متداول يخسر "70" مليون دولار بعد إرسال العملات المشفرة لعنوان حساب خاطئ

افادت تقارير بأن "أحد تجار العملات المشفرة خسر عشرات الملايين من الدولارات في ما يسمى بعملية احتيال "تسميم العناوين". يتم تنفيذ عمليات احتيال تسميم العناوين من قبل اللصوص الذين يقومون بإنشاء حسابات محاكاة ساخرة لعنوان التشفير عبر الإنترنت الخاص بضحيتهم، والتي يستخدمونها لإرسال مبلغ صغير من العملة إلى الضحية على أمل أن يرسلوا الأموال عن طريق الخطأ إلى العنوان المزيف لاحقًا، وفقًا لمنصة تداول العملات المشفرة "Transak".

ونظرًا لأن سلاسل الكتل "بلوكتشين" عامة فمن السهل على المحتالين العثور على عناوين العملات المشفرة الخاصة بالأشخاص وإرسال معاملات وهمية للتصيد الاحتيالي للضحايا.

وأكدت شركة سيرتك "CertiK"، وهي شركة أمنية تعمل بتقنية blockchain، في منشور على موقع "إكس" أنها اكتشفت تحويلًا بقيمة "69.3" مليون دولار من عملة بيتكوين إلى عنوان "مرتبط بتسميم العنوان".

وتُظهر محفظة العملات المشفرة الخاصة بالضحية الآن خسارة إجمالية تبلغ حوالي 97% من أصولها في منصة Coinbase. قيمة تبلغ الحساب الآن أكثر من "1.6" مليون دولار.

وكتبت شركة "PeckShield"، وهي شركة أمنية أخرى، على موقع إكس أن: "المحتالين استبدلوا عملة بيتكوين المسروقة مقابل 23000 إيثريوم ثم قاموا بتحويل الأموال. وقالت صحيفة ديلي هودل إنه يتم تداول إيثريوم بسعر 3116 دولارًا للعملة المعدنية".

وتوصي "Trezor"، وهي منصة أخرى لتداول العملات المشفرة، بالتحقق مرة أخرى من كل عنوان قبل إرسال المعاملة وعدم نسخ عنوان من سجل المعاملات مطلقًا عند تحويل الأموال لتجنب عمليات الاحتيال على العناوين.

وتقول الشركة إن: "إرسال معاملة اختبارية صغيرة قبل إجراء تحويل كبير يعد أيضًا وسيلة فعالة للتحقق من العنوان".

وتتزايد عمليات الاحتيال المتعلقة بالعملات المشفرة، وفقًا لتقرير مكتب التحقيقات الفيدرالي عن جرائم الإنترنت لعام 2023. يقول التقرير إن الاحتيال المرتبط بالعملات المشفرة كلف المستثمرين "3.94" مليار دولار في العام الماضي، وهو ما يشكل أكثر من ثلاثة أرباع خسائر الاحتيال الاستثماري لهذا العام.

ووجدت إحدى الدراسات أن "عمليات الاحتيال المتعلقة بالعملات المشفرة أو ما تسمى بـ"ذبح الخنازير" كلفت المستثمرين "75" مليون دولار من عام 2020 إلى عام 2024. ويبدأ الاحتيال بإرسال المجرمين رسالة نصية برقم خاطئ يستخدمونها كوسيلة لبناء الثقة مع الضحايا".

ويرسل المحتالون دفعات صغيرة إلى الضحية ويجذبونهم إلى القيام باستثمارات مزيفة في العملات المشفرة، ثم يقطعون الاتصال بمجرد أن يرسل الضحية مبلغًا كبيرًا من المال إلى اللص.

ويشير اسم عملية الاحتيال إلى "تسمين الخنزير قبل ذبحه".

وتتضمن معظم عمليات الاحتيال في العملات المشفرة محتالين يحاولون إيقاع الضحايا في عمليات احتيال غير ذات صلة بالدفع لهم بعملة بيتكوين حتى لا يمكن تعقب جرائمهم، وفقًا للجنة التجارة الفيدرالية.

وتقول الوكالة إن: "أفضل طريقة لاكتشاف عمليات احتيال العملات المشفرة هي عدم الثقة أبدًا في أي شخص لن يقبل الدفع إلا بالعملات المشفرة أو الذي يعد بعوائد ربح كبيرة على استثمار مريب".

وتقول لجنة التجارة الفيدرالية: "تعد عمليات الاحتيال الاستثماري إحدى أفضل الطرق التي يخدعك بها المحتالون لشراء العملات المشفرة وإرسالها إلى المحتالين". "لكن المحتالين ينتحلون أيضًا صفة الشركات والوكالات الحكومية والاهتمامات العاطفية، من بين تكتيكات أخرى".