

Caso Revolut: dall'estorsione aziendale alla monetizzazione individuale



© Imagoeconomica

Il data breach Revolut, come già evidenziato in una precedente analisi, non nasce da una falla tecnologica, ma da un **varco di fiducia istituzionale**, sfruttato con pazienza per settimane, forse mesi, attraverso una casella PEC riconducibile alla Prefettura di Reggio Calabria. In quella sede si indicava come l'**asimmetria strutturale** tra i controlli imposti agli utenti finali e quelli, ben più deboli, applicati alle richieste istituzionali tra enti pubblici e operatori finanziari fosse destinata a restare il vero **nodo irrisolto del settore fintech**, indipendentemente dall'esito della vicenda giudiziaria in corso.

I fatti delle ultime ore confermano questa lettura, aggiungendo un tassello che merita un'analisi a sé: gli hacker, dopo aver richiesto un riscatto sceso da **10.000 Bitcoin** a **6.000 Monero** senza ottenere risposta da Revolut,

hanno iniziato a vendere i dati sottratti sul **dark web** e a contattare direttamente le vittime, offrendo la cancellazione dei loro dati in cambio di un pagamento personale. Le vittime italiane accertate sono salite da 8 ad almeno 15, secondo le dichiarazioni degli stessi autori dell'attacco. Tra il materiale diffuso come prova di autenticità: cronologie di transazioni che in alcuni casi superano le 700 pagine, fotografie dei clienti, copie dei documenti d'identità.

Un nuovo paradigma per l'analisi di rischio

Chi si occupa di **digital forensics** conosce bene questa dinamica, anche se raramente la vede confermata con questa nitidezza cronologica. Quando un'organizzazione strutturata rifiuta di negoziare, il criminale non abbandona l'obiettivo: liquida l'asset nel modo più rapido possibile. Il dato rubato, se non genera un riscatto aziendale, viene **frazionato e rivenduto**, oppure usato per tentativi di estorsione su scala individuale, dove la soglia di resistenza della vittima è strutturalmente più bassa.

Non è un dettaglio tecnico, è un **cambio di paradigma nell'analisi del rischio**. Un'azienda ha risorse legali, comunicazione di crisi, assicurazioni cyber, spesso anche un protocollo di risposta agli incidenti. Un singolo cliente, ricevuta una mail con il proprio documento d'identità allegato come prova, non ha quasi mai nessuno di questi strumenti. Ha soltanto la sensazione, fondata, che qualcuno stia commerciando un pezzo della propria identità.

Questo significa che il danno reputazionale generato da un data breach non si esaurisce nella fase acuta della trattativa con gli attaccanti, quella che i media coprono con maggiore intensità. Si trasferisce e si moltiplica nella fase successiva, meno visibile ma più duratura, in cui ogni cliente esposto diventa un fronte separato: una possibile richiesta di

risarcimento, un caso segnalato al Garante, un rapporto di fiducia interrotto in modo irreversibile con il proprio istituto finanziario.

La reazione del regolatore

Un secondo elemento merita attenzione professionale. Il Garante per la protezione dei dati personali ha aperto una verifica che non riguarda soltanto Revolut, ma si estende ai controlli di sicurezza sugli accessi di tutte le banche operanti in Italia. È la conferma istituzionale di quanto sostenevo nella mia prima analisi: **non siamo di fronte a una vulnerabilità isolata di un singolo operatore**, ma a un problema sistemico nel modo in cui il settore finanziario verifica l'autenticità delle richieste provenienti da canali istituzionali.

Fino a quando la verifica dell'autenticità di una richiesta dati resterà affidata alla plausibilità apparente di un dominio email, anche legittimo come pec.interno.it, e non a un protocollo di riscontro strutturato e out-of-band, ogni operatore che gestisce migliaia di richieste istituzionali a settimana sotto scadenze stringenti resterà esposto allo stesso identico schema d'attacco.

Perché il penetration test da solo non basta più

C'è un equivoco che il caso Revolut smonta in modo definitivo, e che vale la pena affrontare con chiarezza tecnica. Anche le infrastrutture che oggi adottano i modelli Zero Trust più maturi, quelli costruiti sul principio "non fidarsi mai, verificare sempre", con micro-segmentazione, accessi a privilegio minimo e MFA resistente al phishing, restano esposte a un tipo di rischio che nessun penetration test è progettato per intercettare.

Il **pentest**, per costruzione, verifica la resistenza di un

perimetro noto: prova a violare sistemi, applicazioni, reti, simulando un attaccante che deve prima entrare. È uno strumento indispensabile, ma fotografa un solo istante della postura di sicurezza interna, e presuppone che il varco debba ancora aprirsi. Nel caso Revolut, il varco non era nei sistemi dell'azienda: era nella fiducia accordata a un interlocutore terzo, apparentemente legittimo, che nessun test di intrusione avrebbe potuto simulare, perché non stava attaccando l'infrastruttura, ne stava semplicemente usando le procedure di risposta previste per le richieste istituzionali.

È qui che una **cyber risk investigation** svolge una funzione che il pentest non può coprire, perché guarda nella direzione opposta. Non chiede "quanto è resistente il mio perimetro a un attacco simulato", ma "cosa è già uscito, attraverso quale canale, ed è oggi in circolazione su mercati e forum del dark web". Sono due domande complementari, non sovrapponibili: la prima valuta la solidità delle difese, la seconda valuta il danno già avvenuto, indipendentemente da quanto le difese fossero solide. Un'**architettura Zero Trust impeccabile** non impedisce che un ente terzo, fuori dal proprio perimetro di controllo, venga compromesso e usato come vettore di fiducia. Lo dimostra, con la forza dei fatti, esattamente il caso che stiamo analizzando.

Le organizzazioni più mature, quelle che hanno davvero interiorizzato la logica Zero Trust, lo hanno capito da tempo: il monitoraggio continuo dell'esposizione sul dark web non è un'alternativa al penetration test, è il suo complemento necessario. Uno protegge ciò che si controlla, l'altro rivela ciò che sfugge al controllo diretto ma che riguarda comunque l'azienda, i suoi dipendenti, i suoi clienti.

Cosa significa per chi gestisce dati sensibili, oggi

La lezione operativa che emerge da questa seconda fase della

vicenda Revolut è tanto semplice quanto spesso disattesa: la domanda corretta da porsi non è se la propria organizzazione subirà un attacco di questo tipo, ma se sia già in grado di rilevare se dati propri, dei propri dipendenti o dei propri clienti, sottratti attraverso un fornitore o un ente terzo compromesso, siano già in circolazione.

È esattamente il tipo di verifica che una cyber risk investigation è progettata per fornire: non una previsione, ma una **fotografia accurata di ciò che esiste già**, in questo momento, sui canali dove i dati rubati vengono scambiati e venduti. Nel caso Revolut, nessuna delle vittime avrebbe potuto prevenire l'attacco con i propri strumenti individuali. Ma un'organizzazione che monitora sistematicamente la propria esposizione avrebbe potuto scoprire l'anomalia settimane prima che diventasse un caso mediatico internazionale, esattamente come indicavo nella mia prima analisi a proposito del fattore tempo come indicatore forense più eloquente di qualsiasi altro segnale tecnico .

La fiducia, una volta tradita su scala istituzionale, non si ripara con un comunicato stampa. Si ricostruisce dimostrando, con evidenze verificabili, di aver saputo vedere per primi ciò che gli attaccanti già sapevano da tempo.