ارتفاع هجمات الفدية مع توظيف الذكاء الاصطناعي وتراجع مدفوعات الفدية



تفيد Dark Reading بأن عددًا متزايدًا من مجموعات الفدية يستخدم الذكاء الاصطناعي لصياغة رسائل تصيد مقنعة وتحديد البيانات الحساسة بسرعة. وترتفع الهجمات بينما تتراجع مدفوعات الفدية.

- ترتفع هجمات الفدية بحسب التقرير.
- تتراجع مدفوعات الفدية رغم زيادة الهجمات.
- تساعد النماذج اللغوية الكبيرة وأنظمة الذكاء الاصطناعي الأخرى المجموعات على صياغة رسائل تصيد مقنعة.
- يساعد الذكاء الاصطناعي المهاجمين أيضًا على تحديد البيانات الحساسة بسرعة.

يصف تقرير نشرته Dark Reading تحولاً في مشهد هجمات الفدية: فالهجمات في ارتفاع، ويعود ذلك جزئيًا إلى الذكاء الاصطناعي، بينما تتراجع المبالغ التي تُدفع للمهاجمين.

ما الذي يذكره التقرير

وفق المصدر، تتيح النماذج اللغوية الكبيرة وأنظمة الذكاء الاصطناعي الأخرى لعدد متزايد من مجموعات الفدية إعداد رسائل تصيد مقنعة وتحديد البيانات الحساسة بسرعة. وتقلل هاتان القدرتان الجهد اللازم للحصول على موطئ قدم داخل الشبكة وتحديد ما يُسرق أو يُشفَّر.

كما يشير عنوان المصدر إلى تراجع المدفوعات. ولا يتضمن المقتطف المتاح لنا أرقامًا أو فترات زمنية أو أسبابًا، لذلك لا نستخلص استنتاجات بشأن الأسباب أو الحجم.

ما معنى ذلك للمؤسسات

النتيجة العملية أن رسائل التصيد ذات الصياغة السليمة يصعب على الموظفين كشفها بالاعتماد على جودة اللغة وحدها، وأن المهاجمين قادرون على الوصول إلى البيانات القيّمة بسرعة أكبر بعد الدخول. ولا ينبغي فهم انخفاض المدفوعات على أنه انخفاض في المخاطر، إذ يذكر التقرير أن حجم الهجمات في ازدياد.

وتستفيد المؤسسات المنظَّمة من مراجعة الأساسيات التي تحد من نقطة الدخول والأثر معًا: حماية البريد الإلكتروني، وتوعية المستخدمين، ومعرفة أماكن البيانات الحساسة، واختبار التعافي. وتقلل هذه الإجراءات التعرض للمخاطر سواء دُفعت فدية أم لا.

ما يجب فعله الآن

1. مراجعة ضوابط أمن البريد الإلكتروني وكشف التصيد على افتراض أن الرسائل ستكون محكمة الصياغة وخالية من الأخطاء اللغوية الواضحة.
2. تحديث برامج التوعية للتركيز على التحقق من الطلبات غير المعتادة بدلاً من البحث عن الأخطاء اللغوية.
3. تحديد أماكن تخزين البيانات الحساسة وتشديد الصلاحيات والمراقبة حولها.
4. اختبار استعادة النسخ الاحتياطية ودليل الاستجابة لهجمات الفدية، بما في ذلك آلية اتخاذ القرار بشأن طلبات الفدية.
5. متابعة الالتزام بضوابط الهيئة الوطنية للأمن السيبراني (ECC) وإطار الأمن السيبراني للبنك المركزي السعودي (SAMA CSF) المتعلقة بحماية البريد والبيانات والاستجابة للحوادث.