Intelligenza artificiale

Se il computer si accorge che la Terra gira attorno al Sole

L'umanità ha dovuto aspettare fino al XVI secolo, con Niccolò Copernico, per rendersi conto che la Terra orbita attorno al Sole. All'intelligenza artificiale sono bastate poche ore. I programmatori le avevano fornito i dati sul movimento del Sole e di Marte osservabili dal nostro pianeta. I ricercatori del Politecnico di Zurigo volevano dimostrare che un computer è in grado di sintetizzare una grande mole di dati e osservazioni in una legge molto semplice. L'obiettivo è applicare questo metodo per arrivare a osservazioni meno scontate di quella che la Terra orbita attorno al Sole. I fisici in questo momento sentono infatti il bisogno di risolvere delle contraddizioni di meccanica quantistica che con la loro mente da sola non riescono a spiegare.

Password

Mettete quelle chiavi in una cassaforte

Fanno gola a molti nella rete, ecco come proteggerle Aspettando l'uso di volto e impronte

di **Rosita Rijtano**

"Tratta le password come le tue mutande": era il riuscito slogan di un manifesto dell'università di Maastricht, in Olanda, che invitava gli utenti a prestare maggiore attenzione alle chiavi d'accesso dei propri servizi online. Il consiglio era di cambiarle spesso, toglierle dalla scrivania e non condividerle con nessuno. Il primo suggerimento si è rivelato non proprio azzeccato, ma il memorandum è passato alla storia. Eppure, «nonostante le campagne di sensibilizzazione, in molti continuano a commettere gli stessi errori», spiega Paolo Dal Checco, consulente informatico forense. La prova? Le classifiche delle password più popolari al mondo, pubblicate periodicamente. Nella top ten si piazzano le stesse da anni. Si va da 123456 ad apriti sesamo, passando per la parola password, nelle sue infinite varianti come pass1, password1, e passw0rd. Altra prassi comune è l'utilizzo della stessa chiave per molteplici servizi, aggiungendo magari una maiuscola all'inizio e una manciata di numeri alla fine. Cattive abitudini dure a morire, nonostante i consigli degli esperti.

Un punto in favore di tutti noi: secondo una ricerca della multinazionale del software Nuance, ognuno gestisce in media 11 account e dovrebbe ricordare almeno 9 codici alfanumerici. Troppi. Ed ecco che si ricorre a banalità o ripetizioni. Le conseguenze Dal Checco le conosce bene: «Capita spesso di aiutare uomini e donne cui è stata compromessa l'email o violato il profilo Facebook. Nella maggioranza dei casi scopriamo che hanno sfruttato una password identica per diversi servizi, alcuni dei quali violati da tempo».

I furti di credenziali sono all'ordine del giorno e non risparmiano nessuno. Lo dimostra la cronaca. ImmuniWeb, costola di Hi-Tech Bridge Sa, una compagnia di sicurezza informatica con base a Ginevra, ha appena individuato nel dark web, la parte nascosta della Rete cui si accede tramite specifici software, 21 milioni di credenziali sottratte a molte delle 500 aziende multimiliardarie che compongono l'annuale lista di Fortune. La scoperta diventa ancor più interessante guardando i dati da vicino: delle 21 milioni di credenziali, almeno 16 milioni sono state compromesse negli ultimi dodici mesi, e il 95% contiene password in chiaro. Tutte alla mercé dei criminali informatici. I metodi per migliorare la sicurezza dei propri account, senza impazzire nel ricordare decine di password, esistono e sono a portata di tutti. Il primo è sfruttare un password manager, cioè una sorta di cassaforte che consente di mettere al riparo le proprie credenziali e di generare automaticamente chiavi d'accesso sicure. Tra gli altri, godono di buona reputazione sia 1Password che KeePass. Il secondo sta nell'adottare un sistema di autenticazione a due fattori. In quest'ultimo caso, per entrare nel proprio servizio digitale è necessario affiancare alla password un secondo elemento. L'opzione più banale è di farsi inviare un numero via messaggio. Una scelta migliore è installare applicazioni che generano dei codici di verifica sullo schermo del proprio smartphone, come Google Authenticator.

La tecnologia si sta muovendo anche in un'altra direzione. Un futuro password free, in cui basterà usare il volto o l'impronta delle dita come lasciapassare. Microsoft è stata tra i primi colossi a crederci. Era il 2015, quando al Computex di Taipei svelò Hello: funzione che permette agli utenti di Windows 10 di accedere al pc, o ad app supportate, attraverso impronta digitale o riconoscimento facciale. Al passato Mobile World Congress di Barcellona Google ha annunciato l'adozione del certificato FIDO2 da parte di Android. Uno standard che permetterà di sfruttare l'autenticazione biometrica con gli smartphone equipaggiati del sistema operativo di Big G.

Stefano Zanero, professore di sicurezza informatica del Politecnico di Milano, giudica il metodo migliore di quello attuale. Anche se non mancano i rischi. «I dati biometrici sono particolarmente sensibili e bisogna progettare i sistemi in modo da proteggerli, diversamente da quanto avviene oggi con le password. Inoltre, la biometria funziona bene sui dispositivi personali. Sfruttarla per autenticarsi da remoto, ad esempio sui siti web, è complesso». Toccherà lavorare. Nel frattempo, dovremo imparare a trattare le password come le nostre mutande. O quasi.

Attacchi imponenti

1 Il furto planetario

Tre miliardi: è la stima finale del numero di utenti coinvolti da un furto di credenziali ai danni di Yahoo! avvenuto nel 2013. La reale portata di quanto accaduto è stata resa nota nel 2017. Nelle mani dei criminali informatici sono finiti nomi, email, indirizzi e password, ma non informazioni finanziarie

2 La collezione

773 milioni di email e 21 milioni di password rubate. È la refurtiva che si trovava in una cartella chiamata "Collection#1", pubblicata sul servizio di archiviazione cloud Mega. Il database di credenziali violate è stato individuato lo scorso gennaio e faceva parte di una collezione ancora più ampia.

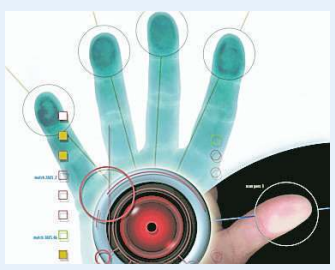
3 Adulteri nel mirino

Nel 2015 Ashley Madison, sito di incontri dichiaratamente dedicato agli adulteri, venne compromesso da un attacco informatico. Nel dark web finirono non solo le password, ma anche nomi e cognomi, indirizzi e-mail, e persino le fantasie sessuali degli utenti.

Adottiamo questi sistemi

1 Il "manager"

Per migliorare la sicurezza dei propri account si può utilizzare un password manager, come 1Password: permette agli utenti di proteggere le credenziali e generare automaticamente chiavi d'accesso sicure. Un altro metodo è adottare un sistema di autenticazione a due fattori.



2 Volto e impronte

La tecnologia va verso un futuro password free, in cui basterà usare il proprio volto o l'impronta delle dita come lasciapassare. Google ha da poco annunciato l'adozione del certificato FIDO2 da parte di Android. Uno standard che permette di sfruttare l'autenticazione biometrica da smartphones.

3 Due fattori

Si può anche adottare un sistema di autenticazione a due fattori. L'opzione più semplice è quella di farsi inviare un numero via messaggio. La scelta migliore è installare applicazioni che generano dei codici di verifica sullo schermo del proprio smartphone, come Google Authenticator.

21 milioni di credenziali sottratte a numerose aziende multimiliardarie