“واشنطن بوست”: اختراق كبير تعرّضت له شبكات الإنترنت بأمريكا.. كيف حدث؟ ولماذا أثار كل هذا الذعر؟

الأربعاء 28 أغسطس 2024 07:58 م

كشفت صحيفة "واشنطن بوست" الأمريكية بشكل حصري نقلًا عن مصادر مطلعة، عن عمليات تجسس نفذها قراصنة صينيون ضد مزودي خدمات الإنترنت في الولايات المتحدة، طالت بيانات الملايين من المواطنين الأمريكيين.

وتدعي المصادر أن عمليات القرصنة الأخيرة والتي استمرت على مدار أشهر، جاءت بدعم من الحكومة الصينية، وهو ما أثار مخاوف في واشنطن.

كما أثار استهداف شركات تزويد خدمات الإنترنت في الولايات المتحدة مخاوف، بسبب ملايين العملاء لدى هذه الشركات.

حيث قال أشخاص مطلعون على الحملات المنفصلة إن الهجمات العدوانية "متطورة بشكل غير عادي"، وشملت الوصول إلى اثنين على الأقل من مقدمي الخدمات الرئيسيين الذين لديهم ملايين العملاء، بالإضافة إلى العديد من مقدمي الخدمات الأصغر حجمًا.

من جانبه، قال براندون ويلز، الذي كان حتى وقت سابق من هذا الشهر المدير التنفيذي لوكالة الأمن السيبراني وأمن البنية التحتية، CISA: "إن الأمر سيئ جدا من حيث الحجم".

إلا أن حجم المستهدفين ليس وحده ما يثير واشنطن، إذ أن هناك اعتقادا بأن الاختراق استهدف موظفين حكوميين، وعسكريين يعملون سرًا، ومجموعات ذات أهمية استراتيجية للصين.

حيث قال اثنان من الأشخاص إنه على الرغم من عدم وجود دليل على أن الاختراق الجديد كان يهدف إلى أي شيء آخر غير جمع المعلومات الاستخبارية، فإن بعض التقنيات والموارد المستخدمة مرتبطة بتلك المستخدمة في العام الماضي من قبل مجموعة مدعومة من الصين تعرف باسم فولت تايفون.

وسبق أن قال مسؤولو المخابرات الأمريكية أن هذه المجموعة سعت إلى الوصول إلى المعدات في موانئ المحيط الهادئ وغيرها من البنية التحتية لتمكين الصين من زرع الذعر وتعطيل قدرة أمريكا على نقل القوات والأسلحة والإمدادات إلى تايوان في حالة نشوب صراع مسلح.

كيف تم الاختراق؟
بحسب المصادر، فإن المتسللين استخدموا ثغرة أمنية لم تكن معروفة من قبل، تُعرف باسم خلل يوم الصفر، في برنامج أنشأته شركة Versa Networks لإدارة الشبكات واسعة النطاق.

واعترفت شركة Versa بالثغرة الأمنية الخطيرة في أواخر الأسبوع الماضي، وحذرت عملاءها المباشرين فقط.

حيث نشرت الشركة التي يقع مقرها في ولاية كاليفورنيا منشورًا على مدونة حول المشكلة، قائلة إنها أصدرت تصحيحًا وأن "العملاء المتأثرين فشلوا في تنفيذ إرشادات تقوية النظام وجدار الحماية".

وفي تقرير منفصل، قالت شركة الأمن Volexity إنها عثرت على تقنية متطورة أخرى قيد التشغيل لدى مزود خدمة إنترنت مختلف لم يذكر اسمه.

وفي هذه الحالة، قالت إن مجموعة قرصنة حكومية صينية متميزة عن Volt Typhoon تمكنت من الوصول إلى مسافة كافية داخل مزود الخدمة لتغيير عناوين الويب الخاصة بنظام اسم النطاق (DNS) التي كان المستخدمون يحاولون الوصول إليها، مما سمح للقراصنة بإدخال أبواب خلفية للتجسس.

بحسب ستيفن أدير، الرئيس التنفيذي لشركة Volexity، فإن التلاعب بنظام أسماء النطاقات (DNS) يعد أمرًا متخصصًا بين مجموعات القرصنة الحكومية الصينية.