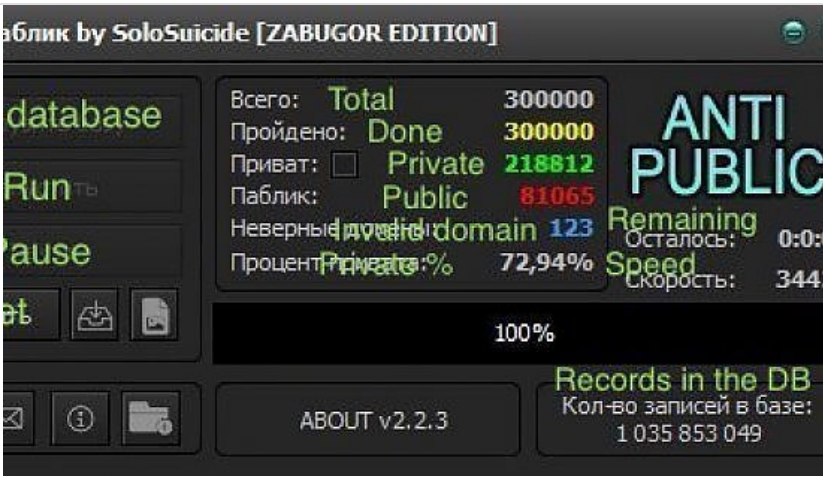
Sicurezza

Milioni di email e password rubate (anche in Italia) sono in un gigantesco archivio nel deep web



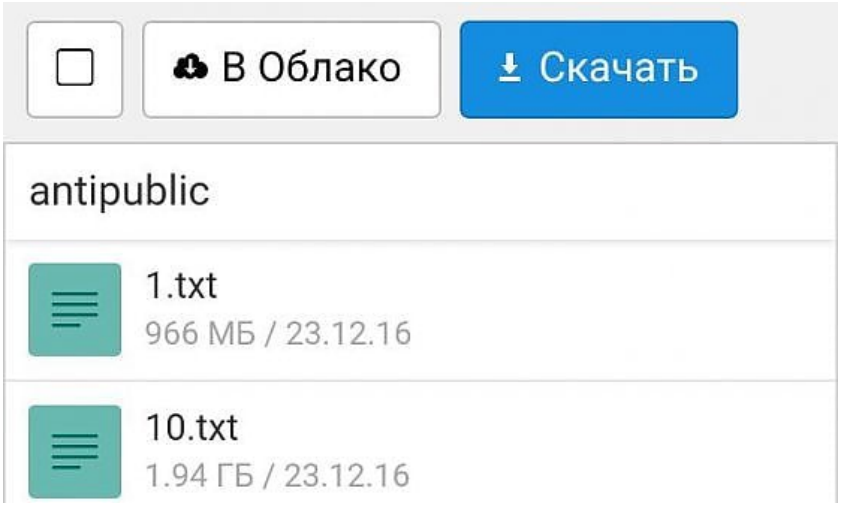
La nuova minaccia si chiama Anti Public, un data leak da 17 Giga. Più di 450 milioni di indirizzi mail da tutto il mondo, centinaia di migliaia di account a rischio tra aziende, polizia, militari, infrastrutture critiche e istituzioni europee. Possono essere usati per prendere il controllo dei server delle organizzazioni a cui sono state rubate

di ARTURO DI CORINTO

26 maggio 2017

POTREBBE essere il più grande furto di credenziali della storia. Oltre 450 milioni di email e relative password scovate nel *deep web* e pronte per essere usate a fini criminali. Un *data leak* di proporzioni mondiali che coinvolge migliaia di organizzazioni, pubbliche e private, dall'Italia agli Stati Uniti. Scovato dagli esperti della Cyber Division di Var Group, Yarix, attraverso una incursione effettuata dagli analisti del proprio partner D3Lab, l'archivio con tutti i dati è adesso al vaglio di esperti e investigatori.

Yarix, azienda italiana di interesse nazionale per la cybersecurity ha subito informato il Ministero dell'Interno per la gestione di questa minaccia mentre gli hacker sotto copertura di D3Lab sono ancora a lavoro nel deep web per carpire maggiori informazioni e proseguire il lavoro di analisi e intelligence. Un lavoro cominciato con le indiscrezioni trapelate nei giorni scorsi negli ambienti underground del deep web, che gli ha consentito di intercettare e acquisire questo gigantesco data leak noto tra i cybercriminali come Anti Public.



Condividi

Nel dettaglio. Si tratta di 457.962.538 email univoche coinvolte, complete di relative password. Per alcuni indirizzi mail sono elencate più password forse perché i singoli indirizzi email sono utilizzati dallo stesso utente per accedere a servizi online differenti, dalla banca al posto di lavoro, dal fisco alle prenotazioni ospedaliere. Le aziende e le organizzazioni coinvolte sono centinaia di migliaia. E tra le vittime italiane di questo vastissimo furto di dati ci sono le Forze dell'ordine e di Polizia, le Forze armate, i Vigili del fuoco, e poi ministeri, città metropolitane, ospedali e università. mentre a livello globale gli indirizzi trapelati sono perfino della Casa Bianca e delle Forze armate americane, di Europol, Eurojust, Parlamento europeo, Consiglio europeo.

Chi è stato? Finora sappiamo almeno il nome di questo gigantesco leak: è **AntiPublic** ed è un gigantesco archivio di mail e password rubate riconducibili ad aziende, istituzioni pubbliche, forze armate e di polizia, università e infrastrutture critiche in tutto il mondo. Diffuso in dieci file .txt numerati coinvolge 13 milioni di domini email e 450 milioni di email univoche con la password in chiaro. Da pochi giorni l'archivio è accessibile da alcuni indirizzi nel deep web, ma i file erano ospitati su una piattaforma cloud russa. Nonostante questo non sappiamo però chi ha creato l'archivio e con quale scopo. Soprattutto non sappiamo se tutte le email sono ancora attive e quante siano le password modificate da quando sono state raccolte e organizzate nell'archivio creato intorno a dicembre 2016. Dalle ricostruzioni, i dati non sono necessariamente accessi diretti alle caselle di posta, ma potrebbe trattarsi anche di combinazioni user/password per servizi digitali.

Dubbi e conferme. Secondo il professore **Fabio Massacci** dell'Università di Trento, esperto di Economia della cybersecurity "bisogna stare attenti che non sia una polpetta avvelenata. Solo un'analisi dettagliata potrà dirci se gli account sono attivi e accessibili. Spesso infatti questi archivi sono messi in vendita per truffare gli acquirenti, creare confusione e depistare attività di intelligence in corso". Consapevoli dei rischi citati dal professore, Yarix ha fatto sapere che gli "hacker bianchi" che hanno individuato l'archivio hanno accertato che una grande quantità di credenziali è confermata e che le password associate agli account sono reali e ancora in uso dagli utenti. Per questo **Mirko Gatto**, CEO di Yarix ci ha detto che "Il colpo d'occhio sui domini presenti in AntiPublic 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". E continua: "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".

L'importanza di cambiare le vecchie password. Il Ceo di Yarix ha ragione da vendere. Alla base del leak c'è proprio il pericoloso fenomeno del 'Password reuse', vale a dire il reimpiego della medesima chiave d'accesso per tutti i siti di servizi online, a partire magari da un nome utente che coincide con il proprio indirizzo di mail aziendale. Un'imprudenza che può compromettere la sfera degli interessi individuali e aprire una breccia nella sicurezza di aziende e organizzazioni di interesse collettivo. Secondo il professore della Sapienza **Roberto Baldoni**, infatti, direttore del Laboratorio Nazionale di Cybersecurity, "Se gli account sono confermati con le password ancora in uso il danno potrebbe essere di proporzioni inimmaginabili. Un simile archivio può essere sicuramente usato per il phishing ma non tanto per la sottrazione fraudolenta di informazioni a casaccio, quanto come punto d'ingresso nel perimetro difensivo di aziende commerciali e organizzazioni con compiti delicati e prendere possesso dei loro server per fare pubblicità, mining di bitcoin o offrire servizi illegali. Ma può accadere di peggio: spesso obiettivo di tali azioni è attaccare target specifici per ulteriori dataleaks e operare cyberspionaggio di alto profilo. Ad esempio, inoculando software dormienti che si attivano quando riconoscono l'informazione per cui sono stati programmati".