CYBER CRIMINE FINANZIARIO
Reati informatici finalizzati alla realizzazione di ingenti guadagni

	2022	2023
Casi	9.229	10.606
Persone indagate (● = 100)	859	917
Somme sottratte *In mln euro*	38,5	40,2

ATTACCHI RANSOMWARE PER TIPOLOGIA DI ATTIVITÀ
Dati in percentuale

TOTALE 100%

Fonte: elaborazione del Sole 24 Ore su dati della Polizia Postale e delle Comunicazioni

Cyber crimine finanziario +15% Imprese a rischio ricatti multipli

Furto dati. Nel 2023 colpite 65 aziende, danno da 19 milioni. Sul mercato anche operatori che svolgono attività di mediazione: versare riscatti non è reato, ma si finisce nelle black list hacker delle società disposte a pagare

Pagina a cura di
Margherita Ceci
Ivan Cimmarusti

«Non avete alcuna possibilità con 500mila dollari o cifre del genere, e non provate a bluffare. Se pagate a breve, accettiamo 6,75 milioni. Se no, iniziamo a pubblicare i dati». «Non stiamo bluffando e voi non conoscete la situazione finanziaria del mio cliente». Non è la sceneggiatura di un thriller, ma uno scambio di battute reale tra un collettivo hacker e un cyber negoziatore che opera per conto di un'azienda vittima di *ransomware*, cioè la tecnica di esfiltrazione dati e informazioni a scopo estorsivo. La nuova figura si sta sviluppando alle spalle di un sistema illecito a sua volta in forte espansione.

Rischi e buco normativo

In verità si tratta di un profilo abbastanza *borderline*, come confermano al Sole 24 Ore fonti inquirenti e investigative. La stessa agenzia delle Entrate, con una risposta a interpello (149/2023), ha detto che il pagamento di un riscatto per riottenere dati trafugati, se pure non costituisca reato, non è comunque deducibile.

Ci si muove, dunque, in un cono d'ombra, o buco normativo, che però rischia di incoraggiare il cyber crime. «Un'impresa che paga una volta – spiega infatti una fonte istituzionale – finirà per essere attaccata più volte perché sarà inserita da parte degli hacker nelle *black list* dei pagatori». In poche parole, aggiunge, «le vittime si devono rivolgere alle autorità competenti» per evitare di ricevere multipli attacchi e, dunque, ricatti.

Secondo Enrico Corradini, legal di Yarix, divisione Digital Security di Var Group, per il quale svolge da sei anni l'attività di cyber negoziatore, «non c'è una normativa che vieta il pagamento di un riscatto cyber. Il Garante della privacy in più occasioni ha ribadito che c'è un buco normativo, non è un reato». Corradini aggiunge che «il 46% di chi sceglie di non pagare, almeno in Italia, è rappresentato da aziende che non pagano per principio, nonostante (con l'incursione hacker, *ndr*) abbiano perso tutto. Ci sono invece società che non badano alla questione di principio per tutelare l'azienda e i dipendenti».

Il cyber negoziatore

I negoziatori in ambito cyber sono figure poco note nel panorama italiano. Si tratta di legali con esperienze nella gestione di conflitti, informatica e diritto internazionale. Il loro obiettivo è abbassare il prezzo della richiesta degli hacker, «generalmente dal 40 al 90% rispetto alla cifra iniziale», spiega Corradini. «Se si tratta di segreti industriali, o di una mole importante di dati personali, il danno reputazionale e le eventuali richieste risarcitorie degli interessati possono davvero mettere in difficoltà l'azienda. È una doppia estorsione: in questo modo, anche quando le aziende hanno dei *backup offline*, e possono quindi ripartire bonificando il sistema e ripristinando i salvataggi, rimane la spada di Damocle della pubblicazione». La mediazione sul prezzo dipende dalla trattativa. I toni sono accomodanti, il linguaggio è colloquiale (frequenti sono gli «*hey guys*» nella trascrizione della negoziazione di cui siamo in possesso). Non c'è un copione da seguire, «si crea una narrazione sulla base dei dati finanziari dell'azienda, di quanto è disposta a pagare, ma anche del contesto socio-economico – dice Corradini –. Nel caso di un attacco a un grande operatore di viaggi avvenuto durante il Covid, ad esempio, la narrazione verteva sulla sproporzione della richiesta (5-10 milioni di euro), in un momento in cui non si poteva viaggiare». In generale, aggiunge, a fronte del pagamento di un riscatto per «2 milioni di euro, la richiesta iniziale può essere di 7,5 milioni o 10 milioni».

Lo scenario criminale

In generale, i crimini finanziari online sono in costante crescita. Secondo i dati del servizio di Polizia postale questi illeciti sono aumentati del 15%, così come il valore, passato da 38,5 milioni a 40 milioni nel 2023. Nell'ultimo anno sono stati violati i sistemi informatici di 65 tra piccole, medie e grandi imprese italiane, con un danno calcolato di 19 milioni di euro.

Nelle più recenti relazioni dei servizi si legge che circa il 47% dei complessivi attacchi hacker ha matrice criminale mentre altri hanno diverse motivazioni. Il 56% delle vittime sono privati, mentre il 53% delle operazioni ha l'obiettivo di «esfiltrare» identità/credenziali soprattutto di imprese. Stando alle passate rielaborazioni della Polizia postale, inoltre, le aziende che hanno ricevuto il maggior numero di incursioni sono l'industria e il manufatturiero, le Pmi, le società di servizi e studi professionali, ma anche il comparto della sanità, dei trasporti, dell'editoria e del bancario.

> **La strategia è quella di investire di più in cybersecurity per minimizzare rischi e costi di ripristino**

Infrastrutture anti-hacker

Al di là della figura *borderline* del cyber negoziatore, la Polizia postale da tempo sostiene il mondo dell'impresa italiana in ambito di tutela delle infrastrutture anti-hacker. Secondo i vademecum, infatti, le aziende dovrebbero sempre adempiere agli obblighi di cybersecurity previsti dalle normative e adottare tutte le precauzioni che permettono in caso di attacco il risanamento dei sistemi. Tuttavia, sul lato pratico questo spesso non succede. «La stragrande maggioranza delle Pmi non segue le *best practice* europee – spiega Alvise Biffi, ceo di Secure Network –, tant'è che l'80-85% di chi ha avuto questi problemi non era adeguatamente preparato ad affrontarli. Eppure, con un investimento molto basso, parliamo di 1.500 euro per le piccole aziende, si potrebbe già avere un *cyber risk rating*, una fotografia dello stato di salute della propria cybersecurity».