هجوم "النقر المزدوج" يهدد ملايين المستخدمين على الإنترنت

الجمعة 10 يناير 2025 10:00 م

كشف تقرير جديد عن أسلوب مختلف في الهجمات الإلكترونية يحمل اسم "النقر المزدوج" (Double Clickjacking) والتي تعتمد على استغلال عملية النقر المزدوج على زر في واجهة الاستخدام داخل صفحة ويب لخداع المستخدمين واختراق حساباتهم.

قال الباحث في الأمن السيبراني باولوس ييبيلو، عبر مدونته، إن هذه الطريقة تتجاوز وسائل الحماية التقليدية التي تعتمدها المواقع الإلكترونية والتطبيقات، وإضافات متصفحات الويب، مما يوسع من نطاق الخطورة.

كيف يعمل أسلوب الاختراق الجديد؟

يعتمد أسلوب "النقر المزدوج" على تصميم المخترق لصفحة ويب مقنعة وجاذبة للمستخدم، بحيث يتمكن من دفعه إلى النقر على زر ما في واجهة الاستخدام، وعند ذلك يتم فتح صفحة أخرى داخل المتصفح، إما في صورة علامة تبويب جديدة (New tab) أو نافذة جديدة كلياً (New Window).

وسيظهر داخل الصفحة الجديدة للمستخدم محتوى يضطره إلى النقر مرتين على أحد العناصر، وقد يكون ذلك، على سبيل المثال، اختبار بتأكيد الهوية البشرية للمستخدم CAPTCHA التقليدي.

وفي الوقت بين النقرة الأولى والثانية، يتم استبدال النافذة الأصلية بأخرى خبيثة، ويحدث هذا سريعاً في لمح البصر، وبمجرد أن ينقر المستخدم على زر الماوس في المرة الأولى، وهو ما يعرف باسم Mousedown، أي أنه أمر يتم تنفيذه بمجرد أن ينقر المستخدم على زر الماوس لأسفل، وقبل أن يرفع إصبعه من على الزر، يتم تنفيذ الأمر.

خطورة فائقة

يتيح هذا التبديل السريع للمهاجمين سرقة أذونات وبيانات حساسة من متصفح المستخدم، مثل الأذونات المستخدمة داخل مواقع الويب المختلفة، مثل نظام أذونات OAuth، الذي تعتمد عليه معظم المواقع الكبرى لتسجيل الدخول.

وتتمثل خطورة الهجوم في أن أنظمة الحماية التي تستخدمها جميع مواقع الويب تركز على الحماية من هجمات معروفة، مثل هجوم Clickjacking، المعتمد على وضع أزرار خفية أسفل عناصر ظاهرة بواجهة استخدام، وبمجرد النقر عليها يؤدي المستخدم أوامر وهو غير واعٍ بتنفيذها داخل متصفحه، إلا أن هذه الأنظمة غير مصممة أو مجهزة لمواجهة الهجوم الجديد.

كما أن هجوم "النقر المزدوج" يمكن استغلاله ضد المستخدمين داخل مواقع الويب وتطبيقات الموبايل والمتصفحات وإضافاتها البرمجية، مما يوسع نطاق المخاطر.

وأضاف الباحث في الأمن السيبراني أن الهجمات أصبحت منتشرة بشكل كبير، حيث أظهرت الاختبارات أن معظم المواقع عُرْضة لهذه الثغرة بشكل افتراضي.

وأشار إلى أن التقنية تُستخدم حالياً لاختراق حسابات OAuth في مواقع كبرى، مما يؤدي إلى سيطرة المهاجمين على الحسابات وإجراء تغييرات حساسة دون علم المستخدم.

وأكد الخبراء أن هذه الهجمات تشكل تهديداً كبيراً، ما يستدعي من المطورين تعزيز أنظمتهم الأمنية لتشمل حماية ضد التفاعلات المتعددة والنقر المزدوج.

كما يُنصح المستخدمون بتوخي الحذر عند التعامل مع أي نوافذ تطلب التحقق بالنقر المزدوج، خاصة في المواقع غير الموثوقة.

وفي ظل تطور هذه التهديدات، يبقى التحديث المستمر لأنظمة الحماية واستخدام أحدث تقنيات الأمان السبيل الأمثل لمواجهة الهجمات الإلكترونية المتطورة.