جوجل تحذر من "أخطر هجوم سيبراني" يستهدف مستخدمي "جي ميل"

الخميس 24 أبريل 2025 08:00 م

أعلنت شركة google عن تعرّض عدد من مستخدمي Gmail لهجوم إلكتروني وصفته بأنه "الأكثر تطورًا حتى الآن"، مشيرةً إلى أن الهجوم استغل ثغرة داخلية في أنظمة الشركة، إلى جانب أسلوب خداع مُحكم استهدف الإيقاع بالضحايا، ما دفع الشركة إلى إصدار تحذيرات أمنية عاجلة.

وكُشف عن تفاصيل الهجوم بعد أن أعلن نيك جونسون، مطور في مشاريع مرتبطة بعملة إيثريوم الرقمية المُشفرة/ETH، عن تلقيه إيميلًا مشبوهًا من عنوان رسمي تابع لجوجل (no-reply@google.com)، يزعم أن الشركة تلقت أمرًا قضائيًا يتعلق بحسابه.

ووفقًا لجونسون، بدت الرسالة وكأنها تنبيه أمني عادي صادر عن google، حيث اجتازت كافة اختبارات التوثيق الرقمية، وظهرت داخل Gmail دون أي تحذيرات أمنية.

تمكن المهاجمون من إرسال الرسالة عبر بريد إلكتروني حقيقي إلى أنفسهم من خلال خوادم google، ثم أعادوا توجيهه إلى الضحية، ما مكّنهم من الحفاظ على الموافقات الأمنية الأصلية التي يتعامل معها Gmail على أنها موثوقة، لكن الهدف النهائي للهجوم كان تقليديًا، وهو توجيه الضحية إلى صفحة مزيفة تهدف إلى سرقة بيانات الدخول.

وفي بيان رسمي، أكدت google علمها بهذا النمط من الهجمات المتطورة، مشيرةً إلى أنها بدأت بالفعل في تطبيق تحديثات أمنية للحد من هذه الثغرة، ودعت المستخدمين للتوقف عن استخدام كلمات المرور التقليدية حتى مع تفعيل خاصية التحقق بخطوتين 2FA، لا سيما في الحالات التي تعتمد فيها الخطوة الثانية على الرسائل النصية/SMS.

وأوضحت google أن المهاجمين باتوا قادرين على خداع المستخدمين للحصول على كلمة المرور، ومن ثم اعتراض رمز التحقق الذي يُرسل عبر الرسائل النصية، واعتبرت أن الخيار الأكثر أمانًا حاليًا هو الاعتماد على تقنية مفتاح المرور/Passkey، التي تربط الحساب بجهاز المستخدم الفعلي، ولا يمكن استخدامها دون الوصول الفعلي إلى الجهاز.

ويتزامن الكشف عن الهجوم، مع ظهور سلالة جديدة من البرمجيات الخبيثة المتطورة على نظام أندرويد تُعرف باسم Gorilla، التي صُممت خصيصًا لاعتراض الرسائل النصية القصيرة التي تحتوي على رموز المرور لمرة واحدة/OTP.

ووفقًا لتحليلات أولية أجراها خبراء أمنيون، تطلب برمجية Gorilla مجموعة واسعة من الصلاحيات عند تثبيتها، تتيح لها الوصول إلى معلومات حساسة، من بينها رقم الهاتف وبيانات شريحة الاتصال، وما أن تحصل على هذه الأذونات، تقوم بإنشاء قناة اتصال مستمرة مع خادم خارجي تابع للمهاجمين، ما يمكّنها من إرسال البيانات المسروقة في الوقت الفعلي، وتنفيذ أوامر إضافية يتم إرسالها لاحقًا.

وتتميّز Gorilla باستخدامها أساليب تمويه متطورة لتفادي أنظمة الحماية، إذ لا تُظهر سلوكيات مشبوهة أثناء التشغيل، ما يجعل اكتشافها أمرًا بالغ الصعوبة، سواء للمستخدمين أو لأنظمة مكافحة الفيروسات.

ويحذّر خبراء الأمن من أن البنية التقنية للبرمجية توحي بإمكانات مستقبلية أكثر خطرًا، تشمل القدرة على عرض صفحات وهمية تُحاكي مواقع إلكترونية معروفة لسرقة بيانات حساسة مثل كلمات المرور أو معلومات البطاقات البنكية. كما تضم البرمجية وظائف غير مفعلة حاليًا، تشير إلى قدرتها على الاستمرار في العمل حتى بعد محاولات الحذف أو إعادة ضبط الجهاز.

ولتفادي هذا النوع من التهديدات، يوصي المختصون بعدم الاعتماد على كلمات المرور وحدها كوسيلة لحماية الحسابات، وحتى عند تفعيل ميزة التحقق بخطوتين، فإن استخدام الرسائل النصية كخطوة ثانية لم يعد آمنًا بالشكل الكافي، ويُعتبر استخدام مفاتيح المرور أو تطبيقات المصادقة الثنائية الخيار الأكثر أمانًا حاليًا.

وفي السياق ذاته، شددت شركة google على أنها لا ترسل رسائل بريد إلكتروني تطلب من المستخدمين اتخاذ إجراءات أمنية بشكل مباشر، مؤكدة أن أي رسالة من هذا النوع تُعد على الأرجح محاولة تصيّد احتيالي تهدف إلى سرقة بيانات المستخدم.