قراصنة كوريا الشمالية يغزون نظام "npm" بفيروس "ذيل القندس"

8 أبريل، 2025

كشفت تقارير أمنية حديثة عن موجة جديدة من الهجمات السيبرانية تقودها مجموعة قرصنة تابعة لكوريا الشمالية.

واستهدف القراصنة هذه المرة نظام npm واسع الاستخدام من قبل مطوري البرمجيات، عبر نشر 11 حزمة خبيثة تتضمن برمجية "BeaverTail" ووسيلة تحميل خفية تتيح التحكم عن بُعد في الأنظمة المخترقة.

وأوضح الباحث الأمني في شركة Socket، كيريل بويتشينكو، أن القراصنة استخدموا طرق تشفير متقدمة لإخفاء الشيفرات داخل الحزم، في محاولة لتجاوز أدوات الكشف الآلي وعمليات المراجعة اليدوية، مما يعكس تطورًا في أساليب التعتيم والتخفي، بحسب تقرير نشره موقع "thehackernews" .

الحزم التي تم تحميلها أكثر من 5600 مرة قبل إزالتها، انتحلت صفات أدوات تطويرية مثل dev-debugger-vite وevents-utils وicloud-cod، وتبين ارتباط بعضها بمستودعات Bitbucket بدلاً من GitHub، في سلوك غير تقليدي يهدف إلى تضليل الجهات الأمنية.

ووفقًا للتقرير، فإن هذه الحزم تحتوي على شيفرات خبيثة قادرة على تحميل وتنفيذ أكواد JavaScript عن بُعد باستخدام دالة eval()، وهو ما يمنح القراصنة سيطرة شبه كاملة على الأجهزة المصابة، ويُسهّل تحميل برمجيات ضارة إضافية مثل InvisibleFerret وTropidoor.

ويبدو أن هذه الحملة ليست معزولة، بل جزء من حملة أوسع تُعرف باسم "المقابلات المعدية"، حيث يستدرج القراصنة الضحايا تحت غطاء فرص توظيف وهمية.

وتبين أن إحدى الهجمات بدأت برسالة بريد إلكتروني مزيفة من شركة تدعى "AutoSquare"، دعت فيها الضحية إلى تحميل مشروع من "Bitbucket"، ليتبين لاحقًا أن المشروع مجرد غطاء لنشر BeaverTail وأداة تحميل خبيثة لملفات DLL.

التحقيقات أظهرت أيضًا أن برنامج Tropidoor – أحد مكونات هذه الهجمات – يعمل في ذاكرة النظام فقط، ويقوم بجمع بيانات حساسة وتشغيل أوامر نظام ويندوز مثل schtasks وreg وping، وهي تقنيات سبق استخدامها في هجمات نفذتها مجموعة "Lazarus"، الجناح السيبراني الشهير المرتبط بنظام بيونغ يانغ.

ويحذر خبراء الأمن السيبراني من هذه الهجمات المتطورة، مشددين على ضرورة الحذر من الروابط والمرفقات المجهولة، خاصة تلك التي تأتي متخفية بفرص توظيف أو مشاريع تطوير مفتوحة المصدر.