



التكنولوجيا والتقنية المالية

18

أخبار الخارج

العدد (17754) - السنة الحادية والخمسون - الأحد 21 جمادى الأولى 1448هـ - 1 نوفمبر 2026م

الذكاء الاصطناعي
أنظمة البيانات
التحول الرقمي والتطوير

للتواصل: hello@array.world

إحدى شركات محفظة ممتلكات البحرين

الشركة الوطنية الرائدة في مجال
الذكاء الاصطناعي والبيانات



ماذا حدث في «بينانس».. وأين ذهبت أموال الناس؟!



نحو 150 حادثة اختراق عام 2025، بحسب تقرير «TRM» لجرائم العملات المشفرة. وقالت «بينانس» إنها ستنتشر تحليلاً فنياً مفصلاً بعد اكتمال التحقيق والتحقق من الحقائق.

تشاو، المؤسس الذي ترك منصب الرئيس التنفيذي، ما زال أكبر مساهم فيها، وقال: إن الواقعة تبدو اختراقاً وإنه يتوقع تغطية أموال المستخدمين بالكامل. وسرق مجرمو الإنترنت 2.87 مليار دولار من الأصول المشفرة في

في المنصات المركزية قد تضغط على الأسعار. ورأى «ستاندرد تشارترد» أن الحادث قد يدفع مزيداً من التداول نحو المنصات اللامركزية.

ولدى «بينانس» أكثر من 335 مليون مستخدم مسجل. وتشانغبينغ

بسهولة؛ ويحتفظ المهاجم بنحو 18270 بيتكوين وكميات ضخمة من الإيثر، بقيمة نحو 2.4 مليار دولار، وهي أصول لا يستطيع أي مُصدر تجميدها، بحسب «InvestmentNews». وباع نحو 325 مليون USDT عبر منصات لامركزية مقابل نحو 122300 إيثر.

كيف حدث الاختراق؟ قالت «بينانس»: إن تحقيقها الأولي يشير إلى أن الحادث قد يكون مرتبطاً بحاسوب محمول لمهندس DevOps مخترق، ما أتاح للمهاجم الوصول إلى الخدمة وتقديم طلبات سحب غير مصرح بها، وإنها لم تجد دليلاً على تسرب أي مفتاح خاص لمحفظة. لكنها قالت لاحقاً: إن التحقيق كشف «نقاط اختراق إضافية»، خلافاً للنتائج الأولية التي أشارت إلى حاسوب واحد، ووصفت الهجوم بأنه «معقد». وترى «TRM» أن الأدلة تشير إلى اختراق البنية التحتية التي توقع بها «بينانس» معاملات المحافظ الساخنة.

من المتهم؟ وقالت «TRM» بدرجة عالية من الثقة: إن مجموعة «TraderTraitor» المرتبطة بكوريا الشمالية، بذرت الهجوم. وقال المتحدث باسم «Chainal»

قالت «بينانس»، أكبر منصة لتداول العملات المشفرة في العالم: إن حادثاً أمنياً أدى إلى سرقة نحو 6.3 مليارات دولار، في ما يبدو أنه أكبر عملية سرقة من نوعها على الإطلاق. وتعهدت المنصة بتحمل جميع الخسائر.

وبحسب شركة «TRM Labs»، خرج نحو 6.36 مليارات دولار من محافظ تابعة للمنصة على عشر شبكات بلوكتشين، معظمه خلال نحو 20 دقيقة بدءاً من الساعة 20:05 بتوقيت غرينتش مساء الخميس. وتنفق قيمة السرقة بنحو أربعة أضعاف اختراق منصة Bybit الذي بلغ 1.5 مليار دولار في 2025، وقد نسبته مكتب التحقيقات الفيدرالي الأميركي إلى بيونغ يانغ. وقالت «بينانس»: إن نحو ثلاثة مليارات دولار جُمِدت على البلوكتشين حتى الآن. وقال باولو أردوينو، الرئيس التنفيذي لشركة «تيثر»: إن شركته جُمِدت نحو 1.6 مليار دولار تتعلق بالواقعة.

وأعلن مجلس الأمن في شبكة «Arbitrum» تجميد 30.5 مليون دولار، فيما جُمِدَ بروتوكول الإقراض «Aave» أسواقه كإجراء احترازي. أما ما تبقى فلا يمكن تجميده

آليات التزييف الدفاعي: رصد الفبركة الرقمية عبر خوارزميات التعلم العميق

النمط وتظهر فجوات تقنية غير مرئية تكشفها خوارزميات الفحص الذكية بسرعة.

ثالثاً: آلية عمل التطبيقات الذكية

(الذكاء الاصطناعي الدفاعي)

تعتمد التطبيقات الحديثة في جوهرها على نموذج تقني يُعرف بالذكاء الاصطناعي الدفاعي، حيث يتم تدريب الخوارزميات بشكل مكثف على ملايين الصور والفيديوهات الحقيقية والمزيفة معاً لرفع كفاءتها. تتعلم البرمجيات من خلال هذا التدريب كيفية استخراج «البصمة الرقمية» أو التوقيع الاصطناعي الخاص بالنماذج التوليدية الشهيرة. فعندما يقوم أي برنامج بتوليد صورة، تترك تلك الشبكة العصبية أثراً رياضياً دقيقاً في شيفرة الصورة، تماماً مثل بصمة الإصبع أو خط اليد البشري. تستطيع التطبيقات الدفاعية مطابقة هذا الأثر بدقة وتحديد البرنامج الدقيق المستخدم في عملية التزييف. علاوة على ذلك، بدأت بعض التطبيقات المتقدمة في دمج تقنيات التشفير وسلسلة الكتل (Blockchain) للتحقق من سلسلة التوريد الرقمية للملف الأصلي وتتبع تاريخ إنشائه وتعديله منذ اللحظة الأولى.

رابعاً: تحديات مواجهة الرقمية المستمرة

على الرغم من الكفاءة العالية والدقة الكبيرة لتطبيقات الكشف الذكية، إلا أنها تواجه تحدياً مستمراً ومستداماً يُعرف في الأوساط التقنية بـ«لعبة القط والفأر». فكلما تطورت خوارزميات الكشف الدفاعية ورصدت نقطة ضعف أو ثغرة معينة في المحتوى المزور، سارع مطورو برامج التزييف والتوليد إلى تحديث أنظمتهم وهندستها لتلافي هذا الخطأ في المرات القادمة. هذا التنافس المحموم يفرض على برمجيات الأمن السيبراني التطوير الذاتي المستمر والاعتماد على التعلم العميق للبقاء خطوة للأمام دائماً. بالإضافة إلى ذلك، فإن عمليات ضغط الملفات وهندستها عند رفعها على منصات التواصل الاجتماعي المختلفة تؤدي أحياناً إلى تلف البيانات الرقمية الدقيقة، مما يزيد من صعوبة مهمة التطبيقات في إجراء الفحص البكسلي بدقة كاملة.

في الختام، إن مواجهة التزييف الرقمي باستعمال التكنولوجيا لم تعد مجرد خيار تقني رفاهي، بل تحولت إلى حتمية أمنية واجتماعية لحماية المجتمعات. توفر تطبيقات الذكاء الاصطناعي اليوم جدار حماية قسوي للغاية قادم وقادر على تحليل التناقضات الحيوية والبصرية بدقة متناهية وسرعة فائقة. ومع ذلك، يبقى دمج هذه البرمجيات الذكية مع الوعي البشري النقدي والتحقق المستمر من المصادر الرسمية هو السبيل الأمثل والضمانة الحقيقية لانتصار الحقيقة وضمان بيئة رقمية موثوقة وأمنة للجميع في المستقبل.



بـقلم:

د. جاسم حاجي

أولاً: تقنيات الكشف في مقاطع

الفيديو المزيفة

تتعتمد تطبيقات كشف التزييف في الفيديو على رصد التناقضات الفيزيائية والحيوية الدقيقة التي تعجز برامج التزييف والتوليد عن ضبطها بدقة كاملة. من أبرز هذه الطرق العلمية فحص النضج الحيوي والتدفق الدموي للأشخاص؛ حيث يمكن للذكاء الاصطناعي تحليل التغيرات اللونية الطفيفة جداً في جلد الوجه الناتجة عن تدفق الدم مع ضربات القلب، وهي تفاصيل بيولوجية معقدة لا تظهر في الفيديوهات المبركة. بالإضافة إلى ذلك، تقوم التطبيقات بمراقبة وتحليل معدل رمش العين وحركتها البؤرية بدقة، فالأشخاص المزيفون رقمياً غالباً ما يرمشون بمعدلات غير طبيعية أو تفتقر عيونهم إلى الانعكاسات الضوئية الحقيقية التي تحاكي البيئة المحيطة بهم. كما يُعد تحليل التزامن الحركي واللفظي محورياً أساسياً في هذه العملية، حيث تدقق الخوارزميات الذكية في مطابقة حركة الشفاه وعضلات الوجه مع الترددات الصوتية المصاحبة لرصد أي تأخير زمني أو تشويه خفي يكشف الفبركة.

ثانياً: خوارزميات تحليل الصور المزورة

في عالم الصور الفابرة، تركز التطبيقات الذكية على فحص العناصر الهيكلية والبكسلية المعقدة للملف. تُستخدم في هذا السياق شبكات عصبية متطورة للغاية يطلق عليها «الشبكات العصبية الانتقافية» (CNN) لتحليل الأنماط المجهرية للصور وتوزيع الألوان. تبحث هذه التطبيقات بذكاء عن عدم الاتساق في توزيع الإضاءة والظلال؛ فإذا كان الضوء القادم على وجه الشخص لا يتطابق هندسياً مع زاوية سقوط الظل على الخلفية أو الأجسام المجاورة، يكشف النظام التزييف فوراً. كذلك، تفحص الخوارزميات حواف الأجسام المقصودة أو المدمجة، حيث تترك البرامج التقليدية أو التوليدية حوافاً ناعمة بشكل مفرط أو مشوهة هندسياً بشكل غير طبيعي نتيجة لعمليات الدمج. ومن الوسائل التقنية المتقدمة أيضاً فحص «الضوضاء الرقمية» للبكسلات (Sensor Noise)، إذ إن كل كاميرا حقيقية تترك نمط ضوضاء فريد ومستمر على الصورة بأكملها، وعند تعديل جزء من الصورة أو توليده رقمياً، ينقطع هذا



SPECTRUM AI™ OCR & AGENTIC RAG MODEL

المركز الأول عالمياً لمدة 30 أسبوعاً متتالياً ضمن فئة النماذج مفتوحة الأوزان



للتواصل: hello@array.world

ARRAY INNOVATION
الرائد الوطني للبيانات والذكاء الاصطناعي