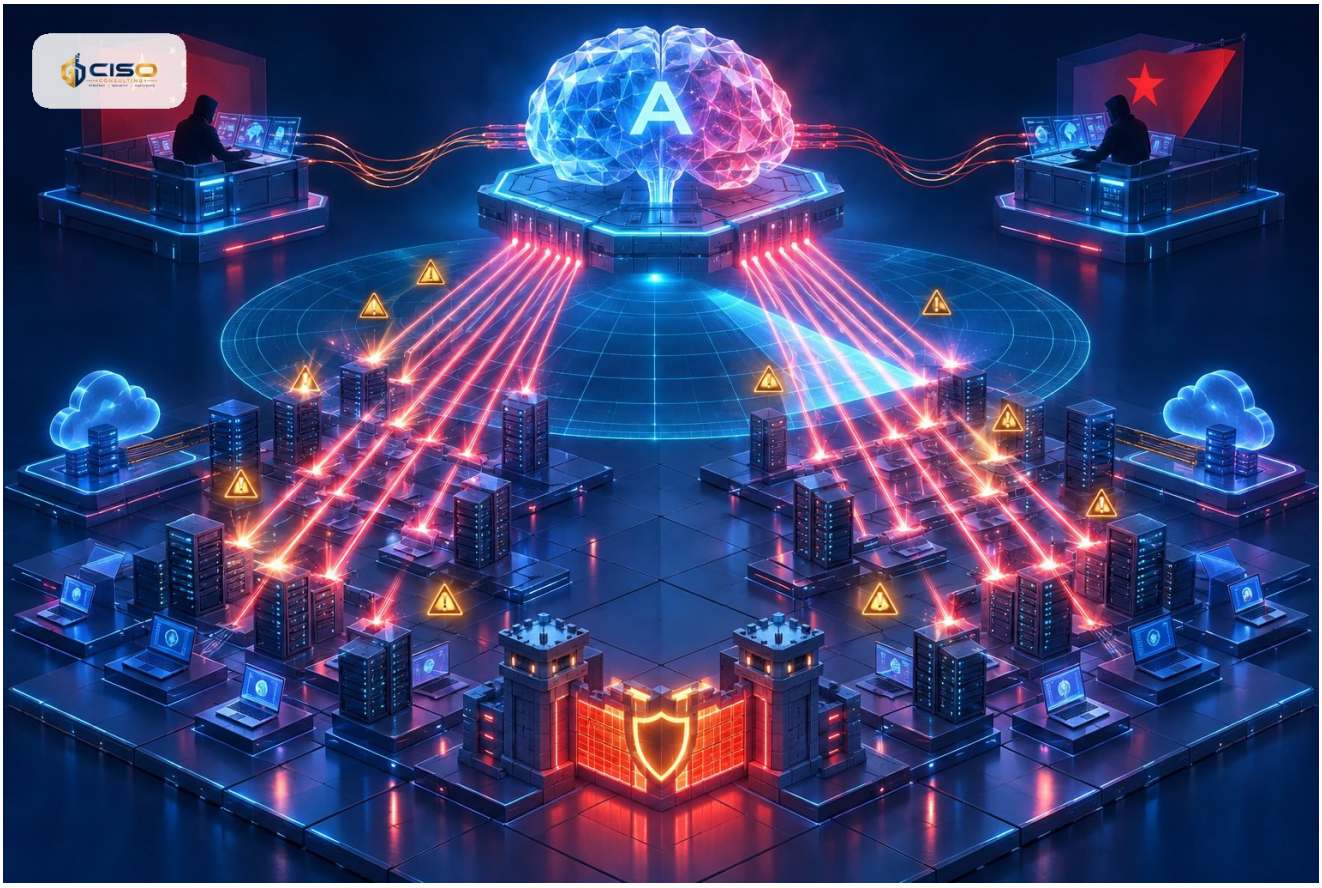
مجموعات مرتبطة بدول تتبنى إطار ARTEX للاختبار الآلي بالذكاء الاصطناعي وفق تحذير مايكروسوفت



تفيد مايكروسوفت بأن مجموعات مرتبطة بالصين وكوريا الشمالية تستخدم ARTEX، وهو إطار مفتوح المصدر يعتمد على نماذج لغوية، لأتمتة الهجمات. وسلوكه السريع والصاخب يمكن رصده.

- ARTEX إطار مفتوح المصدر لاختبار الاختراق يعتمد على نماذج لغوية، نُشر على GitHub في يوليو 2026، ويخطط وكلاء الذكاء الاصطناعي فيه الخطوات وينفذونها لبلوغ هدف يحدده المشغّل.
- رصدت مايكروسوفت حتى نوفمبر 2026 جهات مدعومة من دول وأخرى ذات دوافع مالية، منها Storm-0940 وSleet Onyx وSleet Pearl وTyphoon Crystal وTyphoon Salt، تدمجه في أدواتها.
- شملت الحملات المرصودة البحث في المستودعات العامة عن أسرار مكشوفة، وتمكين اختراق سلسلة الإمداد، وفحص الأنظمة المواجهة للإنترنت.
- سجلت إحدى حملات الرش الكلمي لـStorm-0940 ضد Microsoft 365 أكثر من 151,000 محاولة

دخول فاشلة، وبلغت صلاحيات متقدمة في أقل من ثلاث ساعات.

- لا يضيف ARTEX أساليب جديدة وهو صاخب افتراضيًا، لكن المشغلين يغيّرون عناوين IP ووكيل المستخدم لتجاوز التوقيعات البسيطة.

حذّرت مايكروسوفت لاستخبارات التهديدات من أن مجموعات مدعومة من دول مرتبطة بالصين وكوريا الشمالية بدأت باستخدام ARTEX في هجماتها. وARTEX إطار مفتوح المصدر لاختبار الاختراق يعمل بنماذج لغوية كبيرة؛ إذ يحدد المشغّل هدفًا، ثم يخطط وكلاء الذكاء الاصطناعي الخطوات اللازمة لبلوغه وينفذونها بتدخل محدود.

ما رصدته مايكروسوفت

حتى نوفمبر 2026 رصدت مايكروسوفت جهات مدعومة من دول وأخرى ذات دوافع مالية تدمج ARTEX في أدواتها، منها Storm-0940 وStorm-3358 وPearl Sleet وOnyx Sleet وCrystal Typhoon وSalt Typhoon.
وشملت الحملات المبلّغ عنها البحث في المستودعات العامة عن أسرار مكشوفة، وتمكين اختراق سلسلة الإمداد، وفحص الأنظمة المواجهة للإنترنت.

وفي إحدى حملات الرش الكلمي ضد Microsoft 365 سجّلت Storm-0940 أكثر من 151,000 محاولة دخول فاشلة، بذروة بلغت 2,900 في الدقيقة، ووصلت إلى صلاحيات متقدمة في أقل من ثلاث ساعات. وفي حالة أخرى انتقل وكيل ذكاء اصطناعي من البحث في GitHub عن أسرار العملاء إلى سحب بيانات من Azure Key Vault خلال خمس دقائق.

الرصد ما زال ممكنًا

تؤكد مايكروسوفت أن ARTEX لا يقدم أساليب جديدة، بل يعتمد على أدوات اختبار اختراق شائعة. ويستطيع المهاجمون تغيير عناوين IP ووكيل المستخدم لتجاوز الحظر القائم على التوقيعات، لذا فإن قوائم المؤشرات وحدها ضعيفة الأثر. أما السلوك فيصعب إخفاؤه: دفعات طلبات متنوعة، ومحاولات متكررة سريعة، وانتقال بين مراحل الهجوم بسرعة الآلة، وكلها تظهر في السجلات. وقد خلص المركز الوطني للأمن السيبراني في المملكة المتحدة إلى تقدير مشابه بشأن أطر الهجوم الوكيلة عمومًا، محذرًا من أن الأدوات المقبلة قد تُبنى مع مراعاة التخفي.

والخلاصة العملية أن سرعة الهجوم تتزايد، ما يرفع أهمية حماية الأسرار والمصادقة القوية، ويجعل الرصد القائم على السلوك أولوية.

ما يجب فعله الآن

1. افحصوا مستودعات الشيفرة العامة والداخلية بحثًا عن أسرار وبيانات اعتماد مكشوفة، وغيّروا ما يُعثر عليه منها.
2. فعّلوا المصادقة متعددة العوامل والوصول المشروط في Microsoft 365 وAzure، وأنشئوا تنبيهات لمحاولات الدخول الفاشلة الكثيفة وأنماط الرش الكلمي.
3. قيّدوا الوصول إلى Azure Key Vault وراجعوا بيانات اعتماد التطبيقات والصلاحيات الممنوحة لتطبيقات الأطراف الثالثة.
4. اضبطوا الرصد على السلوك مثل دفعات الطلبات والمحاولات المتكررة السريعة والانتقال السريع بين المراحل، ولا تكتفوا بمؤشرات IP ووكيل المستخدم.

5. راجعوا انكشاف الأنظمة المواجهة للإنترنت وعالجوا ثغراتها فورًا، وقيّموا صلاحيات موردي سلسلة الإمداد في بيئتكم.