Les stratagèmes d'ingénierie sociale liés aux cryptomonnaies ont rapporté aux cybercriminels près de 10 millions de dollars l'an passé

9 juillet 2018

Les experts de Kaspersky Lab ont mis à jour un type de fraude relativement nouveau : le développement des cryptomonnaies n'attire pas seulement les investisseurs mais aussi des cybercriminels poussés par l'appât du gain. Au cours du premier semestre 2018, les produits de la société ont bloqué plus de 100 000 événements déclencheurs liés à des cryptomonnaies, sur de faux sites et d'autres plateformes. Chacune de ces tentatives visait à leurrer un nombre croissant d'utilisateurs crédules par des stratagèmes frauduleux.

Le phénomène des cryptomonnaies et l'engouement qu'elles suscitent ne sont pas passés inaperçus des cybercriminels. Pour réaliser leurs noirs desseins, ceux-ci emploient généralement des techniques classiques de phishing mais vont souvent au-delà des scénarios « ordinaires » que nous connaissons. En s'inspirant des investissements ICO (*Initial Coin Offering*) et de la distribution gratuite de cryptomonnaies, les cybercriminels ont pu abuser aussi bien de l'avidité des détenteurs de monnaie virtuelle que de la naïveté des néophytes.

Certaines des cibles plus prisées sont les investisseurs ICO, qui cherchent à placer leur argent dans des start-ups dans l'espoir d'en tirer profit à l'avenir. A leur intention, des cybercriminels créent de fausses pages web imitant les sites de projets ICO officiels ou bien tentent d'accéder à leurs contacts de façon à pouvoir diffuser un message de phishing contenant le numéro d'un e-portefeuille et incitant les investisseurs à y envoyer leurs cryptomonnaies. Les attaques les plus fructueuses se servent de projets ICO bien connus. Par exemple, en exploitant l'ICO Switcheo au moyen d'une proposition de distribution gratuite de cryptomonnaies, des malfaiteurs ont dérobé l'équivalent de plus de 25 000 dollars après avoir propagé un lien via un faux compte Twitter.

Autre exemple, la création de sites de phishing pour le projet ICO OmaseGo a permis à des escrocs d'empocher plus de 1,1 million de dollars dans cette cryptomonnaie. Les cybercriminels ont été tout aussi intéressés par les rumeurs entourant l'ICO Telegram, ce qui a eu pour effet l'apparition de centaines de sites factices destinés à recueillir de prétendus « investissements ».

Une autre tendance répandue porte sur des escroqueries aux faux dons de cryptomonnaie. La méthode la plus courante consiste à demander aux victimes de faire cadeau d'une petite somme en monnaie virtuelle, en leur faisant miroiter un gain bien plus élevé dans cette même monnaie à l'avenir. Les malfrats vont même jusqu'à utiliser les comptes de personnalités réputées sur les réseaux sociaux, telles que l'homme d'affaires Elon Musk ou le fondateur de la messagerie Telegram, Pavel Durov. En créant de faux comptes et en s'en servant pour répondre aux tweets d'utilisateurs de bonne foi, les escrocs réussissent à tromper des internautes.

Selon les estimations approximatives de Kaspersky Lab, des cybercriminels seraient parvenus l'an dernier à engranger plus de 21 000 ETH (la cryptomonnaie Ether, qui utilise la blockchain générée par la plate-forme Ethereum), soit plus de 10 millions de dollars au cours actuel, grâce aux stratagèmes que nous venons de décrire. Cette somme ne tient même pas compte des attaques de phishing classiques ou des cas de génération d'une adresse individuelle pour chaque victime.

« *Notre étude révèle que les cybercriminels sont passés maîtres dans l'art d'actualiser et de développer leurs ressources afin d'obtenir un maximum de résultats de leurs attaques de phishing liées aux cryptomonnaies. Ces nouveaux stratagèmes de fraude reposent sur des méthodes élémentaires d'ingénierie sociale mais se distinguent des attaques de phishing habituelles car ils peuvent rapporter des millions de dollars à leurs auteurs. Les succès obtenus par ces escrocs donnent à penser qu'ils savent comment exploiter le facteur humain, l'un des éternels maillons faibles de la cybersécurité, pour profiter du comportement des utilisateurs* », commente Nadezhda Demidova, analyste en contenus web chez Kaspersky Lab.

Les chercheurs de Kaspersky Lab conseillent aux utilisateurs d'observer quelques règles élémentaires afin de protéger leurs avoirs en cryptomonnaie :

- Rappelez-vous que rien n'est jamais gratuit et que les offres qui paraissent trop belles pour être vraies doivent être traitées avec scepticisme.
- Vérifiez auprès de sources officielles les informations concernant la distribution gratuite de cryptomonnaies. Par exemple, si vous remarquez une distribution pour le compte de l'écosystème de blockchain Binance, piraté récemment, rendez-vous sur le site officiel pour y obtenir des éclaircissements.
- Vérifiez si des tiers sont liés au portefeuille vers lequel vous envisagez de transférer vos économies. L'une des solutions consiste à faire appel à des navigateurs de blockchain, tels que etherscan.io ou blockchain.info, qui permettent aux utilisateurs de visualiser des informations détaillées sur toute transaction en cryptomonnaie et de déterminer si le portefeuille risque d'être dangereux.
- Vérifiez toujours les liens et données affichés dans la barre d'adresse du navigateur, par exemple que vous y lisez bien « blockchain.info », et non « blackchaen.info ».
- Conservez l'adresse de votre e-portefeuille dans un onglet et accédez-y depuis ce dernier, ce qui évitera une erreur de saisie dans la barre d'adresse, susceptible de vous faire aboutir accidentellement à un site de phishing.

Pour en savoir plus sur le développement du phishing dans le domaine des cryptomonnaies, consultez notre blog sur Securelist.com.

À propos de Kaspersky Lab

Kaspersky Lab est une société de cybersécurité mondiale qui est active sur le marché depuis plus de 20 ans. L'expertise de Kaspersky Lab en matière de « Threat Intelligence » et sécurité informatique vient perpétuellement enrichir la création de solutions et de services de sécurité pour protéger les entreprises, les infrastructures critiques, les gouvernements et les consommateurs à travers le monde. Le large portefeuille de solutions de sécurité de Kaspersky Lab comprend la protection avancée et complète des terminaux et un certain nombre de solutions et de services de sécurité dédiés afin de lutter contre les menaces digitales sophistiquées et en constante évolution. Les technologies de Kaspersky Lab aident plus de 400 millions d'utilisateurs et 270 000 clients à protéger ce qui compte le plus pour eux.

Pour en savoir plus : www.kaspersky.com/fr/

Pour plus d'informations sur l'actualité virale : http://www.securelist.com

Salle de presse virtuelle Kaspersky Lab : http://newsroom.kaspersky.eu/fr/

Blog français de Kaspersky Lab : http://blog.kaspersky.fr/

Hotwire pour Kaspersky Lab

Marion Delmas / Séverine Randjelovic / Noémie Minster / Aliénor Gamerdinger

01 43 12 55 62 / 57 / 73 / 47

KasperskyFrance@hotwireglobal.com