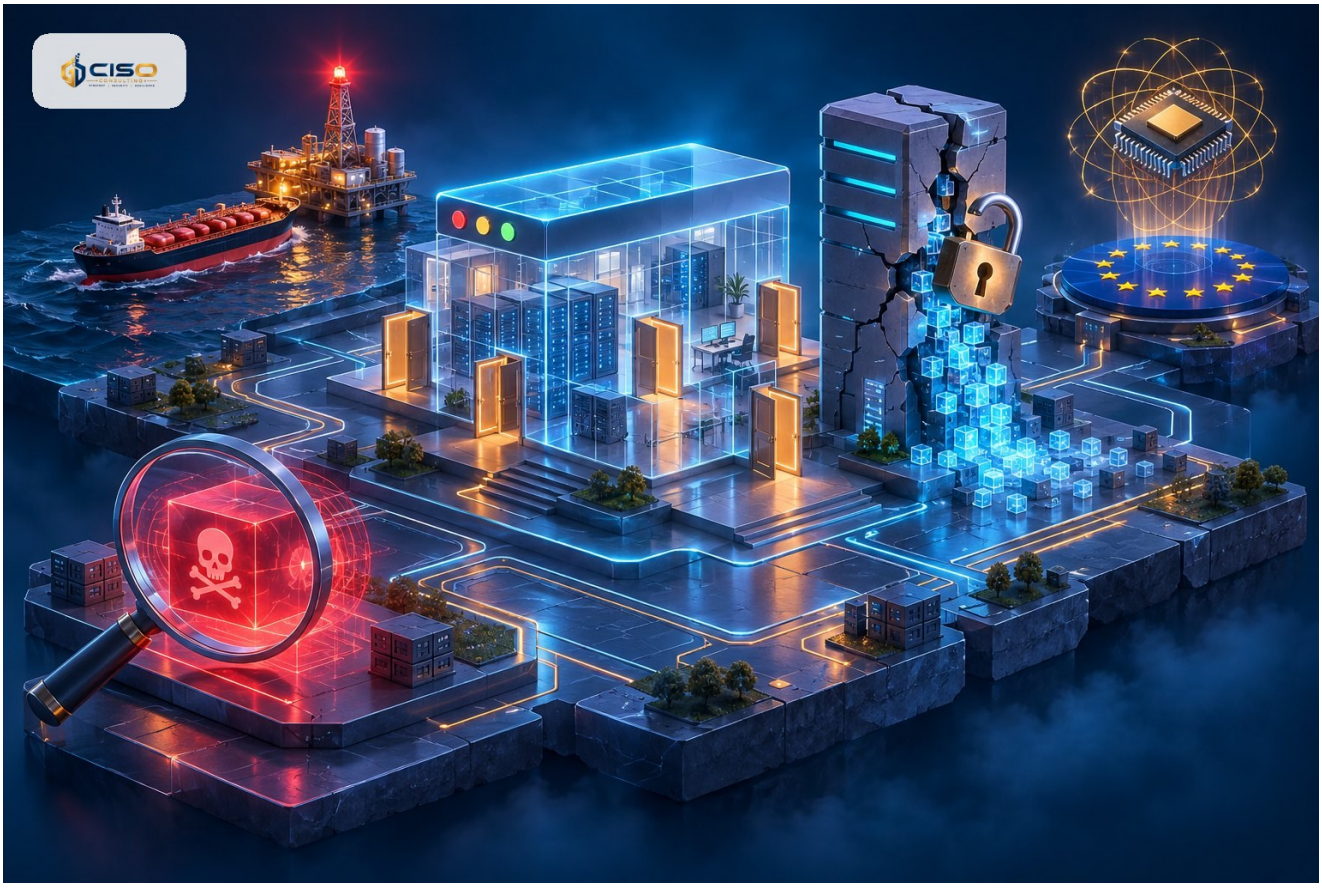
ملخص أسبوعي: مواقع مبنية بالذكاء الاصطناعي مكشوفة واختراق واجهة Radware وهجمات على ناقلات



يغطي ملخص SecurityWeek الأسبوعي مواقع ChatGPT Sites المكشوفة وواجهة Radware غير المحمية وأداة اختراق مدعومة بالذكاء الاصطناعي وقدرات VirusTotal الجديدة وقانون الكم الأوروبي، وفي ذلك دروس في الوصول والتشفير.

- رصدت Pluto عدد 16,666 موقعاً من ChatGPT Sites، منها 12,830 متاحاً للعموم، وثبت كشف بيانات حساسة لدى 27 جهة.
- أفادت تقارير باختراق Radware عبر واجهة إدارة Cloud WAF مكشوفة على الإنترنت، وقد تتأثر بيانات اتصال العملاء وبعض بيانات الاعتماد السحابية وSFTP.
- أفادت Microsoft باستخدام جهات مدعومة من دول ومجرمين الإطار Artex المعتمد على الذكاء الاصطناعي، وبلوغ صلاحيات مرتفعة وترسيخ الوجود خلال دقائق.
- يتضمن قانون الكم الأوروبي المقترح إجراءات لتسريع اعتماد التشفير المقاوم للحوسبة الكمية.

- أصدرت SolarWinds وAdobe تحديثات لثغرات حرجة في Serv-U وعدة منتجات.

يجمع ملخص SecurityWeek الأسبوعي أخباراً قد لا تنال تغطية مستقلة، ويهمّ عدد منها الجهات التي تعتمد على الخدمات السحابية والموردين الخارجيين وأدوات نقل الملفات.

كشف ناتج عن السهولة وواجهات الإدارة

حدد باحثو Pluto عدد 16,666 موقعاً أُنشئ عبر ChatGPT Sites، وهي خدمة تبني تطبيقات الويب وتستضيفها. وكان 12,830 منها متاحاً لأي شخص، وأكدت الفحوص اليدوية كشف بيانات حساسة لدى 27 جهة. وتكون المواقع مرئية لأصحابها ومديريها فقط افتراضياً، لكن يمكن للمالك فتحها على الإنترنت.

وفي خبر منفصل، يشير تقرير داخلي اطلعت عليه BleepingComputer إلى أن Radware تعرضت للاختراق عبر واجهة إدارة Cloud WAF غير محمية ومكشوفة على الإنترنت. وقد تكون بيانات اتصال العملاء وبيانات اعتماد AWS وAzure وتخزين SFTP لدى بعضهم قد تعرضت للخطر. ولم تعلّق الشركة.

مهاجمون أسرع وتحديثات مطلوبة

تفيد Microsoft بأن جهات مدعومة من دول، منها Salt Typhoon، ومجرمين يستخدمون إطار الاختبار الاختراقي Artex المعتمد على الذكاء الاصطناعي للعثور على أسرار مكشوفة في المستودعات العامة وتنفيذ هجمات سلاسل التوريد وتحديد الأنظمة الضعيفة. ويبلغ المهاجمون صلاحيات مرتفعة ويرسخون وجودهم خلال دقائق بحسب التقرير.

وأصدرت SolarWinds تحديثات لثغرات حرجة في Serv-U تشمل رفع الصلاحيات وتنفيذ شيفرة عشوائية. كما عالجت Adobe ثغرات حرجة في Campaign Classic وExperience Manager، إضافة إلى ثغرة حجب خدمة متوسطة الخطورة في InDesign.

مؤشرات بعيدة المدى

يتضمن قانون الكم الذي اقترحته المفوضية الأوروبية إجراءات لتسريع التشفير المقاوم للحوسبة الكمية. وأضافت VirusTotal كذلك كشفاً لبرمجيات الفدية يعتمد على رصد تشفير الملفات أثناء التحليل في بيئة معزولة.

يجمع هذه الأخبار أن الكشف العادي، لا الاستغلال المعقد، هو ما يفتح الباب غالباً. ومن الخطوات المناسبة مراجعة ما هو متاح للعموم.

ما يجب فعله الآن

1. حصر المواقع والتطبيقات المبنية بأدوات الذكاء الاصطناعي أو منخفضة الشيفرة، والتأكد من عدم مشاركتها علناً أو احتوائها على بيانات حساسة.
2. التحقق من عدم تعرض واجهات وأدوات الإدارة للإنترنت، وتقييدها بضوابط الشبكة والمصادقة القوية.
3. عند استخدام Radware Cloud WAF، متابعة إشعارات المورد والنظر في تدوير بيانات اعتماد AWS وAzure وSFTP ذات الصلة.
4. تطبيق تحديثات Serv-U ومنتجات Adobe المتأثرة سريعاً، مع البدء بالأنظمة المواجهة للإنترنت.

5. فحص المستودعات العامة بحثاً عن أسرار مكشوفة وتدوير ما يُعثر عليه.
6. إدراج التشفير المقاوم للحوسبة الكمية في حصر التشفير وخارطة الطريق.