Comment fonctionne l'industrie de la pornographie en ligne

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 septembre 2010

https://www.bortzmeyer.org/internet-for-porn.html

Il y déjà eu plusieurs études sur le monde de la pornographie sur l'Internet, comme l'article de Benjamin Edelman <https://www.bortzmeyer.org/who-buys-porn.html>. Mais cet article de Gilbert Wondracek, Thorsten Holz, Christian Platzer, Engin Kirda et Christopher Kruegel, présenté au "*Ninth Workshop on the Economics of Information Security*" <http://weis2010.econinfosec.org/> apporte du nouveau : les auteurs ont plongé dans ce monde et créé des entreprises participant à ce "*business*", pour mieux l'étudier.

Leur article, "*Is the Internet for Porn ? An Insight Into the Online Adult Industry*", est disponible en ligne <http://weis2010.econinfosec.org/papers/session2/weis2010_wondracek.pdf>. Il est très intéressant et les auteurs ont vraiment pensé à tout dans leur étude de ce sujet. J'imagine bien la tête qu'ont dû faire les avocats de leur université lorsqu'ils ont présenté leur projet « devenir vendeur en e-porno ». Une section de leur article est d'ailleurs consacrée aux règles que leur a fixé leur comité d'éthique, notamment l'interdiction de gagner de l'argent lors de cette expérience. Ils ont donc dû arrêter chaque opération au moment où elle devenait rentable.

Donc, après avoir passé du temps à récolter de longues listes de sites Web porno, nos courageux chercheurs, qui ne reculent devant rien lorsque le progrès de la science est en jeu, ont défini une typologie des différents acteurs. Je pensais personnellement que la même enterprise contrôlait toute la filière, de la prise des photos ou des films jusqu'au site Web. Mais pas du tout. Il existe de nombreux intermédiaires, par exemple des courtiers qui mettent en relation les gens qui reçoivent du trafic (par exemple parce qu'ils détiennent des noms de domaine au nom suggestif) et veulent le monétiser avec les gérants des sites pornos payants qui veulent recevoir du trafic. Le courtier achète aux premiers du trafic qu'ils revendent aux seconds, en prélevant leur part.

L'expérience pouvait ensuite commencer : les auteurs se sont inscrits à plusieurs programmes dans le monde du e-porno, changeant de rôle au fur et à mesure. Le milieu, qu'ils pensaient fermé, s'est au contraire révélé très ouvert et ils ont toujours été acceptés, même lorsque le site Web qu'ils avaient créé

rassemblait toutes les mauvaises pratiques. Par exemple, lors de l'adhésion à un programme d'affiliation, dans six cas sur huit, le site Web n'a enregistré aucune visite avant l'acceptation !

Compte-tenu des sommes en jeu et de l'attitude hypocrite de la société vis-à-vis de la pornographie (légale mais mal vue), il n'est pas étonnant que le milieu du e-porno se caractérise par une éthique assez faible. Ainsi, les chercheurs ont pu vérifier que les promesses (un moteur de recherche spécialisé dans le porno qui affirme que sa base de sites a été compilé manuellement après vérifications, un courtier qui prétend refuser de rediriger du trafic vers des sites utilisant des cadres cachés, ...) étaient rarement tenues. De la même façon, les horreurs comme les astuces JavaScript pour rendre plus difficile la sortie du site sont monnaie courante. Il est parfois difficile de pointer les responsabilités : ainsi, les auteurs ont trouvé une importante proportion de sites Web porno distribuant du "*malware*" mais sans pouvoir être sûr que c'était une décision du gérant du site. Il semble au contraire que les sites Web porno, comme ils reçoivent beaucoup de trafic, sont plus souvent piratés que les autres, par des méchants qui installent le code malveillant ensuite.

Autre escroquerie courante, lors de paiements au clic, les divers systèmes de multiplication, comme de vendre le même clic à plusieurs courtiers. Les auteurs, lorsqu'ils étaient acheteurs de trafic, ont pu voir un seul clic sur un site Web leur être compté 3,8 fois. En sens inverse, lorsqu'ils jouaient le rôle du vendeur de trafic, ils ont pu vendre leur trafic à deux courtiers différents sans être détectés. En combinant les deux techniques (acheter du trafic à un courtier et le rediriger à deux courtiers ou davantage), on gagne de l'argent sans beaucoup se fatiguer...

Le code du site Web des chercheurs a aussi servi à analyser les clients. Le nombre de logiciels vulnérables détectés est important, menant au calcul qu'avec un investissement de seulement 160 US $ (pour acheter du trafic), on peut compromettre 20 000 machines... Si on ne veut pas tout faire soi-même, pas de problème, il existe même des entreprises à qui vous fournissez le code et qui se font payer au nombre d'installations réussies sur les machines des utilisateurs (130 US $ pour mille installations, avec possibilité de choisir le pays, car il est plus intéressant de contaminer une machine norvégienne qu'une coréenne, déjà mise dans toutes les listes noires de la planète). Certains "*malware*" prévenant de leur présence en modifiant le champ `User-Agent:` du protocole HTTP, les auteurs ont pu d'ailleurs voir que bien des visiteurs étaient déjà infectés.

Bref, un monde fort intéressant, où l'important trafic généré crée un écosystème pour toutes sortes de gens pas toujours sympathiques.