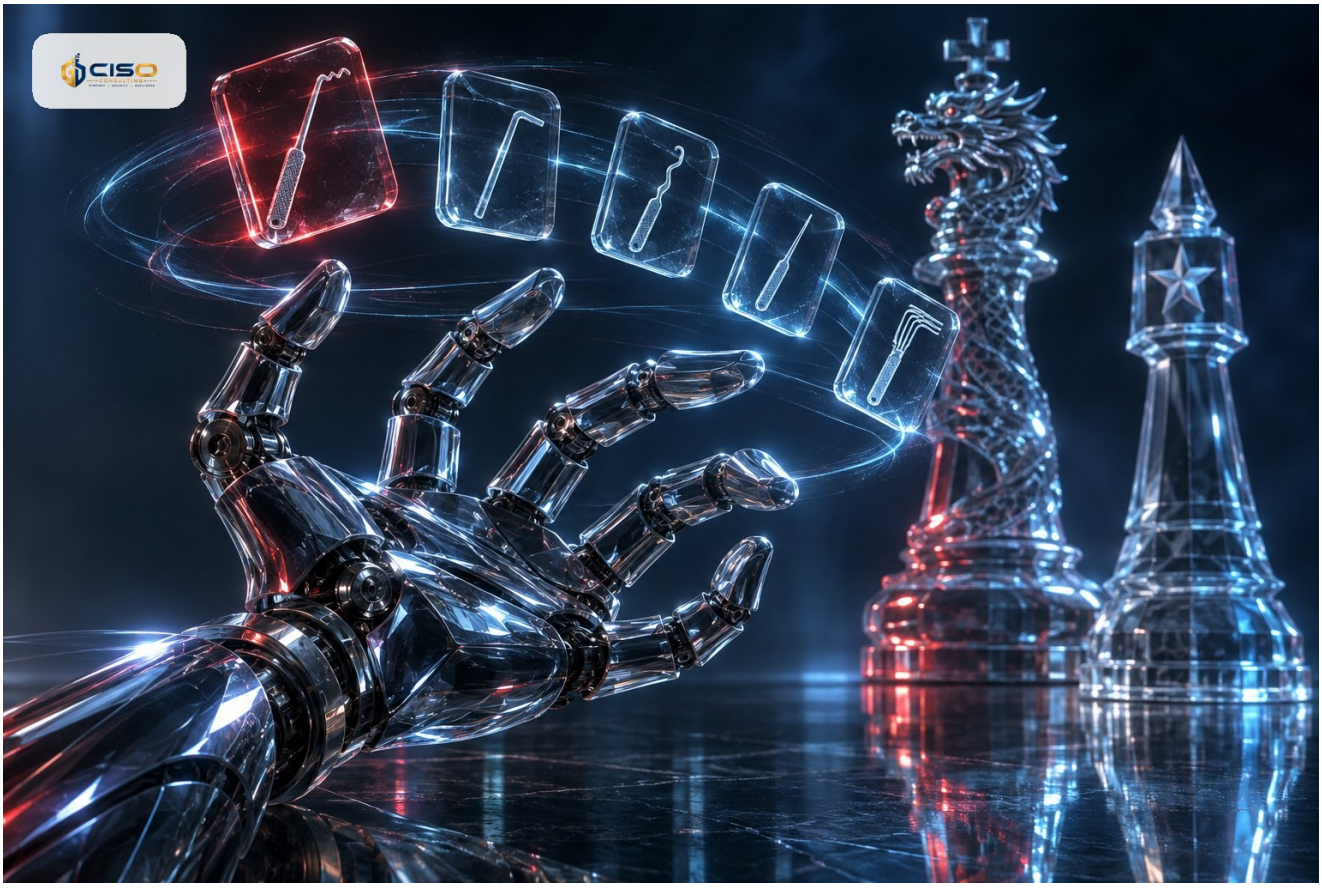
# مايكروسوفت: مجموعات مدعومة من دول تستخدم أداة الذكاء الاصطناعي Artex لتسريع الاختراقات



تفيد مايكروسوفت بأن مجموعات صينية وكورية شمالية مدعومة من دول، منها Salt Typhoon، تستخدم منصة الذكاء الاصطناعي Artex لأتمتة مراحل الاختراق. وأوثق مؤشراتها سلوكي، فلا يكفي الاعتماد على المؤشرات الثابتة.

- تصف مايكروسوفت Artex بأنها منصة تعمل بالذكاء الاصطناعي وتؤتمت عدة مراحل من الاختراق بسرعة الآلة.
- تستخدمها المجموعتان الصينيتان Salt Typhoong Crystal Typhoon في الاستطلاع الشبكي وهجمات بيانات الاعتماد واستغلال تطبيقات الويب.
- لا تضيف الأداة تقنيات هجومية جديدة، بل تعتمد أدوات اختبار اختراق معروفة، ويغيّر المهاجمون عناوين IP وسلاسل user agent لتفادي الحجب القائم على التوقيعات.
- أثبت المؤشرات سلوكي: طلبات كثيرة ومتنوعة في وقت قصير، وإعادة محاولات، وانتقال سريع

إلى المراحل التالية.

- أصدر مكتب FBI تحذيره الخاص قبل أسبوعين، وما زالت نسخ من الأداة متاحة بعد أن أُزيل الكود المصدري الأصلي من GitHub.

نشرت مايكروسوفت تقريراً تفيد فيه بأن جهات تهديد مدعومة من دول وأخرى ذات دوافع مالية تستخدم Artex، وهي منصة تعمل بالذكاء الاصطناعي وتؤتمت عدة مراحل من الاختراق بسرعة الآلة. وسمّت المجموعتين الصينيتين Crystal Typhoon وSalt Typhoon، وذكرت أنهما تستخدمانها في الاستطلاع الشبكي وهجمات بيانات الاعتماد واستغلال تطبيقات الويب. كما تفيد بأن مجموعات كورية شمالية تستخدمها أيضاً.

## ما الذي تفعله الأداة

تتيح Artex للمشغّل تحديد أهداف بعينها ثم توجيه وكلاء ذكاء اصطناعي نحو الجهة المستهدفة. وتقول مايكروسوفت إنها قادرة على الانتقال من الاستطلاع إلى وصول دائم وذي صلاحيات مرتفعة خلال دقائق. وقد أُسيء استخدامها في حملات حديثة للبحث في المستودعات العامة عن أسرار مكشوفة، وتمكين اختراق سلاسل التوريد، وفحص الأنظمة المواجهة للإنترنت بحثاً عن ثغرات للاستغلال.

وتؤكد مايكروسوفت أن Artex لا تقدّم تقنيات هجومية جديدة، بل تعتمد أدوات اختبار اختراق شائعة. وهي لا تحاول افتراضياً إخفاء نشاطها.

## انعكاسات على الكشف

يستطيع المهاجمون تغيير عناوين IP المصدر وسلاسل user agent، لذا قد يفوّت الحجب الثابت أو القائم على التوقيعات البسيطة هذا النشاط. وتصف مايكروسوفت السلوك بأنه المؤشر الأوثق: طلبات متنوعة بكثرة في وقت قصير، وإعادة محاولة صيغ مختلفة من التقنية نفسها، وانتقال سريع إلى مراحل لاحقة. ومن العلامات المميزة حجم كبير من الحركة الشاذة من مصدر واحد خلال مدة وجيزة.

وكان مطوّر الأداة الأصلي قد أزال الكود المصدري من GitHub، لكن نسخاً منه ما زالت متاحة، وتعرض شركة صينية واحدة على الأقل وصولًا تجارياً إلى نسخة منه. كما أصدر مكتب FBI تحذيراً خاصاً بالأداة. ولا يذكر المصدر تفاصيل عن أي نشاط في المملكة العربية السعودية.

## ما يجب فعله الآن

1. إضافة قواعد كشف سلوكية لرصد دفعات الطلبات المتنوعة وإعادة المحاولات والتقدم السريع من مصدر واحد، دون الاكتفاء بقوائم حجب عناوين IP أو user agent.
2. مراجعة الأنظمة وتطبيقات الويب المواجهة للإنترنت من حيث التعرّض وأولويات التحديث، لأن Artex تُستخدم في فحصها واستغلالها.
3. البحث في مستودعات الشيفرة العامة عن أسرار مكشوفة وتدوير أي بيانات اعتماد يُعثر عليها.
4. تعزيز حماية بيانات الاعتماد عبر المصادقة متعددة العوامل ومراقبة هجمات بيانات الاعتماد.
5. مراجعة صلاحيات الموردين وبرمجيات إدارة تقنية المعلومات في ضوء الاستخدام المبلّغ عنه في هجمات سلاسل التوريد.

6. تحديث إجراءات الاستجابة للحوادث لتشمل اختراقات تنتقل من الاستطلاع إلى وصول ذي صلاحيات خلال دقائق.