

DATA LEAK

Rubati 458 milioni di password: sotto attacco Casa Bianca e Parlamento UE

Maxi-furto scoperto da D3Lab e dall'italiana Var Group: finito nel deep web quasi mezzo miliardo di account e-mail e chiavi d'accesso. Nel nostro Paese trafugati i dati di Polizia, ministeri, Comuni, ospedali e università.

di **Andrea Frollà**



Forze dell'Ordine e di Polizia, ministeri, città metropolitane, ospedali e università in Italia. Europol, Eurojust, Parlamento Europeo, Consiglio Europeo e perfino la Casa Bianca nel mondo. Sono queste le vittime illustri di un furto di dati denominato **Anti Public**, che ha portato nel **deep web** un maxi-archivio da **oltre 450 milioni di mail e password**. Diciassette gigabyte di informazioni scovate dagli esperti informatici di **D3Lab** e di **Yarix**, la cyber

division di **Var Group**, holding italiana specializzata nell'Information and communication technology. L'archivio, spiega la il gruppo italiano, "è stato scoperto attraverso una incursione di cyber intelligence che, sulla scorta di indiscrezioni trapelate nei giorni scorsi negli ambienti del deep web, ha consentito di intercettare e poi acquisire il data leak".

Sul dark web sono finiti dieci file in formato txt che, si legge nel comunicato, contengono dati relativi a 13 milioni di domini mail. **Sono state rubati 458 milioni email complete di relative password, riconducibili a centinaia di migliaia di aziende, organizzazioni, istituzioni, infrastrutture critiche e milioni di utenti singoli, in tutto il mondo.**

Il furto dei dati, sostiene 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 – spiega la compagnia - è sconosciuta, così come l'origine dei dati". Gli accertamenti hanno evidenziato che molte delle password associate agli account "sono reali e per alcuni casi vengono ancora utilizzate".

In Italia sono state colpiti "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 la Casa Bianca". 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, dichiara il manager, "**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**". E, mette in guardia Gatto, "l'abitudine di riutilizzare la password del sistema di posta aziendale anche su conti online, e-commerce e altri siti contribuisce ad estendere il raggio d'azione dei cybercriminali a milioni di account privati".