**

Nel caso del furto di gennaio 2026, la sequenza ipotizzata è **fuga di dati personali, contatto mirato mediante impersonificazione, sottrazione degli asset e conversione in Monero**; la coincidenza con la valuta richiesta nel riscatto di IAmNotAVillain è però un elemento di contesto e non dimostra un collegamento operativo. Il caso Revolut rappresenta una variante dello stesso paradigma: l'attore non avrebbe convinto un dipendente a eseguire codice o trasferire direttamente fondi, ma a eseguire una procedura legale sulla base di una richiesta apparentemente istituzionale. Anche i falsi recruiter associati al caso Kraken rientrano nello schema generale di costruzione della fiducia osservato nelle campagne TraderTraitor, senza che il materiale disponibile dimostri un collegamento con Revolut.

Dati i fatti, **il caso Revolut può essere inserito in uno schema già noto di impersonificazione e abuso di procedure, ma con una variante particolarmente insidiosa:** l'uso di una PEC con valore legale apparente e di un documento formalizzato come Ordine europeo di indagine, invece di una semplice richiesta d'emergenza o di un contatto operativo.

La verifica out-of-band, normalmente raccomandata per le operazioni di alto valore, dovrebbe quindi essere applicata anche alle richieste delle autorità quando comportano accesso a dati KYC, identificazione di clienti tramite wallet o divulgazioni massive.

Kraken 2026: estorsione via abuso di accessi interni

Accanto al caso del 2025 — dati consegnati a fronte di richieste presentate come provenienti dalle autorità, poi oggetto della causa Doe v. Kraken — l'exchange ha reso pubblico il 13 aprile 2026 un episodio distinto, con un vettore diverso: non una falsa richiesta esterna, ma l'abuso di accessi interni. La ricostruzione ufficiale è del Chief Security Officer Nick Percoco.

[Confidenza alta] Kraken ha individuato e chiuso due episodi di accesso improprio a dati limitati del supporto clienti, entrambi ricondotti a membri del team di supporto: il primo emerso a febbraio 2025 (un video comparso su un forum criminale, segnalato da una fonte fidata); il secondo più recente, con un nuovo video di attività analoga. In entrambi i casi l'azienda dichiara di aver revocato immediatamente gli accessi e notificato i clienti coinvolti. Complessivamente sarebbero stati potenzialmente visualizzati circa 2.000 account (0,02% dei clienti). *— Base: dichiarazione ufficiale di Kraken, 13/04/2026*

[Confidenza alta] Poco dopo la revoca degli accessi sono arrivate le richieste di estorsione: un gruppo criminale non nominato ha minacciato di distribuire a media e social i materiali di entrambi gli episodi se non fosse stato pagato. L'importo non è stato reso pubblico. La posizione dell'azienda è stata netta: «our systems were never breached; funds were never at risk; we will not pay these criminals; we will not ever negotiate with bad actors». Secondo Kraken i sistemi core non sono stati violati e i fondi non sono mai stati a rischio.

[Confidenza media] Kraken colloca i due episodi in una più ampia attività di reclutamento di insider che, oltre alle aziende crypto, prenderebbe di mira anche i settori gaming e telecomunicazioni, e dichiara di collaborare con le forze dell'ordine federali su più giurisdizioni, ritenendo di disporre di elementi sufficienti per l'identificazione e l'arresto dei responsabili.— Base: dichiarazione aziendale; indagine in corso

[Confidenza: lettura dell'analista] Per il fascicolo il caso aggiunge un tassello: cambia il vettore — l'insider, non la falsa autorità né il canale fidato compromesso — ma non il bersaglio, che resta il patrimonio

informativo di supporto e KYC. Rispetto a Revolut si notano due differenze operative: qui non c'è un canale istituzionale abusato ma un accesso interno; e la posizione pubblica dell'exchange è di rifiuto esplicito del pagamento e della trattativa. La componente insider va quindi trattata come una superficie di attacco a sé, indipendente dalla robustezza dei sistemi.

5-ter. Casi analoghi: consegna di dati a false richieste delle autorità

Il vettore del caso — un'azienda che consegna dati a una richiesta apparentemente proveniente da un'autorità — ha precedenti documentati. La maggior parte riguarda le Emergency Data Requests statunitensi; in Europa lo strumento equivalente è l'OEI, con procedura diversa: è il vuoto che i casi Kraken e Revolut illustrano.

Anno	Soggetti	Descrizione
2016	FBI	Un server di posta dell'FBI usato per inviare falsi avvisi (mittente autentico, contenuto falso)
2022	Apple, Meta, Discord	Dati di utenti consegnati a false Emergency Data Requests da caselle di polizia compromesse (Lapsus$/Recursion)
2022	Binance, Coinbase, Meta, Microsoft	Destinatarie di finte EDR (ricostruzione Krebs)
nov. 2024	Allerta FBI	Aumento di caselle di polizia compromesse e finte citazioni; "Pwnstar" vende false richieste a 1.000–3.000 $
ago. 2025	(mercato)	Account email di polizia e governo in vendita da 40 $ (USA, UK, DE, IN, BR) — Abnormal AI
2025	Kraken	Falsa richiesta da @interno.it: dati consegnati senza provvedimento dell'autorità giudiziaria (precedente italiano)
2026	Revolut	Il caso oggetto del presente documento

[Confidenza alta sull'esistenza dei casi] — *Base: Krebs on Security; Slate; Kodex; Help Net Security/Abnormal AI; atto Doe v. Kraken.*

6. Dati potenzialmente esposti

6.1 Persone coinvolte

Il report non riporta i nomi delle persone coinvolte: tali identificativi non sono necessari per l'analisi e **la loro diffusione aumenterebbe inutilmente il rischio per gli interessat**i.

- **[Confidenza alta]** Revolut non ha reso pubblico un elenco completo né il numero ufficiale delle persone coinvolte. L'azienda ha descritto l'impatto come "limitato" e ha dichiarato di aver contattato direttamente gli utenti interessati. — *Base: dichiarazione di Revolut; Reuters*
- **[Confidenza bassa]** Il threat actor IAmNotAVillain ha dichiarato di aver ottenuto dati relativi a 680 clienti Revolut, selezionati tramite blockchain analysis sulla base delle disponibilità in criptovalute. La cifra è stata ripresa da fonti giornalistiche, ma non è stata confermata ufficialmente da Revolut né verificata indipendentemente. Deve quindi essere classificata come **dato attribuito all'attaccante**, non come conteggio definitivo delle vittime. — *Base: messaggi del gruppo; fonti giornalistiche*

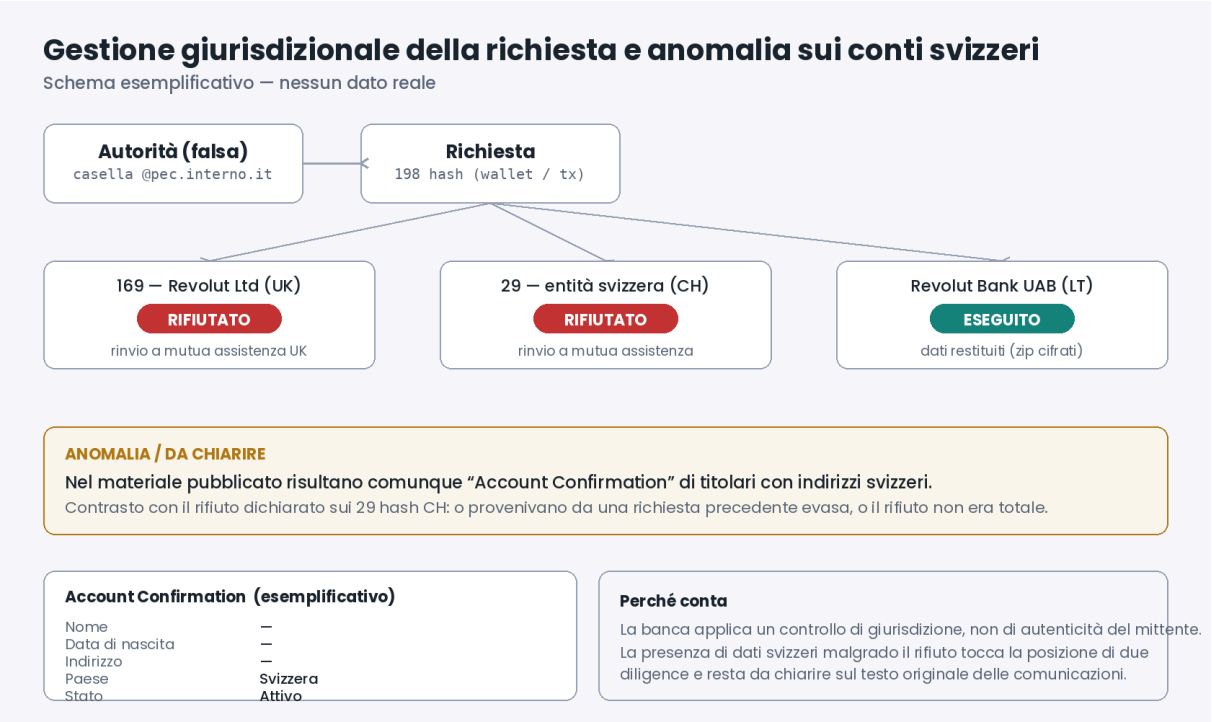
Nota di delimitazione: i 147 GB riguardano una diversa rivendicazione relativa all'eventuale compromissione di sistemi italiani. Non rappresentano la quantità di dati Revolut esposti né il numero delle persone coinvolte.

Autenticità del campione pubblicato. Il materiale diffuso dal gruppo (documenti d'identità, selfie di verifica, "Account Confirmation" ed estratti in formato Revolut) risulta autentico per convergenza di più elementi: coerenza con il formato dei documenti Revolut, conferma da parte dell'azienda dell'avvenuta divulgazione, e riconoscimento pubblico da parte di alcuni interessati. La valutazione è per convergenza, non record per record: non ogni singolo documento è verificabile individualmente. Gli screenshot restano materiale curato e marchiato dal gruppo; l'autenticità dei dati sottostanti è cosa distinta dalla loro presentazione. Nessun dato personale è riprodotto in questo documento. [Confidenza media-alta sull'autenticità del campione] — Base: copia archiviata

della pagina del sito del gruppo (pagina archiviata il 16/09/2026; acquisizione interna, non riprodotta); conferma di Revolut; dichiarazioni pubbliche degli interessati

Struttura dell'archivio. La pagina del gruppo mostra un insieme di archivi "Document Revolut" e, nelle proprietà di cartella, un totale coerente con quanto riferito da KELA: circa 326 MB, 688 file, 204 cartelle. [Confidenza media] — Base: copia archiviata (16/09/2026; acquisizione interna); KELA

Dato svizzero e rifiuto giurisdizionale (thread aperto). Tra i documenti pubblicati compaiono "Account Confirmation" di titolari con indirizzi svizzeri. La risposta del 24/07 indicava però i 29 hash riferiti all'entità svizzera come rifiutati e rinviati alla mutua assistenza. La presenza di dati di conti svizzeri nel materiale pubblicato è quindi da conciliare con il rifiuto dichiarato: o provenivano da una richiesta precedente evasa, o il rifiuto non era totale. Da verificare. [Confidenza bassa] — Base: copia archiviata (16/09/2026); messaggio del 24/07

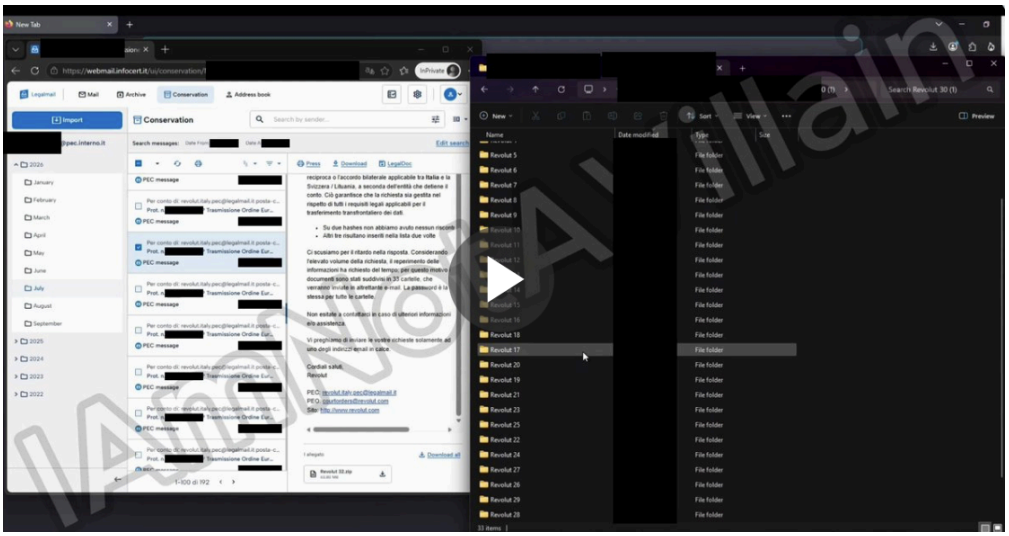


Schema esemplificativo (nessun dato reale): gestione giurisdizionale della richiesta e anomalia sui conti svizzeri.

Richiesta di distruzione della documentazione (thread aperto). In una comunicazione Revolut (versione tradotta pubblicata dal gruppo) l'azienda chiede al richiedente di confermare la distruzione della documentazione già inviata, citando il segreto bancario e la competenza di un'autorità lituana o svizzera. È un artefatto distinto dal semplice rifiuto e rileva ai fini della posizione di due diligence dell'azienda. Da leggere sul testo originale. **[Confidenza bassa]** *— Base: copia archiviata (16/09/2026; versione tradotta)*

6.2 Categorie di dati

Categoria	Dettaglio	Fonte	Confidenza
Identità	nome, data di nascita, indirizzo, email, telefono, professione	avviso Revolut; ZachXBT	Alta
Documenti	passaporto, carta d'identità, patente, permessi di soggiorno	avviso Revolut; pubblicazioni del gruppo	Alta
Biometria KYC	selfie di verifica	avviso Revolut ("may"); pubblicazioni	Alta
Dati bancari	IBAN, estratti conto, storico transazioni in valuta, prelievi	ZachXBT; Duel	Media
Crypto	depositi e prelievi, indirizzi di wallet collegati all'identità	Duel; elenco wallet-KYC pubblicato	Media



Fotogramma del video diffuso tramite Duel, con watermark "IAmNotAVillain": webmail Legalmail/InfoCert di un account @pec.interno.it e cartelle "Revolut" (screenshot ricevuto; video non visionato)

[Confidenza media] Nota sulla qualificazione dei dati. Secondo The CyberSec Guru (12/09), la notifica ai clienti precisa che “no biometric facial telemetry data was involved or compromised”: risulta quindi esposta l’immagine del selfie, non i dati biometrici derivati. La distinzione ha effetti giuridici, perché colloca l’incidente fuori dal regime delle categorie particolari di dati (art. 9 GDPR), pur restando l’immagine utilizzabile per impersonificazione e per tentativi di aggiramento delle verifiche di identità. La formulazione va confermata sul testo della notifica. — *Base: The CyberSec Guru, 12/09/2026*

7. Impatto su KYC, AML e frodi

- **[Confidenza alta]** La combinazione di documento d’identità, selfie, dati bancari e informazioni sui wallet crea un rischio elevato di furto d’identità, impersonificazione e frode nei processi di onboarding o assistenza. Tali dati possono essere riutilizzati per tentare aperture fraudolente di conto, account takeover, richieste di recupero credenziali e contatti mirati con banche, exchange e fintech. Tuttavia, il superamento dei controlli KYC di un altro istituto dipenderebbe dalla qualità dei controlli aggiuntivi, come liveness, verifica documentale, device intelligence e controlli comportamentali. — *Base: natura dei dati esposti*
- **[Confidenza alta]** Se confermata, la selezione delle vittime sulla base di wallet pubblici, saldi o movimenti crypto consente di concentrare l’attività fraudolenta su soggetti ad alto valore. La combinazione di informazioni on-chain e dati KYC può facilitare phishing, vishing, SIM swap, impersonificazione e attacchi mirati all’assistenza clienti. Il metodo di selezione dichiarato dall’attaccante resta però da verificare indipendentemente. — *Base: elenco wallet-KYC; precedenti gennaio 2026*
- **[Confidenza media]** **Esiste un rischio fisico** per le persone i cui dati esposti comprendano indirizzi di residenza e indicatori di disponibilità patrimoniale in criptovalute. Il rischio è coerente con precedenti episodi di minacce e tentativi di intrusione associati a vittime crypto, ma i riferimenti a minacce di rapimento e alle statistiche francesi devono essere mantenuti come evidenza di contesto, non come prova di un rischio specifico per ogni vittima Revolut. — *Base: atto Kraken; Duel; franceinfo*
- **[Confidenza media]** Documenti d’identità e selfie possono essere riutilizzati per creare identità sintetiche, aprire conti utilizzabili come money mule o superare processi KYC presso altri servizi. Le fonti sul rischio di identity mule evidenziano il riutilizzo combinato di documenti e selfie, insieme a controlli su dispositivo, indirizzo, wallet e pattern transazionali. La richiesta di riscatto in Monero documenta una componente estorsiva, ma non prova da sola che i dati siano già stati impiegati per riciclaggio. — *Base: natura dei dati; richiesta di riscatto*
- **[Confidenza media]** La diffusione secondaria dei dati può amplificare il danno: account terzi possono ripubblicare documenti leggibili dopo la chiusura dei canali originari, mentre offerte non collegate di account Revolut su servizi onion alimentano un mercato parallelo di identità e account. Questi due

fenomeni devono restare separati: la presenza di un mercato non dimostra che i dati Revolut siano già stati venduti o riutilizzati. — *Base: post X del 14-15/09; elenchi onion.*

KYC come rischio strutturale per la privacy

Il caso illumina un problema più ampio del singolo incidente. Il framework KYC, nato per contrastare riciclaggio e finanziamento del terrorismo — con obblighi espansi soprattutto dopo l'11 settembre 2001 — assolve una funzione reale, ma, così come è implementato, crea per sua natura archivi centralizzati di identità verificate: documenti, selfie, dati anagrafici, prove di residenza, legati a indirizzi wallet, cronologie di deposito e prelievo, volumi di trading. Un archivio del genere trasforma la piattaforma in un honeypot: per un attaccante un database KYC vale spesso più di un hot wallet, perché abilita furto d'identità, phishing mirato, frodi ed estorsioni. Non a caso, nei casi Coinbase (2025, ~69.000 utenti, dati venduti da un insider) e Revolut (2026, ~680 clienti, dati esfiltrati dopo una richiesta fraudolenta), i dati KYC sono stati sottratti senza toccare direttamente i fondi.

L'effetto più insidioso è che il KYC collega l'identità reale all'attività crypto. Senza, un indirizzo wallet è al più uno pseudonimo; con il KYC l'exchange sa che "indirizzo X = persona Y", e quando quel legame viene esfiltrato — per breach, insider o richiesta abusiva come in questo caso — la pseudonimità cade a monte. Lo stesso vale, in pratica, per le privacy coin: Monero offusca bene on-chain, ma se un utente compra XMR su un exchange KYC e lo preleva sul proprio wallet, è l'exchange a detenere il collegamento "utente → transazione → indirizzo Monero"; se quel collegamento è compromesso, parte della privacy è già rotta prima ancora della blockchain.

Il rischio si moltiplica perché i punti di fallimento non sono solo gli exchange: la verifica dell'identità è spesso delegata a pochi provider specializzati (Sumsub, Persona, Veriff, AU10TIX e simili) che gestiscono i dati KYC di decine di piattaforme. Un incidente su un singolo provider espone in un colpo solo gli utenti di molti operatori: lo mostrano il leak di Sumsub, rimasto non rilevato per mesi, e l'esposizione dei dati di AU10TIX protratta nel tempo, in un panorama in cui si contano decine di violazioni a carico proprio dei verificatori di identità.

[Confidenza alta sui casi; per il resto, dibattito documentato] La critica al KYC così implementato non è una posizione isolata: la sollevano organizzazioni per i diritti digitali (ARTICLE 19, sull'e-KYC obbligatorio come rischio per privacy e libertà d'espressione), analisti di sicurezza, la letteratura su euro digitale/CBDC e la stampa di settore. Il dato più eloquente è di scala: nel 2026 il provider di verifica identità IDMerit ha esposto circa un miliardo di record in 26 Paesi — la conferma, su scala industriale, che i database KYC sono bersagli pericolosi proprio perché costruiti per verificare l'identità. Gli argomenti ricorrenti sono la raccolta eccessiva e la conservazione prolungata di dati sensibili, la condivisione opaca con terze parti (screening sanzioni, PEP, adverse media), e l'esistenza di alternative — prove a conoscenza zero (zero-knowledge) e verifiche non custodial — che permetterebbero di accertare l'identità senza accumulare gli archivi. — Base: ARTICLE 19; Cybernews/Zyphe (IDMerit, 2026); Cointelegraph e Bitcoin.com (caso Revolut); letteratura su CBDC/privacy.

Ne emerge un'asimmetria di fondo: **gli utenti si sottopongono a verifiche continue e sempre più invasive, ma il controllo su chi custodisce quelle identità è comparativamente debole** — e la stessa infrastruttura è quella su cui poggeranno la finanza regolata e i progetti di euro digitale. Il KYC, così com'è, non elimina il rischio: ne sposta una parte sostanziale dalla sfera dei fondi a quella dell'identità e della privacy, rendendo gli utenti più esposti a frodi, estorsioni e sorveglianza mirata. La direzione difendibile non è abolirlo, ma ridurne la superficie: minimizzazione dei dati raccolti, limiti stringenti di conservazione, verifiche riutilizzabili o decentralizzate, e trattamento degli archivi KYC come asset critici al pari dei fondi custoditi.

In termini di incentivi, il KYC protegge in primo luogo la posizione di compliance dell'istituto; il rischio, una volta raccolti i dati, ricade sull'utente — che non ha strumenti semplici per farsi "ripulire" dai database una volta che il dato è esposto. Non è l'esistenza della verifica a essere in discussione, ma un'implementazione che trattiene il beneficio e distribuisce il rischio.

Una precisazione, per non forzare la lettura: non risulta un pattern causale del tipo "una piattaforma introduce il KYC e per questo viene poi attaccata". I casi documentati mostrano che a essere colpite sono piattaforme già pienamente KYC — e i loro provider di verifica — proprio per i dati di identità che

custodiscono, a prescindere da quando il KYC sia stato adottato (Binance nel 2019, Coinbase nel 2025, Revolut nel 2026). Gli exchange con KYC minimo o assente vengono anch'essi attaccati, ma di norma per i fondi (hot wallet, chiavi private), non per dati anagrafici che in gran parte non esistono. Il fattore di rischio non è dunque l'introduzione del KYC in sé, ma la concentrazione centralizzata di identità verificate. **[Confidenza media]** — nessuna evidenza di un pattern causale; ricognizione a campione]

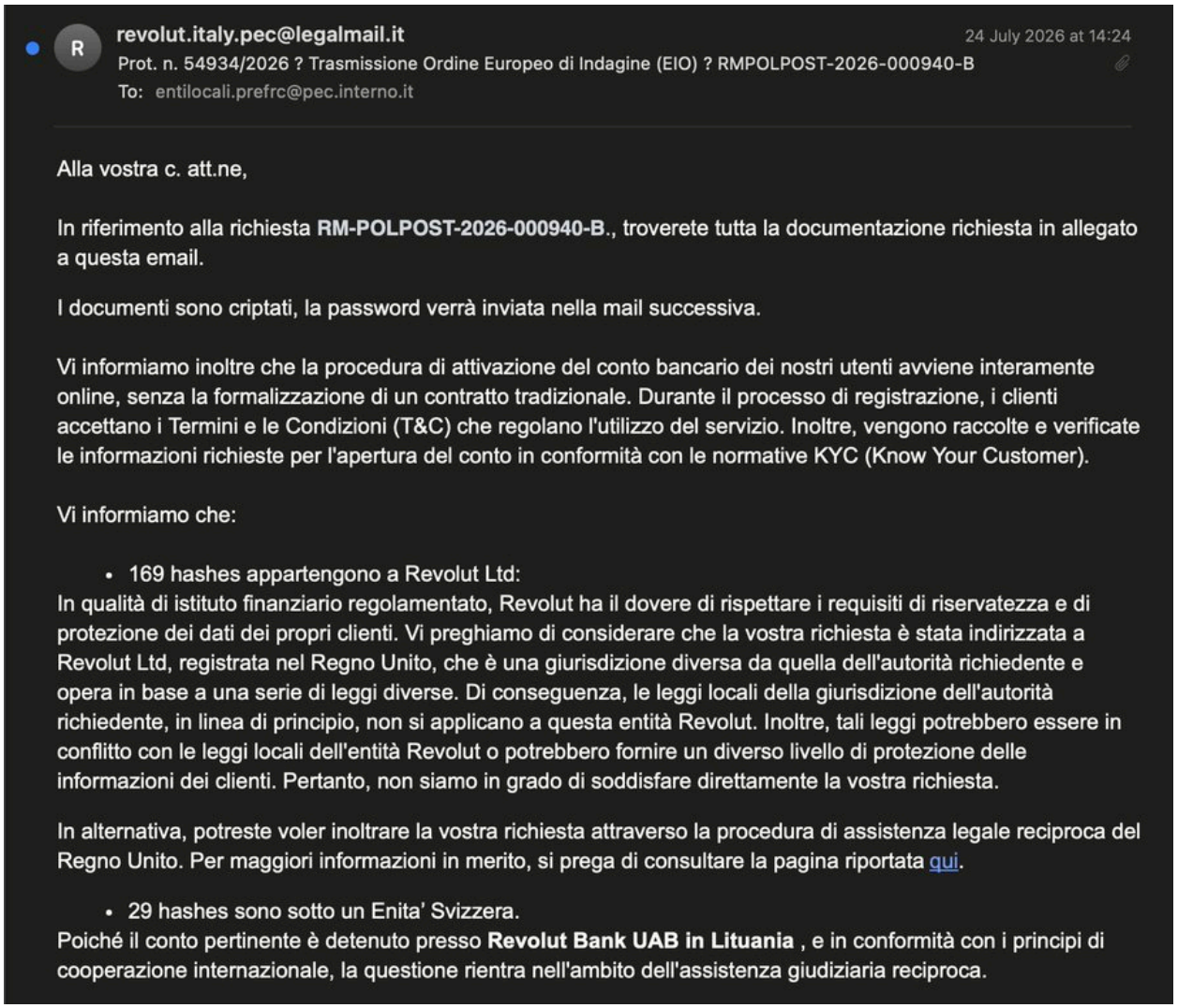
[Confidenza alta sui casi citati; il resto è analisi di policy] — Base: casi Coinbase (2025) e Revolut (2026) trattati nel fascicolo; violazioni di provider di verifica identità (Sumsub, AU10TIX); quadro AML/CFT post-2001.

8. Controlli mancanti o aggirati

Domanda guida: **quale controllo avrebbe dovuto impedire la consegna dei dati?**

Controllo	Stato nel caso	Evidenza
Autenticazione del mittente	**Superata solo sul piano tecnico:** la richiesta proveniva da un dominio/canale governativo autentico e, secondo le ricostruzioni disponibili, i controlli email risultavano coerenti.	PEC; ricostruzioni su SPF/DKIM/DMARC
Verifica indipendente dell'autorità	**Non evidenziata:** non emerge un contatto indipendente con la Procura o con i canali centrali dell'autorità	StrettoWeb; confronto con Kraken, che verificò l'ordine irlandese contattando il tribunale, atto par. 108
Coerenza del canale e della forma	**Possibile controllo mancato:** EIO inviato via PEC da un ufficio prefettizio, firma "Polizia Postale", intestazione Procura di Milano e lettera in inglese non coerente con l'Allegato A	Screenshot dell'EIO e della PEC
Validazione della base giuridica	**Non evidenziata:** assenza di un decreto dell'autorità giudiziaria nella documentazione esaminata	StrettoWeb; atto Kraken, parr. 93 e 99–104
Controllo di giurisdizione	**Applicato ma insufficiente:** avrebbe filtrato la società del gruppo destinataria senza validare l'autenticità sostanziale della richiesta	PEC 24/07
Doppia approvazione	Non noto	—
Alert su richieste massive o anomale	**Non evidenziato per il periodo precedente alla scoperta:** volume, ripetizione e struttura delle richieste avrebbero potuto costituire segnali di anomalia	Fotogramma del video; PEC; 192 messaggi e 33 cartelle, se confermati dalla documentazione
Minimizzazione dei dati	**Non evidenziata:** sarebbero stati trasmessi selfie, estratti conto e storico transazionale potenzialmente più ampi del necessario	Avviso di Revolut; materiale attribuito a Duel
Gestione delle risposte "correttive"	**Potenzialmente controproducente:** il supporto avrebbe indicato come correggere la richiesta e a quale società intestare la documentazione	PEC 24/03; Duel
Tracciamento e audit	**Attivato dopo la segnalazione:** l'audit interno risulta successivo alla scoperta dell'anomalia	PEC di maggio
Protezione della casella istituzionale (lato autorità)	**Non verificabile pubblicamente:** sono riportate credenziali circolanti e non risulta documentata l'applicazione obbligatoria della MFA alla casella coinvolta	Fonte TI; documento del gestore PEC
Canale di risposta e consegna dei dati (e della chiave)	**Mancato: secondo la ricostruzione la risposta è stata inviata allo stesso indirizzo da cui proveniva la richiesta — controllato dall'attaccante — anziché a un canale o dispositivo indipendente e verificato; se i dati fossero stati cifrati, l'invio della chiave sullo stesso canale ne avrebbe annullato la protezione.**	Ricostruzione del caso; Hudson Rock (casella monitorata dall'attaccante)

[Confidenza media] La rapidità della risposta va letta anche alla luce della pressione di sistema: il dovere di cooperare con le autorità, le scadenze strette e il rischio di rilievi di vigilanza, sanzioni o de-risking da parte dei corrispondenti spingono un istituto a rispondere presto e a propendere per l'esecuzione — un bias che l'attaccante ha sfruttato. Ciò non attenua però l'errore operativo specifico: la consegna dei dati (e dell'eventuale chiave di cifratura) è avvenuta sullo stesso canale della richiesta, cioè verso la casella controllata dall'attaccante, invece che su un canale o dispositivo indipendente e verificato. La regola difendibile — coerente con gli avvisi su false richieste delle autorità (FBI, 2024) e con i controlli già indicati — è duplice: verificare l'autorità out-of-band prima di rispondere, e recapitare dati e chiavi solo a un endpoint istituzionale ottenuto in modo indipendente, mai "rispondendo" all'indirizzo entrante. *– Base: ricostruzione del caso; Hudson Rock; FBI PSA su false richieste EDR, 2024*



revolut.italy.pec@legalmail.it 24 July 2026 at 14:24
Prot. n. 54934/2026 ? Trasmissione Ordine Europeo di Indagine (EIO) ? RMPOLPOST-2026-000940-B
To: entilocali.prefrc@pec.interno.it

Alla vostra c. att.ne,

In riferimento alla richiesta **RM-POLPOST-2026-000940-B**., troverete tutta la documentazione richiesta in allegato a questa email.

I documenti sono criptati, la password verrà inviata nella mail successiva.

Vi informiamo inoltre che la procedura di attivazione del conto bancario dei nostri utenti avviene interamente online, senza la formalizzazione di un contratto tradizionale. Durante il processo di registrazione, i clienti accettano i Termini e le Condizioni (T&C) che regolano l'utilizzo del servizio. Inoltre, vengono raccolte e verificate le informazioni richieste per l'apertura del conto in conformità con le normative KYC (Know Your Customer).

Vi informiamo che:

- 169 hashes appartengono a Revolut Ltd:

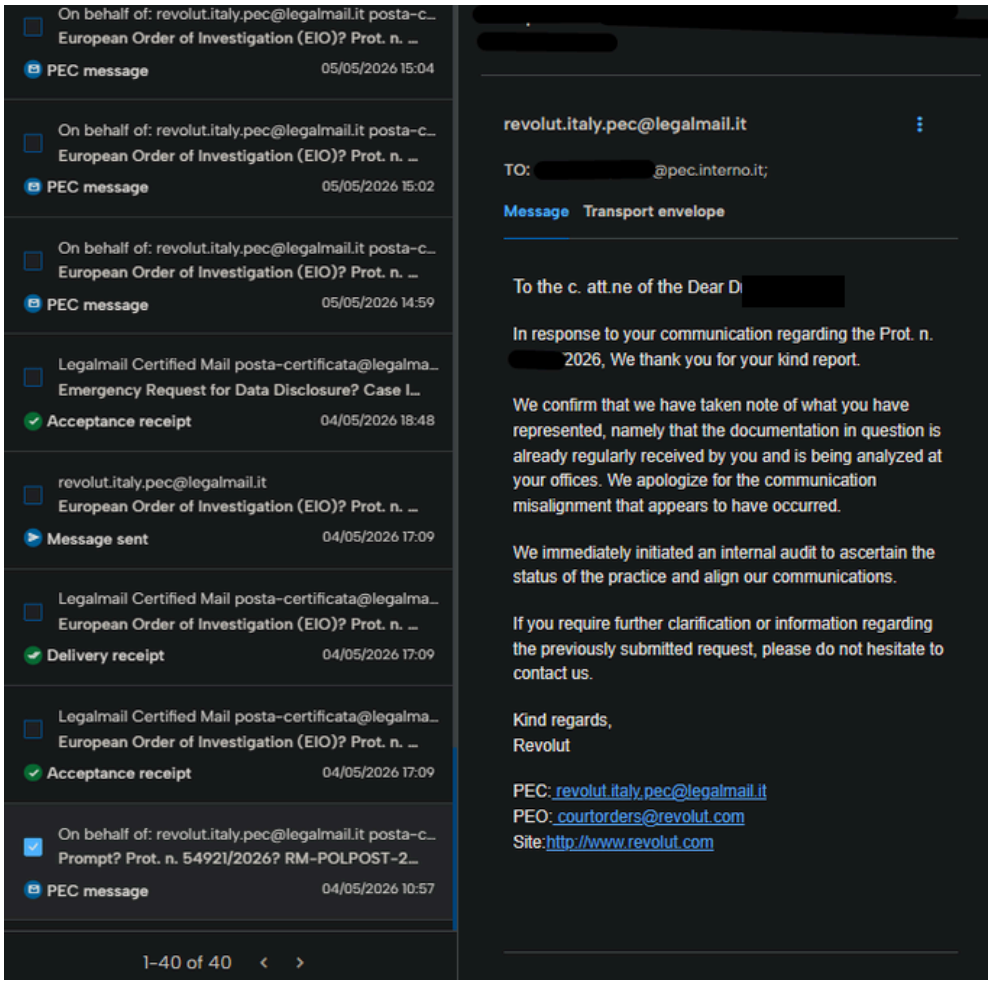
In qualità di istituto finanziario regolamentato, Revolut ha il dovere di rispettare i requisiti di riservatezza e di protezione dei dati dei propri clienti. Vi preghiamo di considerare che la vostra richiesta è stata indirizzata a Revolut Ltd, registrata nel Regno Unito, che è una giurisdizione diversa da quella dell'autorità richiedente e opera in base a una serie di leggi diverse. Di conseguenza, le leggi locali della giurisdizione dell'autorità richiedente, in linea di principio, non si applicano a questa entità Revolut. Inoltre, tali leggi potrebbero essere in conflitto con le leggi locali dell'entità Revolut o potrebbero fornire un diverso livello di protezione delle informazioni dei clienti. Pertanto, non siamo in grado di soddisfare direttamente la vostra richiesta.

In alternativa, potreste voler inoltrare la vostra richiesta attraverso la procedura di assistenza legale reciproca del Regno Unito. Per maggiori informazioni in merito, si prega di consultare la pagina riportata qui.

- 29 hashes sono sotto un Enita' Svizzera.

Poiché il conto pertinente è detenuto presso **Revolut Bank UAB in Lituania** , e in conformità con i principi di cooperazione internazionale, la questione rientra nell'ambito dell'assistenza giudiziaria reciproca.

I documenti attribuiti alla richiesta del 24 luglio mostrano che Revolut - secondo quanto illustrato da Lyudmyla Kozlovska (@LyudaKozlovska su X) - applicava un controllo giurisdizionale: per 169 hash riferiti a Revolut Ltd (Regno Unito) rifiutava la divulgazione diretta indicando l'assistenza legale reciproca britannica; per 29 hash, riferiti a un'entità svizzera con conto presso Revolut Bank UAB in Lituania, rinviava all'assistenza giudiziaria reciproca. La stessa comunicazione indica che la documentazione richiesta era allegata; dalla parte visibile non è possibile stabilire per quali conti. Secondo i file .eml descritti da Duel, gli attori avrebbero usato ID di transazione e indirizzi wallet pubblici come chiavi di ricerca per selezionare clienti crypto di alto valore e ottenerne i dati KYC. Questi elementi rafforzano l'ipotesi di un abuso procedurale mirato, ma non dimostrano da soli che il quadro normativo europeo escluda una verifica sostanziale del richiedente, né che tutti i dati siano stati divulgati secondo lo stesso schema.



Vista della casella – elenco dei messaggi ("1-40 of 40"): tra il 4 e il 5 maggio 2026 risultano invii, ricevute di accettazione e consegna Legalmail e una risposta di Revolut; oggetto degli scambi "European Order of Investigation (EIO)" e "RM-POLPOST". Nome del destinatario oscurato. (screenshot ricevuto; non verificato in modo indipendente)

8-bis. Integrazione del cyber nel processo di risposta alle richieste delle autorità

La tabella della sezione 8 suggerisce che **i principali punti di possibile fallimento siano organizzativi e procedurali, non necessariamente vulnerabilità tecnologiche dell'infrastruttura bancaria**. Nei modelli operativi in cui le richieste delle autorità sono gestite prevalentemente da legale e compliance, senza un punto di controllo strutturato per sicurezza, SOC o CTI, il canale fiduciario può rimanere al di fuori del normale monitoraggio cyber.

Cosa coprono gli strumenti antifrode di settore

- **[Confidenza alta]** Le soluzioni antifrode e di intelligence adottate nel settore coprono soprattutto frodi transazionali, onboarding, credenziali e carte compromesse, oltre ai movimenti tra conti tradizionali e attività on-chain. Le partnership Nasdaq Verafin–Q6 Cyber, Nasdaq Verafin–Alloy e Nasdaq Verafin–Stablecore sono esempi di questa direzione: dark-web intelligence, segnali di rischio identitario, dati consortili e correlazione tra attività finanziarie tradizionali e digitali *— Base: comunicati Nasdaq Verafin*

Questi strumenti possono risultare utili **a valle**, per rilevare l'uso fraudolento di dati KYC sottratti presso altri istituti, ma non sono necessariamente progettati come sistemi di controllo delle richieste di dati provenienti da autorità pubbliche. Una richiesta di divulgazione non è una transazione finanziaria e può quindi non generare gli stessi alert comportamentali.

[Confidenza alta sulla convenzione] Convenzione degli indirizzi PEC delle Prefetture. Gli indirizzi degli uffici seguono uno schema uniforme del tipo <ufficio>.pref<sigla provincia>@pec.interno.it, come risulta dagli elenchi pubblicati dalle singole Prefetture (esempio: Prefettura di Cosenza, snapshot del 22/12/2025, che riporta entilocali.prefcs@pec.interno.it per l'Area II – Raccordo con gli Enti Locali). La prevedibilità dello schema comporta che la coerenza formale dell'indirizzo mittente non costituisce un elemento di verifica: un indirizzo plausibile può essere derivato senza alcun accesso ai sistemi. *— Base: elenchi pubblici delle Prefetture (Internet Archive)*

[Confidenza alta sul dato IPA] Domicilio digitale e IndicePA. Il domicilio digitale della Prefettura di Reggio Calabria censito in IPA è protocollo.prefrc@pec.interno.it, registrato dal 12/04/2019. L'indirizzo utilizzato per le richieste a Revolut (entilocali.prefrc@pec.interno.it) non risulta censito in IPA, che però registra i domicili digitali degli enti e delle loro articolazioni e non ogni casella interna: l'assenza non prova quindi che la casella non esistesse. Ne discende un controllo minimo applicabile da qualunque destinatario: verificare che l'indirizzo mittente corrisponda al domicilio digitale pubblicato in IPA per l'ente indicato e, in caso di difformità, chiedere conferma all'ente su un recapito indipendente. *— Base: IndicePA*

[Confidenza alta sul gestore] Gestore PEC. Il dominio pec.interno.it risulta ospitato su InfoCert Legalmail (record MX mx.cert.legalmail.it). Anche la PEC di Revolut (revolut.italy.pec@legalmail.it) è su Legalmail/InfoCert: mittente e destinatario degli scambi sono quindi sullo stesso gestore, il che rende coerente l'ambiente mostrato negli screenshot (casella @pec.interno.it aperta nella webmail InfoCert). La coerenza dell'ambiente non equivale però all'autenticità dei singoli screenshot, che restano materiale diffuso dall'attore. *— Base: record DNS MX di pec.interno.it*

[Confidenza alta sul funzionamento della PEC] Presidio della casella e tracce del traffico. L'uso prolungato di una casella PEC istituzionale comporta traffico visibile nella casella stessa: ricevute di accettazione e consegna per ogni invio, risposte e solleciti del destinatario, allegati di dimensioni rilevanti che incidono sulla quota disponibile, notifiche del gestore. La mancata rilevazione per diversi mesi implica una di queste condizioni: assenza di presidio sulla casella, cancellazione sistematica dei messaggi da parte di chi la controllava, oppure mancata segnalazione da parte di chi ha visto il traffico. Il log dei messaggi conservato dal gestore PEC per trenta mesi consente comunque la ricostruzione di mittenti, destinatari, date e identificativi, a prescindere dalle cancellazioni effettuate sulla casella. *— Base: disciplina della posta elettronica certificata*

Controlli minimi sulle richieste delle autorità

Controllo	Chi	Descrizione
Verifica out-of-band	legale / compliance	contatto con l'autorità tramite recapiti ufficiali ottenuti in modo indipendente, mai quelli presenti nella richiesta
Coerenza formale	legale	ufficio competente per materia, firma, autorità intestataria, canale previsto (EIO tramite autorità di esecuzione nazionale)
Base giuridica	legale	decreto dell'autorità giudiziaria, numero di procedimento, magistrato identificabile
Doppia approvazione e minimizzazione	legale + sicurezza	obbligatorie per richieste con dati KYC, biometrici o riferite a più clienti
Soglie di volume e frequenza	sicurezza / SOC	alert per mittente su numero di richieste, numero di clienti, liste di hash o wallet
Risposta ai rifiuti	compliance	nessuna indicazione correttiva a un richiedente non verificato

Escalation trigger per richieste istituzionali ad alto rischio

La tabella seguente introduce un decision gate tecnico-organizzativo per il processo di Law Enforcement Response: i trigger non classificano genericamente il rischio, ma indicano quando interrompere la divulgazione automatica e quale owner deve attivare il controllo rafforzato.

Segnale di attivazione	Condizione osservabile	Controllo richiesto / owner
OEI o richiesta transfrontaliera anomala	OEI o richiesta transfrontaliera ricevuta direttamente, oppure proveniente da un ufficio non competente o da un canale non coerente con il procedimento.	Validazione legale out-of-band con l'autorità competente e blocco temporaneo della divulgazione.
Incongruenza documentale	Firma, intestazione, lingua, autorità indicata, numero di procedimento o allegati non coerenti.	Legal review, verifica della base giuridica e preservation di messaggio, allegati e metadati.
Divulgazione ad alto impatto	Richiesta di dati KYC, biometrici, transazionali, crypto o riferiti a più clienti.	Approvazione "four-eyes" da parte di Legale/Compliance/Sicurezza e gate di data minimization prima della consegna.
Richiedente adattivo	Riformulazioni dopo un rifiuto, correzioni progressive, urgenza anomala o richiesta di recapiti alternativi.	Compliance review con escalation SOC/CTI e limitazione delle istruzioni operative fornite al richiedente.
Segnale di canale compromesso	Casella, dominio o infrastruttura associati a credenziali esposte, accessi anomali, abuso noto o comportamento non coerente.	Triage SOC/CTI, verifica con l'ente titolare del canale e innalzamento del livello di rischio.

Regola operativa: la presenza di un trigger ad alto impatto, oppure la combinazione di più trigger, deve sospendere la divulgazione automatica fino al completamento dei controlli rafforzati e alla decisione documentata degli owner coinvolti.

Ruolo del cyber e della CTI

Il cyber e la **Cyber Threat Intelligence (CTI)** dovrebbero intervenire prima della divulgazione dei dati, non soltanto dopo un eventuale abuso. Il loro compito è verificare il contesto tecnico e comportamentale della richiesta, aumentare il livello di rischio quando emergono segnali convergenti e fornire elementi indipendenti a legale, compliance e investigazioni.

Analisi del messaggio

La verifica dovrebbe includere:

- intestazioni complete, Message-ID, percorso SMTP e timestamp;
- autenticazione del dominio, inclusi SPF, DKIM e DMARC;
- storico della casella e del dominio mittente;
- anzianità, competenza e comportamento della casella;
- eventuali anomalie nella firma, negli allegati o nei recapiti;
- uso di una casella nuova, non coerente con l'ufficio dichiarato o non competente per materia.

L'analisi tecnica non dimostra da sola la legittimità della richiesta, ma può evidenziare spoofing, compromissione, inoltri anomali o deviazioni dal normale processo.

Nota: nel report sulle campagne malevole del 2025 (pubblicato il 10/02/2026), il CERT-AGID ha indicato che le campagne via PEC hanno sfruttato soprattutto caselle legittime compromesse, oltre a indirizzi registrati ad hoc e poi dismessi a seguito di segnalazione ai gestori. Il 15/06/2026 ha comunicato di aver gestito, da gennaio 2026, oltre 650 eventi relativi a caselle PEC abusate o registrate per finalità illecite, chiedendo ai gestori il reset delle caselle compromesse e la dismissione di quelle create a scopo malevolo. — Base: CERT-AGID, report 2025; CERT-AGID, avviso del 15/06/2026

Threat intelligence sulle caselle

La CTI può monitorare, nel rispetto della base giuridica e delle regole interne, log di infostealer, combolist, forum e altri spazi criminali per individuare credenziali o riferimenti riconducibili a enti e autorità. Una corrispondenza non prova la compromissione della casella: può riflettere dati vecchi, riutilizzati, falsificati o riferiti a un servizio terzo. Tuttavia, dovrebbe innalzare il livello di rischio e attivare una verifica indipendente; i primi accertamenti della Polizia Postale, riferiti dalla stampa il 18/09, non confermano la sottrazione con l'ente titolare della casella.

Rilevamento dei pattern

È utile correlare automaticamente:

- liste di hash o wallet usate come unica chiave di ricerca;
- richieste di reintestazione o "correzione" dopo un rifiuto;
- urgenza, minacce e scadenze anomale;
- richieste di invio a indirizzi alternativi;
- richieste seriali o incremento improvviso dei clienti coinvolti;
- allegati cifrati e password trasmesse su canali separati;
- ripetizione di oggetti, riferimenti, hash, wallet o modelli documentali.

La correlazione non dovrebbe produrre un rifiuto automatico basato su un singolo indicatore. Dovrebbe invece generare una valutazione di rischio, una conservazione degli artefatti e, quando necessario, un'escalation a sicurezza, legale e compliance.

Condivisione degli indicatori

Gli indicatori verificati possono essere condivisi con **CERTFin**, **CERT-AGID**, **ACN** e con l'ente titolare della casella sospetta, usando i canali appropriati e applicando minimizzazione, controllo degli accessi e tracciabilità. CERTFin si presenta come il CERT del settore finanziario italiano e opera a supporto della prevenzione e gestione delle minacce cyber nel comparto finanziario.La condivisione dovrebbe distinguere chiaramente tra dato osservato, dato verificato, ipotesi analitica, livello di confidenza e azione richiesta dal destinatario.

Esercitazioni congiunte

Sono consigliabili simulazioni legale–compliance–sicurezza su scenari di impersonificazione delle autorità, includendo i casi Kraken e Revolut come scenari di test. L'esercitazione dovrebbe verificare:

- chi riceve e protocolla la richiesta;
- chi valuta autenticità, competenza e base giuridica;
- chi decide la sospensione della divulgazione;
- come si contatta l'autorità tramite un canale indipendente;
- quali evidenze vengono conservate;
- quando e come si effettua la segnalazione esterna.

Obblighi e buone pratiche

- **[Confidenza alta]** **Obbligo generale.** Ill GDPR richiede una base giuridica per il trattamento e la comunicazione dei dati, oltre a misure di sicurezza adeguate e proporzionate al rischio. Il testo del regolamento collega la sicurezza alla valutazione dei rischi e a misure idonee a proteggere riservatezza, integrità e disponibilità. *— Base: GDPR; DORA.* **Ambito finanziario.** DORA si applica dal 17 gennaio 2025 alle entità finanziarie rientranti nel relativo perimetro e disciplina, tra l'altro, gestione del rischio ICT, incidenti, resilienza operativa e relativa governance.
- **[Confidenza media]** **Buona pratica, non necessariamente obbligo specifico.** Non risulta, sulla base delle fonti richiamate, un obbligo generale e dettagliato che imponga a ogni istituto una procedura unica per verificare l'autenticità sostanziale delle richieste delle autorità. Questo non significa che la verifica sia facoltativa: significa che la sua concreta configurazione deriva dall'insieme di obblighi su base giuridica, sicurezza, governance, gestione del rischio e protezione dei dati. *— Base: normativa richiamata; dichiarazioni di Kozlovska e Kodex*

Il limite non è necessariamente l'assenza di tecnologia antifrode, ma la separazione organizzativa tra chi riceve le richieste, chi ne valuta la legittimità e chi monitora i segnali di compromissione. La sicurezza dovrebbe entrare nel processo prima della divulgazione dei dati, non soltanto dopo che i dati sono stati utilizzati per una frode.

9. Indicatori di compromissione

9.1 Indicatori tecnici

Indicatore	Tipo	Stato
entilocali.prefrc@pec.interno.it	Indirizzo e-mail PEC presumibilmente abusato	Riportato da terzi; autenticità e controllo della casella non verificati
Oggetti: “Trasmissione Ordine Europeo di Indagine (EIO)” e “Emergency Request for Data Disclosure”; riferimenti RM-POLPOST-2026-000940-B, Prot. n. 54921/2026 e 54934/2026	Pattern di richiesta	Riportato da terzi
Intestazione “Public Prosecutor’s Office at the Court of Milan”, Via Freguglia 1, lingua inglese e assenza di firma	Documento potenzialmente contraffatto	Riportato da terzi, indicatore documentale.
imnotavillain[.]xyz — registrazione 14/09/2026, (NICENIC INTERNATIONAL GROUP CO., LIMITED; nameserver ns3.my-ndns.com / ns4.my-ndns.com)	Dominio associato all’attore	Confermato tramite WHOIS.
iamnotavillain[.]com — registrar Tucows Domains Inc.; nameserver Njalla; registrato il 15/09/2026 e aggiornato il 16/09/2026.	Dominio associato all’attore	Confermato tramite WHOIS, se verificato con il record originale
revoloot[.]lol -registrar NameSilo, LLC dnsowl.com	Sito di estorsione associato a “Revolut Smilik”	Riportato dal canale Telegram. Server hold e client hold indicano uno stato di sospensione o blocco presso il registro/registrar
@revolutsmilik, t.me/backupsmile1231	Canali di comunicazione	Canale di backup
Session ID (Revolut Smilik) 05a6f11c1dd5897925a29c9b02966d99f62401b0fc6282b3b4f13e59a3bcad805f	Identificativo di contatto	Confermato nei messaggi come indicatore contestuale;
Session ID (IAmNotAVillain) 0548b3c2be496218baa2314386787badfd458a868240a19ede82eabb6a13dd2c26	Identificativo di contatto del gruppo	Scheda CONTACT del sito del gruppo (“Same place for staff, press, and users”). Session ID = chiave pubblica di messenger decentralizzato. Utilizzabile come identificatore/IoC.
Wallet XMR 8BvXFt6v7aSR3Qs9SPgBVLWQzAragHtTiXn3Us3Eh2wLjED1zE4D7a5KxsRE3Wn4e1CjjLJydavscdcwge2UurTUKsgGBXe	Wallet di riscatto Monero (XMR)	Indirizzo completo dal sito di estorsione. Monero occulta importi e controparti: pagamento, saldo e flussi non sono verificabili sulla blockchain da un osservatore esterno (cfr. nota sui limiti della tracciabilità). Utilizzabile solo come identificatore/IoC
ibb[.]co/gBcT44h	URL di image hosting contenente un elenco wallet–KYC	Confermato come link condiviso in un messaggio Telegram; contenuto, provenienza e autenticità da verificare

Nota — Il riscatto in Monero e i limiti della tracciabilità

L'indirizzo XMR del riscatto (8BvXFt6v7aSR3Qs9…UurTUKsgGBXe) non è interrogabile su un explorer come un indirizzo Bitcoin o Ethereum. Monero occulta per progetto tre elementi delle transazioni on-chain: gli importi (RingCT), il mittente (ring signatures) e il destinatario (stealth address). L'analisi diretta sulla blockchain è perciò molto più debole che su Bitcoin: non si segue un flusso "indirizzo A → B → C".

Monero non è però "perfettamente intracciabile". Le view key (chiavi di vista), se condivise volontariamente o sequestrate, permettono di vedere tutte le transazioni in entrata e in uscita di un wallet; tecniche di correlazione temporale, analisi di rete e clustering possono fornire indizi, soprattutto se combinate con dati esterni alla blockchain.

È proprio off-chain che l'anonimato tende a rompersi. Le indagini reali su Monero si appoggiano tipicamente al KYC degli exchange (quando l'XMR entra o esce da una piattaforma regolamentata, l'exchange conosce l'utente e, su mandato, ne consegna i log), alla forensics sui dispositivi sequestrati (estrazione di chiavi private o di vista da wallet e memoria), ai metadati di rete e alle operazioni sotto copertura, e agli errori operativi degli utenti (riuso di identità, leak di IP, view key condivise in modo incauto).

La ricerca sul tracciamento di Monero ha una storia, ed è un inseguimento continuo. Già nel 2017 il riscatto in Bitcoin di **WannaCry** fu convertito in Monero tramite un servizio di scambio, e la traccia utile non fu la blockchain ma i log del servizio; nel 2021 quelle transazioni furono oggetto di un'analisi forense pubblica. Tra il 2024 e il 2025 le rassegne di settore (TRM Labs) e la ricerca accademica dedicata alla forensics dei wallet Monero hanno mostrato due cose convergenti: alcune euristiche on-chain esistono ma la loro efficacia cala man mano che il protocollo si irrobustisce — aumenti obbligatori della ring size, correzioni rapide dei difetti — mentre il tracciamento realmente efficace passa da artefatti off-chain, cioè dai wallet e dai dispositivi. Le operazioni del 2026 confermano il quadro.

Alcuni casi lo mostrano. In Norvegia, nel 2026, la Kripos ha impiegato un nuovo metodo di tracciamento di Monero in un'operazione internazionale su forum del dark web conclusa con 28 arresti in più Paesi — non "leggendo la blockchain", ma combinando il tracciamento dell'XMR con indagini tradizionali e cooperazione internazionale. Nel caso Vastaamo, in Finlandia, la polizia ha dichiarato di aver "tracciato" un pagamento in Monero, ma l'attribuzione è avvenuta attraverso altri elementi (dati degli exchange, sequestri, la parte in Bitcoin dell'operazione); la pretesa di un tracciamento puramente on-chain è contestata dagli esperti.

Per il caso in esame ne discende che, per un osservatore esterno (stampa, utenti, concorrenti), è praticamente impossibile verificare se il riscatto sia stato pagato: la scelta del Monero rende il pagamento non verificabile sulla blockchain. Solo le autorità, con accesso agli exchange, ai wallet sequestrati o alle chiavi di vista, potrebbero in prospettiva ricostruire i flussi. Restano le vie indirette già note: verificare se l'indirizzo è segnalato (Chainabuse, feed di threat intelligence), il che collegherebbe la campagna ad altre, oppure un'eventuale transaction key pubblicata da chi paga.

Verifica diretta (20/09/2026). L'indirizzo non è interrogabile su un block explorer pubblico e la sua decodifica ne conferma la natura di subaddress mainnet; le chiavi di vista e di spesa che alcuni explorer mostrano sono quelle pubbliche, ricavabili dall'indirizzo stesso, e non consentono né di vedere né di spostare fondi. Verificare gli effettivi incassi richiederebbe la chiave di vista privata del wallet, che non è pubblica: un controllo tentato con la sola chiave pubblica non produce corrispondenze valide ed è privo di valore probatorio. L'indirizzo, inoltre, non risulta segnalato su Chainabuse né presente in fonti pubbliche indicizzate: nessun footprint pubblico noto alla data. **[Confidenza alta** — verifica diretta]

[Confidenza alta sul funzionamento di Monero; media sui limiti operativi del tracciamento] — Base: caratteristiche del protocollo Monero; TRM Labs (rassegna 2024); Forensic Science International: Digital Investigation (wallet forensics, 2025); CyberScoop/Neutrino (WannaCry, 2017) e analisi di N. Bax (2021); Euronews, TechNadu (Norvegia, Kripos 2026); BleepingComputer (caso Vastaamo).

9.2 Indicatori comportamentali per un istituto

I seguenti segnali possono indicare richieste fraudolente, impersonificazione di autorità o tentativi di elusione dei normali controlli legali. Nessun singolo indicatore è conclusivo: la valutazione dovrebbe basarsi

sulla combinazione dei segnali, sulla verifica indipendente dell'autorità richiedente e sulla coerenza del procedimento

- Richieste provenienti da domini istituzionali, ma da caselle o uffici non competenti per materia.
- Incoerenza tra ufficio mittente, firma, autorità intestataria e procedimento dichiarato.
- Ordini europei di indagine o richieste di assistenza giudiziaria ricevuti direttamente, anziché tramite il canale dell'autorità di esecuzione competente.
- Liste estese di hash di transazioni o indirizzi wallet usate come unica chiave di ricerca, senza ulteriori elementi identificativi o contesto probatorio.
- Assenza di decreto, numero di procedimento verificabile o riferimento a un magistrato identificabile.
- Richieste ripetute dallo stesso mittente, con volume crescente o con un numero sempre maggiore di clienti coinvolti.
- Richieste di "correzione" o reintestazione dopo un rifiuto formale o una richiesta di integrazione.
- Linguaggio d'urgenza, minacce, scadenze anomale o richiesta di invio a un indirizzo alternativo.
- Allegati cifrati con password trasmessa tramite canale separato, soprattutto quando il volume dei dati richiesti è elevato.
- Richieste indirizzate a più società del gruppo senza una chiara motivazione giurisdizionale o una delimitazione del perimetro.
- Ripetizione degli stessi riferimenti, oggetti, hash o wallet in messaggi successivi, anche dopo risposte negative o richieste di chiarimento.

Criterio di escalation

La presenza simultanea di più segnali dovrebbe attivare una verifica rafforzata prima di qualsiasi divulgazione di dati. In particolare, l'istituto dovrebbe sospendere l'adempimento operativo quando la richiesta presenta incoerenze tra autorità, competenza, procedimento e canale di trasmissione, oppure quando il mittente tenta di sostituire il normale iter con urgenza, pressione o recapiti alternativi.

La verifica dovrebbe comprendere almeno:

- autenticazione del mittente tramite un canale indipendente e già noto;
- controllo dell'autorità, dell'ufficio e del procedimento nei registri o nei contatti istituzionali appropriati;
- esame dell'integrità degli allegati e delle intestazioni tecniche;
- conferma della base giuridica, dell'ambito soggettivo e temporale e dei dati effettivamente richiesti;
- registrazione della richiesta, degli esiti delle verifiche e delle eventuali anomalie.

Gli indicatori costituiscono segnali di rischio e non provano, da soli, né la falsità della richiesta né la compromissione dell'identità istituzionale.

10. “*Lessons learned*” per un istituto bancario

- **[Confidenza alta]** Un dominio istituzionale autentico non dimostra, da solo, l’autenticità sostanziale della richiesta. Anche la PEC certifica l’invio e la consegna del messaggio, ma non prova che la persona che controlla la casella sia il soggetto autorizzato a formulare quella richiesta. *— Base: casi Kraken e Revolut; dichiarazione di Kodex*
- **[Confidenza alta]** Un rifiuto formale che spiega nel dettaglio come correggere intestazione, giurisdizione, formato o riferimenti procedurali può fornire all’attaccante una guida per superare il controllo successivo. Questo non significa eliminare le motivazioni dei rifiuti. Significa adottare una **risposta controllata**. *— Base: PEC 24/03 e 24/07; atto Kraken*
- **[Confidenza media]** Lo schema è plausibilmente trasferibile agli istituti italiani perché le autorità e molte organizzazioni utilizzano la PEC per comunicazioni formalmente rilevanti. Tuttavia, non va presentato come prova che ogni banca riceva o gestisca le richieste con procedure identiche. Il dato di contesto è significativo: CERT-AGID Il 15/06/2026 ha comunicato di aver gestito, da gennaio 2026, oltre 650 eventi relativi a caselle PEC abusate o registrate per finalità illecite, chiedendo ai gestori il reset delle caselle compromesse e la dismissione di quelle create a scopo malevolo. *— Base: CERT-AGID, report 2025; CERT-AGID, avviso del 15/06/2026*
- **[Confidenza media]** Gli investimenti in antifrode su transazioni, onboarding e attività on-chain possono non coprire il processo di risposta alle richieste delle autorità. Il rischio nasce nella zona di confine tra compliance, ufficio legale e sicurezza informatica. *— Base: comunicati Nasdaq Verafin agosto-settembre 2026* Le recenti iniziative di Nasdaq Verafin mostrano una crescente integrazione tra segnali di rischio, identità e prevenzione delle frodi lungo il ciclo di vita del cliente; ciò non dimostra però che il problema delle richieste fraudolente alle autorità sia automaticamente coperto da tali strumenti.La lezione operativa è istituire un controllo trasversale prima della divulgazione, con criteri di escalation condivisi e responsabilità chiaramente assegnate.
- **[Confidenza media]** Dopo l’incidente, il danno non resta limitato al database o al processo interno. Può estendersi a: diffusione secondaria dei dati, uso mediatico e politico del caso, pressione regolatoria e perdita di fiducia nei canali istituzionali. *— Base: sezioni 7 e 13*

11. Confidence assessment

Valutazione	Confidenza	Principali lacune
Abuso del processo di risposta alle autorità, non intrusione nei sistemi Revolut	Alta	La natura esatta dell'accesso e del flusso operativo resta da documentare integralmente
Uso di un dominio governativo italiano legittimo	Alta	Manca una conferma pubblica completa del Viminale; resta da stabilire se la casella sia stata compromessa o clonata; sul caso specifico
Casella riferita all'ufficio Enti Locali della Prefettura di Reggio Calabria	Media	Attribuzione basata su screenshot e stampa; nessuna conferma ufficiale pubblica dell'ente
Circa 680 clienti selezionati tramite blockchain analysis	Bassa	Numero e metodo sono attribuiti all'attaccante o riportati dalla stampa; non confermati da Revolut
Richieste protratte per diversi mesi, con durata precisa non confermata	Media	Le fonti divergono sulla durata precisa e sulla data iniziale; usare "per diversi mesi" salvo conferma documentale puntuale
Schema analogo al caso Kraken del 2025	Alta	L'analogia riguarda l'abuso di richieste apparentemente provenienti da autorità; non implica identità degli attori
Stesso attore del caso Kraken 2025	Bassa	Nessun collegamento tecnico o probatorio indipendente
Accesso ai sistemi delle forze dell'ordine e sottrazione di 147 GB	Bassa	Rivendicazione dell'attaccante e screenshot di una cartella, senza verifica indipendente I primi accertamenti della Polizia Postale, riferiti dalla stampa il 18/09, non confermano la sottrazione dei 147 GB.
Capacità di attacco	Media	L'attore ha dimostrato capacità almeno moderate di abuso procedurale e social engineering, sfruttando canali istituzionali, conoscenza dei flussi di risposta e selezione mirata delle vittime. Non sono invece sufficienti le evidenze disponibili per attribuire una capacità tecnica avanzata o una compromissione sofisticata dei sistemi.
Riscatto di 3 milioni di dollari in XMR	Media	La richiesta di 6.000 XMR è riportata dalla stampa; non risulta confermata come richiesta ricevuta direttamente da Revolut
Rischio replicabile verso banche italiane	Media	Non risultano, nel materiale esaminato, casi indipendenti in cui una banca italiana abbia già subito lo stesso schema

11-bis. Domande aperte

La casella entilocali.prefrc@pec.interno.it era attiva prima del 2026? Quando è stata creata e su richiesta di quale utenza?

Risulta tuttora attiva oppure è stata dismessa, e in quale data?

Cosa mostrano i log conservati dal gestore PEC, per almeno trenta mesi ai sensi dell'art. 11, comma 2 del DPR 68/2005, sul traffico dei mesi interessati?

Il punto di ingresso è stato il furto di credenziali, un abuso di privilegi amministrativi o un'attivazione per via procedurale?

Quando l'amministrazione si è accorta dell'uso anomalo della casella?

A quale indirizzo sono state effettivamente recapitate le richieste in Revolut, e come sono state instradate tra succursale italiana ed entità lituana?

Cosa dice il testo originale della comunicazione in cui Revolut chiede la distruzione della documentazione già inviata, e in quale fase è stata inviata?

I documenti di conti svizzeri presenti nel materiale pubblicato sono compatibili con il rifiuto giurisdizionale dichiarato il 24/07, o provengono da una richiesta precedente effettivamente evasa?

Nota: si tratta di elementi che dipendono da registri interni e da atti di indagine coperti dal segreto investigativo. La loro assenza in questo documento non va letta come esclusione di alcuna ipotesi.

12. Raccomandazioni

Immediate

- Rendere obbligatoria la verifica out-of-band per ogni richiesta di dati da parte di un'autorità: contattare l'ufficio competente tramite recapiti ufficiali ottenuti indipendentemente, mai tramite i recapiti presenti nella richiesta.
- Controllare la coerenza tra mittente, firma, autorità intestataria, base giuridica, oggetto, perimetro dei dati e canale previsto.
- Per un EIO, verificare autorità emittente, autorità di esecuzione, formulario, lingua, procedimento e trasmissione tramite il canale appropriato. L'EIO è basato sul riconoscimento reciproco e segue un modello standardizzato
- Bloccare preventivamente le richieste che usano liste di hash o wallet come unica chiave di ricerca, che riguardano molti clienti o che richiedono KYC, documenti d'identità o dati biometrici.
- Applicare un blocco rafforzato quando la richiesta proviene da una casella nuova, da un ufficio non competente o da un mittente già associato a richieste anomale.
- Avviare una revisione retrospettiva delle richieste evase negli ultimi 18 mesi, iniziando da quelle ricevute da caselle non competenti per materia, con volume elevato o con indicatori ripetuti.

Di processo

- Richiedere la doppia approvazione di legale e sicurezza per richieste massive, transfrontaliere o contenenti dati KYC, biometrici o finanziari.
- Applicare minimizzazione: divulgare soltanto i dati necessari, per il periodo e lo scopo indicati nel procedimento.
- Definire soglie di volume e frequenza per mittente, dominio, ufficio e cliente; generare alert automatici al superamento delle soglie.
- Creare un registro centralizzato e immutabile delle richieste, con mittente, timestamp, verifica effettuata, base giuridica, dati divulgati, approvazioni ed esito.
- Usare risposte standard ai rifiuti, senza spiegare al richiedente non verificato quali controlli interni deve superare o come correggere la richiesta.

- Predisporre un percorso separato per le emergenze, con richiamata obbligatoria, approvazione documentata e revisione successiva.
- Conservare messaggio originale, intestazioni, allegati, log, decisioni e comunicazioni di verifica per consentire audit e analisi forense.

Di ecosistema

- Condividere indicatori verificati con CERTFin, CERT-AGID e ACN, secondo i canali applicabili e con adeguata minimizzazione dei dati. CERTFin promuove la condivisione tempestiva di informazioni su minacce, vulnerabilità, incidenti e lezioni apprese nel settore finanziario.
- Segnalare le caselle istituzionali sospette all'ente titolare e al gestore PEC competente, distinguendo tra abuso della casella, spoofing e compromissione non ancora provata.
- Valutare l'uso di canali giudiziari sicuri e strumenti di scambio verificato. eEDES supporta lo scambio digitale di EIO e richieste di assistenza giudiziaria tra autorità competenti
- Formare compliance, legale, law-enforcement response e sicurezza sull'impersonificazione delle autorità.
- Eseguire esercitazioni con scenari basati sui casi Kraken e Revolut, includendo PEC compromessa, richiesta urgente, lista di wallet, rifiuto formale e tentativo di reintestazione.
- Monitorare menzioni dell'istituto e dati dei clienti su Telegram, forum e siti di estorsione, con procedure per preservare le evidenze senza interagire con gli attori.
- Preparare un piano di comunicazione per i clienti coinvolti, includendo phishing, estorsione, doxxing e, quando appropriato, rischi fisici.

Nessuna richiesta deve essere considerata automaticamente autentica soltanto perché proviene da una casella o da un dominio istituzionale. **L'istituto deve tuttavia rispettare i termini di risposta applicabili attraverso un percorso accelerato di autenticazione:** verifica out-of-band, controllo del procedimento, conferma della competenza e risposta interlocutoria o motivata quando la divulgazione non può ancora essere eseguita.

13. Contesto geopolitico e normativo

Il caso può essere inserito in un dibattito più ampio sulla fiducia nei canali istituzionali, sull'uso coercitivo dei sistemi finanziari e sulla sicurezza dei meccanismi di cooperazione giudiziaria. Occorre però distinguere il testo effettivo delle norme e delle risoluzioni dalle interpretazioni politiche sviluppate a partire dal caso Revolut.

Repressione finanziaria transnazionale

- **[Confidenza alta]** La Dichiarazione dell'Aia dell'Assemblea parlamentare OSCE include una risoluzione sulla repressione finanziaria transnazionale e sull'uso strumentale di strumenti AML/CFT, cooperazione giudiziaria, INTERPOL e legislazione cyber. Il testo riguarda soprattutto l'abuso di strumenti autentici da parte di Stati stranieri per sorvegliare, intimidire o esercitare coercizione economica oltre i propri confini. *Base: post di Kozlovska su X; testo della risoluzione* **La risoluzione OSCE PA non sembra disciplinare direttamente la falsificazione o il furto di una casella istituzionale di uno Stato UE**. Il collegamento con Revolut è analogico e politico, non una conseguenza testuale della risoluzione.
- **[Confidenza media]** Il thread di Kozlovska del 17 settembre 2026 precisa il meccanismo: accanto allo spyware — oggetto lo stesso giorno di un'allerta congiunta NCSC-FBI-AIVD su strumenti iraniani contro dissidenti e giornalisti — operano canali più silenziosi e spesso più efficaci, tutti "sotto copertura di legittima cooperazione internazionale": assistenza giudiziaria (MLAT), notice INTERPOL (Red, Diffusion e le più recenti Silver e Purple), richieste AML/CFT su base FATF, e procedimenti civili, arbitrali o penali aperti su suolo europeo. La tesi è che, con l'impilarsi di identità digitale, verifica dell'età e proposte come "Chat Control", le stesse richieste interstatali che oggi congelano un conto potranno domani

revocare l'accesso a un servizio: "Stati come l'Iran non avranno bisogno di violare nessuno; chiederanno a una controparte UE di segnalare l'identità digitale di un bersaglio".

- **[Confidenza media]** Il nesso con il caso è architetturale, non di attore. Il modello KYC fa di ogni utente un "nodo identificato" — identità verificata legata a conti, carte, wallet e storico transazioni — collocato in database di compliance esposti a richieste di autorità nazionali ed estere. Lo stesso "canale fidato" che in questo caso è stato abusato con una richiesta fraudolenta di matrice criminale può, nella prospettiva della repressione finanziaria transnazionale, essere azionato da uno Stato con richieste formalmente legittime, senza alcun "hack". Va però tenuta ferma la distinzione: nulla collega l'incidente Revolut a un'operazione statale — l'attore è criminale e il movente resta aperto. Ciò che i due piani condividono è la vulnerabilità dell'architettura fidata, non il soggetto che la sfrutta. Il Parlamento europeo (raccomandazione del 16 giugno 2026) e l'Assemblea parlamentare OSCE (Aia, luglio 2026) hanno chiesto misure proprio su questo terreno.
- **[Confidenza alta** sui documenti; media sul nesso architetturale, che è analitico] — Base: L. Kozlovska (X, 17/09/2026); allerta congiunta NCSC-FBI-AIVD (settembre 2026); Parlamento europeo, raccomandazione sulla repressione transnazionale (16/06/2026); OSCE PA, Aia (luglio 2026).

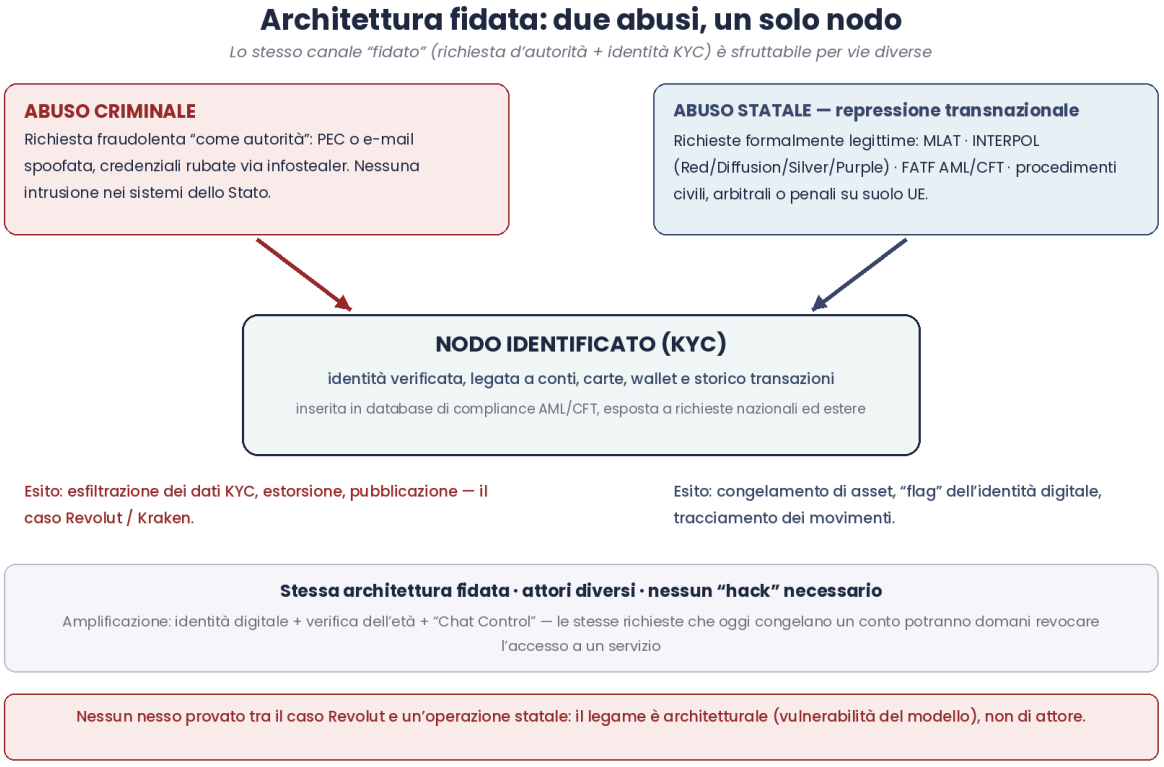


Figura — L'architettura fidata e i suoi due abusi: lo stesso nodo identificato (KYC) è raggiungibile da una richiesta fraudolenta criminale o da una richiesta interstatale formalmente legittima. Il legame tra i due piani è di metodo, non di attore.

Responsabilità dell'azienda e delle regole

- **[Confidenza media]** Il dibattito si divide tra una lettura che attribuisce la responsabilità principale all'azienda, per avere effettuato verifiche insufficienti sull'autenticità sostanziale delle richieste, e una lettura che evidenzia i limiti del quadro normativo, caratterizzato da obblighi di cooperazione rapida, assenza di una procedura unica e dettagliata per verificare ogni richiesta e crescente concentrazione dei dati attraverso meccanismi come DAC8. Le due interpretazioni non si escludono: un istituto può essere tenuto a rispondere entro termini brevi e, nello stesso tempo, dover adottare controlli indipendenti per evitare di divulgare dati a un soggetto non autorizzato. Le dichiarazioni del cliente coinvolto, di Duel e di Lyudmyla Kozlovska, insieme al contenzioso francese su DAC8, sostengono l'esistenza del dibattito, ma non consentono da sole di determinare la responsabilità giuridica definitiva di Revolut o l'illegittimità

del regime normativo. *— Base: dichiarazioni di un cliente coinvolto, di Duel e di Kozlovska; Consiglio di Stato francese su DAC8*

- **[Confidenza media]** Da qui una lettura che il fascicolo condivide: in questo caso a essere "bucato" non è stato un sistema di Revolut — non c'è stata intrusione né furto di fondi — ma il sistema. La falla sfruttata è strutturale: il canale con cui un'istituzione è tenuta a dar seguito a una richiesta apparentemente proveniente da un'autorità, e il modello che concentra in archivi centralizzati le identità verificate. Qualunque operatore che segua le stesse regole è esposto allo stesso vettore; Revolut è l'istanza in cui il problema è emerso, e le sue carenze di verifica — richieste evase per mesi senza controlli adeguati — lo hanno aggravato, ma non ne sono la radice. In questa prospettiva ha un fondamento l'allarme, sostenuto tra gli altri da Lyudmyla Kozlovska (Open Dialogue Foundation), secondo cui i meccanismi di sorveglianza finanziaria e di verifica dell'identità, nati contro riciclaggio e terrorismo, possono essere dirottati e trasformati in strumenti di abuso e di rischio proprio per le persone che dovrebbero proteggere. *— Base: analisi del fascicolo; L. Kozlovska / Open Dialogue Foundation ("hijacking financial surveillance").*

DAC8 e concentrazione dei dati

- **[Confidenza media]** Il contenzioso francese promosso da Bull Bitcoin e Paymium riguarda il decreto nazionale di attuazione della DAC8 (décret 2025-1276) e gli obblighi di raccolta e trasmissione di dati fiscali sugli utenti di cripto-attività. Il 14 settembre 2026 il Conseil d'État ha respinto la domanda di sospensione in via d'urgenza (référé-suspension, n. 519158), ritenendo che la sola possibilità di un rischio di violazione dei dati, di probabilità molto bassa, non costituisca urgenza; il giudizio di merito resta pendente. Il caso Revolut può essere utilizzato come argomento politico sul rischio di concentrazione e trasferimento dei dati, ma non dimostra che la DAC8 abbia causato l'incidente né che il regime DAC8 sia il canale giuridico utilizzato per ottenere i dati. La connessione è di policy e governance dei dati, non di causalità tecnica. — Base: bitcoin.fr; decisione del Conseil d'État n. 519158.

Francia e rischio fisico

- **[Confidenza media]** La Francia, tra i Paesi maggiormente interessati dai rischi criminali legati al settore cripto e sede della nuova licenza bancaria di Revolut dal 10 agosto 2026, costituisce un contesto rilevante per comprendere la dimensione geopolitica e regolatoria del caso. Il tema si collega sia all'ondata di rapimenti e attività estorsive rivolte a operatori e soggetti coinvolti nelle cripto-attività, sia al contenzioso promosso da Paymium e Bull Bitcoin contro l'attuazione francese della DAC8. Il collegamento è tuttavia di contesto e non dimostra che il caso Revolut sia stato causato dalla DAC8, né che l'incidente sia direttamente connesso ai rapimenti avvenuti in Francia. *— Base: franceinfo; PNACO; Cointelegraph*

e-Evidence ed eEDES

- **[Confidenza media]** Il sistema informatico decentrato previsto dal regolamento (UE) 2023/1543 collega le autorità competenti ai fornitori di servizi per gli ordini europei di produzione e conservazione. Lo scambio tra autorità giudiziarie per OEI e assistenza giudiziaria è invece affidato a eEDES, il cui portale di implementazione di riferimento risulta ancora in preparazione sul portale e-Justice. — Base: EUR-Lex; Eurojust; portale e-Justice *— Base: Commissione europea; EUR-Lex*

Dimensione reputazionale e quotazione

Il caso si colloca in una fase in cui Revolut prepara una possibile quotazione. Secondo la stampa (Economy Magazine, 18/09/2026), il fondatore Nik Storonsky valuta un doppio listino a Londra e sul Nasdaq, con orizzonte indicato al 2028 e subordinato alle condizioni di mercato; dopo una vendita secondaria di quote nel luglio 2026 la valutazione privata è stimata intorno ai 115 miliardi di dollari, con il Financial Times che indica fino a 200 miliardi come possibile valutazione in IPO. La stessa fonte riporta che dei circa 680 clienti coinvolti solo 8 sarebbero italiani, la maggior parte in Francia, Svizzera e altri Paesi europei.

Ipotesi — movente (aperto). Il movente non è determinabile e non va chiuso. La richiesta di riscatto in Monero indica una componente economica, ma non esaurisce la questione: la scelta di operare attraverso una casella governativa italiana reale è deliberata e strategica. In Italia la PEC ha valore legale e gode di un livello di fiducia istituzionale elevato; agganciare l'operazione a quel canale conferisce credibilità e impatto molto maggiori di una richiesta ordinaria, ed è ciò che ha fatto "sembrare vera" la richiesta agli occhi di chi doveva eseguirla. Massimizzare credibilità e impatto in questo modo è compatibile sia con un fine economico (l'imbarazzo pubblico forza il pagamento) sia con un fine di danno reputazionale o sistemico, tanto più in una fase pre-quotazione. Gli elementi disponibili non permettono di privilegiare l'una o l'altra: vanno tenute entrambe aperte. Il danno reputazionale resta comunque un effetto reale, a prescindere dall'intenzione.

[Confidenza media] La forma stessa dell'estorsione rafforza l'apertura del movente. Una richiesta puramente economica passa di norma per un canale diretto e riservato con la vittima; qui la domanda di riscatto (3 milioni di dollari, ~6.000 XMR) è stata avanzata pubblicamente — sul sito del gruppo, su Telegram e tramite la stampa — mentre Revolut dichiara di non aver ricevuto alcun contatto diretto né di aver negoziato, e non risulta alcun pagamento. Una richiesta pubblica senza canale diretto riduce la probabilità di incasso ma massimizza il danno reputazionale, e si accompagna alla retorica esplicita dell'intermediario (Duel), che dichiara di voler rendere pubblico "ogni elemento" per mostrare "il fallimento di Revolut" e "la stupidità del modo in cui il KYC è condotto oggi". È un profilo compatibile con un movente misto — economico ma anche reputazionale e ideologico — più che con un'estorsione "pulita". Ciò non implica una regia esterna né un nesso causale tra l'adozione del KYC e l'attacco: la selezione di bersagli ricchi di dati e ad alta visibilità è un effetto di opportunità (honeypot), non una prova di orchestrazione. — *Base: Reuters (16/09/2026); dichiarazione di Revolut; Hudson Rock / Duel.*

[Confidenza media sui dati IPO; movente indeterminato — ipotesi economica e reputazionale entrambe aperte] — *Base: Economy Magazine (18/09/2026); Financial Times (citato)*

Casi analoghi — violazioni emerse in prossimità di quotazioni, acquisizioni o vendite di quote. Non stabiliscono un nesso con il caso Revolut; documentano che, in prossimità di operazioni straordinarie, un incidente di sicurezza produce impatti finanziari e reputazionali misurabili e che i punti deboli ricorrenti sono la comunicazione tardiva e le anomalie interne.

Caso	Anno	Evento societario	Impatto documentato
Yahoo	2013–14 (rivelate 2016)	Acquisizione da Verizon	Prezzo tagliato di 350 mln (4,8 → 4,48 mld); multa SEC 35 mln per disclosure tardiva; class action 117,5 mln
Uber	2016 (occultata fino al 2017)	Investimento SoftBank / cambio vertice	Occultamento; CSO condannato nel 2022 per aver nascosto il breach
Equifax	2017	— (titolo quotato)	Tre dirigenti vendettero azioni prima della disclosure; indagini SEC/DOJ per insider trading
Coinbase	gen.–mag. 2025	Società quotata	~69.461 clienti; estorsione 20 mln rifiutata; costo stimato fino a 400 mln; cause per il calo del titolo
Robinhood	nov. 2021	Pochi mesi dopo l'IPO (lug. 2021)	~7 mln clienti; social engineering su un addetto al supporto; tentata estorsione
Deloitte	2017	Breach del revisore → IPO dei clienti	Studio peer-reviewed: un breach dell'auditor nei 90 giorni prima dell'IPO di un cliente si associa a −4,1% sul prezzo d'offerta (~8,9 mln $ di capitale mancato); effetto amplificato da copertura mediatica e gravità del breach
Kraken	2025 (causa 2026)	Preparazione IPO (obiettivo Q1 2026, poi rinviata)	Secondo l'atto di denuncia (allegazioni): dati di un cliente ad alta esposizione consegnati a richieste spoofate come autorità italiana, senza decreto; a seguire minacce,

			sorveglianza e tentato ingresso in abitazione della vittima
Revolut	2022	Prima dell'attuale percorso di quotazione	~50.000+ clienti; social engineering su un dipendente; esposti dati anagrafici e, in alcune ricostruzioni, copie di documenti e cronologie transazioni

[Confidenza alta sui fatti dei singoli casi; allegazioni per Kraken] — Base: Wikipedia/BankInfoSecurity (Yahoo); The Register (Uber); CNN/SEC (Equifax); CoinCentral (Coinbase); Huntress (Robinhood); The Accounting Review — studio peer-reviewed (Deloitte); atto Doe v. Payward, Bloomberg (07/03/2025), Fortune (25/09/2025) (Kraken); SecurityWeek/Infosecurity (Revolut 2022).

Fuori dalla stretta prossimità a un'operazione straordinaria, altri episodi recenti documentano l'impatto reputazionale e di mercato dei breach. TalkTalk (2015): alla comunicazione dell'attacco il titolo perse il 10,7% in una seduta, seguito da una sanzione record dell'autorità britannica di protezione dei dati. UBS e Pictet (2025): un attacco al fornitore Chain IQ espose circa 130.000 record del personale UBS, poi comparsi su un sito del dark web, senza compromettere i dati dei clienti — un caso di rischio di filiera. Bank of Baroda (2026): la compromissione delle credenziali e-mail di un dipendente portò all'esposizione di record di clienti, con un incidente confermato dall'istituto.

[Confidenza alta sui fatti dei singoli casi] *— Base: The Register/ICO (TalkTalk); Reuters/SWI swissinfo (UBS–Pictet); The Asian Banker/The Record (Bank of Baroda).*

Posizionamento competitivo e capitali internazionali

Revolut è ormai un attore sistemico nel retail bancario italiano: oltre 5 milioni di clienti (maggio 2026) e quinta banca del Paese per numero di clienti, con transazioni per oltre 50 miliardi di euro (+78% su base annua) e depositi in forte crescita. Con l'IBAN italiano è passata da strumento per viaggi e spese occasionali a conto principale per molti clienti ("IBAN effect"). Un incidente di sicurezza su un operatore di questa scala ha quindi un impatto diretto sulla fiducia nel sistema bancario e fintech in Italia. Kraken ha un profilo diverso — exchange crypto, non banca retail — ma, servendo clienti dell'Unione europea, ricade nel perimetro regolamentare MiCA, AML/CFT e GDPR: un incidente influisce sulla percezione del rischio crypto in UE e sulla fiducia degli investitori.

[Confidenza alta sui dati di mercato] — Base: Il Sole 24 Ore, MilanoFinanza, Teleborsa, Il Giornale d'Italia (Revolut Italia, maggio 2026); quadro regolamentare MiCA/AML/GDPR.

[IPOTESI, confidenza bassa] Sul piano geopolitico-economico, sia Revolut sia Kraken sono player a forte capitale internazionale — Revolut orientata a una quotazione anche a Wall Street oltre che a Londra, Kraken con radici statunitensi e percorso di quotazione negli Stati Uniti — che crescono sottraendo quote al sistema bancario nazionale sul retail e sugli investimenti, con un modello fondato su capitali internazionali più che su depositi e credito locali. In questa lettura, un incidente di sicurezza su operatori di questo tipo può essere interpretato anche come segnale di vulnerabilità del modello fintech in una fase di riassetto degli equilibri tra capitale internazionale e sistemi bancari nazionali. È una chiave di contesto, non un elemento probatorio: non emerge alcun nesso documentato tra il caso e interessi di questo tipo, e va tenuta separata dai fatti dell'incidente.

[IPOTESI, confidenza bassa] L'approdo a una quotazione statunitense allarga, più della sola adozione del KYC, il perimetro di compliance e di esposizione: un operatore quotato negli USA è più sensibile alle richieste OFAC e alle pressioni su quali asset listare o quali utenti geobloccare, e le policy dei player dominanti tendono a diventare standard di fatto globali — il che salda questa dimensione con l'architettura di sorveglianza descritta più avanti. È una prospettiva che tocca interessi diversi: i cypherpunk vi leggono una cooptazione delle crypto da parte della finanza tradizionale; gli attivisti per la privacy, un'espansione della sorveglianza finanziaria; i competitor non quotati e la DeFi, un vantaggio regolatorio per i grandi; parte dei regolatori e degli investitori istituzionali, un rischio sistemico e reputazionale. Restano però grievance e interessi — chi è infastidito da una quotazione — non attori del caso: nessuno di questi risulta collegato all'incidente, e la distinzione tra chi ha un interesse e chi ha agito resta ferma.

Cui prodest — gli interessi toccati

La domanda che un'analisi di questo tipo non può eludere è cui prodest: a chi giova, in questa fase, che la fiducia in Revolut si incrini. Non è una questione di prova — non emerge alcun elemento che colleghi l'incidente a un concorrente — ma di logica di mercato, e come tale va posta.

Revolut, con oltre 5 milioni di correntisti in Italia, Revolut si colloca tra le prime cinque realtà bancarie operanti nel paese per numero di clienti retail, avvicinandosi ai volumi tipici di un operatore sistemico e cresce erodendo allo stesso tempo quote di depositi al retail bancario tradizionale, flussi di pagamento e di cambio valuta, e risparmio investito, crypto compresa. **Ogni terreno su cui avanza è un terreno che qualcun altro presidia.** Un incidente che colpisce proprio la promessa su cui quella crescita si regge — un conto digitale sicuro e affidabile — non danneggia soltanto Revolut: rallenta la migrazione dei clienti più prudenti verso il modello fintech e, per sottrazione, avvantaggia chi da quella migrazione ha più da perdere. Le banche tradizionali, verso cui una parte della clientela più conservatrice può tornare; i neobank concorrenti, su cui possono spostarsi i nuovi flussi; e, sul fronte degli investimenti in cripto-attività, i veicoli percepiti come più istituzionali.

Quest'ultimo punto è il più concreto. Nel marzo 2025 BlackRock ha quotato in Europa un ETP fisico su Bitcoin (IB1T, commissione dello 0,15%), un prodotto regolamentato e negoziato in borsa che offre esposizione alla criptovaluta senza che l'investitore debba custodire un wallet o affidare a un'app retail i propri documenti e le proprie chiavi. Tra "comprare Bitcoin dentro Revolut" e "comprare un ETP quotato tramite la propria banca o il proprio broker", ogni episodio che rafforza la narrazione «sulle app retail i dati non sono al sicuro, meglio i veicoli regolamentati» sposta valore verso i secondi. Non serve immaginare una regia perché l'effetto si produca: è sufficiente la struttura del mercato.

Resta fermo il limite dell'analisi: il movente competitivo è strutturale, non dimostrato. Nessun elemento indica un attacco orchestrato da un concorrente, e questa lettura va tenuta separata dai fatti dell'incidente. Ma la mappa degli interessi che un caso come questo tocca è essa stessa parte del quadro, e per un'analisi ignorarla sarebbe una lacuna.

[**Confidenza: alta** sui fatti di mercato; la lettura "cui prodest" è un movente strutturale, non dimostrato] — *Base: Il Sole 24 Ore, MilanoFinanza (Revolut Italia); CoinDesk (risultati Revolut 2025); Bloomberg, CoinDesk (ETP Bitcoin BlackRock, 03/2025)*.

Per non confondere i piani, conviene distinguere chi ha agito, chi ne trae vantaggio e chi ne fa un tema pubblico:

Livello	Chi	Statuto
Perpetratore (chi ha agito)	Criminalità a movente economico — nel caso, IAmNotAVillain (estorsione)	Documentato · confidenza alta
Beneficiari strutturali (nessuna prova di coinvolgimento)	Banche tradizionali e asset manager (la fiducia che rientra dal fintech, i veicoli "regolamentati" tipo ETP); neobank concorrenti; sul piano geopolitico, Stati (repressione transnazionale)	Nessuna evidenza di coinvolgimento
Voci (chi usa il caso nel discorso)	Movimento cypherpunk / anti-KYC, NGO per i diritti digitali, comunità Monero.	Ideologico · non operativo — non sono autori

Beneficiario e voce non implicano autore: il legame è di metodo e di interesse, non di responsabilità. Il perpetratore documentato resta criminale-economico.

14. Pattern emersi e ricostruzione dell’operazione

Ricostruzione dell'operazione (ipotesi di analisi)

1. Accesso a una casella PEC istituzionale [Confidenza media-bassa]
Le richieste sono partite da una casella del dominio @pec.interno.it che la stampa riferisce all’ufficio Enti Locali della Prefettura di Reggio Calabria. Restano aperte due alternative: la compromissione della casella, ipotesi sostenuta dal gruppo e da Duel che parlano di credenziali sottratte tramite infostealer, oppure la clonazione dell’indirizzo. Secondo Il Sole 24 Ore (18/09) gli investigatori non hanno la certezza che sia stato compromesso un computer della Prefettura o del Viminale e stanno stabilendo se la casella sia stata “bucata” oppure clonata; la Polizia Postale non avrebbe finora riscontrato falle nei sistemi del Ministero. Una terza alternativa emerge da The CyberSec Guru (12/09, aggiornato il 15/09), secondo cui l’attacco avrebbe sfruttato un account di posta non autorizzato creato all’interno dell’infrastruttura dell’agenzia governativa; l’articolo la presenta come elemento confermato da Revolut, ma non ne cita il testo: va verificata sulla notifica o sulla dichiarazione ufficiale dell’azienda. *— Base: stampa (indagine della Procura di Reggio Calabria); dichiarazioni dell'attore e di Duel; pattern CERT-AGID sulle caselle PEC compromesse; Il Sole 24 Ore e ANSA (18/09).*

[IPOTESI, confidenza bassa] Abuso di privilegi amministrativi. L’attivazione o l’uso della casella sarebbe avvenuto tramite un’utenza dotata di privilegi sul dominio di posta, per compromissione dell’account amministrativo o per condotta di un soggetto interno. L’ipotesi è coerente con l’assenza di falle riscontrate nei sistemi, con la mancata pubblicazione e il mancato censimento dell’indirizzo e con la durata prolungata dell’operazione; non trova però riscontri nel materiale disponibile e non spiega, da sola, la rivendicazione di dati provenienti da più uffici delle forze dell’ordine. Elementi dirimenti: data di creazione della casella, richiesta di attivazione e primi accessi presso il gestore PEC. In alternativa, un infostealer che abbia colpito l’utenza amministrativa anziché quella d’ufficio produrrebbe lo stesso esito.

2. Più autorità dichiarate dallo stesso mittente [Confidenza media]
Dalla stessa casella risultano inviate, tra il 4 e il 5 maggio 2026, comunicazioni con riferimenti ad autorità diverse: un OEI a nome della Procura della Repubblica presso il Tribunale di Milano, una "Emergency Request for Data Disclosure" e una pratica con riferimento "RM-POLPOST". Oggetti e testi sono in inglese con calchi dall'italiano ("European Order of Investigation", "c. att.ne"). — Base: screenshot della casella PEC e del documento OEI diffusi pubblicamente; non verificati in modo indipendente.

3. Anomalie rilevabili alla ricezione [Confidenza media]
Il documento indica come Stato di esecuzione la Lituania e come destinatari la procura generale lituana e Revolut Bank UAB, ma è stato trasmesso direttamente alla PEC della succursale italiana di Revolut (revolut.italy.pec@legalmail.it). La trasmissione diretta alla banca, anziché all'autorità di esecuzione competente dello Stato indicato, appare incompatibile con il normale meccanismo di riconoscimento ed esecuzione dell'OEI (dir. 2014/41/UE, art. 9) e avrebbe dovuto richiedere verifiche supplementari. Ulteriori elementi da verificare alla ricezione: coerenza tra autorità emittente (procura) e dominio del mittente (Ministero dell'Interno), firma, uso del modulo standard (Allegato A). Da soli, questi elementi non dimostrano la falsità del documento, che è stata però confermata successivamente da Revolut.
— Base: documento OEI; screenshot PEC; direttiva 2014/41/UE.

4. Gestione come pratica ordinaria [Confidenza media]
Il 5 maggio la PEC italiana di Revolut risponde alla casella @pec.interno.it confermando che la documentazione è "regularly received" e in analisi, e si scusa per un "communication misalignment", avviando un audit interno. Secondo i documenti citati da Kozlovska, a luglio Revolut applica un filtro giurisdizionale (rifiuto per Revolut Ltd e per l'entità svizzera, 198 hash), ma per i conti presso Revolut Bank UAB esegue le richieste restituendo archivi cifrati con documenti, selfie e dati di conto.— Base: screenshot PEC; post di Kozlovska del 15 e 16/09 (che su questo punto non coincidono).

5. Ripetizione e monetizzazione [Confidenza media-bassa]
Le richieste, costruite su indirizzi di wallet e ID di transazione pubblici, sarebbero proseguite per sei mesi secondo l'attore e la stampa italiana, cinque secondo Kozlovska. Seguono l'estorsione (prima 10.000 BTC,

poi 6.000 XMR con countdown), la frattura tra IAmNotAVillain e Revolut Smilik, la pubblicazione in vendita di un "KYC kit" da parte di Duel e la comparsa di siti con il nome del gruppo.*— Base: canali Telegram; siti di estorsione; KELA; CoinDesk; pagina duel.com/merch; WHOIS.*

Pattern

[IPOTESI] 1. Il bersaglio è il canale di fiducia, non il sistema. Coinbase (addetti del supporto corrotti), Kraken 2025 e Revolut 2026 (false richieste delle autorità): in nessun caso risulta una violazione dei sistemi delle aziende. La compromissione riguarda l'anello esterno, cioè caselle istituzionali e personale di supporto, e l'attacco passa dalle procedure in cui l'azienda è tenuta a collaborare. Reperti: sezioni 0.2, 2, 3; conferme di Revolut e Kraken.

[IPOTESI] 2. Poca competenza, grande impatto. Credenziali di caselle istituzionali in circolazione; sito da modello o generato con IA, ospitato su hosting gratuito con cronologia accessibile (KELA); domini registrati in serie e bloccati in pochi giorni; lite pubblica tra gli attori. Per ottenere dati KYC di centinaia di clienti ad alto patrimonio basta l'accesso a una casella. Nota: secondo fonti investigative riferite da Il Sole 24 Ore (18/09) gli inquirenti considerano l'operazione “molto sofisticata”; questa valutazione diverge da quella che emerge dagli indicatori tecnici disponibili. Reperti: sezioni 1.3, 4, 4-bis; KELA; record WHOIS; codice del sito; Il Sole 24 Ore (18/09).

[IPOTESI] 3. L'attaccante impara dalle risposte dell'azienda. Kraken 2025: email, poi finto ordine irlandese quando Kraken richiede un tribunale. Revolut 2026: a marzo Revolut indica la società cipriota per le crypto; a maggio arriva un OEI intestato a Revolut Bank UAB; a luglio Revolut distingue per giurisdizione (Revolut Ltd, entità svizzera, Revolut Bank UAB). Ogni rifiuto formale indica come confezionare la richiesta successiva. Reperti: atto Kraken par. 106-108; PEC del 24/03, 04/05, 24/07.

[IPOTESI] 4. Dai dati pubblici all'identità, fino al rischio fisico. [Confidenza media sul metodo di selezione; bassa sul collegamento con aggressioni concrete] Secondo le fonti del caso, le richieste false usavano indirizzi di wallet e ID di transazione pubblici come chiavi di ricerca ("spray and pray"), ottenendo in risposta documenti, selfie e dati di conto. La combinazione tra dati blockchain osservabili e dati KYC esposti può quindi facilitare l'identificazione e la selezione di potenziali bersagli ad alto patrimonio. Il rischio è coerente con la crescita di estorsioni, rapimenti e "wrench attack" contro soggetti legati alle criptovalute (caso Kraken; minacce di rapimento riferite da Duel; ricatti personali a figure del settore riportati da GovInfoSecurity). Non è dimostrato, sulla base delle fonti disponibili, che i dati sottratti nel caso Revolut siano stati usati in un'aggressione fisica. Reperti: post di Korra; Kozlovska 16/09; Incrypted 16/09; elenco wallet-KYC; sezione 7.4; GovInfoSecurity.

[IPOTESI] 5. Dopo l'incidente, ognuno usa il caso. Attaccanti (estorsione, riscatto ridotto a 6.000 XMR con countdown, scissione Villain/Smilik); Duel (contatto con l'hacker e pubblicazione in vendita di un "KYC kit" con documento e selfie di una persona); siti con il nome del gruppo che si presentano come fonti indipendenti (.net, .info); fornitori di sicurezza (marketing); Kozlovska/ODF (riforma FATF, DAC8). I dati continuano a circolare dopo la chiusura dei canali. Reperti: sezioni 4-bis, 6.1, 6.1.1, 6.1.2, 7; pagina duel.com/merch; WHOIS .net/.info.

[IPOTESI] 6. Il canale delle richieste delle autorità non ha un responsabile. Il settore investe su frodi transazionali, onboarding e crypto (Nasdaq Verafin); **gli strumenti di verifica esistono ma sono volontari** (Kodex) o non ancora a regime (e-Evidence, applicabile dal 18/08/2026, per gli ordini ai fornitori; eEDES, tra autorità, con portale di riferimento in preparazione); il 19/09 la sottosegretaria all'Interno Wanda Ferro riferisce in risposta parlamentare di approfondimenti in corso delle strutture di sicurezza cibernetica del Ministero e di interlocuzioni dell'ACN con Revolut; secondo i documenti citati, Revolut applica controlli di giurisdizione, non di autenticità; il dibattito si divide tra responsabilità dell'azienda e responsabilità delle regole. Reperti: sezioni 0.3, 0.3.1, 3.4, 6.3.

Sintesi. Non emerge un attacco tecnico sofisticato ai sistemi di Revolut, ma lo sfruttamento di una procedura: una casella istituzionale reale, documenti verosimili, conoscenza della struttura societaria del gruppo (in parte ricavata dalle risposte formali della stessa Revolut) e solleciti per creare urgenza. I punti di controllo mancati riguardano la coerenza tra autorità dichiarata e mittente, il circuito di trasmissione dell'OEI e la conferma dell'autorità emittente attraverso un canale indipendente.

14.2 Un pattern più ampio: l'abuso dei canali fidati

Il vettore dei casi Revolut e Kraken — una richiesta presentata come proveniente da un'autorità — è un caso particolare di un pattern più ampio: l'abuso di un canale certificato o fidato per arrivare a informazioni sensibili su bersagli di valore. Un terzo caso, di natura diversa, lo illustra. Nel 2024–2025 in Italia lo spyware Graphite di Paragon Solutions — prodotto venduto a governi e agenzie di intelligence — è stato usato per colpire, tramite WhatsApp, decine di persone: giornalisti, attivisti e, secondo quanto riportato da più testate nell'ottobre 2025, il finanziere Francesco Gaetano Caltagirone, grande azionista di un istituto bancario sistemico.

Caso	Canale fidato	Meccanismo	Obiettivo e contesto
Paragon (2024–2025)	WhatsApp, usato per comunicazioni private e professionali	Sfruttare la fiducia nel canale (chat con contatti noti) per veicolare spyware zero-click	Sorvegliare bersagli sensibili: giornalisti, attivisti e un grande azionista bancario; posta in gioco su asset finanziari strategici
Kraken (2025)	E-mail che appare istituzionale (law enforcement), con logo e linguaggio d'autorità	Convincere il team compliance che la richiesta è legittima e ottenere i dati di un cliente "whale"	Informazioni finanziarie sensibili, poi usate per estorsione e sorveglianza; contesto crypto, grandi patrimoni, regolazione UE
Revolut (2026)	PEC certificata su un dominio statale reale	Usare un canale formalmente perfetto (autenticazione allineata) per richiedere dati KYC e crypto dei clienti	Dati di "crypto whale", poi richiesta di riscatto e minaccia di leak; contesto fintech pre-IPO, fiducia del mercato

[Confidenza: alta sull'esistenza dei casi; il "filo" è un pattern di metodo, non un attore né una campagna comune] — Base: Sky TG24, MilanoFinanza, L'Espresso, TechCrunch, Citizen Lab, Amnesty International (caso Paragon); sezioni precedenti (Kraken, Revolut).

Il filo comune non è un attore né una campagna, ma un metodo: sfruttare la fiducia riposta in un canale — WhatsApp, e-mail istituzionale, PEC — per acquisire informazioni su target rilevanti (attivisti, azionisti bancari, clienti crypto ad alto patrimonio), in contesti in cui il controllo dell'informazione ha valore strategico. Va tenuta ferma una differenza sostanziale: Paragon è uno strumento di sorveglianza venduto a Stati e agenzie, con una cornice di autorizzazione, mentre i casi Kraken e Revolut sono frode criminale per impersonificazione. **Ciò che li accomuna è solo la leva** — la fiducia nel canale — non l'attore, la legalità o il movente.

È però questa leva a definire il rischio. Che un grande azionista bancario sia sorvegliato mentre si gioca una partita sul controllo di un istituto sistemico, e che nello stesso periodo exchange e fintech crypto vengano indotti a consegnare dati di clienti ad alto patrimonio, disegna un quadro coerente. Per un istituto che risponde a richieste delle autorità la lezione è netta: l'autenticità del canale non è mai, da sola, prova della legittimità di chi lo usa.

15. «27 wallet d’identità»: la lettura in epigrafe

La citazione posta in apertura del fascicolo — «27 wallet d’identità = 27 superfici d’attacco» — legge i 27 Stati membri dell’UE come altrettanti «wallet d’identità»: ciascuno con la propria infrastruttura di identità digitale (in Italia SPID e PEC; a livello europeo eIDAS 2.0 e i wallet nazionali), le proprie autorità (ministeri, prefetture, unità AML) e i propri canali «fidati» (PEC, caselle istituzionali, portali di mutua assistenza). Ogni Stato è un nodo di fiducia nell’architettura europea; e ogni nodo è, allo stesso tempo, una superficie di attacco potenziale.

Il caso Revolut illustra la tesi: è bastato compromettere una singola casella PEC riconducibile a una prefettura italiana per ingannare una piattaforma globale, ottenere dati KYC di clienti di più paesi e avviare un’estorsione. Non è il difetto di un singolo sistema, ma una conseguenza strutturale di un’architettura che poggia su identità nazionali certificate, cooperazione interstatale «fidata» e piattaforme KYC tenute a riconoscere tutti questi canali. La sicurezza complessiva non è data dal livello medio dei 27 sistemi, ma dal livello dell’anello più debole che le piattaforme riconoscono come legittimo.

Su questa base l’autore della citazione parla di «sovranità operativa»: ciò che pesa non è dichiarare 27 identità digitali europee, ma chi, in concreto, sa inviare una richiesta da un canale istituzionale e farla riconoscere come ufficiale — per proteggere i propri cittadini o per colpire un avversario. È lo stesso meccanismo descritto in §13.2: un attore statale non ha bisogno di «attaccare l’Europa» se può compromettere una casella, o ottenere che un’autorità terza inoltri una richiesta apparentemente legittima contro un obiettivo (cfr. l’approfondimento sulla repressione transnazionale).

[**Confidenza:** la lettura «più wallet, più superfici» e la nozione di «sovranità operativa» sono l’interpretazione dell’autore della citazione, non un fatto accertato; i fatti del caso Revolut sono trattati nelle sezioni relative.]

16. Perché l'Italia

Resta una domanda: **perché l'Italia**. Non per una debolezza generica, ma per una combinazione specifica di fattori. Il primo è tecnico. La PEC è un sistema quasi unico al mondo: dà valore legale di notifica a un messaggio e certifica mittente e consegna, ma non chi sta effettivamente usando la casella in quel momento. Una casella compromessa consente perciò di inviare richieste formalmente perfette, con autenticazione allineata. La superficie è ampia — centinaia di migliaia di caselle pubbliche e private — e poco conosciuta all'estero, dove i team di verifica non hanno gli strumenti per distinguere una PEC autentica da una abusata. CERT-AGID ha gestito oltre 650 eventi di phishing e spam via PEC nel solo 2026, con più abusi nei primi cinque mesi dell'anno che in tutto il 2025.

Il secondo fattore è strategico. L'Italia è uno dei maggiori mercati bancari europei ed è un laboratorio della regolazione finanziaria dell'Unione: dall'euro digitale — la cui fase preparatoria in BCE si è conclusa, con orizzonte di lancio verso il 2029 — al quadro sui cripto-asset. Ottenere informazioni su grandi azionisti bancari, su operatori fintech e crypto attivi in Italia e sui flussi di capitale significa avere visibilità su strategie di aggregazione bancaria e sull'orientamento regolatorio italiano in sede europea.

Il terzo fattore è di contesto interno: sono aperte partite ad alta tensione sul controllo di asset bancari strategici, in cui figure che sono al tempo stesso grandi azionisti ed editori rendono la sorveglianza digitale uno strumento per leggere mosse e alleanze ed esercitare pressione. Il quarto è di percezione: operare "dall'Italia", con PEC e domini istituzionali reali, permette di mimetizzarsi nel traffico istituzionale autentico, di sfruttare la frammentazione amministrativa per rendere più difficile l'attribuzione, e di contare sul fatto che un incidente "made in Italy" venga derubricato a problema locale quando invece tocca la fiducia nel banking digitale europeo e il dibattito regolatorio dell'Unione.

[IPOTESI, confidenza bassa] Messi in fila, questi elementi suggeriscono una lettura: l'Italia non come vittima casuale, ma come piattaforma di accesso a informazioni finanziarie e patrimoniali strategiche, dove un canale certificato tecnicamente sfruttabile, un ruolo di primo piano nella regolazione finanziaria europea, partite interne ad alta posta e una percezione internazionale che sottovaluta il rischio italiano si combinano. **È una chiave di lettura, non una prova: nessun elemento collega i casi a una regia unica, e i tre episodi restano distinti per attore, natura e legalità.**

[Confidenza: alta sui fatti (PEC/CERT-AGID, mercato bancario, euro digitale); la lettura d'insieme è interpretativa, **confidenza bassa**] *— Base: CERT-AGID (oltre 650 eventi PEC nel 2026); BCE (euro digitale, orizzonte 2029); sezioni precedenti.*

L'informazione finanziaria e patrimoniale è un asset strategico, e i canali fidati (WhatsApp, PEC, email istituzionali) sono i vettori privilegiati per acquisirla, legalmente o meno.

Fonti principali

- Reuters, 12/09/2026 — conferma di Revolut
- Atto Doe v. Payward Ventures (Kraken), CGC-26-634771 — https://kr-internet-law.sfo3.digitaloceanspaces.com/uploads/Complaint-Doe-v.-Payward-Ventures-Inc-DBA-Kraken-FILED-03.06.26.pdf
- Kraken Security Update (Nick Percoco, CSO Payward/Kraken), X, 13/04/2026 — https://x.com/c7five/status/2043720915330969743; CoinDesk e Unchained, 13/04/2026 (estorsione via abuso di accessi interni)
- The Register, 14/09/2026 — https://www.theregister.com/cyber-crime/2026/09/14/revolut-falls-for-fake-government-requests-hands-over-customer-data/5296118
- StrettoWeb, 15/09/2026 — https://www.strettoweb.com/2026/09/reggio-calabria-hacker-usano-una-pec-della-prefettura-per-rubare-dati-ai-clienti-revolut-indaga-la-polizia-postale/2142679/
- Silere non possum, 15/09/2026 — https://silerenonpossum.com/it/casella-viminale-caso-revolut-ministero-silenzio/
- KELA — https://www.kelacyber.com/blog/revolut-data-breach/
- City AM — https://www.cityam.com/revolut-facing-ransom-request-after-hackers-obtain-customers-data/
- Krebs on Security, FBI e EDR false (11/2024) — https://krebsonsecurity.com/2024/11/fbi-spike-in-hacked-police-emails-fake-subpoenas/
- AML Intelligence, 15/09/2026 — https://www.amlintelligence.com/2026/09/analysis-revolut-breach-puts-renewed-scrutiny-on-fake-law-enforcement-data-requests/
- CERT-AGID, PEC compromesse — https://cert-agid.gov.it/tag/pec/
- HKCERT, caso Twitter 2020 — https://www.hkcert.org/blog/case-study-on-bitcoin-scam-incident-a-combined-social-engineering-and-privilege-escalation-attacks
- Security4Web3, 09/06/2026 — https://security4web3.com/blogposts/post33-social-engineering-attacks-crypto
- The Hacker News, Coinbase — https://thehackernews.com/2025/05/coinbase-agents-bribed-data-of-1-users.html
- Yahoo Finance, furto da 282 milioni — https://sg.finance.yahoo.com/news/hacker-steals-282-million-crypto-185613887.html
- Nasdaq IR, comunicati Verafin — https://ir.nasdaq.com/news-and-events/press-releases
- OSCE PA, Dichiarazione dell'Aia 2026 — https://www.oscepa.org/en/documents/annual-sessions/2026-the-hague/declaration-32/5581-the-hague-declaration-eng/file
- franceinfo, PNACO 11/09/2026 — https://www.franceinfo.fr/economie/bitcoin/cryptomonnaies-plus-de-70-enlevements-et-sequestrations-recenses-sur-les-huit-premiers-mois-de-2026-d-apres-le-parquet-national-anticriminalite-organisee_8188352.html
- Potomac Law, e-Evidence — https://www.potomaclaw.com/news-EU-e-Evidence-Rules-Become-Operational-on-August-18-2026-US-Companies-with-European-Operations-Should-Prepare-Now
- Fascicolo di raccolta "27 wallet d'identità = 27 superfici d'attacco" (uso interno), con tutte le fonti, gli screenshot e le versioni discordanti
- Duel/Korra (X), post di Kozlovska
- Matrice Digitale, Agenda Digitale e circolare del Ministero della Giustizia (per la nota PEC)
- Kodex, CoinDesk, Cointelegraph, Chainalysis, Butler Brief
- whoxy/NameSilo,
- Commissione europea / EUR-Lex.
- Cybernews, 27/07/2026 — annuncio di vendita di 75 milioni di record Revolut
- The CyberSec Guru, 12/09/2026 (agg. 15/09) — categorie di dati e formulazione della notifica
- IndicePA — domicilio digitale della Prefettura di Reggio Calabria (dal 12/04/2019)

- Elenchi PEC delle Prefetture, versioni archiviate (Internet Archive, 22/12/2025)
- DDay / Il Sole 24 Ore, 18–19/09/2026 — accertamenti Polizia Postale e Cnaipic sui 147 GB — https://www.ilsole24ore.com/art/revolut-primi-accertamenti-non-confermano-furto-147-gigabyte-dati-viminale-AJcNmXGB

Hudson Rock, 15/09/2026 — infostealer e credenziali pec.interno.it compromesse — https://www.hudsonrock.com/blog/revolut-hackers-used-infostealers-for-elaborate-social-engineering

- Corriere della Calabria, 18/09/2026 — risposta della sottosegretaria Wanda Ferro (ACN, Polizia Postale, DNAA)
- Economy Magazine, 18/09/2026 — quotazione e valutazione Revolut (cita Financial Times)