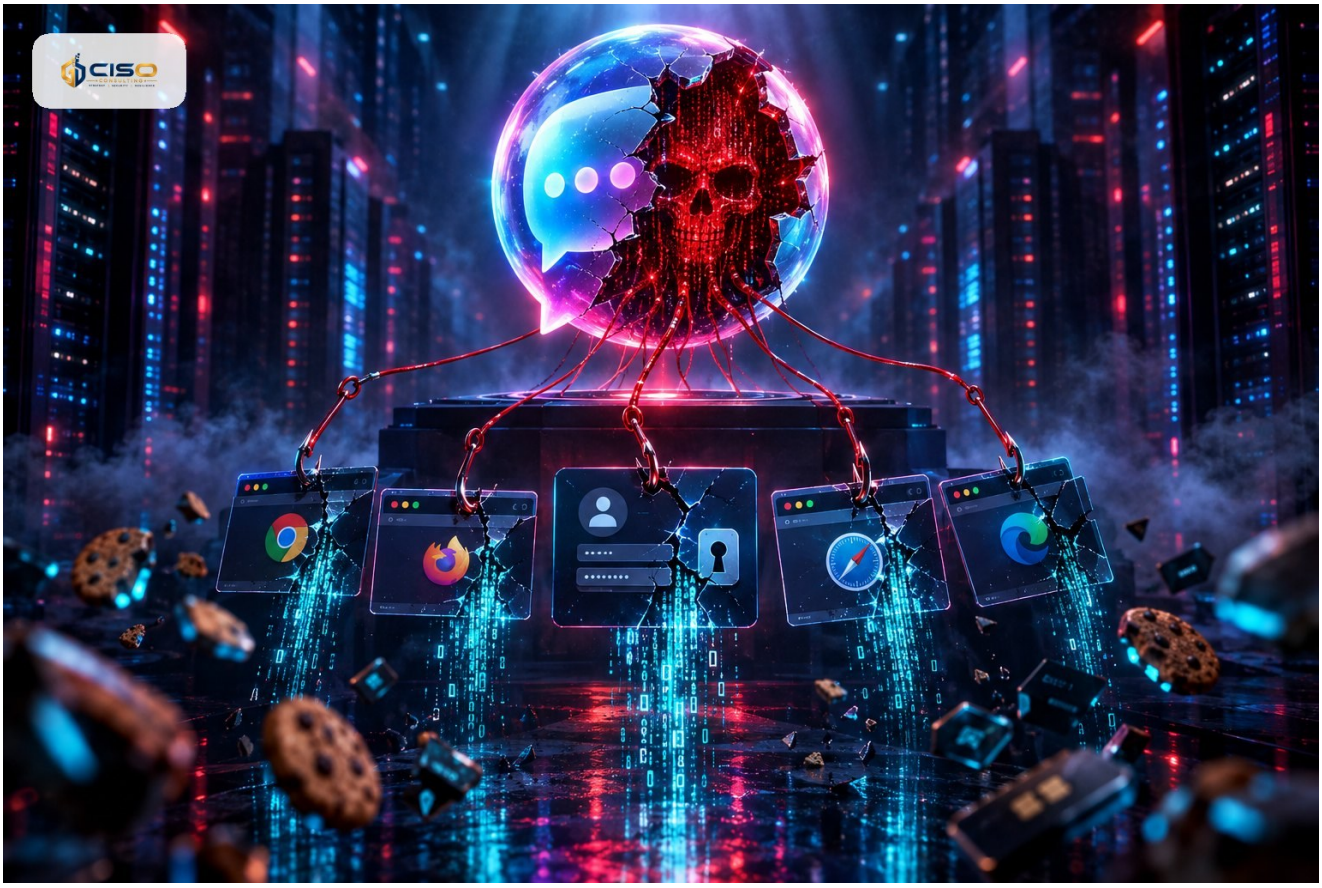
حملات أدوات ذكاء اصطناعي مزيفة تستهدف حسابات الشركات وجلسات المتصفح



ربطت ANY.RUN بين 1,258 تحليلًا عاماً في بيئتها المعزولة وحملات تنتحل منتجات ذكاء اصطناعي شائعة لنشر البرمجيات الخبيثة والاستيلاء على حسابات الشركات، بين أبريل وأكتوبر 2026.

- ينتحل المهاجمون صفة منتجات ذكاء اصطناعي شائعة لنشر البرمجيات الخبيثة.
- تشمل الأهداف سرقة جلسات المتصفح واختراق حسابات الشركات.
- ربطت ANY.RUN بين 1,258 تحليلًا عاماً في بيئتها المعزولة وهذه الحملات بين أبريل وأكتوبر 2026.
- شكلت الشركات الأمريكية 16% من الأهداف المنسوبة إلى دول بعينها.
- تزيد الحملات الضغط التشغيلي على مزودي خدمات الأمن المُدارة الذين يخدمون العملاء المتضررين.

ما الذي ورد في التقرير

يفيد موقع The Hacker News بأن مهاجمين ينتحلون صفة منتجات ذكاء اصطناعي معروفة بهدف نشر برمجيات خبيثة وسرقة جلسات المتصفح واختراق حسابات الشركات. وقد ربطت ANY.RUN، وهي مزود لتحليل البرمجيات الخبيثة، بين 1,258 تحليلًا عاماً في بيئتها المعزولة وحملات ذكاء اصطناعي مزيفة رُصدت بين أبريل وأكتوبر 2026.

وشكلت الشركات الأمريكية 16% من الأهداف التي أمكن نسبتها إلى دولة بعينها. ويشير التقرير إلى أن هذه الحملات تزيد الضغط التشغيلي على مزودي خدمات الأمن المُدارة (MSSPs) الذين يدعمون هذه الشركات.

أهمية الأمر في المملكة

يتناول المصدر شركات أمريكية ولا يصف نشاطاً داخل المملكة. ومع ذلك فالأسلوب غير مرتبط بموقع جغرافي: قد يبحث الموظفون في أي جهة عن أدوات ذكاء اصطناعي فيحمّلون نسخة مقلدة أو يسجلون الدخول إليها. وسرقة جلسات المتصفح قد تمنح المهاجم وصولًا إلى حسابات العمل دون الحاجة إلى كلمة المرور، ما يجعل الكشف المبكر مهماً.

ولا يتضمن المقتطف المتاح تفاصيل عن عائلات البرمجيات الخبيثة أو النطاقات المستخدمة أو أساليب الكشف، لذا لا نخمّن فيها.

التوجه العملي

يُنصح بالتعامل مع أدوات الذكاء الاصطناعي غير المعتمدة بوصفها خطراً يُدار، لا مسألة سياسات فحسب. وفّروا للموظفين مساراً معتمداً وواضحاً للأدوات التي يحتاجونها، وتأكدوا من قدرة المراقبة الأمنية لديكم، سواء داخلية أو عبر مزود خدمات مُدارة، على رصد التنزيلات المشبوهة وعمليات تسجيل الدخول غير المعتادة مبكراً.

ما يجب فعله الآن

1. انشروا قائمة بأدوات الذكاء الاصطناعي المعتمدة والمصادر الرسمية للحصول عليها.
2. ذكّروا الموظفين بعدم تثبيت برامج أو إضافات متصفح للذكاء الاصطناعي من روابط أو إعلانات غير موثوقة.
3. راجعوا مدة صلاحية جلسات المتصفح والخدمات السحابية، وفعّلوا المصادقة متعددة العوامل على حسابات العمل.
4. اسألوا مزود الخدمات المُدارة أو مركز العمليات الأمنية لديكم عن كيفية كشف تنزيل ذكاء اصطناعي مزيف أو جلسة مسروقة.
5. جهّزوا خطوة استجابة لإلغاء الجلسات وإعادة تعيين بيانات الاعتماد عند الاشتباه باختراق حساب.