

## La madre di tutte le fughe di dati: da Google a Meta, compromesse 16 miliardi di credenziali

Le **fughe di dati** si verificano ormai con una regolarità preoccupante. Invece di intervenire con decisione per arginare il problema, le grandi aziende tecnologiche hanno promosso la normalizzazione del fenomeno, consolidando l'idea che queste falle siano un inevitabile sottoprodotto del progresso digitale. Negli ultimi giorni, tuttavia, questo velo di assuefazione si è squarciato con la scoperta di un gigantesco archivio contenente circa **16 miliardi di credenziali rubate**, tra password e informazioni di login. Un bottino che gli esperti non esitano a definire "la madre di tutte le violazioni informatiche".

Il *database* è stato individuato grazie al lavoro della redazione di [Cybernews](#), la quale ha iniziato a darne notizia il 18 giugno, aumentando la copertura giornalistica man mano che emergeva la reale portata della minaccia. Il materiale rinvenuto è vastissimo: si parla di una **trentina di fonti differenti** aggregate in un'unica raccolta, in cui ogni singolo file contiene da decine di milioni fino a 3,5 miliardi di righe di dati. Secondo la testata, fatta eccezione per un database già segnalato il mese scorso da [Wired](#), tutti gli archivi risultavano inediti anche per gli analisti che operano nel settore della cybersicurezza.

Le credenziali compromesse coprono praticamente ogni tipologia di servizio digitale. Tra i nomi più noti compaiono **Google, Meta e Apple**, tuttavia la mole dell'archivio è tale da far ritenere probabile il coinvolgimento di piattaforme come GitHub, Telegram e diversi portali governativi. I ricercatori descrivono l'archivio come un "**progetto di sfruttamento di massa**", in grado di garantire ai cybercriminali "un accesso senza precedenti alle credenziali personali, utilizzabili per l'acquisizione di account, il furto di identità e campagne di phishing altamente mirate".

Il danno alla sicurezza informatica è quindi trasversale e sistemico, ma non riconducibile a un singolo attacco. L'origine della raccolta è attribuita piuttosto alla proliferazione di **malware del tipo infostealer**, programmi malevoli progettati per trafugare dati sensibili dai dispositivi degli utenti. In questo senso, alcuni esperti ipotizzano che il gigantesco archivio sia una sedimentazione di informazioni trafugate negli ultimi anni, suggerendo quindi una minaccia meno pressante di quella ventilata invece dai toni dello scoop. *Cybernews* non è d'accordo e sostiene che molti dei dati sarebbero "nuovi", non riciclati da precedenti fughe, il che rappresenterebbe un'insidia decisamente urgente.

Verificare origine e dettagli di questo grande archivio è peraltro un compito estremamente difficile. I reporter lo hanno notato solamente grazie al fatto che i cybercriminali hanno configurato male i propri servizi di hosting, lasciando che i file fossero disponibili in chiaro online. Si è trattato di un errore di breve durata e che **non ha permesso analisi approfondite**, né tantomeno ha offerto la possibilità di capire se questo nuovo allarme rappresenti un pericolo reale o se sia un problema ormai secolarizzato. Nel dubbio, vale

La madre di tutte le fughe di dati: da Google a Meta, compromesse  
16 miliardi di credenziali

comunque la pena aggiornare le proprie password e, ove possibile, passare a sistemi di verifica più complessi, quali l'autenticazione a due fattori.



## Walter Ferri

Giornalista milanese, per *L'Indipendente* si occupa della stesura di articoli di analisi nel campo della tecnologia, dei diritti informatici, della privacy e dei nuovi media, indagando le implicazioni sociali ed etiche delle nuove tecnologie. È coautore e curatore del libro *Sopravvivere nell'era dell'Intelligenza Artificiale*.