Il Sole 24 ORE

IN ITALIA COINVOLTE ANCHE POLIZIA E UNIVERSITÀ

Mezzo miliardo di indirizzi email bucati in tutto il mondo. In Italia coinvolte anche polizia e università

—di **Biagio Simonetta** | 26 maggio 2017

Diciassette gigabyte di dati sensibili sono finiti nel deep web, e sono coinvolti account italiani e internazionali di primo livello. In Italia sono interessate Polizia, Vigili del Fuoco, ministeri, città metropolitane, ospedali e università. Mentre a livello globale il fatto riguarda Casa Bianca, forze armate Usa, Europol, Eurojust, Parlamento Europeo e Consiglio Europeo.
È un "data leak" di proporzioni enormi, quello su cui hanno messo le mani gli esperti della Cyber Division di Var Group, attraverso una incursione di cyber intelligence effettuata dagli analisti di D3Lab.
Questi ultimi, in seguito ad indiscrezioni trapelate nei giorni scorsi negli ambienti underground del deep web, hanno intercettato e poi acquisito il data leak noto tra i cybercriminali come "Anti Public". Si tratta di 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.
Yarix, che sta seguendo il tutto da vicino, è già in contatto con il Ministero dell'Interno per la gestione di questa minaccia nei confronti dei soggetti pubblici e privati di maggiore interesse strategico nazionale.
Mentre gli ethical hackers sotto copertura di D3Lab sono ancora a lavoro per carpire maggiori informazioni e proseguire il lavoro di analisi e intelligence.

Cosa c'è in quei diciassette gigabyte

Dalle prime notizie emerse, il pacchetto da diciassette giga, è stato diffuso attraverso 10 file .txt. Sono 13 milioni i domini mail coinvolti, mentre sono poco meno di mezzo miliardo (457 milioni) le mail univoche coinvolte, complete di relative password. Per alcuni indirizzi mail sono presenti più password: questo fa presupporre che il singolo indirizzo sia stato impiegato per più servizi online. Sono coinvolte, inoltre, centinaia di migliaia di aziende/organizzazioni e milioni di utenti singoli, in tutto il mondo. E le password sono pubblicate in chiaro.

L'archivio, secondo le prime indiscrezioni, è stato creato nel dicembre del 2016. Ma è solo negli ultimi giorni che è comparso, massivamente, nel deep web attraverso una piattaforma cloud russa. Ovviamente, la provenienza del data leak è sconosciuta, così come l'origine dei dati.
«Il colpo d'occhio sui domini presenti in Anti Public – ha commentato Mirko Gatto, Ceo di Yarix – 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 al quotidiano dei 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».