COMUNICATO STAMPA

Exploit.IN: continua l'affioramento di data leak

Dopo Anti Public è la volta di ***Exploit.IN***: 593 milioni di account coinvolti, con password e ID accessibili nel dark web. Secondo analisi Yarix, il 45% dei dati non è riconducibile ad Anti Public.

Immediata la segnalazione al Ministero dell'Interno da parte di Yarix, che sta collaborando per la messa in sicurezza dei dati sensibili potenzialmente a rischio. Istituzioni, infrastrutture critiche e aziende ancora nel mirino dei cyber criminali.

A pochi giorni dalla denuncia di Anti Public, la **Cyber Division di Var Group** ha segnalato al Ministero dell'Interno la presenza nel dark web di un nuovo data leak, noto come **Exploit.IN**. Un archivio di credenziali rubate in grado di fornire illegalmente le chiavi di accesso (password e ID) a circa **593 milioni di account**, riconducibili ad **aziende**, **istituzioni pubbliche**, **forze armate e di polizia**, **università** e **infrastrutture critiche** in tutto il mondo.

Exploit.IN ha fatto la prima comparsa sulla piattaforma *HIBP* (Have I Been Pwned) lo scorso 5 maggio e, rispetto ad Anti Public, rappresenta un **dump di dimensioni ancora maggiori**. Fino alla denuncia di Yarix, le autorità non erano state allertate di questo nuovo rischio latente online.

*Data la mole di dati da processare, non è ancora possibile stabilire se gli account presenti nei 2 leak siano relativi solo a utenti "vecchi" datati o se siano ancora in uso. Le prime rilevazioni effettuate dagli analisti di **D3Lab** indicano, tuttavia, che – malgrado una parziale sovrapposizione di dati con Anti Public – esiste in Exploit.IN un **45% di credenziali nuove**, non emerse in data leak precedenti.*

Una interpretazione dei fatti

Secondo **Mirko Gatto, CEO di Yarix**: "*L'affioramento a distanza ravvicinata di dump di così vaste proporzioni ci dice molto del probabile modus operandi della cybercriminalità internazionale: dopo essere stati illegalmente acquisiti, i dump sono stati prima rivenduti/utilizzati tra organizzazioni criminali e successivamente pubblicati online, nell'intento di alimentare caos*".

I rischi da fronteggiare

La magnitudo dei rischi che Exploit.IN e i recenti data leak possono implicare può essere di scala diversa. "*Al momento, il rischio più elevato si chiama **Credential Stuffing**: coppie di username/password, acquisite illegalmente, vengono riversate automaticamente e in gran numero nei siti web, fino a trovare il match con un account esistente. A quel punto, il cybercriminale è dentro il sistema e può sfruttarlo per i propri scopi*" – continua **Gatto** – "*Nel peggiore dei casi, potrebbe materializzarsi un **attacco informatico massiccio** (in stile WannaCry) che renda manifesta una infiltrazione silenziosa, avvenuta nelle settimane precedenti alla nostra denuncia alle autorità. Siamo già al lavoro per evitare che si realizzi lo scenario estremo di attacchi simultanei alle istituzioni, alle aziende e a personaggi chiave del sistema politico ed economico*".

Soggetti a rischio e numeri

- Senato della Repubblica: 101 account presenti – 32 new entry
- Governo Italiano: 56 account presenti, tutti nuovi
- Camera dei Deputati: 18 account presenti – 6 new entry
- Palazzo Chigi: 48 account presenti – 17 new entry
- Finmeccanica: 21 account presenti – 5 new entry

"Anche nel caso di Exploit.IN, siamo i primi a far affiorare un archivio di credenziali trafugate, disponibili in chiaro nel dark web dai primi di maggio e capaci di arrecare danni seri ai gangli vitali del nostro sistema economico e istituzionale. Siamo orgogliosi di poter offrire un servizio al Paese, traducendo la nostra attività di cyber intelligence in strumenti concreti di contrasto alla criminalità informatica", conclude **Gatto**.