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



مسرّع Web3 وهمي يعرض أرصدة ذكاء اصطناعي مجانية وأدوات برمجة وتدقيقًا أمنيًا يوزّع برمجيات سرقة البيانات وأبوابًا خلفية على أجهزة Windows وmacOS عبر حزم npm خبيثة، بحسب Elastic.

- الطُّعم هو مسرّع Web3 وهمي يَعِد بأرصدة ذكاء اصطناعي مجانية لـ Anthropic Claude وGoogle Geminig إضافة إلى أدوات برمجة وتدقيق أمني.
- تُنقل الحمولات الخبيثة عبر حزم npm خبيثة.
- تستهدف الحملة أنظمة Windows وmacOS معًا.
- أفادت Elastic بأن الأدوات سلّمت برمجيات سرقة معلومات وأبوابًا خلفية.
- يشير العنوان أيضًا إلى اختطاف حركة وكلاء الذكاء الاصطناعي، ولا يتضمن المقتطف الذي راجعناه تفاصيل إضافية عن ذلك.

رُصد مسرّع Web3 وهمي يوزّع برمجيات خبيثة على أجهزة المطورين عبر حزم npm خبيثة. ووفق Elastic، سلّمت هذه الأدوات برمجيات لسرقة المعلومات وأبوابًا خلفية لأنظمة macOS وWindows.

آلية الحملة

يقدّم المشغّلون أنفسهم على أنهم برنامج مسرّعات أعمال، وتستهدف العروض المطورين والفرق التقنية: أرصدة ذكاء اصطناعي مجانية لـ Anthropic Claude Google Geminig، وأدوات برمجة، وخدمات تدقيق أمني. وتُستخدم حزم npm وسيلةً لإيصال الشيفرة الخبيثة.

ويذكر عنوان المصدر أيضًا اختطاف حركة وكلاء الذكاء الاصطناعي، لكن الجزء المتاح لنا من التقرير لا يشرح كيفية ذلك، لذا ينبغي عدم افتراض تفاصيل قبل مراجعة التحليل الفني الكامل.

أهمية الأمر للجهات المنظَّمة

تستهدف برمجيات سرقة المعلومات عادةً بيانات الاعتماد وغيرها من البيانات على الجهاز، بينما تمنح الأبواب الخلفية المهاجم وصولاً مستمرًا. وغالبًا ما تملك أجهزة المطورين صلاحيات إلى الشيفرة المصدرية والخدمات السحابية والأنظمة الداخلية، فقد يصبح جهاز مطوّر مخترق نقطة دخول إلى بيئات أوسع. كما أن عروض الأرصدة المجانية والتدقيق تبدو مقنعة للعاملين التقنيين، ما يجعل المخاطرة هندسة اجتماعية بقدر ما هي تقنية.

والاستجابة العملية هي اعتبار أي حزم أو برامج غير مطلوبة غير موثوقة حتى يثبت العكس مهما بدت مغرية، والتحقق مما إذا كانت حزم من هذا النوع قد وصلت فعلاً إلى بيئتكم.

ما يجب فعله الآن

1. البحث في أجهزة المطورين وأنظمة البناء عن حزم npm مثبّتة حديثًا من ناشرين غير معروفين أو مرتبطة بعروض مسرّعات أو أرصدة مجانية.
2. اشتراط الموافقة والمراجعة قبل إضافة اعتماديات npm جديدة، واستخدام سجل داخلي أو قائمة سماح حيثما أمكن.
3. تذكير المطورين والعاملين التقنيين بعدم التفاعل مع عروض غير مطلوبة لأرصدة ذكاء اصطناعي أو أدوات أو تدقيق أمني مجاني.
4. التأكد من تغطية أجهزة المطورين على Windows وmacOS بأدوات EDR، وتصعيد أي مؤشرات على نشاط برمجيات سرقة أو أبواب خلفية.
5. عند تثبيت حزمة مشبوهة، عزل الجهاز وتدوير بيانات الاعتماد والرموز التي كان بإمكانه الوصول إليها، ومنها مفاتيح خدمات الذكاء الاصطناعي.
6. مراجعة تحليل Elastic الكامل لاستخراج مؤشرات الاختراق وإضافتها إلى أدوات الكشف.