Capacités marketing des plateformes de fraudes publicitaires : la face cachée du marketing digital

Jean-Loup Richet

IAE de Paris, France

Résumé :

Bannières, liens promotionnels, publicités sur les réseaux sociaux ou encore les moteurs de recherche, les canaux publicitaires ne manquent pas sur le web. Si les dépenses en marketing digital augmentent tous les ans, 10 à 20 % de celles-ci partent directement dans les poches de cybercriminels. La fraude publicitaire est un réel enjeu pour les praticiens. Cependant, cet enjeu rencontre assez peu d'échos dans la littérature académique. Au travers d'une web ethnographie de plateformes de fraudes publicitaires, nous nous sommes intéressés aux capacités marketing déployées par ces plateformes cybercriminelles pour développer et délivrer de la valeur aux fraudeurs. Cette investigation nous amène à conceptualiser une typologie de fraudes publicitaires, mais également à contribuer aux théories des plateformes de collaboration.

Mots clés :

Fraude publicitaire, capacités marketing, plateforme, cybercrime, ethnographie

Capacités marketing des plateformes de fraudes publicitaires : la face cachée du marketing digital

1. Fraude publicitaire : un enjeu de plus en plus important pour les praticiens

Au début des années 2000, la fraude publicitaire était l'une des raisons principales pour lesquelles les praticiens étaient hésitant à se lancer dans le web marketing (Advertising Age, 2006). Où en sommes-nous aujourd'hui ?

Chaque année, les dépenses des marketeurs américains augmentent de plus de 10 % : cela représentait un total de 72,5 milliards de dollars en 2017 (IAB, 2017). Et pourtant, les pertes économiques liées à la fraude publicitaire ne cessent d'augmenter, atteignant les 6,5 milliards de dollars en 2017 (ANA, 2017). Ces pertes, si elles peuvent sembler élevées, ne sont cependant que la face émergée de l'iceberg. En effet, les statistiques disponibles ignorent les cas de fraudes réalisées sur le périmètre des deux géants publicitaires que sont Facebook et Google, qui représentent un tiers des dépenses des marketeurs américains (Fou, 2017). Ces montants ne prennent pas non plus en compte les cas de fraudes sur les impressions publicitaires — techniques de fraudes visant à générer artificiellement des affichages publicitaires, qui seront comptabilisés à tort et facturés à l'annonceur. La fraude publicitaire est donc toujours un problème de taille pour les praticiens (Fou, 2017).

Les tendances technologiques laissent présager le renforcement des attaques massives menées par des robots (ANA, 2017). L'usage de robots alimentés par l'Intelligence Artificielle permettra aux fraudeurs de conjuguer scalabilité et adaptation : mener des attaques à grande échelle, mais autant efficaces dans l'imitation des comportements humains, permettant d'outrepasser les contrôles et les règles de détection des fraudes (Hitaj et al. 2017; Bahnsen et al. 2018).

2. Les plateformes cybercriminelles

Les communautés criminelles traditionnelles se sont adaptées aux tendances technologiques pour développer leurs profits : le crime organisé développe de nouvelles activités comme la revente de fausses identités sur le web, les arnaques en ligne, le phishing, les money mules (Choo, 2008; Wall, 2003). Néanmoins, ces communautés traditionnelles de type « click and mortar » différent sensiblement des « pure players » du web, ces communautés en ligne dont les activités sont mises en œuvre entièrement sur le web : conception de logiciels malveillants, fraude publicitaire en ligne, attaques informatiques et réseaux de robots (Richet, 2015; Van der Wagen & Pieters, 2015). Ces communautés cybercriminelles sont faiblement couplées, favorisant le lien faible, les projets temporaires, l'anonymat, l'expertise technique, et ont fréquemment une dimension transnationale permise par les NTIC (Brenner, 2002).

Les communautés cybercriminelles ont néanmoins besoin de « cadres de convergence » (Soudijn & Zegers, 2012), des espaces de partage en ligne où ils pourront échanger de l'information, de la connaissance, rechercher de nouveaux partenaires d'affaires ou des missions. Ces « cadres de convergence » sont des lieux de rassemblement plus ou moins persistants, facilitant les interactions entre criminels et leurs échanges (Felson, 2006). La littérature s'intéressant à l'organisation de la cybercriminalité a peu développé la

conceptualisation de ces lieux d'échanges (Leukfeldt, 2014; Soudijn & Zegers, 2012). Les plateformes permettent justement ces échanges en mettant en relation les différents groupes et parties prenantes en réduisant leurs coûts de transaction (Gawer, 2011; Tiwana, 2014). Les plateformes sont des lieux où se mêlent coopération et compétition (Tiwana & Konsynski, 2010), permettant la coordination spatio-temporelle d'acteurs hétérogènes et interdépendants (Isckia, 2011).

Le concept de plateforme est particulièrement intéressant pour explorer la complexité des communautés cybercriminelles, également partagées par des problématiques de compétition et coopération (Lusthaus, 2013), de co-production nécessitant des formes distribuées de coordination (Wall, 2015), et permettant la mise en relation des parties prenantes diverses (Wall, 2007).

3. Ouvrir la boîte noire de la fraude publicitaire

Les recherches antérieures se sont intéressées principalement à un type de fraude, la fraude au clic — des scripts ou robots destinés à (1) cliquer sur les publicités des concurrents pour leurs faire épuiser leurs budgets publicitaires ; ou (2) cliquer sur les publicités d'un site donné pour que le propriétaire du site génère des revenus publicitaires (pay per click). Les recherches se sont ainsi intéressées aux fraudes et à leurs impacts sur les revenus des moteurs de recherche (Wilbur et Zhu, 2009) ou encore les cas de fraudes aux clics liées à des fraudes à l'affiliation marketing (Edelman et Brandi, 2015). Cependant, « *le sujet de la fraude publicitaire n'a pas eu beaucoup d'échos dans le monde académique depuis Wilbur et Zhu (2009)* » (Lamberton et Steven, 2016, p.158). C'est ce hiatus entre recherche et pratique que nous nous proposons d'explorer, au travers de notre recherche sur la face cachée du marketing digital.

Sur le plan conceptuel, la littérature existante à la frontière du marketing et des SI n'a pas étudié suffisamment dans le détail les mécanismes et les origines des différents types de fraudes publicitaires.

Sur le plan théorique, notre recherche souhaite développer la théorie des plateformes au prisme des théories en marketing (Yadav et Pavlou, 2014). Nous nous concentrerons en effet sur le rôle des capacités marketing (Moorman et Day, 2016) dans le contexte des plateformes cybercriminelles promouvant les fraudes publicitaires — des capacités de perception et de réactivité au marché (génération de connaissances, dissémination et réponse) et des capacités relationnelles (gestion de la relation avec les parties prenantes de la plateforme et gestion de la marque de la plateforme). Ces capacités marketing, capacités de connaissance du marché, de gestion des clients et de la marque ont été peu étudiées dans le contexte du marketing digital (Moorman et Day, 2016).

4. Méthodologie de la recherche

4.1 Une ethnographie des plateformes de black hats SEO

Notre recherche est basée sur une web ethnographie réalisée sur 12 mois, de Décembre 2017 à Décembre 2018 (Arnould et Wallendorf, 1994). Les formes de conversations observées dans le cadre d'une web ethnographie sont asynchrones, engagent de nombreux interlocuteurs simultanément (effectifs comme potentiels), avec une temporalité d'échanges étendue (Garcia, Standlee, Bechkoff, & Cui, 2009). Dans cette approche de nature abductive,

nous avons émis des observations empiriques que nous avons progressivement conceptualisées puis théorisées.

Nous nous sommes intéressés aux plateformes de « black hats SEO » — place de marché cybercriminelles et lieux d'échanges d'information autour des fraudes liées au SEO (optimisations frauduleuses du positionnement dans les moteurs de recherche), arnaques publicitaires ou cybercriminalité.

En particulier, nous avons travaillé sur (1) l'identification des capacités marketing développées par les « gérants » des plateformes et (2) l'évaluation de la performance des plateformes (effets des capacités marketing, rétention, fidélisation, etc.).

La méthode de recherche pourrait sembler aux antithèses des préconisations de la littérature : l'éthique de la recherche impose de révéler aux observés qu'ils font l'objet d'une recherche et d'obtenir leur accord (consentement éclairé), de différencier les éléments publics des éléments privés, de maintenir la confidentialité et l'anonymat des sujets, et enfin de se présenter en tant que chercheur (Kozinets, 2002; Wilson & Peterson, 2002). Néanmoins, dans le contexte de recherches sur la cybercriminalité, les investigations adoptent les codes des agences de renseignement et d'enquête digitale (Broséus et al., 2016; Ciardhuáin, 2004; Hunton, 2011). Le contexte change en effet la pertinence des préconisations méthodologiques : les criminels utilisent des pseudonymes et prennent particulièrement soin de leur anonymat (usage de VPN, Tor, emails jetables, fausses identités voire vol d'identité), il n'y a pas d'éléments privés dans le contexte de communautés d'affaires, l'accord des observés est impossible, car il mettrait immédiatement fin à la recherche (Lillis, Becker, O'Sullivan, & Scanlon, 2016; Raghavan, 2013). Enfin, la divulgation de l'affiliation du chercheur serait particulièrement dangereuse pour ce dernier (Adler, 1998).

4.2 Enjeux de données : une exploration des plateformes cybercriminelles

Les plateformes qui font l'objet de notre étude peuvent être accédées de deux façons. Certaines proviennent de l'internet classique (clear web), facilement accessible via les moteurs de recherche, et nécessitant une inscription. D'autres proviennent d'un darknet (Tor dans notre cas), accessible via la connaissance de l'adresse précise du service caché (.onion), inscription et éventuellement test à l'admission. Ces plateformes enregistrent tous les échanges utilisateurs, donc nous avons pu accéder à tous les échanges publics passés entre membres de 2011 à 2018.

Nous avons sélectionné quatre plateformes basées sur les suggestions d'un panel d'expert du Cepol et d'Europol. Notre sélection comprenait deux plateformes du clear web, et deux plateformes du darknet.

4.3 Collecte et analyse des données

Nous avons réalisé des notes de terrain et d'observation (n=240) pendant toute la période de web ethnographie (Décembre 2017 à Décembre 2018), accompagnées d'enregistrements sous forme d'image des discussions objet de notre observation (n=180). Nous n'avons pas réalisé d'interactions et sommes restés observateurs passifs des échanges commerciaux et d'informations. Des mesures ont été prévues pour réduire les biais liés à la collecte et à l'interprétation des données. Un panel d'expert du Cepol et d'Europol a été sollicité tout au long de la recherche pour évaluer les notes de terrain. De plus, nous avons comparé nos observations avec des données externes fournies par Europol et Interpol sur la

cybercriminalité. Enfin, notre expertise auprès d'Europol et nos connaissances dans le domaine de la cybercriminalité nous ont permis de reconnaitre plus facilement les codes de ces organisations criminelles (Emerson et al., 2011), et étaient nécessaires pour la validité interne de notre recherche (Patton 2005).

Notre stratégie d'analyse de données est inspirée de la théorie enracinée (Birks et al., 2013). Dans un premier temps, nos codes descriptifs et analytiques nous ont permis de développer une compréhension des plateformes de fraude publicitaire et de leurs caractéristiques. Ensuite, dans une seconde phase de codage sélectif, nous nous sommes concentrés sur l'identification et la documentation des capacités marketing et de la performance de ces plateformes. Enfin, dans une dernière étape, nous avons cherché à déterminer des relations causales entre les propriétés identifiées de nos données (Charmaz, 2006) dans le but d'affiner notre théorisation (Glaser et Strauss, 1999).

5. Résultats préliminaires

Nos résultats préliminaires laissent à penser que les dynamiques entre capacités marketing et performance de la plateforme sont amplifiées par des effets de réseau. En particulier, nous mettons en avant le rôle central de la variété requise pour le développement de la plateforme cybercriminelle dans sa capacité à développer et délivrer de la valeur à ses utilisateurs. L'exemple de la Figure 1 ci-dessous montre un appel à collaboration entre un développeur spécialiste en création de malware et des spécialistes des fraudes marketing. Le but est d'infecter des utilisateurs avec un malware afin que ces utilisateurs infectés puissent être utilisés dans une fraude à l'affiliation marketing (CPA).

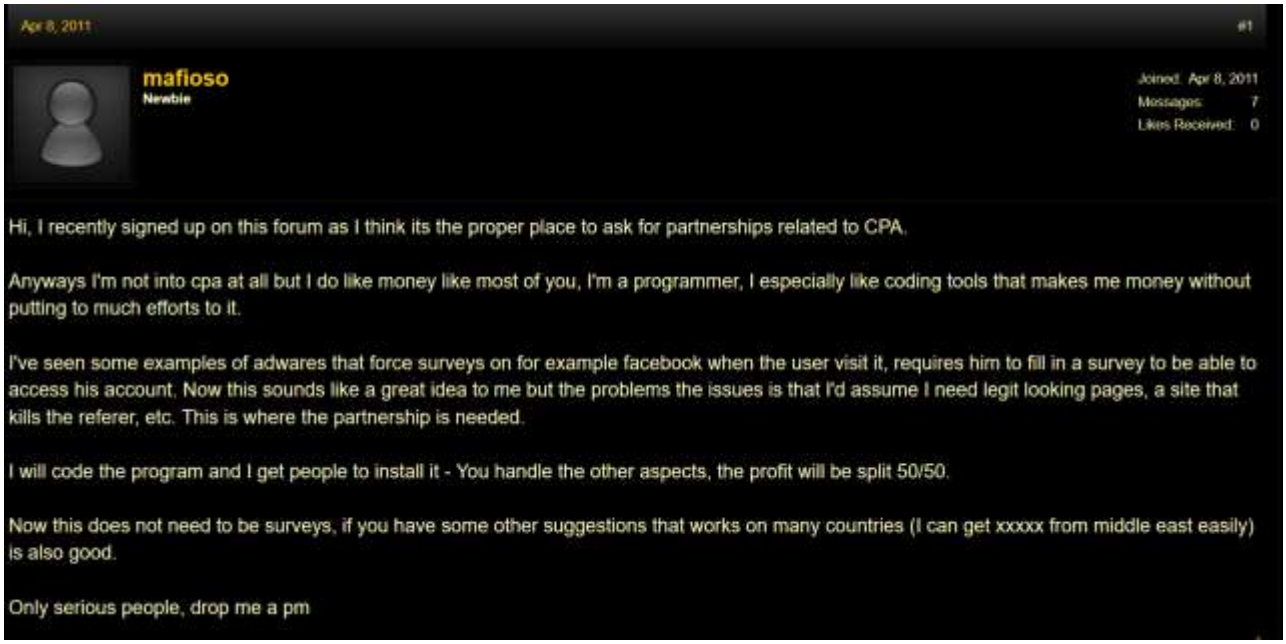

Figure 1 : diversité de profils utilisateurs de la plateforme de fraude publicitaire

Nos résultats préliminaires suggèrent que la variété requise est centrale, tant dans le renforcement des capacités marketing que comme condition nécessaire à la performance de la plateforme de fraude publicitaire.

Ensuite dans notre exploration de la contribution des capacités marketing à la performance de la plateforme, nous avons documenté des cas de user-led innovations (co-création de robots de fraudes publicitaires comme sur la Figure 2, usages disruptifs et frauduleux d'outils de big data ou de machine learning, etc.).

Figure 2 : cas d'innovations collaboratives mises en œuvre par les utilisateurs de la plateforme

Notre papier entend également fournir une typologie des fraudes publicitaires : liées à l'utilisateur (fraudes sociales, de recherche et à l'impression) ou à l'attribution (fraudes aux clics, à la conversion ou aux données).

6. Limitations et conclusion

Notre travail de recherche comporte plusieurs limitations, liées aux difficultés de mesures de la performance et de l'effort marketing dans le contexte de communautés cachées ou difficiles d'accès. Les études quantitatives en sont d'autant plus complexifiées.

L'analyse des données est encore en cours, mais nos résultats préliminaires nous suggèrent plusieurs contributions pratiques et théoriques potentielles.
Nous répondons tout d'abord à un fort besoin des praticiens (ANA, 2017) :
– publicitaires : besoin de surveiller les tendances cybercriminelles pour protéger leurs clients et proposer le meilleur service (la sécurité comme avantage compétitif).
– marketeurs : protéger la marque (surveiller les tendances pour repérer les faux sites usurpant la marque dans le cadre d'une fraude publicitaire), et remettre en question la transparence des régies publicitaires (sources de trafic, pratiques d'extension d'audience, etc.).
– Agences de renseignement et de lutte contre la cybercriminalité : combattre les plateformes de fraude publicitaire en perturbant la façon dont elles délivrent de la valeur à leurs utilisateurs, et la façon dont ces plateformes combinent et déploient leurs capacités marketing. Réduire les effets de réseau en attaquant la variété requise (renforcer les contraintes sur tous les composants de la chaine de valeur, comme les développeurs par exemple).

Enfin, nous contribuons à la littérature sur les plateformes de collaboration et répondons à un besoin de recherches dans ce domaine à la frontière entre SI et marketing (Yadav et Pavlou, 2014 ; Moorman et Day, 2016). En effet, nos résultats préliminaires nous amènent à penser le rôle d'intermédiation de la variété requise dans la relation entre capacités marketing et performance de la plateforme. Adresser la variété requise crée de la valeur pour l'utilisateur, permet la co-création d'innovations utilisateurs tout en renforçant les capacités marketing par le fait d'effets de réseaux.

Références

Advertising Age. (2006). *Search Marketing Fact Pack 2006*. (AdAge)

Adler, P. (1998). *Ethnography at the edge: Crime, deviance, and field research*. UPNE.

Brenner, S. W. (2002). Organized cybercrime-how cyberspace may affect the structure of criminal relationships. *NCJL & Tech.*, *4*, 1.

Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., & Décary-Hétu, D. (2016). Studying illicit drug trafficking on Darknet markets: structure and organisation from a Canadian perspective. *Forensic science international*, *264*, 7-14.

Choo, K.-K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in organized crime, 11*(3), 270-295.

Ciardhuáin, S. Ó. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, *3*(1), 1-22.

Felson, M. (2006). *The ecosystem for organized crime*. European Institute for Crime Prevention and Control, affiliated with the ….

Garcia, A. C., Standlee, A. I., Bechkoff, J., & Cui, Y. (2009). Ethnographic approaches to the internet and computer-mediated communication. *Journal of contemporary ethnography*, *38*(1), 52-84.

Gawer, A. (2011). *Platforms, markets and innovation*. Edward Elgar Publishing.

Hunton, P. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital Investigation*, *7*(3), 105-113. https://doi.org/10.1016/j.diin.2011.01.002

Isckia, T. (2011). Ecosystèmes d'affaires, stratégies de plateforme et innovation ouverte : vers une approche intégrée de la dynamique d'innovation. *Management & Avenir, n° 46*(6), 157-176. https://doi.org/10.3917/mav.046.0157

Kozinets, R. V. (2002). The field behind the screen: Using netnography for marketing research in online communities. *Journal of marketing research*, *39*(1), 61-72.

Leukfeldt, E. R. (2014). Cybercrime and social ties. *Trends in organized crime*, *17*(4), 231-249.

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. *arXiv preprint arXiv:1604.03850*.

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, *14*(1), 52-60.

Raghavan, S. (2013). Digital forensic research: current state of the art. *CSI Transactions on ICT*, *1*(1), 91-114. https://doi.org/10.1007/s40012-012-0008-7

Richet, J.-L. (2015). *Decentralized Cryptographic Information Black Market*. Cybercrime, Cybersecurity and Cyberwarfare.

Soudijn, M. R., & Zegers, B. C. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in organized crime*, *15*(2-3), 111-129.

Tiwana, A. (2014). *Platform ecosystems aligning architecture, governance, and strategy*. Morgan Kaufmann Publishers.

Tiwana, A., & Konsynski, B. (2010). Complementarities Between Organizational IT Architecture and Governance Structure. *Information Systems Research*, *21*(2), 288-304. https://doi.org/10.1287/isre.1080.0206

Van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British journal of criminology*, *55*(3), 578-595.

Wall, D. (2003). *Crime and the Internet*. Routledge.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

Wall, D. (2015). Dis-organised crime: Towards a distributed model of the organization of cybercrime. *The European Review of Organised Crime*.

Wilson, S. M., & Peterson, L. C. (2002). The anthropology of online communities. *Annual review of anthropology*, *31*(1), 449-467.