ANSAit Tlc

Nel deep web archivio con 450 mln mail e password rubate

Polizia postale indaga, sembra materiale frutto vecchi attacchi

Nel deep web archivio con 450 mln mail e password rubate © ANSA/AP

CLICCA PER INGRANDIRE +

ROMA - Si chiama Anti Public e sarebbe un "gigantesco archivio di mail e password rubate e riconducibili ad aziende, istituzioni pubbliche, forze armate e di polizia, università e infrastrutture critiche in tutto il mondo", Italia compresa: è il 'data leak' da 17 gigabyte individuato dagli esperti informatici di D3Lab e di Yarix, la cyber division di Var Group Spa, holding italiana specializzata nell'Information and communication technology. La Polizia postale indaga, anche se da un primo esame sembrerebbe materiale oggetto di vecchi attacchi informatici, già noti.

L'archivio, si legge in una nota di Var Group, è diffuso in dieci file .txt e coinvolge 13 milioni di domini mail; oltre 450 milioni (457.962.538) email complete di relative password; centinaia di migliaia di aziende, organizzazioni, istituzioni, infrastrutture critiche e milioni di utenti singoli, in tutto il mondo. Il data leak, secondo Yarix, "è stato probabilmente creato a dicembre 2016" e "a partire da maggio 2017 sta circolando in maniera massiccia nel deep web, tramite una piattaforma cloud russa. La provenienza del data leak è sconosciuta, così come l'origine dei dati". Gli accertamenti finora svolti hanno evidenziato, si legge nel comunicato, che in gran parte "le password associate agli account sono reali e per alcuni casi vengono ancora utilizzate". Illustri le vittime: "in Italia, Forze dell'Ordine e di Polizia, Forze Armate, ministeri, città metropolitane, ospedali e università" mentre "a livello globale, Forze armate Usa, Europol, Eurojust, Parlamento Europeo, Consiglio Europeo" e perfino "la Casa Bianca".

"Il copioso materiale informatico è attualmente oggetto di accurata analisi da parte degli operatori del Cnaipic della Polizia postale e delle comunicazioni", si legge in una nota della stessa Polizia, secondo cui "da una prima verifica si tratterebbe di una raccolta di informazioni datate, frutto di attacchi informatici risalenti, già oggetto in passato di divulgazione". "Sono presenti all'interno del database pubblicato nel darkweb - conferma la Polizia postale - circa 450 milioni di credenziali (userid e password), riferibili a circa 13 milioni di domini di posta elettronica worldwide,

probabilmente frutto di una collazione di diversi 'data breach' alcuni dei quali risulterebbero vecchi di anni". Gli specialisti informatici della Postale "stanno analizzando i dati acquisiti per le necessarie verifiche e per la puntuale informazione delle strutture di sicurezza cyber del Paese".

La Polizia postale infine "consiglia" - "nonostante si tratti di dati risalenti e, da una sommaria verifica non privi di errori nella indicazione delle caselle e delle password" - di "effettuare comunque, come da prassi comune, il periodico cambio della password di accesso per escludere eventuali intrusioni, utilizzando una combinazione efficace di numeri, lettere maiuscole e minuscole e caratteri speciali".

Secondo Mirko Gatto, Ceo di Yarix, "il colpo d'occhio sui domini presenti in Anti Public rivela e conferma l'estensione della vulnerabilità in cui viviamo: dalla Casa Bianca all'intero sistema militare e accademico in Italia, abbiamo davanti la fotografia esatta della nostra fragilità, che si nutre di una cultura della sicurezza ancora ampiamente acerba. Dalle organizzazioni più strutturate ai singoli individui, è imperativo che tutti cambiamo i nostri comportamenti, alla luce della consapevolezza che la criminalità informatica è in grado di nuocere a tutti i livelli".