اختراق شركة إسرائيلية يكشف ثغرات في تطبيقات أمريكية معدلة

الجمعة 9 مايو 2025 08:00 م

كشف موقع Media 404 عن اختراق إلكتروني طال شركة إسرائيلية غير معروفة نسبيًا تُدعى TeleMessage، تزود وكالات حكومية أمريكية بنسخ معدلة من تطبيقات المراسلة المشفرة مثل سيجنال وواتساب وتيليجرام ووي شات.
وأدى الاختراق إلى تسريب بيانات حساسة لموظفين حكوميين وشركات مالية، مما أثار مخاوف عميقة بشأن أمن الاتصالات الحكومية.

شركة مجهولة في قلب الاتصالات الحكومية
رغم أن TeleMessage لا تتمتع بشهرة واسعة، إلا أنها تلعب دورًا بالغ الأهمية في البنية التحتية للاتصالات لدى بعض المؤسسات الأمريكية.

الشركة تقدم خدمات أرشفة رسائل تستهدف موظفي الوكالات الفيدرالية، عبر نسخ "معدلة" من تطبيقات مشفرة شهيرة. هذه النسخ تتيح تحويل الرسائل، بما فيها تلك المُرسلة عبر قنوات يفترض أنها آمنة وخاصة، إلى خوادم تخزين لمراجعتها لاحقًا من قبل الجهات الرسمية.

إلا أن هذه التعديلات، كما تُظهر الحادثة الأخيرة، جاءت على حساب أمن البيانات ذاتها.

15 دقيقة فقط لاختراق أدوات بمستوى حكومي
في تصريح مثير، قال المخترق لموقع Media 404 إن عملية الاختراق استغرقت أقل من 20 دقيقة، وتمت عبر بوابة تصحيح النظام (debugging) التي احتوت على أسماء مستخدمين وكلمات مرور مفعّلة.

وبمجرد الدخول، تمكن من الوصول إلى أنظمة التحكم الخلفية، واعترض الرسائل أثناء أرشفتها دون الحاجة إلى تحميل قاعدة بيانات كاملة.

تسريب بيانات موظفين حكوميين وشركات كبرى
من بين البيانات التي حصل عليها المخترق: أسماء وأرقام هواتف وعناوين بريد إلكتروني لموظفين في الجمارك وحماية الحدود الأمريكية (CBP)، وشركات مالية كبرى مثل Coinbase وGalaxy Digital، ومؤسسات أخرى في وول ستريت.

كما تضمنت البيانات رسائل جماعية تناقش تشريعات مالية حساسة، من بينها مشروع قانون للعملات المشفرة كان قيد المناقشة في مجلس الشيوخ الأمريكي، إلى جانب رسائل مرتبطة بمواقف سياسية تخص الرئيس السابق دونالد ترامب.

في إحدى الرسائل، ظهر نقاش داخلي بين أعضاء مجموعة لها صلة بشركة Galaxy Digital، حول دعم بعض نواب الحزب الديمقراطي لمشروع قانون العملات الرقمية، وذلك قبل يوم واحد من صدور بيان معارض من عدد من النواب.

صورة واحدة أثارت الزلزال
الحدث لم يكن ليثير هذه الضجة لولا صورة التُقطت لعضو الكونغرس الجمهوري مايك والتز أثناء اجتماع رسمي وهو يستخدم النسخة المعدلة من تطبيق سيجنال، وقد نشرتها وكالة رويترز.

هذه الصورة دفعت TeleMessage إلى حذف موقعها الإلكتروني بالكامل، وسط صمت تام من جانبها تجاه التسريبات.

وبحسب Media 404، جاءت الصورة بعد تقرير من مجلة The Atlantic أشار إلى استخدام كبار المسؤولين لتطبيق سيجنال في نقاشات أمن قومي حساسة، ما زاد من أهمية ما كشفه الاختراق.

بنية تحتية تجارية.. وغياب الضمانات الأمنية
التحقيق أشار إلى أن الخادم الذي تم اختراقه مستضاف على بنية سحابية تابعة لـ Amazon AWS في ولاية فيرجينيا الشمالية، وهو ما يعني أن الاتصالات المُعدلة كانت تمر عبر بنية تجارية عامة، يمكن الوصول إليها في حال وجود ثغرات.

تطبيق سيجنال، من جانبه، نفى أي مسؤولية عن النسخ المعدلة، مؤكدًا أنه لا يمكن ضمان الأمان أو الخصوصية في نسخ يتم تطويرها من قبل أطراف ثالثة.

وهذا التصريح يُبرز التحدي الحقيقي الذي تواجهه المؤسسات عند الاعتماد على نسخ "خاصة" من أدوات يُفترض أنها تحمي الخصوصية بالتشفير التام.

تحقيقات وتحذيرات.. ولا رد من الشركة
في محاولة للتحقق من صحة التسريب، تواصل Media 404 مع عدد من الأرقام التي ظهرت ضمن البيانات، وتمكّن من التثبت من هوية بعض الموظفين، واستخدم أدوات تحقيق مفتوحة المصدر مثل OSINT Industries لتأكيد ارتباط المعلومات المسربة بأسماء ومناصب حقيقية.

أما TeleMessage، فاختارت عدم الرد على الأسئلة الصحفية، فيما استمر الجدل على الساحة الأمريكية بشأن مدى فاعلية الرقابة على الشركات التي تطور أدوات تُستخدم لمعالجة بيانات حكومية وأمنية.

تقارير

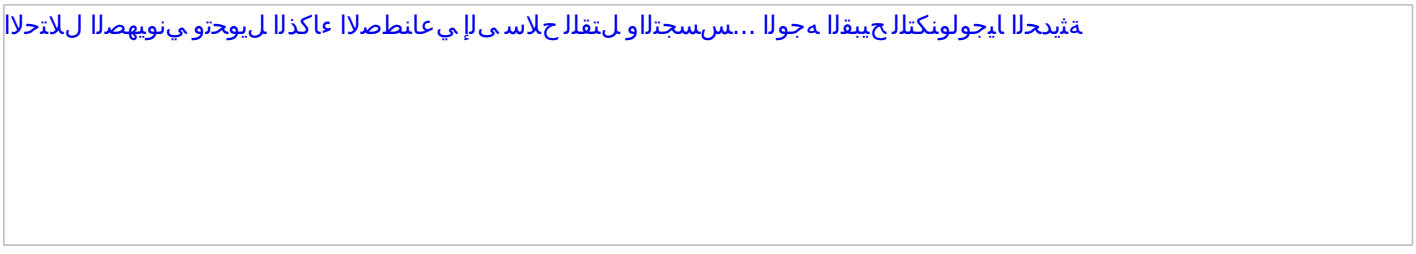
من الأطباء إلى المحامين والعسكريين ومن سيناء للوراق إلى مطروح... لا أمان لأحد بمصر في ظل حكم السيسي

الأربعاء 16 أبريل 2025 07:20 م
تقارير

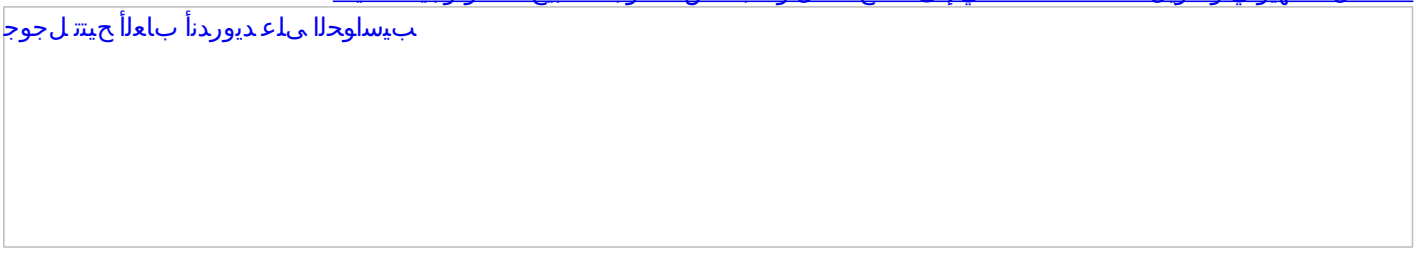
ديون على المكشوف... لماذا يشتري الأجانب 41.3 مليار دولار من ديون مصر؟

الأربعاء 16 أبريل 2025 04:30 م

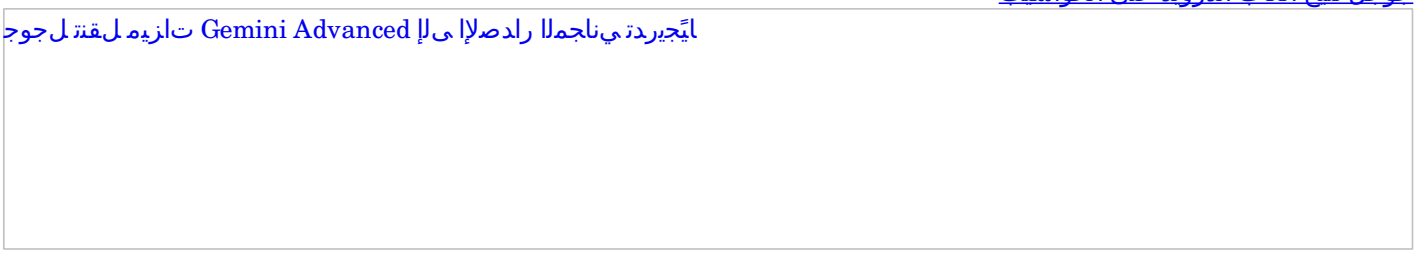
مقالات متعلقة



الاحتلال الصهيوني وتحويل الذكاء الاصطناعي إلى سلاح للقتل والتجسس... الوجه القبيح للتكنولوجيا الحديثة



جوجل تتيح ألعاب أندرويد على الحواسيب



جوجل تنقل ميزات Gemini Advanced إلى الإصدار المجاني تدريجيًا

تضررت منه مصر ودول عربية.. منصة "إكس" تعرضت لهجوم سيبراني غير مسبوق.. ما مصدره؟