
Celebrity Crypto **Scam** Factory

La grande chaufferie qui met les réseaux sociaux en ébullition.

Celebrity Crypto **Scam** Factory,

la grande chaufferie qui met les réseaux sociaux en ébullition.

Une campagne mondiale d'arnaque sévit depuis plusieurs mois sur les réseaux sociaux, en particulier Facebook, Instagram et X. La tactique repose sur la diffusion massive de publicités mensongères usurpant l'identité de célébrités et de grands médias d'information pour promouvoir des offres frauduleuses de trading automatisé dans les cryptomonnaies. Basée sur le modèle économique du marketing d'affiliation, l'escroquerie met en jeu un écosystème tentaculaire où différents programmes sont conduits simultanément.

Le Lab Nameshield a enquêté et analysé 1948 contenus publiés entre mi-octobre 2023 et fin mars 2024 avec près de 500 noms de domaine différents.

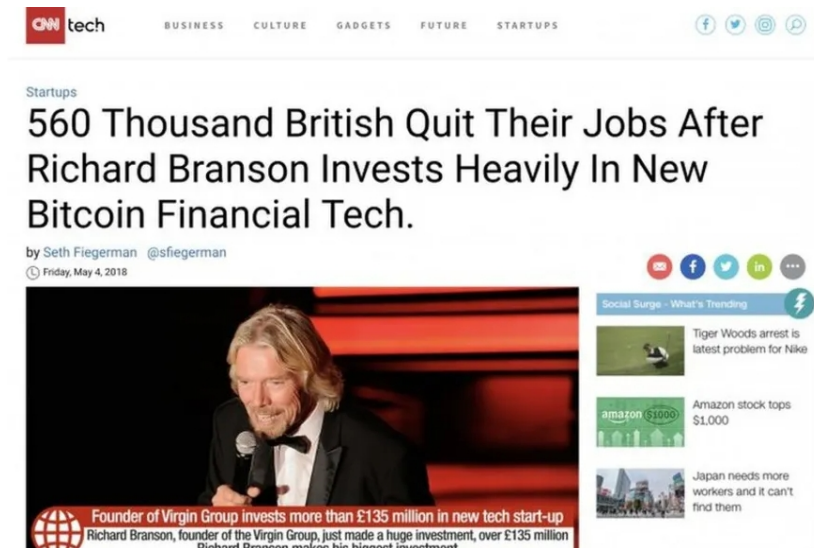
Lors de nos investigations, nous avons identifié une plateforme d'affiliation du nom de TraffiCon, connectée à un ensemble de publications trompeuses sur le site de blogging Medium. Nous avons également découvert un kit contenant tout le nécessaire pour décliner l'arnaque sur différentes cibles géographiques. Cet arsenal nous a mis sur la piste d'une application, promue sur un canal Telegram, permettant de détourner des comptes sociaux légitimes pour la propagation des annonces malicieuses.

[#Scam](#) [#FakeAds](#) [#CryptoTrading](#) [#FraudNetwork](#) [#Kit](#)

Une recette déclinée sur quatre continents

Le concept n'est pas nouveau. Dès mai 2018, le fondateur du groupe *Virgin*, Richard Branson, lançait l'alerte¹ sur de faux articles aux couleurs de CNN titrant sur un investissement record qu'il aurait effectué dans le Bitcoin et qui aurait conduit des milliers de britanniques à quitter leur emploi pour suivre son exemple (cf. fig. 1).

[fig.1 - Premier cas de détournement de l'image d'une célébrité pour promouvoir des investissements en bitcoin²](#)



Un *hoax* non dénué de plausibilité *a priori*, compte tenu de communications réelles de *people* – y compris Richard Branson lui-même – ayant manifesté dès 2013 leur intérêt pour les cryptomonnaies³. Très vite, la formule est industrialisée et déclinée dans plusieurs langues, sur divers sites d'information réputés et sur des personnalités connues du grand public, pour vanter des plateformes de robot trading répondant à des dénominations changeantes (cf. fig. 2).

De nombreux pays répartis sur quatre continents⁴ sont visés à travers des contenus mettant en scène leurs célébrités nationales⁵. Martin Lewis en Grande-Bretagne, Melissa Satta en Italie, Caroline Derpienski en Pologne, Anders Lund Madsen au Danemark, Normand Brathwaite au Canada, Sam Kerr en Australie, Ana Castela au Brésil, Filipe Matos au Portugal... et bien d'autres ont vu leurs noms dévoyés. En France, Alessandra Sublet, Eve Gilles, Elise Lucet et Anne-Sophie Lapix ont le plus souvent servi d'appâts ces derniers mois, aux côtés de vedettes du monde du spectacle tels que Redouane Bougheraba, Virgine Efira ou Florent Pagny.

1- Richard Branson, Beware of fake bitcoin scam stories. May 3, 2018. <https://www.virgin.com/branson-family/richard-branson-blog/beware-fake-bitcoin-scam-stories>

2- BBC News, Fake BBC News page used to promote Bitcoin-themed scheme. Jan. 17, 2019. <https://www.bbc.com/news/technology-46905475>

3- Coinkickoff, A timeline of Celebrity Crypto Endorsements. Mar 7, 2024. <https://coinkickoff.com/fr/celebrity-crypto-endorsements/>

4- Dans notre étude, nous avons relevé des contenus ciblant, à travers des célébrités locales, une trentaine de pays : la Grande-Bretagne, la France, l'Inde, l'Australie, le Canada, l'Italie, Singapour, les Philippines, l'Irlande, la Pologne, le Mexique, l'Afrique du Sud, l'Allemagne, les Pays-Bas, la Belgique, la Malaisie, le Danemark, le Portugal, la Turquie, le Japon, le Chili, l'Espagne, la Slovaquie, l'Équateur, la Corée du Sud, la Hongrie, l'Indonésie, la Slovaquie, la Tchéquie, le Brésil... Le continent africain ne semble pas visé par cette campagne.

5- Les profils des personnalités choisies sont variés : présentateurs télé, journalistes, entrepreneurs, humoristes, acteurs, chanteurs, sportifs, politiciens...

fig.2 - Nous avons dénombré 239 dénominations différentes, 63 % d'entre elles préfixées par le mot « Immediate »



Dès 2020, Confiand⁶ décrit le mécanisme de cette escroquerie et expose son fonctionnement identique au marketing d'affiliation où des rabatteurs se chargent de diffuser en masse les supports publicitaires qui draineront les internautes vers une offre d'investissement dans des options binaires⁷. A l'époque, ils empochent 600\$ par lead converti⁸. L'un d'eux, baptisé **FizzCore**, est actif depuis 2018 et cible plus particulièrement le Royaume-Uni, l'Allemagne et l'Italie, ainsi que la France.

En 2022, Group-IB⁹ identifie un autre acteur, visant l'Europe francophone et dont les agissements remontent également à 2018 : **CryptoLabs**. Il aurait permis de générer 480 millions d'euros de gains en usurpant une quarantaine de marques des secteurs bancaire et financier. Plus récemment, l'ONG Qurium¹⁰ a mis en évidence le rôle de la société russe **RPT Company** et de la plateforme d'affiliation **Keitaro** dans la propagation de posts sponsorisés usant de personnalités françaises sur Facebook.

Le Lab Nameshield a également enquêté et examiné 1948 contenus publiés entre mi-octobre 2023 et fin mars 2024 avec près de 500 noms de domaine différents¹¹. Lors de nos investigations, nous avons détecté un ensemble de publications mensongères sur Medium présentant un pattern typique. Nous avons ainsi identifié une plateforme d'affiliation du nom de **TraffiCon**, appartenant au groupe israélien **Affilomania**. Nous avons également découvert un **kit** contenant tout le nécessaire pour décliner l'arnaque sur différentes cibles géographiques. Cet arsenal nous a mis sur la piste d'un logiciel, **SantaChek**, permettant de détourner des comptes sociaux légitimes pour la diffusion des publicités malicieuses.

6- Confiand, Fake Celebrity-Endorsed Bitcoin Scam Abuses Ad Tech to Net \$1M in 1 Day», Jan 27, 2020. <https://blog.confiant.com/fake-celebrity-endorsed-scam-abuses-ad-tech-to-net-1m-in-one-day-ffe330258e3c>

7- Les options binaires sont des dispositifs financiers permettant de spéculer sur la hausse ou la baisse d'un titre (une action, une monnaie, un indice boursier, etc.) durant un bref laps de temps.

8- Le maillon suivant, composé d'une armée de commerciaux s'employant à soutirer l'argent des prospects, touche 3000\$ par escroqué.

9- Group-IB Europe, Anatomizing CryptosLabs: a scam syndicate targeting French-speaking Europe for years. Dec 7, 2022. <https://www.group-ib.com/media-center/press-releases/cryptoslabs-invest-scam/>

10- Qurium, A Journey into the Crypt of Cloned Media. Mar 26, 2024. <https://www.qurium.org/alerts/into-the-crypt-of-cloned-media/>

11- Nicenic International Group (39%) et Namecheap (25%) sont les deux principaux registrars, devant Squarespace Domains (12%) et Hostinger (10%). Les services de Cloudflare sont majoritairement employés (51%) pour masquer l'origine des IPs, et dans une proportion moindre mais notable, de Sucuri (24%) et Google Cloud Platform (14%).

Un narratif ancré en deux temps et un enfumage organisé

Le principe du narratif employé est simple et suit deux phases d'ancrage suivies d'un vaste brouillage :

1. Une nouvelle sensationnelle a été censurée : nous allons vous révéler son contenu, avec le crédit d'un média de confiance.
2. Cette nouvelle a été relayée sur une grande chaîne nationale : à n'en plus douter, elle est vraie.
3. Des mèmes grossiers inondent l'espace publicitaire et compliquent la tâche d'identification des contenus critiques.


Le scénario le plus souvent utilisé est le suivant (cf. fig.3-5) :

Lors d'une émission télévisée, une personnalité aurait révélé une « information financière » d'une « envergure » à même d'« ébranler les fondements de la société », propos qui lui auraient valu d'être qualifiée d'« irresponsable » par le présentateur et auraient suscité l'interruption de l'interview « par les autorités »...

Fig.3 - En France, l'émission Quotidien est très souvent détournée

Chilam Hotel
Sponsorisé

L'animateur de l'émission "Quotidien", Yann Barthès, a qualifié Ève Gilles de "irresponsable" et a déclaré en direct que "l'information financière d'une telle envergure peut ébranler les fondements de la société française".




LEMONDE.FR
L'interview a été interrompue par les autorités, mais il était déjà trop tard, car Ève Gilles avait déjà tout...

S'inscrire

Loopwall
Sponsorisé

Yann Barthès, le présentateur de l'émission "Quotidien", a qualifié Redouane Bougheraba d'"imprévoyant" et a exprimé en direct que "la révélation d'une information financière d'une telle envergure peut fragiliser les fondements de la société française".



LEMONDE.FR
L'interview a été interrompue par les autorités, mais il était déjà trop tard, car Redouane Bougheraba...

Fig.4 - Mais aussi « C à Vous » et les journaux de TF1

Janetas
Sponsorisé

L'animatrice de l'émission "C À Vous", Anne-Élisabeth Lemoine, a qualifié Marc Simoncini de "irresponsable" et a déclaré en direct que "l'information financière d'une telle envergure peut ébranler les fondements de la société française".



LEMONDE.FR
L'interview a été interrompue par les autorités, mais il était déjà trop tard, car Marc Simoncini...

En savoir plus

Foklajjo
Sponsorisé

Anne-Claire Codray, présentatrice de LE13H, a qualifié l'acteur Gilles Lellouche d'"irresponsable" et a déclaré à l'antenne qu'"une information financière de cette ampleur pourrait ébranler les fondements de la société française".




LEMONDE.FR
L'entretien est interrompu par les autorités, mais il est trop tard car Judith Godrèche a déjà tout...

En savoir plus

Fig.5 - Ailleurs dans le monde : Grande-Bretagne, Inde, Italie, Canada

Anna Dello Russo
Sponsorisé

"ITV News" host Mary Nightingale called Robert Peston "irresponsible" and said on the air that "financial information of this magnitude could shake the foundation of Britain society."




JYWLOVELXT.COM
The interview was interrupted by the authorities, but it was too late, as Robert Peston had already...
Product Description: Regular Adds 3.5" of toilet seat

[En savoir plus](#)

Galactic Grove
Sponsorisé

Nadia Leonardo, the host of the famous "FACE TO FACE" program, called Raditya Dika "irresponsible" and said live on air that "financial information of this scale can shake the foundations of Indonesian society."



DETIC.COM
The interview was interrupted by the authorities, but it was too late, as Raditya Dika had already...

[En savoir plus](#)

Healthy Body Quest
Sponsorisé

Il mistero dell'origine dei soldi di Isabella Ferrari per una vita lussuosa è stato svelato. Il pubblico è sotto shock.



ENLIGHTYSAX.COM
L'intervista è stata interrotta dalle autorità, ma era già troppo tardi perché Isabella Ferrari avev...

[En savoir plus](#)

Weld Jam Bouzbal
Sponsorisé

"Breakfast Television" host Sid Seixeiro called Mary Berg "irresponsible" and said on the air that "financial information of this magnitude could shake the foundation of Canadian society."



AIGLORYCA.COM
The interview was interrupted by the authorities, but it was too late, as Mary Berg had already...

[En savoir plus](#)

L'image servant d'accroche est le plus souvent tirée d'une émission ayant véritablement eu lieu. Jusqu'ici, une certaine plausibilité est ménagée. Le lien attaché à l'encart pointe sur un faux article reproduisant l'identité visuelle d'un site de presse en ligne réputé¹² (cf. fig.6). On y découvre la transcription de l'interview fictive, suivie d'un test du système de trading réalisé par l'un des « rédacteurs en chef ». Naturellement, cette expérience fait la démonstration, relevé bancaire (factice) à l'appui, de gains faramineux obtenus sans effort.

Sorte d'interface de prévente, l'article se termine par une incitation à s'inscrire sur la plateforme avec une marche à suivre rédigée pour être tout à la fois rassurante et pressante (date limite pour bénéficier de la gratuité de l'enregistrement). Le lien « fourni » par l'usurpé conduit sur un site de trading au nom et/ou au design changeants. D'autres célébrités, telles que Bernard Arnault et Cyril Hanouna¹³, sont là pour vanter, à leur insu, les bénéfices du système, ainsi que des témoignages affichant des bénéfices par milliers.

12- En France, Libération et Le Monde sont les plus imités. Ailleurs, de nombreux médias de référence sont aussi usurpés : BBC News, CNN, Forbes, The Telegraph, The Guardian, CCN, La Republica, RTBF, Euronews, El Pais ou encore El Mundo.

13- Ailleurs, Bill Gates ou encore Jeff Bezos sont souvent « convoqués »...

Fig.6 - Faux article du journal Le Monde relatant l'interview fictive

Consulter le journal

Se connecter

Guerre en Ukraine | Le direct | Les cartes | Vos questions | La contre-offensive ukrainienne

INTERNATIONAL - ACTUALITÉS

La Banque Centrale de France poursuit Elise Lucet pour ses déclarations en direct à la télévision



En direct, Elise Lucet a regretté d'avoir révélé la vérité. Mais il était déjà trop tard

Le scandale a éclaté lors d'une émission en direct lorsque Elise Lucet a accidentellement révélé son secret sur le programme. De nombreux téléspectateurs ont prêté attention aux mots « accidentels » de Elise Lucet et ont commencé à envoyer des messages à l'antenne. Cependant, l'émission a été interrompue par un appel de la Banque de France, qui a exigé que le programme soit immédiatement arrêté.

Un guide rapide pour commencer à gagner de l'argent sur Trade 5.0 Avapro.

- 1 Utilisez le lien fourni par Alessandra Sublet.
- 2 Recharger votre solde. Le dépôt minimal pour commencer le programme est de 250 euros.
- 3 Attendez un appel téléphonique de l'opérateur de la plate-forme pour confirmer l'enregistrement.
- 4 Après le rechargement du compte, le programme commencera à faire des transactions en quelques minutes.
- 5 L'argent peut être retiré à tout moment et arrive sur le compte dans les 2 à 3 heures (selon la banque).
- 6 Jusqu'à la fin de la journée du 22.03.2024 inclus, l'enregistrement des comptes sera encore gratuit.

VISITER LE SITE OFFICIEL

Dès le lendemain apparaissent des vidéos (cf. fig.7) ancrant un peu plus l'événement dans le réel en le relayant dans un journal télévisé truqué¹⁴, dont les premiers mots sont presque toujours : « Déclarations choquantes en direct : tous les citoyens français ne sont plus tenus de travailler ». Ces deepfakes, bien qu'ayant été conçues à l'aide d'une « IA », accusent pour la plupart un certain amateurisme. D'une qualité médiocre (ton monocorde et « voix de robot » parfois très éloignée du timbre de la personne, mouvements des lèvres non synchronisés avec la parole, raccords d'images approximatifs...), elles trompent difficilement l'œil attentif.

Fig.7 - Posts sponsorisés contenant des deepfakes

Documentário Grafitando Floripa
Sponsorisé

L'animateur de l'émission "Quotidien", Yann Barthès, a qualifié Ève Gilles de "irresponsable" et a déclaré en direct que "l'information financière d'une telle envergure peut ébranler les fondements de la société française".



Nanceleta
Sponsorisé

L'animateur de l'émission "Quotidien", Yann Barthès, a qualifié Alessandra Sublet de "irresponsable" et a déclaré en direct que "l'information financière d'une telle envergure peut ébranler les fondements de la société française".



Beautiful lotus
Sponsorisé

L'animateur de l'émission "Quotidien", Yann Barthès, a qualifié Redouane Bougheraba de "irresponsable" et a déclaré en direct que "l'information financière d'une telle envergure peut ébranler les fondements de la société française".



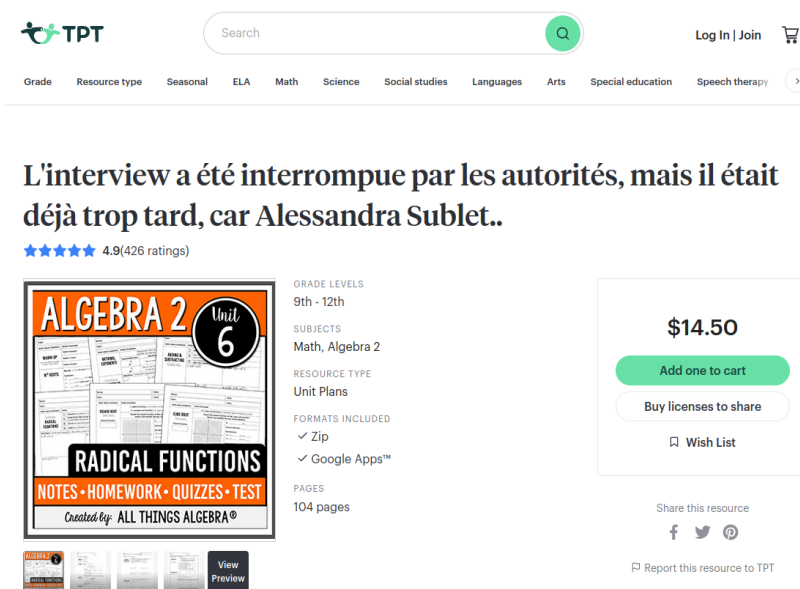
14- En France, on y retrouve fréquemment les JT de TF1, parfois de France 2 ou de France 24.

A ce stade de l'analyse, de nombreux éléments indiquent que les publications de type *infox* – articles et vidéos – sont le produit d'une automatisation réalisée sans la supervision d'un natif de la langue¹⁵:

- elles sont pour la plupart conçues dans une langue littérale, avec une grammaire hasardeuse ou un vocabulaire en décalage avec le contexte, comme le ferait un mauvais logiciel de traduction, et mélangent parfois plusieurs langues (contenus écrits) ;
- elles sont souvent truffées d'incohérences entre les noms des interviewés, des intervieweurs, des émissions mais aussi entre les images, les « marques » de plateforme ; entre le nom de domaine qui la plupart du temps imite le monde.fr mais renvoie à une page aux couleurs de liberation.fr...

Cependant, le choix des personnalités nous semble refléter une certaine immersion dans la culture cible, avec une attention portée au bruit médiatique qui entoure les *people* à un instant T. Notamment, les publicités détournant les images d'Alessandra Sublet et d'Eve Gilles prennent appui sur les titres racoleurs de la presse à scandale, suite à des interviews réelles dont les séquences les plus « punchy » ont été ôtées de leur contexte et amplifiées. Il se peut que des « consultants pays » ou des cellules locales travaillent bel et bien à la sélection des célébrités en fonction de leur actualité.

Fig.8 - Exemple d'atterrissage sur une page de vente en ligne avec un titre issu du hoax initial



The screenshot shows a product listing on the TPT website. The title is 'L'interview a été interrompue par les autorités, mais il était déjà trop tard, car Alessandra Sublet..'. Below the title is a 4.9 star rating with 426 reviews. The product image shows a document titled 'ALGEBRA 2 Unit 6 RADICAL FUNCTIONS' with sub-sections for 'NOTES • HOMEWORK • QUIZZES • TEST'. To the right of the image, there are details: GRADE LEVELS (9th - 12th), SUBJECTS (Math, Algebra 2), RESOURCE TYPE (Unit Plans), FORMATS INCLUDED (Zip, Google Apps™), and PAGES (104 pages). On the far right, the price is \$14.50, and there are buttons for 'Add one to cart', 'Buy licenses to share', and 'Wish List'. At the bottom, there are social sharing icons and a 'Report this resource to TPT' link.

Toutes les publications ne conduisent pas systématiquement vers un faux article de presse. Il arrive qu'elles pointent vers des pages de e-commerce sans aucun rapport avec les cryptomonnaies (vente de produits naturels, de livres pour enfants, de tee-shirts, etc.) - cf. fig. 8. Ceci permet de tromper le dispositif de vérification des contenus sponsorisés mis en place par Meta, comme l'a largement documenté Confiant dans son étude¹⁶. Mais selon Qurium¹⁷, certaines boutiques en ligne pourraient jouer un rôle dans le blanchiment de l'argent soutiré aux victimes.

15- Nous nous sommes plus particulièrement penchés sur les contenus ciblant la France et faisons l'hypothèse que les publications conçues sur le même schéma, pour d'autres pays, connaissent ces lacunes. The Journal dresse un constat semblable in « Arrested, disgraced, injured: Cryptocurrency scams promote hoax stories about Irish celebrities », Mar 10, 2024. <https://www.thejournal.ie/cryptocurrency-scam-x-facebook-youtube-maura-derrane-fake-ads-6318787-Mar2024/>

16- Confiant, Jan 27, 2020. op.cit. De notre côté, nous avons par ailleurs noté des cas de renvois expéditifs sur des sites légitimes tels que le monde.fr, rtve.es ou encore google.fr, esquives similaires à celles que nous observons régulièrement dans les campagnes de phishing.

17- Qurium, Mar 26, 2024. op.cit.

Au cloacking s'ajoute le flooding lorsque quantité de mèmes grossiers (cf. fig. 9-10) viennent saturer l'espace publicitaire et noyer les encarts contenant les liens critiques. Certaines célébrités y sont représentées le visage tuméfié, balaféré ou déformé par les pleurs ; elles sont parfois entourées de policiers ou placées derrière des barreaux : les accusations qui pèsent sur elles ont été confirmées, nous dit-on, et elles risquent leur carrière.

Fig.9 - Exemples de mèmes brocardant des personnalités françaises

News News
Sponsorisé

La France entière est abasourdie par la nouvelle d'hier. Elise Lucet a dit adieu à sa vie ordinaire.

20 minutes
Sponsorisé

LA FRANCE ENTIÈRE EST ABASOURDIE PAR LA NOUVELLE D'HIER. ELISE LUCET A DIT ADIEU À SA VIE ORDINAIRE.

USDP Women Committee
Sponsorisé

L'animateur de la célèbre émission "69 minutes sans chichis" Joëlle Scoriels a qualifié Virginie Efra d'"irresponsable" et a déclaré en direct qu'"une information financière de cette ampleur pourrait ébranler les fondements de la société française".

EFIRA VIRGINIE
Toute la FRANCE sous le choc!

Martial Lawrence Layman Francia
Sponsorisé

Anne-Sophie Lapix regrette d'avoir révélé la vérité. Mais c'est trop tard.

LE SCANDALE QUI A CHOQUÉ LE MONDE
ANNE SOPHIE LAPIX

Mizo National Front
Sponsorisé

Le scandale qui a choqué tout le monde

TF1 LE SCANDALE QUI A CHOQUÉ LE MONDE
LA SEULE PHRASE D'ANNE SOPHIE LAPIX À NOTER SA CARRIÈRE

THRIVEMOVEMENT.CLUB
Anne Sophie Lapix brise le silence
Misses 6-16. A favorite with quilters and clothing artists, this coat originated in Central Asia, where it L...

En savoir plus

Brandon Johnson
Sponsorisé

La conversation a été interrompue par les autorités, mais il était trop tard, étant donné que Virginie Efra avait déjà tout raconté.

LE FIGARO
Virginie Efra NE COMPRENAIT PAS QUEL MAL ALLAIT ARRIVER À CE QUI SE DIRAIT À L'ANTENNE

Fig.10 - Ailleurs dans le monde...

Misty Hollows
Sponsorisé

The mystery of the origin of Cillian Murphy's money for a luxurious life has been revealed. The public is in shock.

CILLIAN Ó MURCHÚ
TÁ POBLAHT NA SEICE I GCRUACHÁS

QUIETHINL.COM
The interview was interrupted by the authorities, but it was too late as Cillian Murphy had already...

En savoir plus

Cangri Burguer
Sponsorisé

During the heated argument, Matt Shirvington questioned the veracity of Sam Kerr words, calling her a "liar" in front of thousands of live viewers

Sam Kerr
Australia is in shock

UPINVESTMENTMANAGEMENT.COM
She didn't realise the camera kept recording..

Learn More

Emerald Cove
Sponsorisé

The mystery of the origin of Jeremy Clarkson's money for a luxurious life has been revealed. The public is in shock.

JEREMY CLARKSON DIDN'T NOTICE THE CAMERA CONTINUING TO RECORD.

IS THIS THE END OF HIS CAREER?

CLOSETKEXV.COM
The interview was interrupted by the authorities, but it was too late as Jeremy Clarkson had already sai...

Learn More

Les réseaux de diffusion

La nébuleuse Facebook

Sur Facebook, ces publicités émanent de pages piratées ou de comptes fictifs réactivés. Dans de rares cas, elles sont de création récente (2024).

Inscrites dans diverses catégories, elles sont le plus souvent restées sans activité ou ont été laissées à l'abandon par leur propriétaire pendant plusieurs mois, voire années (cf. fig. 11-13). Parfois, elles comptent des likes et des followers malgré l'absence de publications. Les fraudeurs les ressuscitent avec un post sans grand intérêt – un changement de photo de profil ou de couverture – les renomment parfois (cf. fig. 14). Lors de nos investigations, nous avons observé jusqu'au détournement de pages de ministères ou d'hommes politiques étrangers pour la diffusion simultanée d'annonces dans différentes langues.

Fig. 11 - Exemples de page fictive dont la création et l'unique activité remontent à plus d'un an

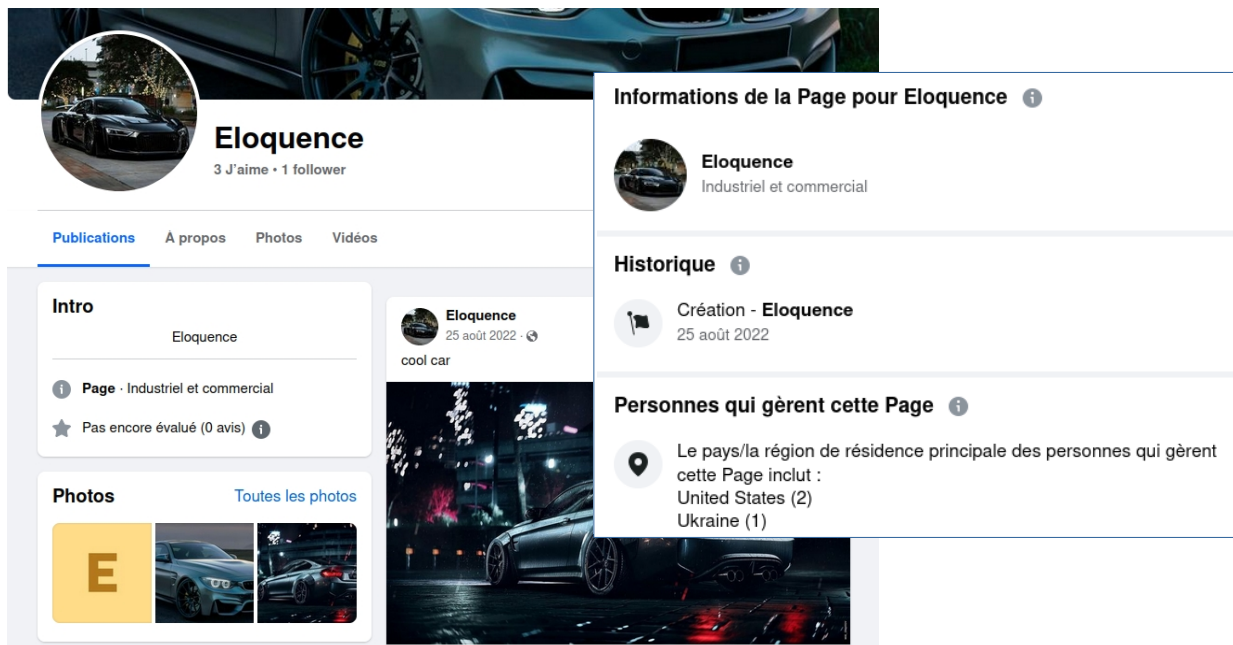


Fig. 12 - Exemple de page à forte audience, piratée après abandon par son propriétaire (dernière activité : 5 juin 2023)



Fig. 13 - Certaines pages sont animées par plusieurs individus basés dans différents pays

PetLovers
104 J'aime • 107 followers

Informations de la Page pour PetLovers

Historique

- Création - **PetLovers**
1 septembre 2022

Personnes qui gèrent cette Page

Le pays/la région de résidence principale des personnes qui gèrent cette Page inclut :

- Georgia (7)
- Ukraine (6)
- Indonesia (4)
- United States (4)
- Austria (1)
- Latvia (1)
- Pakistan (1)

Fig. 14 - Exemple de page piratée, renommée, réactivée avec un changement de photo de profil récent (21 fév. 2024)

Ryan Cassius
351 J'aime • 346 followers

Informations de la Page pour Ryan Cassius

Historique

- A remplacé le nom par **Ryan Cassius**
21 février 2024
- Création - **DreamLandNepal.com**
25 décembre 2009

Sur notre échantillon de cibles françaises, nous avons identifié près de 700 pages émettrices différentes. Au sein des multiples constellations d'annonceurs, un réseau se dessine nettement qui rassemble les diffuseurs d'encarts utilisant des noms de domaines ou des sous-domaines proches de lemonde.fr et liberation.fr ou contenant le terme-clef « news » (cf. fig.15).

Ils ont été enregistrés sous différents pseudonymes - « Cucu », « Monde.US », « Ivan Ivanon », « Boris Lieqr », « Yanis Fardogis » ou encore « Martin Hofsteder », auprès de Nicenic International Group Co Ltd, registrar et hébergeur basé à Hong-Kong. Les liens associés aux encarts ont la particularité de renvoyer directement sur des sous-pages (p.ex. [https://economy.lemonde2024fr\[.\]com/JRSdT4W9](https://economy.lemonde2024fr[.]com/JRSdT4W9)) faisant majoritairement la promotion de **Trade 5.0 Avapro**¹⁸ au moment de leur consultation.

18- Deux sites sont référencés sous cette dénomination par les moteurs de recherche : tradeavapro.com, déposé chez MainReg Inc., et imperialgo.org, enregistré chez eNom. Outre un design plus élégant et des signes de professionnalisme qui font cruellement défaut au second, on note que le premier, affichant une adresse à Singapour, communique non pas sur « Trade 5.0 Avapro » mais sur « Trade Avapro 5.0 ».

Par ailleurs, un certain « Ivan Ivanov » est apparu à plusieurs reprises dans divers enregistrements (cf. fig.17). Souvent associé à l'email ivanov.ivan27062706@gmail.com sous des déposants changeants tels que **Vavebit** (Ukraine) ou **Bittrade** (New-York), il est à l'origine d'une multitude de sites web proposant du trading automatisé en cryptomonnaies, bien au-delà de ceux analysés dans la présente étude²⁰ (cf. fig.18).

[Fig.18 - Exemples de sites de cryptotrading créés sous des noms déposés par Vavebit avec l'email \[ivanov.ivan27062706@gmail.com\]\(mailto:ivanov.ivan27062706@gmail.com\) au dernier trimestre 2023](#)



Le jeu de piste Medium

En consultant un moteur de recherche avec une requête de la forme {nom de la personnalité} + {nom de la plateforme}, on constate que plusieurs publications existent par ailleurs. On les trouve fréquemment sur la plateforme de blogging Medium sous des titres du type : « *Marine Le Pen Immediate X4 Urex Avis - arnaque ou légitime ?* » (cf. fig.19).

[Fig.19 - Exemple de fausse publication sur Medium détournant l'image de Marine Le Pen](#)



20- Plusieurs noms de domaine enregistrés en 2023, pour la plupart chez PDR Ltd, sont préfixés ou suffixés par « bit », tels que bitraxer.com, andexbit.com, mefexbit.com, bittrelo.com, bitxnano.com...

Nous avons pu en détecter plus de 400, déclinées en français et en anglais et émises par presque autant de comptes différents. Leur contenu est quasi identique à celui des faux articles de presse diffusés via Facebook, suggérant un seul et même fournisseur ou bien un clonage pur et simple par un copycat.

Exploitant le référencement particulièrement performant de Medium, cette méthode évite l'achat d'espaces publicitaires²¹ mais voit son impact limité aux requêtes effectuées sur un moteur de recherche. Elle a aussi la particularité de transiter par trois noms de domaine distincts avant de conduire l'internaute sur des pages d'offres au design bien différent des templates utilisés par la nébuleuse Facebook :

- le premier nom, inintelligible (p.ex. vggv6km8[.]com), est difficilement détectable sur des critères orthographiques ou lexicaux ;
- le deuxième (p.ex. hgktracking[.]com) sert d'intermédiaire ;
- le troisième, très explicite (p.ex. intelligent-money-offers[.]net), donne accès à la page de vente.

[Fig.20 - Exemple de fausse publication sur Medium détournant l'image de Thomas Piketty](#)

Thomas Piketty Immediate 700 NeuPro Avis — arnaque ou légitime?

 Zidgum · Follow
9 min read · Feb 19, 2024



La Banque Centrale de France poursuit Thomas Piketty pour ses déclarations en direct à la télévision



Parmi les différents affiliés opérant sous ce schéma, le plus prolifique dans notre jeu de données exploite le domaine d'entrée **snbghlytrk[.]com**, enregistré chez Nicenic International Group Co Ltd et pointant vers l'IP 192.124.249.11 appartenant à Sucuri-Sec – concurrent direct de Cloudflare²².

21- OCCPR, Down the Bitcoin Funnel: The Tech Firms Driving Investors to Ruin with Fake Celebrity News. Dec 1, 2020. <https://www.occrp.org/en/fraud-factory/down-the-bitcoin-funnel-the-tech-firms-driving-investors-to-ruin-with-fake-celebrity-news>

22- Un autre affilié, ayant opté pour Squarespace Domains (nouvel acquéreur de Google Domains) et Google Cloud Platform, s'appuie essentiellement sur les domaines finaux offerdomin.com et intelligent-money-offers.net/.com dont les sites web sont tous deux hébergés aux Pays-Bas (COGENT Communications) sur les IPs 185.142.239.207 et 185.142.239.82. Le premier est intermédié par srft.co, le second, par hgktracking.com. Leurs pages de vente comprennent un script communiquant avec une API dont le point d'entrée contient 'intgrtn'.

Il utilise le domaine final **official-platform[.]com** dont le site web est à ce jour hébergé en France sur un VPS d'OVH avec l'IP 162.19.231.202. Quatre autres noms pointent *actuellement*²³ vers cette adresse : **official-site-offer[.]com**, **official-site-platform[.]com**, **best-money-deal-daily[.]com** et **newsbbi[.]com**. Les deux premiers portent une grande variété d'offres de trading et sont disponibles dans plus de 120 langues (quand les sites des réseaux de Facebook en comptent moins d'une quarantaine) ; le troisième est l'intermédiaire vers la destination finale et communique avec **www.hitsteps[.]com**, une plateforme d'analyse de trafic web, concurrente de Google Analytics ; le quatrième est lié au serveur sur lequel sont testés les templates pour différentes marques.

Fig.21 - Exemple de fausse publication sur Medium

```
console.log(offer_id+ country_code);
formdata.append("offer_id", offer_id);
formdata.append("aff_id", aff_id);
var requestOptions = {
  method: 'POST',
  headers: myHeaders,
  body: formdata,
  mode: 'cors',
  redirect: 'follow'
};
fetch("https://regapi.trafficon.co/secured-registration", requestOptions)
```

Les pages de vente envoient les données de formulaire sur un sous-domaine de **trafficon[.]co** (cf. fig.21). Ce nom est associé à quantité de sites frauduleux, la plupart en rapport avec le bitcoin (cf. fig.22). Une recherche sur urlscan.io affiche 3353 résultats, le premier remontant au 15 octobre 2019.

Fig.22 - Extrait d'un historique sur urlscan.io

ynappsystems.com/pages/th.html	Public	3 years	🌐	2 MB	56	7	3	🇺🇸
the-code-sys.com/?clickID=8aa52fcd37d24982b34a9a2cb4b70e43&aff=Code&c=DE&tid=10...	Public	3 years	🌐	912 KB	41	9	3	🇺🇸
btc-profit-today.com/ru/?clickID=&aff=&c=RU&tid=1024ac88083f263901a16f018cc36a&...	Public	3 years	👤	561 KB	36	9	3	🇺🇸
btc-profit-now.com/?clickID=cbd13eebeae52319e2b95bd5ff8a5f0a&aff=&c=DE&tid=1024...	Public	3 years	🌐	1 MB	42	10	6	🇺🇸
www.bitcoin-revolution-apps.com//?clickID=a0d800f4e272495b47f189196d2b5a1a&aff=...	Public	3 years	🌐	1 MB	59	12	5	🇺🇸
btc-revolution.cc/?clickID=ff29f1b62f6b4f35b06c28d22134a437&aff=&c=DE&tid=1024c...	Public	3 years	🌐	212 KB	45	8	4	🇺🇸
www.bitcoinrev1.com/	Public	4 years	👤	1 MB	55	8	4	🇺🇸
invest-in-uber.com/	Public	4 years	🌐	1 MB	60	11	3	🇺🇸
bitcoin-revolution-apps.com/	Public	4 years	🌐	1 MB	60	12	4	🇺🇸
bitcoin-billion-club.com/de/?clickID=april15_1&aff=woqkucumtcl06ucuhnpkvkd4&c=D...	Public	4 years	👤	1 MB	83	9	3	🇺🇸
cryptonexlabs.com/	Public	4 years	👤	1 MB	40	4	2	🇺🇸
yuan-payments.com/	Public	4 years	🌐	2 MB	32	10	4	🇺🇸
cryptoinfographic.com/?aff_id=1039&aff_sub5=all_default&&clickID=5e5d75360ffee2...	Public	4 years	🌐	965 KB	22	7	2	🇺🇸
bitcoinrev1.com/	Public	4 years	👤	1 MB	49	7	4	🇺🇸
invest-with-libra.com/?clickID=10295d4f4d011fe36bb2163ec0cf8d&aff=&c=DE&tid=102...	Public	4 years	🌐	2 MB	103	10	4	🇺🇸
codenet-systems.com/?clickID=102faa19623a186f3b5c84b12e34e3&aff=&c=DE&tid=102da...	Public	4 years	👤	880 KB	38	11	5	🇺🇸
www.libra-trading-tool.com/?clickID=1025a9ab11d04ae0ff3c6ecf074bdb&aff=&c=DE&ti...	Public	4 years	🌐	2 MB	21	7	4	🇺🇸
invest-in-libra.com/?clickID=x&aff=&c=NL&tid=x&aff_id=1057	Public	4 years	👤	675 KB	24	6	3	🇺🇸

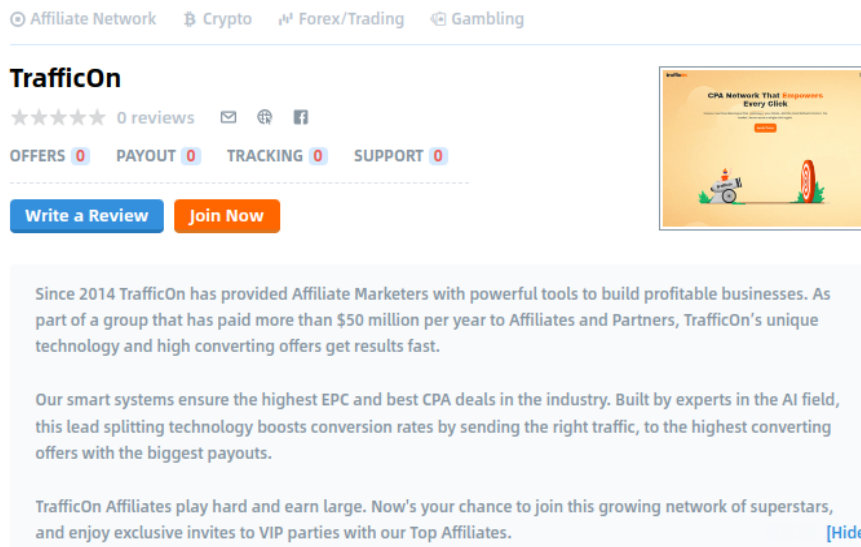
(3353 results in total, 1200 shown)

Load more...

23- Ces domaines, tous déposés chez des registrars différents, ont vu plusieurs IPs au cours de leur «existence».

Le site commercial est accessible à l'adresse [www.trafficon\[.\]io](http://www.trafficon[.]io). Il s'agit d'une plateforme d'affiliation active depuis 2014 et spécialisée dans le trading sur CFD, les cryptomonnaies, l'achat d'actions et d'ETF, ainsi que dans l'iGaming (jeux d'argent et de hasard en ligne).

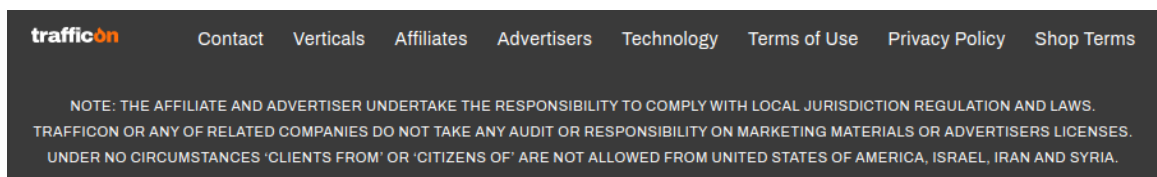
Fig.23 - Extrait d'une revue sur [www.affpaying\[.\]com](http://www.affpaying[.]com)



TrafficOn Network (Metsada 7, Bnei Brak, Israël) applique des programmes par gains au clic (EPC) ou à la commission (CPA) avec un paiement minimum de 100\$ et se vante d'appartenir à un groupe ayant généré plus de 50 millions de dollars par an au profit de ses affiliés et partenaires (cf. fig.23).

Ce groupe, c'est **Affilomania**²⁴. Il siège à Tel Aviv mais tient ses bureaux à Bnei Brak, tout comme TrafficCon. Fondé en 2013, il ne tarde pas à se faire connaître pour ses activités illicites. En 2018, son nom apparaît dans une vaste fraude aux options binaires. *Times of Israel*, qui relate les faits²⁵, souligne que les Etats-Unis ont pris dès 2016 des sanctions contre des firmes israéliennes opérant ce type d'offres. La Knesset a quant à elle rendu l'industrie des options binaires illégale en octobre 2017. Ce qui explique que TrafficCon interdise formellement à ses affiliés et annonceurs de cibler ces pays (cf. fig.24).

Fig.24 - Note en bas de page du site www.trafficon.com



24- Il possède également BOAElite, une autre plateforme d'affiliation, et Profitit, société développant un CRM.

25- Times of Israel, In latest crackdown, US goes after marketers of Israeli Internet fraud. Sept 29, 2018. <https://www.timesofisrael.com/in-latest-crackdown-us-goes-after-marketers-of-israeli-internet-fraud/>

Times of Israel explique que les options binaires ont été introduites en Israël dans les années 2000 par des vétérans de l'industrie du jeu en ligne originaires des États-Unis (y compris des expatriés israéliens), du Canada et d'Allemagne, mais aussi par des personnalités du crime organisé de l'ex-Union soviétique. Un appel d'air créé par une politique fiscale très libérale, pratiquée depuis 2008, et une absence de coordination internationale. En effet, la loi Milchan permet aux nouveaux immigrants de ne pas déclarer ni de payer d'impôts pendant dix ans sur les revenus provenant de l'étranger. Sous la pression de l'OCDE, dans sa lutte pour la transparence financière, la déclaration est récemment devenue obligatoire. Mais l'exonération de taxes sera maintenue. Plus de précision dans l'article de Globes : New immigrants will need to report income and assets abroad. Feb 26, 2024. <https://en.globes.co.il/en/article-new-immigrants-will-need-to-report-income-and-assets-abroad-1001472163>

Malgré sa réputation entachée, la société mène une vie tout à fait « normale » : elle participe à des salons et communique par la voix de ses managers²⁶. Elle sera même présente au prochain IGB Affiliate qui aura lieu à Barcelone en janvier 2025.

Elle soigne aussi et stimule particulièrement son réseau. Un système de récompense a été mis en place par le biais d'une boutique dédiée, le « Candy Shop » (cf. fig.25) : pour chaque prospect converti en client, l'affilié empoche des « TraffiCoins »²⁷ qui lui permettent d'« acheter » des produits haut-de-gamme (Rolex, Breitling, MacBook, iPhone, ...) de provenance inconnue et d'une valeur marchande pouvant dépasser 100 000€.

Fig.25 - Exemples de produits proposés sur le Candy Shop

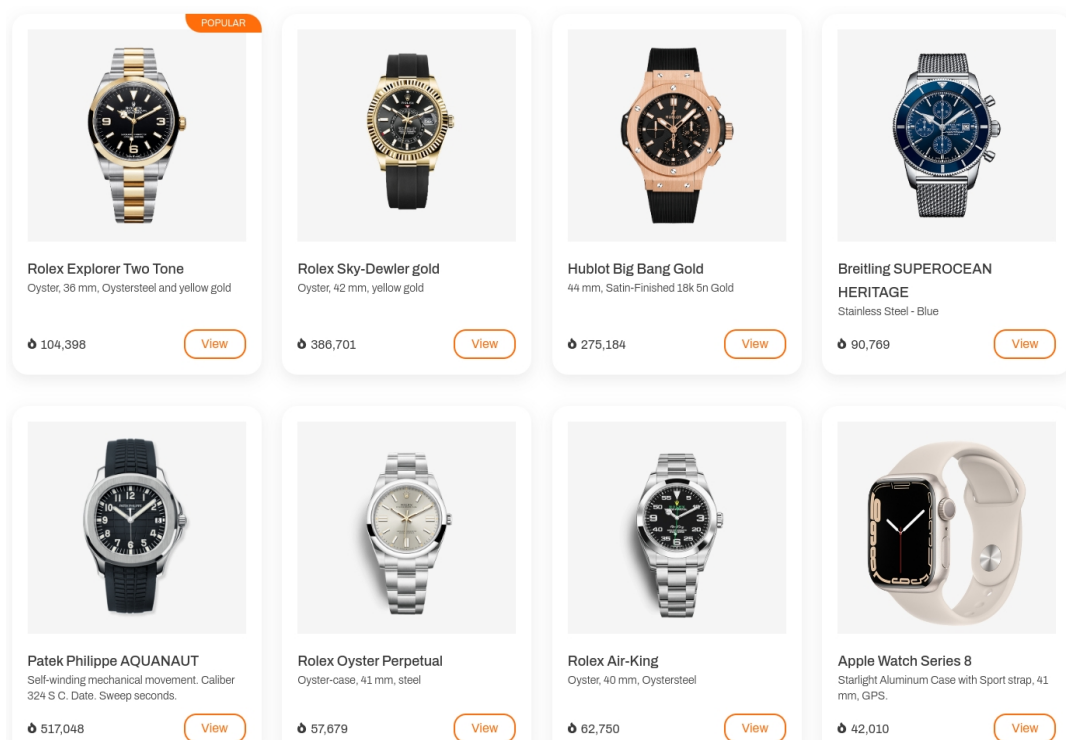


Fig.26 - Témoignage d'un postulant chez Affilomania exprimant des doutes sur les activités de l'entreprise

11 sept. 2023

Entretien pour Affiliate Account Manager

Employé anonyme, Bnei Brak

— Aucune offre — Expérience neutre — Entretien moyen

Candidature

J'ai postulé en ligne. Le processus a pris 1 semaine. J'ai passé un entretien chez Affilomania (Bnei Brak) en sept. 2023

Entretien

About 1 hour interview with the heads of the department. Then 1 hour with HR. Quite a broad questionary. Did not fully understand how does their software works. I wouldn't say that the company is transparent.

26- Vidéo dans laquelle un manager de TraffiCon est interviewé, à l'occasion d'un salon professionnel. <https://www.facebook.com/sigmaworld.official/videos/feedback-sigma-sean-sebag-trafficon/542712686340048/>

27- Dans un communiqué, TrafficOn explique que l'intérêt de ces pièces numériques est qu'elles ne subissent les fluctuations d'aucune devise... Source : <https://www.igamingaffiliateprograms.com/article/trafficon-launched-trafficoins-for-its-affiliates-241498/>

Une fabrique à arnaque dans un kit multi-géo, multi-plateforme

Le kit²⁸ que nous avons pu nous procurer contient de quoi décliner l'arnaque dans une trentaine de langues (cf. fig.27) et sur différentes plateformes (Facebook, Google, Bigo, ...), avec tous les éléments nécessaires au déploiement des pages d'infox, de boutiques en ligne et d'offres de trading. Elles sont construites de manière à être intégrables dans le CMS WordPress et gérées via un control panel.

Fig.27 - Arborescence de landers crypto liés à des publicités sur Facebook ciblant des pays commençant par A

- ▼ Offers crypto FB
 - ▼ AM
 - > AM Ameria Invest/AM Ameria Invest [land1] 1807
 - > AM Gazprom
 - > AM Tesla/AM Tesla Land 3 [land3] 0410
 - ▼ AU [new keitaro]/AU ANZ
 - > AU ANZ Land 1 [land1] 2602
 - > AU ANZ-Q Land 2 [quiz] 2602
 - > AU-CA [new keitaro]/AU-CA Tesler/AU-CA Tesler Land 1 2802
 - ▼ AU
 - ▼ AU ANZ
 - > AU ANZ Land 1 [land1] 2311
 - > AU ANZ-Q Land 2 [quiz] 2911
 - > AU Best Signals/AU Best Signals Land 1 [land1] 1003
 - ▼ AU Commonwealth Bank
 - > AU Commonwealth Bank Land 2 [land1] 0611
 - > AU Commonwealth Bank-Q Land 1 [quiz] 2111
 - > AU MetaMusk/AU MetaMusk [land1] 2806
 - ▼ AZ
 - > AZ ChatGPT Profit/AZ ChatGPT Profit [land1] 3107
 - ▼ AZ Gazprom
 - > AZ Gazprom Land 1 [land1] (without video) 1702
 - > AZ Gazprom-Q Land 2 [quiz] 0203
 - ▼ AZ Kapital Invest

Les informations issues du formulaire sont transmises à un CRM sur le domaine **solutionsulting[.]com** (enregistré le 7 juin 2023, chez Namecheap) afin de valider l'ajout du nouveau prospect (cf. fig.29). Ce CRM, dont l'interface de connexion s'adresse à des russophones, est hébergé sur un serveur de Digital Ocean localisé en Allemagne.

²⁸- Ce kit ne contient pas les modèles de faux articles Le Monde et Libération mais d'autres grands médias internationaux y sont contrefaits, tels que Forbes, TVN ou SBS Nitv.

La promotion de faux investissements en cryptomonnaies n'en représente qu'une partie. Il renferme en effet bien d'autres schémas d'arnaque répandus sur les réseaux sociaux. Tels que les quizzes permettant de remporter des lots fictifs sous réserve d'en payer la livraison ou les soldes trop belles pour être vraies. Nous avons pu voir des templates de cible française, usurpant de grandes marques (Dior, Apple, Dell, Samsung, ...).

A l'heure où nous écrivons, nous n'en avons pas terminé l'analyse.

Une fois l'inscription vérifiée, les données sont transférées à une plateforme d'affiliation (cf. fig.28). La mention '[new keitaro]' figurant sur certains dossiers indique qu'une nouvelle voie de communication avec Keitaro²⁹ est disponible. Elle est en effet possible via **keitaro-leadar[.]ink** mais aussi via **nanometer[.]space**, ce que confirme l'analyse technique.

Fig.28 - Extrait du script de transfert de données à la plateforme d'affiliation

```
var matches = document.cookie.match(new RegExp("(?:^|; )' + 'subid' + '=[^;]*'"));
var subId = matches ? decodeURIComponent(matches[1]) : undefined;
document.getElementById('pb').src =
  'https://keitaro-leadar.ink/f6c793a/postback?subid=' + subId + '&status=lead';

var matches = document.cookie.match(new RegExp("(?:^|; )" + 'subid' + "=[^;]*"));
var subId = matches ? decodeURIComponent(matches[1]) : undefined;
document.getElementById("pb").src = "https://nanometer.space/8a30ddc/postback?subid=" + subId +
  "&status=lead";
```

Fig.29 - Extrait du script de validation du lead comportant une période d'« oubli » de 21 jours

```
'lastName' => $lastName,
'phone' => $phone,
'email' => $email,
'offer' => $offer,
'target' => $target,
'creo' => $creo,
'buyer' => $buyer,
'country' => $country,
'ip' => $ip,
'source' => 'facebook',
'lang' => 'en'
]
);
$opts = [
  'http' => [
    'method' => 'POST',
    'header' => 'Content-type: application/x-www-form-urlencoded',
    'content' => $postdata
  ],
  'ssl' => [
    'verify_peer' => false,
    'verify_peer_name' => false,
  ]
];

$context = stream_context_create($opts);
$result = file_get_contents('https://api.solutionsulting.com/api/leads/add', false, $context);

// Double check condition
if ($saved = json_decode($result, true)['saved'] === 'true') {
  echo 'success';
} elseif ($errors = json_decode($result, true)['errors']['phone']['custom'] === 'Double: lead with this phone has been added less than 21 days ago')
  echo 'double_phone';
} elseif ($errors = json_decode($result, true)['errors']['email']['custom'] === 'Double: lead with this email has been added less than 21 days ago')
  echo 'double_email';
} elseif ($errors = json_decode($result, true)['errors']['email']['email'] === 'The provided value is invalid') {
  echo "invalid";
```

Dans ce kit, on trouve également de précieuses informations aspirées dans les navigateurs de propriétaires de comptes sociaux. Cookies, historique de navigation, données de formulaires, identifiants et mots de passe, des profils entiers ont été exfiltrés³⁰. Tous ces éléments sont rassemblés dans un dossier qui recèle de quoi tromper le dispositif de sécurité de Meta (et bien d'autres plateformes), jusqu'aux fingerprints de la victime (cf. fig.30).

29- Société opérant une plateforme d'affiliation pointée par Qurium dans son enquête. op. cit.

30- Rien n'indique l'origine du siphonnage initial mais il est probable qu'il fasse suite au téléchargement d'un plugin malicieux agissant comme un infostealer : <https://www.malwarebytes.com/blog/threat-intelligence/2023/07/criminals-target-businesses-with-malicious-extension-for-metas-ads-manager-and-accidentally-leak-stolen-accounts>

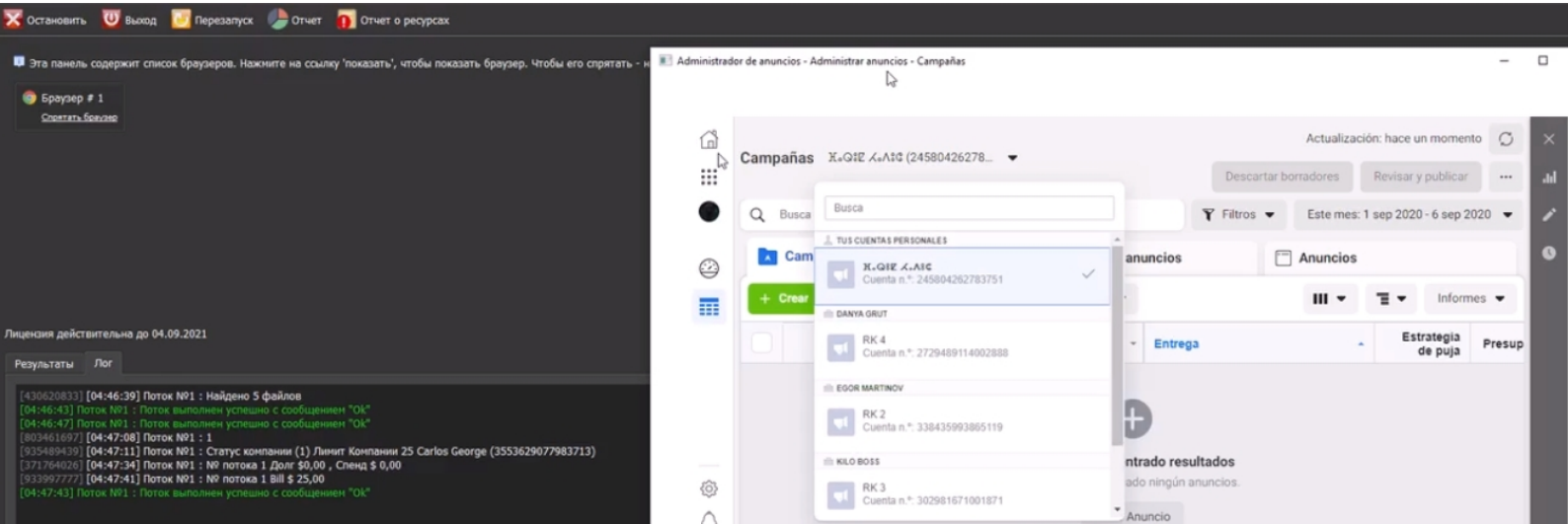
Fig.30 - Extrait du fichier 'Information.txt'

```

UID: mrd-
OS: Windows 10 Enterprise x64
UserName: sassa
ComputerName: SASA
DateTime: 17.10.2022 03:12:19
UserAgent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)
Keyboard Languages: Arabic
Display Resolution: 1680 x 1050
CPU: AMD Ryzen 5 3500X 6-Core Processor core 6
RAM: physical 2047MB , virtual 2047MB
GPU: NVIDIA GeForce GTX 1050 Ti
    
```

Promu sur un canal Telegram russe, le logiciel **SantaChek** permet d'exploiter ces données et de s'introduire en toute furtivité dans le compte³¹ (cf. fig.31). Le but est d'en extraire l'EAAB - jeton d'accès statique à l'API de Facebook, mais aussi de s'assurer qu'il pourra être utilisé sans difficulté pour les besoins de campagnes frauduleuses. En sortie, un fichier spécifique dresse le profil de l'annonceur : son statut (actif / inactif), sa devise, son type (prépayé / facturé) et son état (limite de facturation, montants déjà dépensés, dettes...). Il est alors vendu comme « vérifié ».

Fig.31 - Copie d'écran d'une vidéo de démo de SantaChek sur le compte d'un annonceur espagnol



Le logiciel embarque de nombreuses fonctionnalités, comme celle d'étendre la durée de vie des cookies, et ne se limite pas au détournement de comptes Facebook. Instagram, Google Ads, Youtube, Twitch, Steam, Battle, Netflix, Airbnb, Amazon, Tinder, LinkedIn, Badoo... sont dans le viseur ainsi que Gmail ou Hotmail pour l'envoi de spams.

Plusieurs individus sont à la manœuvre, chargés d'extraire les fameux « checks » qui sont répertoriés sur un canal de vente dédié (cf. fig.32). Les plus convoités sont ceux pour lesquels les annonceurs légitimes n'ont pas configuré de limite de budget ('unlim') et/ou ont opté pour le prépaiement ('PREPAY'). Grâce au dossier fourni, les fraudeurs s'emparent du tableau de bord de l'annonceur et y configurent librement la diffusion de publicités trompeuses. Il peuvent aussi ajouter de nouveaux utilisateurs pour gérer les pages, modifier leurs noms... Une prise de contrôle totale face à laquelle les victimes sont démunies³².

31- SantaCheck intègre le changement automatique de *fingerprints* en fonction du compte introduit, à l'aide de la suite applicative BrowserAutomationStudio : <https://fp.bablosoft.com/>

[Fig.32 - Exemple de « logs » vendus sur un canal Telegram](#)

```

ACTIVE_5.0$_0.0$_1500.0$_0$_PREPAY_USD_PK_15_STORED_BALANCE_SIV_W5X
ACTIVE_8.14$_0.0$_-0.02$_0$_PREPAY_PHP_PH_9_STORED_BALANCE_uho_BJF
ACTIVE_129.48$_0.09$_-0.02$_0$_PREPAY_PHP_PH_117_STORED_BALANCE_xYR_cnb
ACTIVE_842.33$_0.0$_-0.02$_0$_PREPAY_PHP_PH_515_STORED_BALANCE_Wnk_Q5Y
  
```

(ru) 🧨 ЛОГ СО СПЕНДОМ ПРЕДОПЛАТА 🧨

LIMIT 1500 and unlimX

💎 Spend-Billing-Limit

👤 ОТМЕЧАЙТЕ И СРАЗУ КИДАЙТЕ СКРИН.

D'autres logiciels que SantaChek (accessible sous licence à 100\$ par mois) se monnaient sur des canaux Telegram. Ils font partie des nombreux outils exploités dans la chaîne d'arnaque. Parmi eux, le kit révèle également l'utilisation de **Palladium**, système de *Cloaking-as-a-Service* spécifiquement conçu pour déjouer les robots de surveillance dans ce genre d'opérations (cf. fig.33). Capable de détecter et de contourner quatre types de modération, il permet aux clients de « protéger leurs ressources » et d'assurer une bonne durabilité à leurs campagnes publicitaires.

[Fig.33 - Offre Palladium traduite de l'ukrainien vers le français à l'aide de Google Translate](#)



PALLADIUM des algorithmes propriétaires pour la protection et l'optimisation du trafic, non ciblé ont été mis en œuvre.

Principal À propos du service Avantages FAQ Contacts **Plans Tarifaires**

Gloire à l'Ukraine! Gloire aux héros !

- ✓ Un système complexe à plusieurs étapes avec évaluation des coefficients et répartition par zones à risque, chaque utilisateur est évalué sur son score de confiance IP en plus des algorithmes.
- ✓ La plus grande base de données de modération d'adresses IP compte plus de 200 000 adresses IP résidentes et mobiles (nous ne stockons pas les adresses IP des robots).
- ✓ Détection et blocage de 4 types de modération.
- ✓ Détecte les embouteillages et les messages système avec précision.
- ✓ Mises à jour et optimisation constantes.
- ✓ Assistance VIP, ainsi que conseils sur les problèmes techniques et le lancement de campagnes.
- ✓ 4 types d'intégration de scripts Palladium.

Notre service est aussi automatisé que possible et nous ne vous transférons pas la responsabilité des résultats. Nous ne vous proposons pas beaucoup de paramètres parmi lesquels choisir : nous avons construit des algorithmes qui gèrent complètement toutes les menaces. Nous bloquons tout type de trafic indésirable et suspect (bots, modération, fermes de robots, proxy, vpn, services d'espionnage, concurrents et autre trafic non ciblé) qui ne sont pas vos utilisateurs cibles.

Les sites clients avec protection Palladium vous permettent de maximiser les dons et la durée de vie de vos comptes. Nous permettons à nos clients de faire évoluer et d'optimiser pleinement leurs campagnes publicitaires, en plaçant la protection de leurs ressources entre des mains fiables.

Le site web de Palladium est par défaut consultable en russe avec le nom de domaine **palladium[.]expert**. Sur les deux autres versions disponibles, en ukrainien (ua.palladium[.]expert) et en anglais (en.palladium[.]expert), il affiche un franc soutien à l'Ukraine. Schizophrénie quelque peu déroutante mais pas si étonnante. Tout au long de l'étude, nous avons pu observer à quel point le crime organisé ne connaît pas de frontière. On note également que le détail de l'offre (cf. fig.33), sans grande ambiguïté sur le type d'activités qu'elle se propose de dissimuler, manque curieusement à la version anglophone.

32- Mashable, Facebook scammers are hacking accounts and running ads with stolen money. Oct 29, 2021. <https://mashable.com/article/facebook-ad-manager-scam-hack>

Quand le piège se referme...

Une fois que l'internaute a renseigné le formulaire d'inscription (cf. fig.34), il est livré à un centre d'appels agissant comme une véritable salle de « chaufferie »³³ où chaque téléopérateur est rompu à l'art de la manipulation psychologique.

A réception des coordonnées, un individu se faisant passer pour un gestionnaire de compte téléphone à la victime et l'incite à payer entre 250€ afin et 300€ afin d'accéder à la plateforme. Selon le cas, le téléchargement d'une application spécifique est requise pour pouvoir « investir » davantage.

Fig.34 - Exemple de site cible Trade 5.0 Avapro

Le tableau de bord fourni affiche au départ des bénéfices modestes mais suffisants pour susciter de plus grands espoirs. Les fraudeurs, armé d'un argumentaire bien ficelé, obtiennent des investissements de plus en plus importants. Parfois, ils permettent à l'escroqué de retirer une petite somme d'argent afin de gagner d'autant mieux sa confiance. Lorsque ce dernier tente de récupérer ses fonds, des frais de retrait, des problèmes fiscaux et autres prétextes fumeux lui sont opposés. Il ne reverra plus jamais son argent.

Les « pigeons » les plus prometteurs – et les plus vulnérables – sont transférés à « l'équipe de rétention » dont la mission est de soutirer l'argent des clients « jusqu'au dernier centime ». Les témoignages de cette machination qui pour certains a englouti les économies d'une vie ne manquent pas³⁴.

33- Ainsi appelée du fait des techniques de vente agressives qu'elle pratique. Investopedia, Boiler Room Definition, How It Operates, Common Scams. April 18, 2022. <https://www.investopedia.com/terms/b/boilerroom.asp>

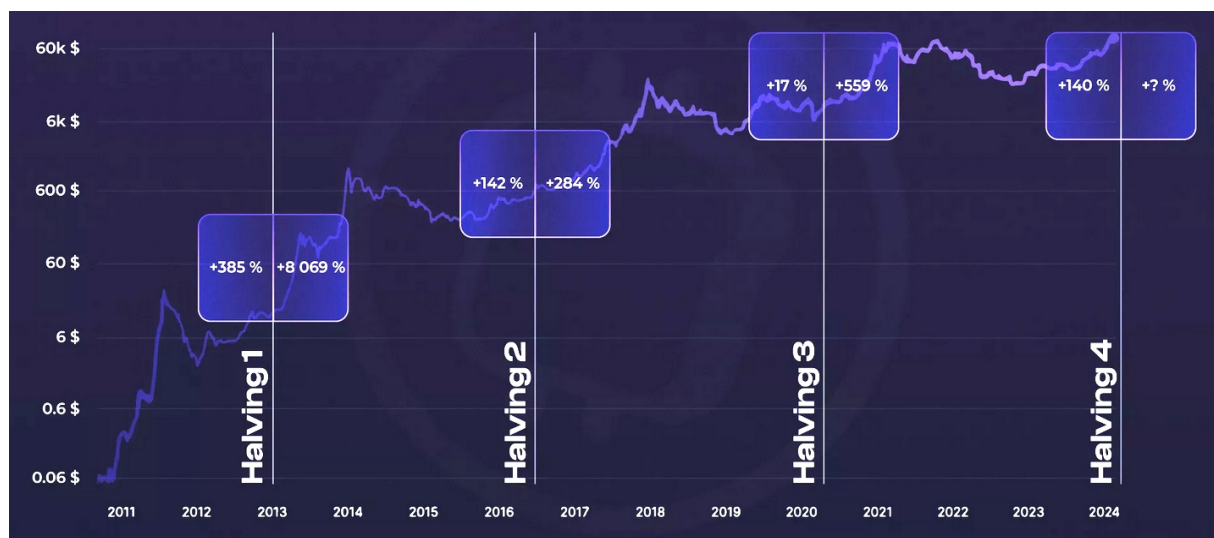
34- OCCPR, Down the Bitcoin Funnel: The Tech Firms Driving Investors to Ruin with Fake Celebrity News. Dec 1, 2020. <https://www.occrp.org/en/fraud-factory/down-the-bitcoin-funnel-the-tech-firms-driving-investors-to-ruin-with-fake-celebrity-news>

Un vaste *pump-and-dump* à l'approche du Bitcoin halving de 2024 ?

Si son procédé est notoire, la campagne d'arnaque qui sévit depuis plusieurs mois frappe par son ampleur inédite. Pourquoi une telle avalanche maintenant ?

Une explication pourrait se trouver dans l'imminence du *halving* de 2024, attendu mi-avril. Se produisant environ tous les quatre ans, ce mécanisme permet de réguler la quantité de tokens en circulation sur le marché. Jusqu'ici, il s'est traduit par une hausse significative de la valeur du BTC dans les 12 à 18 mois qui l'ont suivi (cf. fig.35). En gonflant artificiellement la demande avant l'événement, cette vague d'escroquerie pourrait avoir pour objectif d'augmenter le prix des actifs – qui a connu un pic record le 11 mars dernier avec plus de 72 000\$ – rendant le *halving* encore plus rentable qu'espéré.

Fig.35 – Evolution du prix du bitcoin au fil des halving³⁵



Dans les opérations de *pump-and-dump*³⁶, les salles de chaufferie jouent un rôle majeur. Nos recherches sur le sujet ont vu le nom de « Milton Group » revenir fréquemment. Cette organisation créée en 2016 et initialement basée à Kiev possède plusieurs centres d'appels en Ukraine, en Albanie et en Géorgie. Elle s'est illustrée dans la fraude aux options binaires sous un mode opératoire similaire à celui qui nous occupe³⁷: des victimes appâtées par des publicités sur Facebook exploitant des célébrités puis ferrées par des agents commerciaux sans scrupules.

Malgré les mises en cause dont il fait l'objet dès 2018 et les perquisitions dans ses centres albanais fin 2022, Milton Group, devenu Brain Pro LLC et installé à Lviv depuis 2021, poursuit ses activités³⁸. Nous n'avons pas poussé l'investigation jusqu'aux centres d'appels mais il se pourrait que cette organisation soit impliquée dans la vaste escroquerie en cours.

35- Cryptoast, Qu'est-ce que le halving du Bitcoin (BTC) et quels sont ses effets ? 9 avril 2024. <https://cryptoast.fr/halving-explication-impacts-bitcoin-crypto/>

36- Manipulation de marché consistant à faire massivement acheter des actions en usant de la ruse (p.ex. fausses informations) afin d'en faire grimper le prix (*pump*) et de revendre ses actions avec une forte plus-value. Les victimes ayant investi voient alors la valeur de leurs actifs chuter (*dump*). Investopedia, How Does a Pump-and-Dump Scam Work ? Jan 13, 2022. <https://www.investopedia.com/terms/b/boilerroom.asp>

37- OCCPR, Trail of Broken Lives Leads to Kyiv Call Center, Mar 2, 2020. <https://www.occrp.org/en/fraud-factory/trail-of-broken-lives-leads-to-kyiv-call-center>

38- Antikor, Milton group call centers are robbing people again. Feb 14, 2024. https://antikor.com.ua/en/articles/683358-koll-tsenry_milton_group_snova_grabjat_ljuddej_kak_skandaljnoj_organizatsii_udaetsja_izbegatj_nakazaniya