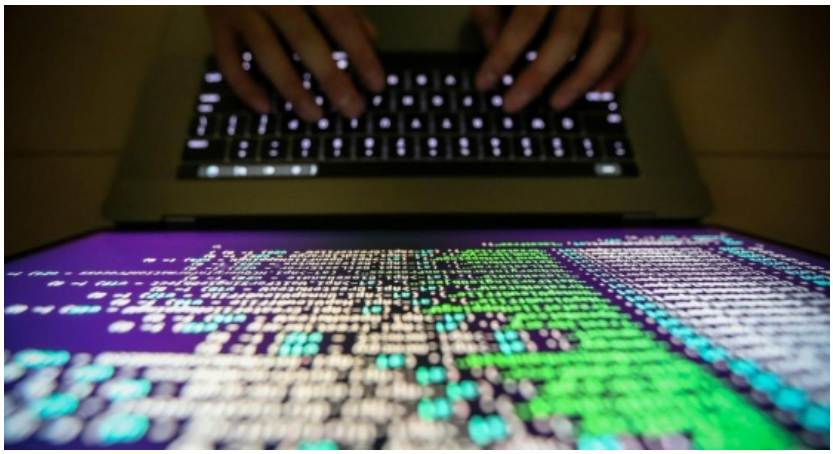
il mattino di Padova

Colossale furto di e-mail scoperto dal Veneto: «Gli hacker ci spiano»

Archivio di 458 milioni di indirizzi con relative password scoperto nel "deep web" dalla Yarix di Montebelluna
di Fabio Poloni

HACKER EMAIL PASSWORD

27 maggio 2017



TREVISO. Siamo nudi. Sanno tutto: password e chiavi d'accesso. Di privati, aziende, ministeri, enti governativi. E poi banche, ospedali, università. «Ho provato a controllare, uno per uno, tutti i nomi delle aziende e delle banche locali che mi venivano in mente. C'erano tutti», dice Mirko Gatto, che ha tolto il coperchio a questo inquietante vaso di Pandora digitale.

È uno sterminato archivio con quasi 458 milioni di indirizzi e-mail e relative password "in chiaro". Il più grande *data leak*, furto di credenziali, della storia. Dal Veneto alla Casa Bianca passando per il parlamento europeo.

A scoprirlo nel "deep web", la faccia scura della rete, quella non accessibile ai comuni *browser*, è stata l'azienda montebellunese Yarix, realtà di punta nel settore della sicurezza informatica. Un buco nero digitale che apre scenari inquietanti. Chi c'è dietro? E adesso cosa succede?

Al momento si sa che questo archivio di dati rubati "pesa" circa 17 gigabyte ed è suddiviso in dieci file di testo (.txt). È caricato su una "cloud", nuvola digitale, che porta in Russia. Yarix l'ha scoperta il 5 maggio scorso, ma pare sia stata creata a dicembre del 2016.

«E questo buco di sei mesi è terrificante», dice Gatto, che di Yarix - azienda che fa parte di Var Group - è amministratore delegato. Sono entrati ovunque, e non sappiamo per fare cosa. Soldi, certamente, perché le informazioni hanno un valore.

Altissimo, in alcuni casi: archivi aziendali, progetti, brevetti. Ma anche dal punto di vista della sicurezza pubblica e dei dati sensibili - come quelli sanitari - lo scenario è inquietante. In questo caso ci sono dentro forze di polizia e pure i vigili del fuoco.

«Chi ruba dati è un gruppo di hacker che solitamente prima cerca di monetizzare, con vendite o ricatti, poi li cede ad altre "crew" di hacker in cambio di altri dati. A lavoro terminato, come in questo caso, li pubblicano in chiaro, accessibili». Motivo? «Creare anarchia e paura». Benvenuti in "Mr. Robot". Una breccia devastante, perché dalle mail violate si apre tutto.

«Anche perché - spiega ancora Gatto - quasi tutti usano password uguali o simili per posta, social network, reti aziendali, home banking».

Siamo nudi, insomma, e il problema è che lo siamo da mesi senza saperlo.

«Quel che fa più paura è ciò che non vedi», spiega l'ad di Yarix, perché se scopri un virus informatico lo puoi debellare, ma se non sai di essere spiato sei totalmente esposto. L'azienda di Montebelluna in queste ore frenetiche è 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», e nel frattempo gli *ethical hackers* (i buoni, insomma) sotto copertura «sono ancora a lavoro nel deep web per carpire maggiori informazioni e proseguire il lavoro di analisi e intelligence».

Molte di quelle password rubate, tra quelle controllate, sono ancora attive: la porta, insomma, è rimasta aperta. «Cambiare le password di frequente e usarne di diverse è la prima regola», spiegano a Montebelluna.

«Il colpo d'occhio sui domini presenti in questo archivio, ribattezzato "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».

HACKER EMAIL PASSWORD