حملة CyberXero تجمع بين Claude Code وCobalt Strike لاستهداف جهات أوكرانية



كشف باحثون عن حملة وصول أولي معززة بالذكاء الاصطناعي تستهدف مواقع WordPress ومنصات التجارة الإلكترونية والبنية التحتية الحرجة في أوكرانيا، وتجمع بين Cobalt Strike وطبقة تنسيق مبنية على Claude Code من Anthropic.

- الحملة ذات مسارين وتركّز على الحصول على الوصول الأولي.
- تشمل الأهداف مواقع WordPress ومنصات التجارة الإلكترونية وجهات البنية التحتية الحرجة في أوكرانيا.
- تجمع بين أدوات هجومية شائعة مثل Cobalt Strike وطبقة تنسيق بالذكاء الاصطناعي تعمل بـ Claude Code.
- يشير عنوان الخبر إلى سرقة أكثر من 628,000 سجل أوكراني.
- يُتتبَّع النشاط تحت اسم CyberXero.

ما الذي ورد في التقرير

نشر باحثون في الأمن السيبراني تفاصيل حملة تستعين بالذكاء الاصطناعي في مرحلة الوصول الأولي إلى الأنظمة. وبحسب التقرير فهي ذات مسارين وتستهدف مواقع WordPress ومنصات التجارة الإلكترونية وجهات البنية التحتية الحرجة في أوكرانيا. ويُنسب النشاط إلى CyberXero، ويذكر عنوان الخبر أن أكثر من 628,000 سجل أوكراني قد سُرقت.

آلية عمل الحملة

تجمع الحملة بين أدوات هجومية شائعة مثل Cobalt Strike وطبقة تنسيق بالذكاء الاصطناعي تعمل بواسطة Claude Code من Anthropic. وأهمية ذلك للمدافعين لا تكمن في ثغرة جديدة بقدر ما تكمن في قدرة الذكاء الاصطناعي على تنسيق أدوات معروفة، وهو ما قد يقلل الجهد اليدوي على المهاجم. ولا يتضمن المقتطف المتاح تفاصيل تقنية إضافية مثل ثغرات محددة أو مؤشرات اختراق أو نسبة كاملة للجهة المنفذة، لذلك لا نستنتج أكثر مما ورد.

الصلة بالجهات في المملكة

الأهداف المذكورة، من مواقع عامة مبنية على WordPress وتجارة إلكترونية وبنية تحتية حرجة، شائعة كذلك في المملكة. وينبغي للجهات المنظمة اعتبار الخبر تذكيرًا بمراجعة انكشاف منصات المحتوى المرتبطة بالإنترنت، والتأكد من أن قدرات الكشف تغطي أنماط نشاط Cobalt Strike أياً كانت طريقة تنسيق المهاجم. ويُستحسن الرجوع إلى التقرير الأصلي للاطلاع على التفاصيل التقنية عند توفرها.

ما يجب فعله الآن

1. حصر مواقع WordPress ومنصات التجارة الإلكترونية المكشوفة على الإنترنت والتأكد من تحديث النواة والإضافات والقوالب.
2. التحقق من قدرة أنظمة EDR ومراقبة الشبكة على كشف Cobalt Strike والسلوكيات اللاحقة للاختراق.
3. مراجعة حسابات المسؤولين وتفعيل المصادقة متعددة العوامل في لوحات إدارة المحتوى والتجارة الإلكترونية.
4. مراجعة حجم بيانات العملاء المحتفظ بها في أنظمة التجارة الإلكترونية وتطبيق تقليل البيانات وضوابط الوصول بما يتوافق مع نظام حماية البيانات الشخصية.
5. تحديث نماذج التهديد وخطط الاستجابة للحوادث على افتراض أن المهاجمين قد يستخدمون الذكاء الاصطناعي لتسريع خطوات الاختراق.
6. متابعة التقرير الأصلي للحصول على مؤشرات الاختراق وإضافتها إلى أدوات الكشف عند نشرها.