

# Une arnaque mondiale aux cryptomonnaies démasquée

L'ONG européenne Check First a ouvert le capot des arnaques polluant Facebook. Elle a découvert une machinerie impliquant un réseau tentaculaire et qui peut coûter cher aux plus crédules.

PHILIPPE LALOUX

Incroyable, Alexander De Croo ne savait pas que la caméra tournait encore quand il a dévoilé son secret pour faire fortune ! » « Comment ce site détesté par les banques m'a rendu millionnaire en un rien de temps. » « Attention, ce site qui va vous rendre riche sera bientôt interdit en Belgique. »... Elles pullulent, et polluent le web, singulièrement Facebook et Instagram. Grosses comme une maison, ces pubs peuvent parfois provoquer un irrésistible mécanisme psychomoteur : le clic. On appelle ça du *putaelic*.

Ici, le traquenard est d'autant plus redoutable qu'il se camoufle sous un vernis d'authenticité : l'identité graphique, indûment clonée, de sites de médias reconnus. Dont *Le Soir*. Pour attirer les gobe-mouches, ils mettent en scène de fausses interviews de célébrités (politiques, médiatiques, culturelles...). Lesquelles dévoilent le secret de leur indécente fortune à des stars du petit écran (Yann Barthes, Bertrand Chamero, François De Brigode...). Exemple : Elio Di Rupo confiant sa recette magique pour devenir scandaleusement riche à la présentatrice du JT de la RTBF, Ophélie Fontana. Dans le pire scénario, l'engrenage de clics entraîne inexorablement le lecteur candide à dégainer ses coordonnées et sa carte de crédit. Et se faire ponctionner jusqu'à 1.000 euros par mois. Pour rien, bien sûr.

Derrière ces campagnes bidon vantant les rendements abracadabrantesques de pseudo-cryptomonnaies, une gigantesque machinerie de désinformation internationale. Depuis 2019, au moins, elle plume des bataillons d'Européens crédules, dont de nombreux Belges, pris au piège de ce qui apparaît comme l'une des plus grandes escroqueries de l'histoire du web.

Check First, une ONG européenne basée en Finlande qui lutte contre la désinformation, a ouvert le capot de l'arnaque. Son enquête minutieuse, dont *Le Soir* a pu lire les résultats, a permis de remonter la filière, indice après indice. Publiée ce jeudi, elle donne le vertige tant la roublardise tient de la haute ingénierie. Cette enquête est un voyage à travers les plateformes, la désinformation, les pièges d'ingénierie sociale, l'usurpation d'identité, les « call-centers », les plateformes d'investissement douteuses, des entreprises louches basées dans les Pays baltes. Mais ce réseau alambiqué fomenté par les escrocs traverse les Amériques, l'Europe et l'Asie du Sud.

## Un réseau de 500 pages Facebook

« Au cœur de l'opération, on retrouve plus de 1.500 publicités achetées sur Facebook conduisant sur 60 faux sites web de médias », avance Guillaume Kuster, cofondateur et directeur de Check First. Cliquer sur n'importe quel lien sur ces sites web finirait par amener les victimes à se retrouver au téléphone avec un escroc essayant de les inciter à « investir » dans une entreprise très lucrative.

Démontons la fusée, étage par étage. Le point de départ, ce sont donc ces publicités suspectes diffusées sur Facebook. On a compris la recette : langage sensationnel, montages photos de célébrités... Il faut que ça claque et que ça clique. En fouillant les métadonnées, Check First a pu estimer à 1,5 million d'affichages de publicités pour l'en-



semble des campagnes observées pendant deux semaines. Chaque campagne coûtant en moyenne 100 dollars pour 3 ou 4.000 affichages. Qui publie ces pubs ? C'est le premier étage de la fusée : un réseau complexe de près de 500 pages Facebook, touchant une communauté globale de plusieurs millions de personnes.

Certaines de ces pages ont été créées de toutes pièces diffusant du contenu *putaelic* à la noix (« Ce piton a englouti huit chats », « Dix secrets pour un ventre plat, le 6° va vous étonner »...). D'autres, en revanche, ont été littéralement volées. Check First a pu en identifier 90. Les victimes ? Des petits artistes régionaux, généralement nord-américains qui gèrent, seuls, des communautés d'environ 150.000 abonnés. « Les escrocs réussissent à les convaincre de leur confier la gestion de leur page Facebook pour gonfler leur impact sur les réseaux sociaux », raconte Guillaume Kuster. Cupides, ils leur accordent tous les droits d'administration. Le tour est joué. « Sans piratage, c'est de la pure ingénierie sociale. »

## Fake pur jus

Cette « ferme » de 500 pages, gérée quasi exclusivement depuis le Bangladesh, est utilisée par les fraudeurs pour brouiller les pistes et passer les maigres filtres de Facebook contre ce type d'arnaques. Un cheval de Troie, apparemment digne de confiance, pour lancer ces campagnes publicitaires frauduleuses. Celles-ci pointent toutes vers le deuxième étage de la fusée : les faux sites de médias. Une soixantaine de marques de presse sont ainsi usurpées : *Le Monde*, *Die Welt*, *France 24*, *El País*... La Belgique n'y échappe pas, avec des titres comme *De Tijd*, *De Morgen*, *La Libre*, *La DH*, la RTBF ou *Le Soir*. Les adresses web (URL) de ces sites, totalement loufoques, ne devraient pourtant pas faire illusion (c'est l'indice le plus fiable d'une arnaque). Cela n'empêche pas certains de tomber dans le panneau. Il n'est pas inutile de rappeler que ces médias, qui bien souvent se battent avec Meta pour bloquer ces publicités, ne sont pas associés à ces campagnes.

Usant des codes journalistiques, ce sont donc ces sites qui publient ces fameuses interviews bidon de personnalités. Check First a comptabilisé 177 noms de domaines, dans 38 pays, dont 20 au sein de l'Union européenne. Du *fake* pur jus. La patte de ChatGPT et de traduc-

teurs automatiques crève les yeux. Mais certains n'y voient que du feu. Le piège se referme : tous les liens présents sur ces sites pointent irrémédiablement vers un formulaire d'inscription à une plateforme d'investissements prétendument miraculeux. C'est le troisième étage de la fusée. En réalité, un aspirateur à données personnelles : nom, prénom, adresse mail. Et surtout le numéro de téléphone, dont une opératrice de call-center local (un « 0466 » en Belgique) s'empare à la vitesse de la lumière. Souvent jusqu'au harcèlement. Parfois jusqu'au quatrième étage de la fusée. Fatal, celui-là.

En se faisant passer pour une victime potentielle, Check Point s'est ainsi vu redirigé vers une plateforme d'e-commerce. « Combien êtes-vous prêt à investir (par mois) », interroge la plateforme. « Entre 250 et 500 euros ? 500 et 800 ? Plus de 1.000 euros ? » C'est l'option retenue par l'ONG, le tout gentiment accompagné par « Allison », du call-center. « Allison » a envoyé un lien par e-mail vers une page de paiement pour un produit de 999 €, relate Guillaume Kuster. « Cette page ne portait aucune description de produit. En examinant ce site web de plus près, nous avons constaté qu'il offrait du coaching vidéo pour investisseur. Et que notre carte de crédit serait débitée chaque mois de ce montant. » La plateforme de paiement était basée en Estonie, vraisemblablement au cœur de l'escroquerie.

Il est impossible d'évaluer le nombre de victimes. Mais, avance Guillaume Kuster, « le simple fait qu'une opération d'escroquerie de cette taille soit possible, fonctionne apparemment depuis des années et mobilise autant de moyens suggère à quel point elle peut être lucrative ». « Une autre conclusion de l'existence de cela est le dysfonctionnement d'un éventail de mesures de protection, de lois, de processus d'application des politiques et de vérification », pointe l'enquête de Check First.



A gauche, le point de départ, à savoir des publicités suspectes diffusées sur Facebook. A droite, un faux site du « Soir ». Les liens présents sur les faux sites mènent aux étapes suivantes de l'arnaque. © DR.

## Adrien Devyver : « Je passe pour un arnaqueur »

Adrien Devyver, animateur à la RTBF, fait partie des personnalités dont l'image a été usurpée par les escrocs pour piéger les internautes. L'affaire remonte à deux semaines. Dans une interview bidon qu'il aurait accordée au chroniqueur Bertrand Chamero, mais à l'évidence générée par intelligence artificielle, il vante les prétendus mérites d'une plateforme d'investissement. Le tout emballé sur un faux site du *Monde*. Sauf que plusieurs de ses followers seraient tombés dans le panneau. Ce qui révolte l'animateur.

« J'ai reçu des centaines d'appels et de messages de personnes qui m'ont alerté ou qui se posaient vraiment la question de savoir si c'était une bonne idée d'investir sur cette plateforme. Là, j'ai paniqué. Le service juridique de la RTBF a immédiatement pris l'affaire en main. Toute la difficulté sera de faire aboutir le dossier car, visiblement, le site en question est hébergé aux Etats-Unis, ce qui pourrait, sans doute, impliquer qu'un juge d'instruction s'en saisisse. »

« Il était aussi urgent de communiquer pour démentir l'affaire car je commençais aussi à recevoir des messages de personnes qui affirmaient avoir cliqué sur le lien, misé et perdu de l'argent. D'autres me disaient que cela faisait



Adrien Devyver. © PHOTO NEWS.

des jours qu'ils étaient inondés d'appels de cette prétendue plateforme pour les convaincre d'investir. Un autre qui affirmait qu'ils avaient pris le contrôle de son PC... »

« C'est vraiment triste que des gens se sont fait avoir. Mais le pire, c'est le sentiment que c'est moi qui les aurais arnaqués, en quelque sorte. Mon image est évidemment écornée. Et même si on a communiqué sur l'arnaque, il n'en reste pas moins que beaucoup de personnes n'auront pas vu mes alertes, celles de la RTBF et de certains médias. Donc eux sont sans doute convaincus que je suis un arnaqueur. C'est très compliqué à gérer. »

« Je ne peux aussi qu'inviter les gens à redoubler de prudence face à ce type de sites. C'est tellement évident que l'adresse Web des sites vers lesquels renvoient ces pubs est complètement bidon et que l'on n'est pas sur le site officiel du *Monde*... » PH.L.