

وكلاء ذكاء اصطناعي ذاتيون يُستخدمون في مهاجمة أكثر من 1200 موقع إلكتروني لشركات



استخدم مجرم ناطق بالصينية وكلاء ذكاء اصطناعي ذاتيين لمهاجمة أكثر من 1200 موقع، ووصل إلى مواقع أكثر من 100 شركة. وتمكن باحث من رصد النشاط لأن المشغلين تركوا لوحات التحكم مكشوفة.

- حاول وكلاء ذكاء اصطناعي ذاتيون اختراق أكثر من 1200 موقع بمساعدة بشرية شبه معدومة.
- وصل الوكلاء إلى مواقع تعود لأكثر من 100 شركة.
- من الشركات المذكورة شركة Deere لصناعة المعدات الزراعية.
- تمكن باحث أمني من مراقبة النشاط لأن المشغلين تركوا لوحات التحكم مفتوحة على الإنترنت.

يصف تقرير مجرمًا ناطقًا بالصينية ووجه وكلاء ذكاء اصطناعي ذاتيين نحو مواقع شركات، وترك لهم محاولة الاختراق بتدخل بشري يكاد يكون معدومًا.

ما الذي ورد في التقرير

حاول الوكلاء الوصول إلى أكثر من 1200 موقع، ونجحوا في بلوغ مواقع تعود لأكثر من 100 شركة، ومن بين الشركات المذكورة Deere لصناعة المعدات الزراعية. وتمكن باحث أمني من مراقبة العملية لأن المشغلين تركوا لوحات التحكم الخاصة بهم مكشوفة على الإنترنت.

ولا يوضح المقتطف المتاح تقنيات الهجوم ولا الثغرات المستغلة ولا ما فعله المهاجمون بعد الوصول، ولذلك لا ينبغي افتراض أي من ذلك.

أهمية الخبر للجهات المنظمة

يبيّن التقرير أن الوكلاء الآليين قادرون على توسيع نطاق المحاولات ضد المواقع المواجهة للإنترنت بجهد محدود من المهاجم. لذا تستحق الأصول الإلكترونية المكشوفة مراجعة دورية، مع الانتباه إلى سرعة اكتشاف النشاط غير المعتاد والتعامل معه.

لا يستدعي الخبر حالة طوارئ، لكنه مناسب للتحقق من سلامة التعرض الخارجي والمراقبة قبل أن يُوجّه نشاط مماثل نحو الجهة.

ما يجب فعله الآن

1. تحديث سجل المواقع وتطبيقات الويب المواجهة للإنترنت، بما فيها المواقع المنسية أو التجريبية.
2. التأكد من مراقبة سجلات تطبيقات الويب وأن الفحص الآلي المكثف يولّد تنبيهات.
3. مراجعة حالة التحديثات وضوابط الوصول للأصول الإلكترونية العامة.
4. التحقق من عدم كشف واجهات الإدارة والتحكم على الإنترنت.
5. اختبار إجراءات الاستجابة للحوادث الخاصة باختراق المواقع.