

# UK AD CAMPAIGN

## Royaume-Uni



### Description du programme

Le UK Ad Campaign est une campagne publicitaire ayant pour but de dissuader les jeunes hommes âgés entre 13 et 22 ans de commettre des attaques par cheval de Troie ou par déni de service (*Denial of Service* (DoS)). Les annonces payantes encouragent des rôles éthiques en matière de cybersécurité.

### Thématiques

La campagne publicitaire cible seulement:

- Les chevaux de Troie
- Les attaques par déni de service

### Intervention

- Il s'agit d'une campagne publicitaire en ligne à travers des publicités Google (Google Ads);
- Lorsqu'un individu recherche Google les termes «booter» ou «stresser» à partir d'une adresse IP provenant du Royaume-Uni, une annonce payante apparaîtra sur la première page des résultats et avertissant que l'utilisation de ces services pour attaquer d'autres personnes en ligne est illégale.
- Les annonces payantes renvoient à des publiportages ou encore au Cybersecurity Challenge du Royaume-Uni, qui rend ludique les concepts de sécurité informatique, par l'entremise d'ateliers, de jeux ou encore de défis, dans le but de favoriser l'utilisation adéquate du potentiel présent chez ces jeunes hommes.

### Le programme en quelques mots

**Objectif du programme:** L'objectif global de la campagne publicitaire est de dissuader l'utilisation des chevaux de Troie et des attaques par déni de service (DoS).

**Population cible:** jeunes hommes âgés entre 13 et 22 ans

**Date de mise en oeuvre:** décembre 2017

**Statut du programme:** N/D

**Organisation instigatrice:** National Crime Agency (NCA)

**Portée géographique:** nationale

## Évaluation du programme

L'évaluation de la campagne publicitaire a été réalisée dans le cadre d'un [article](#) publié par l'IMC, rédigé par Ben Collier, Richard Clayton, Daniel R. Thomas et Alice Hutchings en 2019.

Afin d'évaluer le programme, les auteurs ont utilisé les données suivantes, collectées sur une base hebdomadaire:

- le nombre d'attaques par déni de service par semaine
- L'implantation du programme en question.
- Les signalements des booters eux-mêmes sur le nombre d'attaques qu'ils ont commis.

## Résultats et impacts

- La campagne publicitaire a provoqué une réduction du nombre d'attaques sur les adresses IP britanniques. À titre de comparaison, alors que les États-Unis et le Royaume-Uni présentent des taux similaires d'attaques, lors de la campagne publicitaire, ce taux a réduit considérablement au Royaume-Uni, atteignant presque zéro.
- La campagne publicitaire a conduit à une réduction durable du nombre d'attaques.
- L'augmentation des attaques au Royaume-Uni provient d'une demande accrue pour les attaques par déni de service par les nouveaux utilisateurs qui entrent sur le marché des booters. La campagne aurait eu un effet de dissuasion au niveau de l'engagement de ces nouveaux utilisateurs, pendant une période d'environ 7 à 8 mois.
- Bien que les publicités n'affectent pas le comportement de ceux qui sont déjà impliqués dans ce type d'attaque, la campagne semble avoir stoppé l'augmentation des attaques par déni de service au Royaume-Uni durant la période durant laquelle elle était active.
- En 30 jours, l'annonce a généré plus de 5,3 millions d'impressions et 57 000 cliques.



Chaire de recherche  
en prévention de la cybercriminalité

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.



[www.prevention-cybercrime.ca](http://www.prevention-cybercrime.ca)



<https://www.linkedin.com/company/crpc-rccp>



@CRCP\_RCCP