OVATION
AMERICAS

Infolettre Mars 2022

CRYPTO-MONNAIE CONFIDENTIALITÉ & SÉCURITÉ Protégez vos actifs (Partie1)

Les revenus de l'escroquerie cryptographique en 2021 ont dépassé 7,7 milliards de dollars, en hausse de 81% par rapport à 2020, selon la plate-forme de données blockchain Chainalysis.

La confidentialité et la sécurité de votre portefeuille cryptographique sont une partie cruciale de la façon dont vous réussirez à

investir dans la cryptographie. Une fois que vous détenez votre crypto-monnaie dans des portefeuilles, vous devez être conscient que tous les types de portefeuilles cryptographiques - même les portefeuilles de disque dur les plus sécurisés - sont exposés à un certain risque d'être piratés et drainés. Bien que la technologie blockchain soit conçue pour être extrêmement sécurisée et qu'une base de données blockchain soit presque impossible à pirater, des erreurs humaines et des risques physiques existent toujours. Les risques peuvent varier et changer constamment, mais voici quelques-unes des façons les plus largement vues de perdre toutes vos cryptos du jour au lendemain.

Logiciels malveillants de vol de clés

Un logiciel malveillant voleur de clés analyse le disque dur de votre ordinateur ou de votre appareil mobile à la recherche de vos clés privées cryptographiques. Un logiciel malveillant voleur de clés peut pénétrer dans votre appareil lorsque vous visitez des sites Web douteux, suivez des liens d'escrocs, ouvrez des pièces jointes non sécurisées ou téléchargez des logiciels à partir de sources non fiables. Une fois que vous avez téléchargé un logiciel malveillant voleur de clés sur votre ordinateur ou un appareil mobile, il analyse instantanément les disques durs à la recherche de vos clés privées cryptographiques et les transmet à un pirate. Si vous ne sécurisez pas vos portefeuilles cryptographiques avec une authentification à deux facteurs en plus de la clé, la personne contrôlant le logiciel malveillant aura désormais accès à vos

comptes et pourra transférer vos avoirs en quelques secondes.

Trojan

Un trojan ou cheval de Troie est un autre type de logiciel malveillant de vol de crypto. Les chevaux de Troie ne « volent » pas réellement vos crypto-monnaies, mais scannent vos disques durs pour la quantité exacte de cryptos que vous possédez. Ensuite, ils chiffrent malicieusement vos disques durs et vous envoient des e-mails et affichent des messages pour demander des rançons. Même les échanges bien protégés peuvent rencontrer de tels ransomwares, et parfois les utilisateurs n'ont pas d'autre moyen de faire face au dilemme lorsque le ransomware menace de formater les disques durs si les utilisateurs ne paient pas la rançon dans un certain laps de temps.

Arnaque de sortie

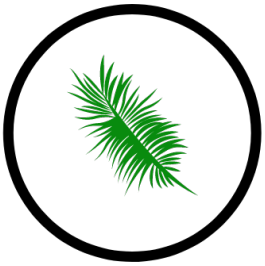
Une arnaque de sortie fait référence au moment où les bourses, les intermédiaires ou les gestionnaires disparaissent avec l'argent des investisseurs. C'est une version cryptographique d'une vieille astuce de confiance qui existe depuis des siècles. Dans le passé, les gestionnaires de fonds ou les fondateurs de startups pouvaient s'enfuir avec l'argent des investisseurs. Dans l'industrie de la cryptographie, les échanges peuvent disparaître avec les dépôts de leurs utilisateurs; les gestionnaires ou les propriétaires de projets cryptographiques pourraient s'enfuir avec les fonds collectés lors d'une offre initiale de pièces de monnaie (ICO). En raison de la nature décentralisée et anonyme du monde de la cryptographie et des

cadres réglementaires limités, il peut être plus difficile de retracer les escrocs et de récupérer les fonds par rapport aux escroqueries traditionnelles. Les escroqueries de sortie ont lieu fréquemment, les utilisateurs doivent apprendre à repérer les escroqueries potentielles avant de faire des investissements cryptographiques.

Phishing

Une attaque de phishing est généralement menée via des e-mails, des messages ou des médias sociaux. Vous pouvez recevoir un e-mail ou un message vous demandant de prendre des mesures, notamment l'envoi de votre code d'authentification, de votre mot de passe, de votre numéro de carte de crédit ou d'autres informations d'identification. Cependant, l'e-mail n'est pas légitime ou ne tente pas d'usurper l'identité de quelqu'un d'autre. Si vous répondez à ces e-mails de phishing et leur donnez des informations, vos avoirs cryptographiques peuvent être volés. Ne faites pas confiance à quiconque vous demande vos informations d'identification et vos mots de passe.

Perte des appareils



Après tout, il y a la façon démodée de perdre vos biens – de perdre littéralement vos appareils mobiles (ou ordinateurs portables). Toute personne qui trouve votre appareil ou le vole physiquement peut également tenter de le déverrouiller. S'ils réussissent à déverrouiller votre appareil, ils peuvent accéder à vos avoirs cryptographiques stockés dans les portefeuilles de cet appareil, ainsi qu'à vos comptes bancaires, e-mails, mots de passe, comptes de

médias sociaux et tout ce qui a de la valeur connecté à votre appareil.

Comment protéger et sécuriser vos avoirs

1. Prenez des mesures de sécurité Internet de base. Utilisez des mots de passe forts et mis à jour. Ne visitez pas de sites suspects et ne cliquez pas sur des liens suspects. N'utilisez pas le « WiFi gratuit ». Utilisez des outils de sécurité Internet tels que des programmes antivirus et des VPN. Activez l'authentification à 2 facteurs pour tous vos comptes.

2. Rappelez-vous que vous êtes le maillon faible. En fait, pirater le code d'une blockchain ou passer à travers le système de sécurité d'un site Web est très difficile et nécessite des compétences spécialisées que la plupart des criminels ne possèdent pas. Il est beaucoup plus facile pour un voleur d'usurper l'identité d'une partie de confiance ou de vous envoyer des liens compromis dans l'espoir que vous cliquerez dessus.

3. Soyez toujours prudent et revérifiez chaque notification que vous recevez. La prudence vous éloigne des promoteurs cryptographiques douteux, des échanges suspects qui peuvent disparaître à tout moment, des e-mails et des messages de phishing, etc. Choisissez judicieusement vos sources de téléchargement de logiciels et d'applications - les sites Web officiels et les magasins comme l'App Store d'Apple peuvent être un bon choix (bien que le Google Play Store ait été identifié comme

une source majeure de logiciels malveillants Android). Si un rappel apparaît lorsque vous essayez d'accéder ou de télécharger quoi que ce soit, lisez le rappel et réfléchissez à la question de savoir si vous souhaitez toujours accéder et télécharger ce que vous avez prévu.

4. Compte tenu de tous les risques et escroqueries mentionnés ci-dessus, il est préférable de contrôler votre propre portefeuille stocké localement avec une application logicielle open source qui stocke, accepte et transmet des monnaies virtuelles directement à partir de votre ordinateur, l'une des options les plus sûres pour sécuriser vos actifs de crypto-monnaie. Lorsque votre portefeuille est déconnecté d'Internet, aucun pirate ne peut le voir et l'attaquer directement. La sécurité cryptographique est une question de bonnes habitudes personnelles.

   On estime que 23% de toutes les crypto-monnaies ont été perdues en raison de portefeuilles inaccessibles, si vous supprimez le fichier ou perdez l'accès, vous avez perdu votre argent à l'intérieur. Veuillez ne pas faire partie de cette statistique. Nous considérons les monnaies virtuelles comme un outil parmi d'autres pour protéger la confidentialité ou l'anonymat en ligne et jamais un investissement. Dans l'ensemble, la plupart de nos clients n'en ont aucune utilité.

Continuons à apprendre et restez à jour sur les questions de cybersécurité pour nous donner les meilleures chances d'éviter les piratages et les escroqueries coûteux.

OVATION
AMERICAS