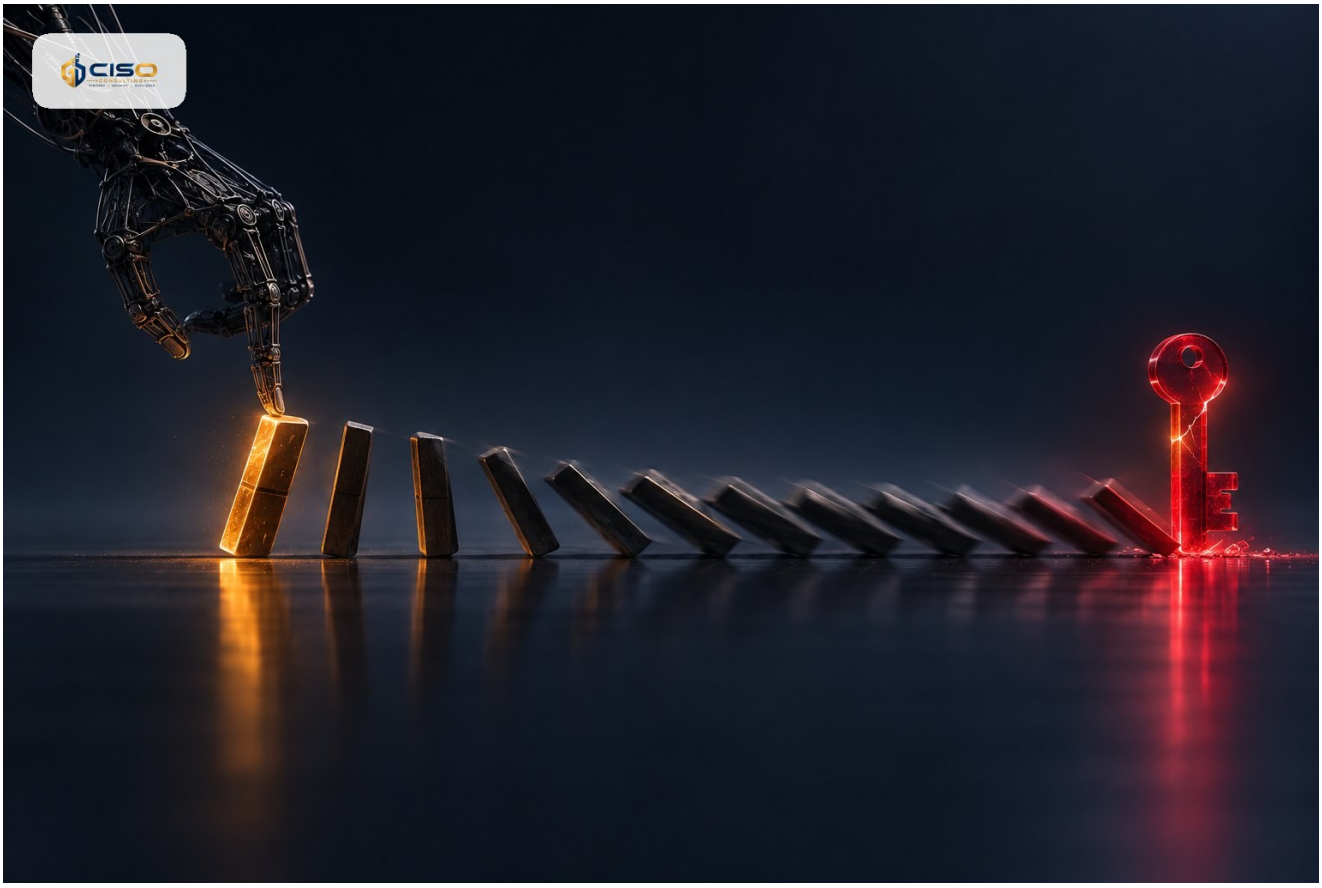
مكتب التحقيقات الفيدرالي يحذّر من إطار ARTEX للذكاء الاصطناعي الذي يؤتمت الهجمات حول العالم



يفيد مكتب التحقيقات الفيدرالي بأن جهات تهديد عدة تستخدم إطار ARTEX القائم على الذكاء الاصطناعي منذ أغسطس 2026 لتسريع الاختراقات، وأحيانًا للوصول إلى صلاحيات مرتفعة خلال أقل من ثلاث ساعات.

- تفيد نشرة FLASH الصادرة عن المكتب بأن ARTEX استُخدم منذ أغسطس 2026 على الأقل ضد جهات مالية وحكومية وتقنية ودفاعية وصحية وغيرها.
- ARTEX إطار مفتوح المصدر مكتوب بلغة Go، يرتبط بنماذج لغوية كبيرة خارجية ويوجّه وكلاء ذكاء اصطناعي للاستطلاع والاستغلال ورفع الصلاحيات وسرقة البيانات.
- وصلت بعض الاختراقات إلى صلاحيات مرتفعة في أقل من ثلاث ساعات، والأداة فعّالة خصوصًا ضد الأنظمة المهمَلة مثل بوابات الشركاء والخدمات القديمة وتكاملات الأطراف الثالثة.
- من الحالات المذكورة هجوم سلسلة التوريد على ConnectWise Cloud Backup الذي طال

مستأجري Microsoft 365، وهجمات على بنوك كورية جنوبية، وحملة المجموعة Vapor Panda.

- أُزيل المستودع الأصلي في أكتوبر، لكن النسخ المتفرعة والمؤرشفة والإصدار التجاري ARTEX PRO ما زالت متاحة.

أصدر مكتب التحقيقات الفيدرالي نشرة FLASH يحذّر فيها من استخدام جهات تهديد عدة لإطار ARTEX، وهو إطار اختبار اختراق مدعوم بالذكاء الاصطناعي، لأتمتة هجمات على جهات في قطاعات متعددة. ويقول المكتب إن إساءة استخدامه رُصدت منذ أغسطس 2026 على الأقل.

ما الذي يفعله ARTEX

ARTEX إطار مفتوح المصدر مكتوب بلغة Go، ولا يأتي بنموذج ذكاء اصطناعي خاص به، بل يرتبط بنماذج لغوية كبيرة خارجية منها Anthropic Claude وOpenAI GPT وDeepSeek وGLM وGrok وKimi. يحدد المشغّل أهدافه، فيحوّلها وكلاء ذكاء اصطناعي متخصصون إلى أوامر للاستطلاع واكتشاف الثغرات واستغلالها ورفع الصلاحيات وسرقة البيانات بأقل تدخل بشري.

ويشير المكتب إلى أن بعض الاختراقات انتقلت من الاستهداف الأولي إلى صلاحيات مرتفعة في أقل من ثلاث ساعات، وأن الأداة تتيح لجهات أقل خبرة تنفيذ عمليات معقدة ضد أهداف متعددة في وقت واحد. وهي فعّالة بوجه خاص في كشف الضعف في الأصول المهمَلة مثل بوابات الشركاء وتطبيقات الموظفين والخدمات القديمة وتكاملات الأطراف الثالثة.

الحوادث المذكورة وتوفر الأداة

تشير النشرة إلى هجوم سلسلة التوريد على ConnectWise Cloud Backup في أكتوبر، حيث استُخدمت هويات تطبيقات مخترقة للمصادقة إلى مستأجري Microsoft 365 لدى العملاء. ونسبت Microsoft الحملة إلى Storm-0940 التي استخدمت ARTEX في الاستطلاع وتخمين كلمات المرور وإساءة استخدام أذونات التطبيقات السحابية. كما تذكر هجمات على بنوك كورية جنوبية كشفت بيانات نحو 67,000 شخص، وتقرير CrowdStrike عن المجموعة Vapor Panda التي استهدفت أكثر من 200 جهة في 14 دولة.

أزال المطوّر مستودع GitHub الأصلي في 8 أكتوبر، لكن النسخ المتفرعة والمؤرشفة والمعرّبة، إضافة إلى الإصدار التجاري ARTEX PRO، لا تزال متاحة. وبحلول مطلع نوفمبر رصد باحثون أكثر من 1,600 وحدة تحكم ARTEX مكشوفة.

موارد الدفاع

تتضمن النشرة، ومدتها 13 صفحة، مؤشرات الاختراق، مع تنبيه المكتب إلى أن عناوين IP قد تكون تغيّرت. وأصدر الباحث MalwareMustDie حزمة كشف مفتوحة المصدر ودليل تعامل يصنّف المؤشرات بحسب درجة الثقة.

ما يجب فعله الآن

1. حصر التطبيقات المواجهة للإنترنت وبوابات الشركاء والخدمات القديمة وتكاملات الأطراف الثالثة، وإغلاق أو تقييد ما لا حاجة إليه.
2. تقييد الوصول إلى واجهات الإدارة السحابية ومراجعة أذونات التطبيقات في Microsoft 365 وغيرها من

البيئات السحابية، خاصة تطبيقات النسخ الاحتياطي والأطراف الثالثة.

3. مراجعة سجلات المصادقة بحثًا عن تخمين كلمات المرور وتغييرات غير متوقعة في بيانات الاعتماد أو الصلاحيات وتسجيلات دخول غير معتادة للتطبيقات.
4. تطبيق حدود للمعدّل على واجهات API الحساسة وإطلاق تنبيهات عند ارتفاع الطلبات الآلية أو نقل بيانات كبيرة.
5. إدخال مؤشرات الاختراق الصادرة عن FBI وقواعد الكشف الصادرة عن MalwareMustDie في أدوات المراقبة، مع التعامل مع مؤشرات IP على أنها مؤقتة والتحقق من الإنذارات الكاذبة.
6. إدراج سيناريوهات الاختراق المسرَّع بالذكاء الاصطناعي في خطط الاستجابة للحوادث، لأن وقت التفاعل قد لا يتجاوز ساعات.