

# Il furto in Rete di 773 milioni di mail

19 Gennaio 2019

Scoperto il più grande attacco hacker della storia. Nell'archivio illegale anche 21 milioni di password

Federico Cella

È come un enorme elenco del telefono, dove però si trovano email e password rubate. È la scoperta delle ultime ore, una «collezione» — chiamata appunto Collection #1, nome che lascia supporre l'esistenza di altre — di dati sensibili, chiavi d'accesso a siti di ecommerce, social network e altri servizi, messa in bella mostra sulla Rete.

Secondo il ricercatore australiano che ha scoperto questo archivio per criminali, Troy Hunt, è «la più grande violazione di dati della storia». L'esperto di cybersicurezza l'ha trovato sul sito di file sharing Mega, creato dall'ex pirata Kim Dotcom, con appunto il nome di Collection #1: una cartella dal peso di 87 gigabyte piena di dati sottratti negli anni, in vari attacchi informatici. Ciò che impressiona è la mole di queste identità digitali esposte: 773 milioni di email (772.904.991 per la precisione) e più di 21 milioni (21.222.975) di password.

Un tesoro per i malintenzionati, anche se la maggior parte di queste utenze risultano trafugate da tempo, e dunque forse non più valide. Ma secondo Hunt, 140 milioni di queste email sono «nuove», cioè mai apparse sui forum utilizzati dai cybercriminali dove ancora si trovano (da Mega i file sono stati fatti sparire). Sono indirizzi che fanno riferimento a privati, aziende e istituzioni. «Sembra una collezione casuale, fatta per massimizzare il numero di credenziali accessibili agli hacker. Non c'è uno schema, solo la ricerca di massima esposizione», ha spiegato Hunt a Wired. L'esperto di sicurezza informatica, proprio per l'enormità dei dati esposti, invita a controllare la «purezza» della propria email sul sito di servizio che gestisce il suo team chiamato «Have I been pwned?» che letteralmente significa: «Sono stato bucato?». Se fate questa operazione, è molto probabile che una o più delle email che utilizzate per creare account online risultino compromesse. In questo caso non bisogna avere paura: il consiglio è di cambiare immediatamente le password e di sceglierne di nuove con cura — sul sito del Corriere vi proponiamo una guida per farlo al meglio —, magari abbinandole a cosiddetti sistemi di doppia autenticazione (come la richiesta di confermare la propria identità con la ricezione di un sms).

«L'Italia è interessata a questa fuga di dati al pari di molti altri Paesi», ha spiegato Ivano Gabrielli, responsabile del Cnaipic, il Centro nazionale anticrimine informatico. «Stiamo allertando una serie di obiettivi potenzialmente a rischio, a partire da infrastrutture critiche e profili istituzionali». Per i cittadini privati il consiglio è prestare ancora più attenzione alle email che si riceveranno nelle prossime settimane: questa esposizione di dati può dare il via ad attacchi di phishing volti a rubare credenziali e numeri di carte di credito. Messaggi

«strani», inusuali o con richieste sospette vanno cestinati e per nessuna ragione vanno cliccati i link proposti.

Fonte: