جرائم التشفير تتجاوز ال (41) مليار دولار خلال العام الماضي

شهد العام 2024 أكبر تدفق للأموال إلى الجهات غير القانونية، عبر العملات المُشفرة بحسب تقرير لمؤسسة تحليلات العملات المُشفرة "Chainanalysis"، التي أكدت أن جرائم التشفير وصلت إلى "51.3" مليار دولار، لتجاوز خلال آخر 5 سنوات نحو "189" مليار دولار.

وذلك رغم أن تقديراتها التي حصرتها حتى الآن للمبالغ المُرسلة للحسابات غير القانونية خلال العام الماضي تقتصر على "40.9" مليار دولار، وذلك في ظل تتبعها فقط العناوين غير القانونية التي تمكنت من التعرف عليها حتى الآن.

ومن بين تلك المبالغ المُثبتة تم تحويل "10.8" مليار دولار إلى المحافظ التابعة للخدمات والأفراد الذين يرتكبون الجرائم الإلكترونية مباشرةً، مثل القرصنة والابتزاز والاحتيال، بالإضافة إلى أولئك الذين يسهلون هذه الأنشطة من خلال بيع البنية التحتية والأدوات اللازمة.

وقالت المؤسسة في تقرير لها، إن:""في السنوات الأخيرة، أصبحت العملات المشفرة أكثر انتشاراً

وشيوعاً، وعلى الرغم من أن النشاط غير القانوني في سلاسل الكتل كان يركز في السابق بشكل كبير على الجرائم الإلكترونية، إلا أن العملات المُشفرة تُستخدم الآن أيضًا لتمويل وتسهيل جميع أنواع التهديدات، بدءاً من الأمن القومي وحتى حماية المستهلك".

ومع ازدياد قبول العملات المشفرة، أصبح النشاط غير القانوني على سلاسل الكتل أكثر تنوعاً، فهناك بعض الجهات غير القانونية التي تعمل أساسًا خارج السلسلة ولكنها تنقل إليها الأموال لغسلها.

وأشارت إلى أن:"نسبة المعاملات غير القانونية لإجمالي العمليات على سلسلة الكتل تراجعت إلى 0.14% من 0.61% في 2023، لكنها توقعت ارتفاع تلك النسب مع مراجعة قيم العمليات غير المشروعة، لكنها توقعت أن تبقى أقل من 1% كما كان الحال تاريخياً".

أبرز الاتجاهات

وقالت المؤسسة إن:"الكيانات الخاضعة للعقوبات، بما في ذلك الأفراد الذين يعملون في ولايات خاضعة للعقوبات، غالبًا ما تكون لديها حوافز أكبر لاستخدام العملات المستقرة بسبب التحديات في الوصول إلى الدولار الأميركي عبر الوسائل التقليدية، مع رغبتها في الاستفادة من استقرار الدولار".

وأشارت إلـ:"ارتفاع حجم الأموال المسروقة بنسبة 21% مقارنة بالعام السابق لتصل إلى "2.2" مليار دولار، على الرغم من أن الحصة الأكبر من الأموال المسروقة جاءت من خدمات التمويل اللامركزي (DeFi)، إلا أن الخدمات المركزية كانت الأكثر استهدافًا في الربعين الثاني والثالث من العام".

واستحوذت الهجمات الإلكترونية من قبل القراصنة الكوريين الشماليين على أكثر من أي وقت مضى، حيث تم سرقة "1.34" مليار دولار، ما يمثل 61% من إجمالي المبالغ المسروقة خلال العام.

كما وأشارت إلى أن:"بعض هذه الهجمات تبدو مرتبطة بعاملين في مجال تكنولوجيا المعلومات من كوريا الشمالية، الذين يتسللون إلى شركات العملات المشفرة وشبكات Web3، مستخدمين تقنيات متطورة".

وشهد عام 2024 انتشاراً كبيراً للاحتيال عالي ومنخفض التقنية، حيث كانت عمليات الاحتيال الاستثمارية ذات العوائد المرتفعة وعمليات الاحتيال المعروفة باسم "ذبح الخنازير" من بين الأنواع الأكثر نجاحاً.

ولوحظ الاستخدام المتزايد للذكاء الاصطناعي في مجال الاحتيال، ويتماشى هذا الاستخدام مع اتجاه أوسع عبر مجموعة من الجرائم الإلكترونية، حيث ظهرت خدمات تستخدم الذكاء الاصطناعي لتجاوز متطلبات "اعرف عميلك" (KYC)، بحسب المؤسسة.

وذكرت أن:"عمليات الاحتيال المتعلقة بأجهزة الصراف الآلي للعملات الرقمية أصبحت مصدر قلق متزايد، خاصة فيما يتعلق بكبار السن".

الفدية والدارك ويب

على الرغم من أن برامج الفدية لا تزال تحقق إيرادات بمئات الملايين من الدولارات، فإن التدخلات المتعددة من قبل وكالات إنفاذ القانون وتراجع رغبة الضحايا في دفع الفدية قد أثرت عليها.

ومع ذلك، كان عام 2024 عاماً نشطاً، حيث استمرت الهجمات بمعدلات عالية، وتمكنت بعض مجموعات برامج الفدية من تحقيق مدفوعات، ولكن بمبالغ أقل.

توقعات المستقبل

على صعيد "دارك ويب" تراجعت إيراداته إلى 2 مليار دولار مقارنةً بـ 2.3 مليار دولار تقريبًا في عام 2023، بينما انخفضت إيرادات مواقع الاحتيال بأكثر من النصف لتصل إلى 220.1 مليون دولار.

ويُعزى هذا الانخفاض الكبير جزئيًا إلى عملية مشتركة بين الولايات المتحدة وهولندا استهدفت نظام الدفع المجهول "UAPS"، وهو معالج مدفوعات بالعملات المشفرة دعم مئات مواقع الاحتيال.

مع تطور النظام التشغيلي للعملات المشفرة، تتطور أيضًا أساليب المجرمين، فمن المتوقع أن يشهد المستقبل مزيداً من التنوع في الجرائم المشفرة، بالإضافة إلى زيادة استخدام التكنولوجيا المتقدمة مثل الذكاء الاصطناعي لتحسين تكتيكات الاحتيال والاختراق.