مسرّع Web3 وهمي يستخدم حزم npm خبيثة لنشر برمجيات سرقة البيانات والأبواب الخلفية



يروّج مسرّع Web3 وهمي لبرمجيات سرقة المعلومات والأبواب الخلفية على أنظمة Windows وmacOS عبر حزم npm خبيثة، مستخدماً أرصدة ذكاء اصطناعي مجانية وأدوات برمجة وفحوصات أمنية كطُعم.

- تستهدف الحملة أجهزة Windows وmacOS معاً.
- تنقل حزم npm الخبيثة برمجيات سرقة المعلومات وأبواباً خلفية.
- يقوم الطُعم على عرض أرصدة مجانية لـ Google Geminig Anthropic Claude وأدوات برمجة وفحوصات أمنية.
- تعود النتائج إلى Elastic، كما يشير عنوان الخبر إلى اختطاف حركة بيانات وكلاء الذكاء الاصطناعي.

ما الذي ورد في التقرير

وفق ما نشره موقع The Hacker News، يعمل مسرّع Web3 وهمي على توزيع برمجيات خبيثة لسرقة المعلومات وأبواب خلفية على أنظمة Windows وmacOS. تتم عملية التوزيع عبر حزم npm خبيثة، أما الذريعة فهي عرض أرصدة ذكاء اصطناعي مجانية لـ Anthropic Claude Google Geminig، إضافة إلى أدوات برمجة وفحوصات أمنية.

وينقل التقرير عن Elastic أن الأدوات سلّمت برمجيات سرقة معلومات وأبواباً خلفية لأجهزة macOS وWindows. ويذكر العنوان كذلك اختطاف حركة بيانات وكلاء الذكاء الاصطناعي، غير أن المقتطف المتاح لا يشرح آلية ذلك.

أهمية الخبر

يستهدف الطُعم المطورين والفرق التقنية التي تثبّت الحزم وتجرّب أدوات الذكاء الاصطناعي بسرعة. وقد تكشف برمجية سرقة أو باب خلفي على جهاز مطوّر بيانات اعتماد وتمنح المهاجم موطئ قدم، فيتجاوز الخطر الجهاز الواحد. وتبدو الأرصدة والفحوصات المجانية عرضاً جذاباً، ولذلك تستحق هذه العروض التدقيق.

ولا يذكر المقتطف أسماء الحزم أو المسرّع أو عدد الضحايا أو الجهة المنفذة، لذا لا نتكهن بها.

الخطوات المقترحة

يُنصح بالتعامل مع أي عروض غير مطلوبة لأرصدة أو أدوات أو فحوصات مجانية على أنها غير موثوقة حتى يتم التحقق منها، ومراجعة طريقة حصول المطورين على اعتماديات npm وتثبيتها. وتجد أدناه نقاط بداية عملية.

ما يجب فعله الآن

1. تنبيه المطورين والفرق الهندسية من العروض غير المطلوبة لأرصدة الذكاء الاصطناعي أو الأدوات أو الفحوصات الأمنية المجانية، واشتراط التحقق قبل التفاعل معها.
2. حصر تثبيت حزم npm في مستودعات معتمدة أو نسخة داخلية، ومراجعة الاعتماديات المضافة حديثاً قبل استخدامها.
3. تشغيل أدوات التطوير على أجهزة مُدارة مزودة بحماية EDR على نظامي Windows وmacOS.
4. البحث في الأجهزة وأنظمة البناء عن حزم npm غير مألوفة ثُبّتت حديثاً، وتدوير بيانات الاعتماد على أي جهاز يُعثر فيه على حزمة منها.
5. مراجعة إعدادات أدوات الذكاء الاصطناعي ووكلائه ومفاتيح API المستخدمة، مع إبقاء المفاتيح محدودة الصلاحية وقابلة للإلغاء.