هجمات تصيد احتيالي متطورة تتجاوز المصادقة الثنائية وتسرق حسابات "جيميل"

السبت 22 فبراير 2025 08:00 م

حذر باحثو الأمن في "سلاش نيكست" (SlashNext) من هجمات تصيد احتيالي متقدمة تتجاوز المصادقة الثنائية، من خلال اختطاف الجلسة واعتراض بيانات الاعتماد في الوقت الفعلي، وفقا لموقع "ذا صن".

وظهرت هذه الهجمات أول مرة في أواخر يناير/كانون الثاني الماضي على يد مجموعة قراصنة تُدعى "أستاروث" (Astaroth)، إذ يُرسل المهاجم رابطا عبر البريد الإلكتروني إلى الضحية وبمجرد النقر عليه سيعيد توجيهه إلى صفحة تسجيل دخول مزيفة تطابق الصفحة الشرعية.

ولن يكون هناك تحذيرات أمنية لأن معظم الأشخاص سيعتقدون أنها صفحة حقيقية، وعندما يقومون بإدخال بيانات تسجيل الدخول في الصفحة المزيفة، ستظهر عند المهاجم مما سيمنحه حق الوصول إلى حساباتهم.

وأضاف الباحثون أن حملة التصيد الجديدة لا تقتصر فقط على سرقة بيانات تسجيل الدخول فقط، بل تتجاوز رمز المصادقة الثنائية الذي يعتبر خط الدفاع الأول ضد هجمات التصيد الاحتيالي، وذلك من خلال التقاط رموز المصادقة وملفات تعريف الارتباط الخاصة بالجلسة فور إنشائها، مما يتيح للمهاجمين تجاوز حماية المصادقة الثنائية بسرعة ودقة، وهذا يعني أنه إذا تلقيت رسالة نصية تتضمن رمزا للوصول إلى حسابك فيمكن للمهاجمين اعتراضها.

ورغم وجود عمليات تصيد احتيالي مشابهة تستهدف بيانات تسجيل الدخول من خلال صفحات مزيفة، فإن "سلاش نيكست" حذرت في تقريرها من أن مجموعة "أستاروث" متطورة بشكل خاص بسبب قدرتها على التقاط جميع بيانات المصادقة في الوقت الفعلي.

وقال الباحثون إن "الهجمات الجديدة من أستاروث ترفع مستوى التوقعات بشكل كبير مما يجعل أساليب التصيد الاحتيالي التقليدية وإجراءات الأمان الخاصة بها غير فعالة إلى حد كبير".

يذكر أن مجموعة "أستاروث" عرضت خدماتها على شبكة الإنترنت المظلم بسعر 2000 دولار، إذ يمكن لمجرمي الإنترنت شراؤها مع 6 أشهر من التحديثات.

الذكاء الاصطناعي يقود هجمات التصيد الاحتيالي

في وقت سابق من هذا الأسبوع وصل تحذير لمستخدمي "جيميل" (Gmail) ينذرهم بعملية احتيال جديدة مدعومة بالذكاء الاصطناعي تسرق معلوماتهم الشخصية وتخترق حساباتهم، وقد حذر مكتب التحقيقات الفدرالي "إف بي آي" من هذه الهجمات لأول مرة في مايو العام الماضي، ولم تشهد عمليات التصيد المدعومة بالذكاء الاصطناعي سرقة أموال الحسابات فقط، بل وصلت إلى سرقة هويات الضحايا، بحسب "ذا صن".

وقال روبرت تريب الوكيل في مكتب التحقيقات الفدرالي "يستغل المهاجمون الذكاء الاصطناعي لإنشاء رسائل صوتية ومقاطع فيديو ورسائل بريد إلكتروني مقنعة جدا بهدف تنفيذ هجمات تصيد احتيالي ضد الأفراد والشركات على حد سواء"، وأضاف "يمكن أن تؤدي هذه الأساليب المتطورة إلى خسائر مالية مدمرة وتشويه للسمعة واختراق للبيانات الحساسة".