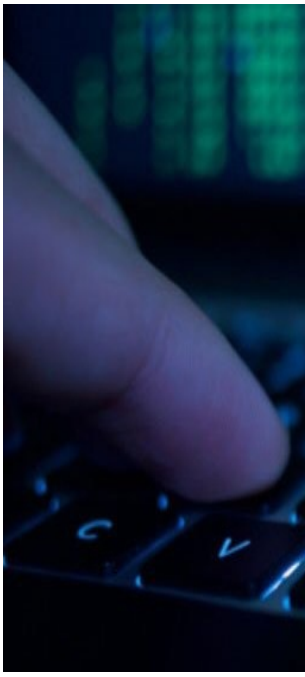
هجوم معلوماتي جديد يكشف ثغرة كارثية في حماية المستخدمين عالميا



افادت تقارير صحفية حديثة، بأن:"أكثر من "184" مليون كلمة مرور من حسابات أبل وغوغل وفيسبوك ومايكروسوفت، سُرّبت على الانترنت، وكانت مخزّنة في ملف نصي عادي غير مشفّر. وشمل خرق البيانات أيضًا أسماء مستخدمين وكلمات مرور لمواقع حكومية وتجارية ومصرفية".

وعُثر على قاعدة بيانات غير آمنة على الإنترنت تحتوي على ملايين من عناوين البريد الإلكتروني، وكلمات المرور، وعناوين URL، ومواقع إلكترونية تعود إلى شركات، مثل: أبل، وغوغل، وفيسبوك، ومايكروسوفت، وإنستغرام، وسناب شات، وغيرها.

ورغم إمكانية تغيير كلمات المرور، فإن ما يثير القلق هو أن قاعدة البيانات تضمنت أيضًا معلومات شديدة الحساسية، مثل: بيانات اعتماد تسجيل الدخول للبنوك والحسابات المالية، بالإضافة إلى تلك الخاصة بمنصات الرعاية الصحية والبوابات الحكومية.

والأخطر من ذلك، أن قاعدة البيانات هذه كانت مخزّنة على شكل ملف نصي عادي وغير مشفّر، على خلاف

أغلب قواعد البيانات التي تُشفّر المعلومات الحساسة لمنع وقوعها في الأيدي الخطأ.

وكما احتوت قاعدة البيانات غير المؤمّنة على بيانات اعتماد تجارية قد يستخدمها مجرمو الإنترنت لسرقة سجلات الأعمال، والتجسس على الشركات، وزرع برمجيات الفدية. وتبين لاحقًا أنها احتوت كذلك على بيانات اعتماد تسجيل دخول لبضع خدمات حكومية، بالإضافة إلى محادثات شخصية.

وبحسب تحليل الخبراء للبيانات المسربة، تبين أن:"عملية الاختراق تمت بواسطة نوع من برامج سرقة المعلومات الخبيثة، مثل Stealer Lumma، المصمّمة لسرقة بيانات حساسة تشمل أسماء المستخدمين وكلمات المرور وأرقام بطاقات الائتمان من مواقع إلكترونية وأنظمة مخترقة، ثم بيعها على الإنترنت المظلم".

وأظهرت البيانات، أن:"الأشخاص الذين يستخدمون اسم المستخدم ذاته وكلمة المرور ذاتها على خدمات متعددة، هم الأكثر عرضة لمثل هذه الهجمات".

إذ بمجرد حصول مجرمي الإنترنت على بيانات الدخول الخاصة بك، يمكنهم استخدامها لارتكاب عمليات احتيال وسرقة هوية، أو تنفيذ عمليات نصب إلكترونية.

ورغم عدم وجود طريقة مضمونة للحماية من هذه الاختراقات، ينصح الخبراء باتباع إجراءات وقائية، أبرزها: استخدام كلمات مرور قوية وفريدة، وتغيير كلمات المرور بانتظام، وتفعيل المصادقة متعددة العوامل (2FA) كلما أمكن، كما توفّر غوغل أداة مجانية تتيح للمستخدمين التحقق مما إذا كانت بيانات اعتمادهم تسرّبت على الإنترنت المظلم.