https://ricochets.cc/Ne-jamais-eteindre-son-telephone-une-nouvelle-approche-a-la-culture-de-la.html

Ne jamais éteindre son téléphone : une nouvelle approche à la culture de la sécurité

- Les Articles -
Date de mise en ligne : samedi 15 décembre 2018

Dans les années 80, un/e anarchiste qui voulait, par exemple, mettre le feu à un bâtiment, élaborait son plan et en même temps elle/il regardait s'il n'y avait pas de dispositifs d'écoute chez lui/elle. A la fin des années 90, le/la même anarchiste éteignait le téléphone et utilisait des messages cryptés sur internet. **Dans les années 2020, il nous est nécessaire de repenser notre stratégie : la collecte d'informations s'est améliorée et nous devons tenir compte aussi de cela.**

Pour commencer, regardons comment l'analyse des données est utilisée. Pour ce faire, nous devons parler de trois choses : les métadonnées, les modèles et les réseaux. Cela semble ennuyeux et difficile, mais je ne suis pas un technicien et je ne vais pas vous ennuyer avec un langage technique ; je ferai les choses les plus simples possibles.

Métadonnées (metadata) : dans le contexte de l'activité en ligne, « le contenu » signifie « le message qu'on envoie » tandis que « métadonnées » signifie « tout sauf le contenu ». Si par exemple vous envoyez à un ami un texte à propos d'un dîner, le contenu peut être : « Allons dîner » et les métadonnées peuvent être : « Message envoyé le 01/04/2018 à 11h32, depuis le numéro 0478239055 au numéro 079726823, en utilisant Signal ».

Cette information est enregistrée par votre téléphone, même si l'application crypte votre vrai message. Vos métadonnées sont très peu protégées par la technologie et très peu protégés par la loi. Peu importe dans quel pays vous êtes, la plupart de vos métadonnées sont librement accessibles aux services spécialisés, indépendamment du fait que vous soyez suspectés de quelque chose ou pas.

Modèles (templates) : que vous vous en rendiez compte ou pas, vos métadonnées ont un modèle. Si vous travaillez toute la journée, vous pouvez avoir une configuration (pattern) très uniforme ; s'il n'y a pas un travail, votre modèle peut être plus flexible, mais vous avez un modèle. Si quelqu'un veut connaître le rythme de votre journée, il peut le faire très facilement, parce que votre modèle est dans les métadonnées.

Par exemple : peut-être que vous utilisez le Wi-Fi dans votre bar préféré la plupart des dimanches soirs, jusqu'à minuit, vous vous levez vers 10h du matin et contrôlez votre messagerie Signal, vous utilisez votre Navigo pour aller en cours le lundi aprèm, et vous passez environ 1 heure sur Timblr deux fois par jour. Tout cela fait partie de votre modèle.

Réseau : Vous avez un réseau en ligne. Vos amis sur Facebook, les personnes dans l'agenda de votre portable, le Dropbox que vous partagez avec vos collègues, tou.te.s celles/ceux qui achètent en ligne les billets pour le même concert punk que vous, les personnes qui utilisent le même Wi-Fi que vous. Prenez vos réseaux, combinez-les avec les réseaux d'autres personnes et les agrégats (clusters) se montreront tous seuls. Votre entourage de travail, votre famille, votre milieu activiste, etc.

Si vous participez au milieu anarchiste, cela est susceptible d'être tout à fait évident de par toutes vos petites connections au réseau, comme aller voir le même groupe de musique et connaître les mêmes personnes que les autres anarchistes. Même si vous n'avez jamais cliqué sur une page Facebook d'anarchistes, ou jamais cliqué sur le bouton « j'y vais » d'un événement anarchiste sur Facebook, c'est difficile de cacher votre réseau.

Maintenant, disons que vous avez commis un crime, quelque chose qui porterait à des investigations sérieuses.

Supposons que dimanche à 3 heures du matin, vous et vos amis alliez incendier la maison d'un nazi. (Bien sûr, je ne dirais jamais à aucun de vous de faire quelque chose comme ça) C'est évident que ce sont les anarchistes qui l'ont fait, mais il n'y a pas de pistes. Vous vous appuyez sur une culture de la sécurité traditionnelle : vous brûlez vos

notes, vous essayez de ne pas parler de vos plans à côté d'appareils technologiques et vous ne laissez aucune trace physique.

Mais puisque vous avez commis un crime cette nuit-là, vos métadonnées seront très différentes de votre rythme habituel : vous restez dans votre bar habituel jusqu'à 2 heures du matin pour attendre vos amis, vous ne vous réveillerez pas à 10 heures pour contrôler votre messagerie Signal ou vous resterez sur Tumblr seulement pendant une heure de la journée. Vous n'irez pas en cours. Votre modèle de métadonnées est très diffèrent de votre modèle normal. Les modèles de métadonnées de vos amis sont différents aussi. Si l'un de vous est maladroit, ils peuvent générer un signal de métadonnées hautement suspect, par exemple le téléphone est éteint à 2h30 de la nuit et il est activé à 4 heures du matin. Vous ne seriez pas les premiers.

Si je voulais résoudre ce crime en utilisant l'analyse des données, je procéderais de la sorte :

- mettre un logiciel à analyser les configurations du milieu anarchiste local, afin d'identifier le 300 personnes les plus liées au milieu anarchiste ;

- mettre un deuxième logiciel à analyser des extraits de métadonnées de ces 300 personnes des derniers mois, afin d'identifier les changements les plus importants dans ces métadonnées, ce dimanche soir, tout comme toute activité de métadonnée hautement suspecte ;

- exclure les variations de configuration qui ont un motif évident ou un alibi évident (des personnes qui sont en vacances, celles qui sont à l'hôpital, celles qui ont perdu leur travail, etc.)

- procéder à une étude plus approfondie de ceux/celles qui restent.

C'est ça : de l'énorme nombre de personnes que je ne pourrais pas interroger en même temps, je peux rapidement en identifier un petit nombre, de façon à pouvoir les contrôler de près. Ainsi, je pourrais vous trouver et vous chopper.

Et du coup ?

Si une culture de la sécurité traditionnelle ne nous protège pas comme avant, comment nous adapter ? Eh bien, je n'ai pas de réponses, mais pour commencer je dirais : connaissez votre réseau et connaissez votre modèle.

Dans le cas de l'exemple de toute à l'heure : quittez le bar à minuit, rentrez chez vous et mettez le téléphone sur votre table de chevet. Contrôlez les applications que vous contrôlez habituellement avant d'aller dormir et mettez votre réveil à 10h. Retournez au bar sans téléphone. Réveillez vous à 10h du matin et contrôlez votre messagerie Signal. Ramenez-vous en cours ou demandez à un amis de voyager avec votre Navigo et n'utilisez pas de technologie chez vous pendant qu'il le fait. Tenez-vous en à votre modèle. N'éteignez jamais le téléphone.

Vous pouvez aussi manipuler votre réseau, mais cela est beaucoup plus difficile. Ne pas utiliser de smartphone de manière générale et abandonner toute activité sociale sur internet - cela demande une motivation sérieuse. Connaître votre modèle de données et s'assurer qu'il apparaisse ordinaire est plus facile.

Certaines des anciennes règles s'appliqueront encore : ne pas parler du crime à côté d'appareil munis de microphones, ne pas se vanter après des actions qui ont eu du succès, etc. D'autres règles, comme « éteindre le

téléphone quand on organise des actions illégales », doivent être changées, puisque leur métadonnée paraît trop inhabituel. Personne d'autre déconnecte son téléphone. Nous devenons suspects quand nous le faisons.

Cela est seulement une idée de comment nous pouvons mettre à jour notre culture de la sécurité. Peur-être qu'il y a d'autres personnes avec d'autres idées, meilleures, sur comment le faire. Si une discussion commence, on peut arriver quelque part.

Enfin : il faut continuer à s'adapter

Comme la technologie change, de plus en plus d'informations émergent, y compris des données sur lesquelles nous avons très peu de contrôle. En sont des exemples les smart-TV et les panneaux publicitaires qui écoutent chaque mot que nous disons dans les lieux publiques, ainsi que le ton de notre voix quand nous parlons. A l'heure actuelle, les projets d'analyse de données utilisent des logiciels de lecture de plaques minéralogiques afin de comparer des configurations de circulation de véhicules. Cela en dit long sur le le fait qu'ils seront bientôt prêts à faire de même avec la reconnaissance faciale, après quoi la présence de notre visage dans l'espace public deviendra partie de nos métadonnées. Des informations supplémentaires signifient une analyse des données plus précise. Notre métadonnée pourrait bientôt être trop vaste, ce qui veut dire qu'il sera trop difficile pour nous d'en tenir compte et de le reconstituer complètement. Cela signifie qu'il nous faudra adapter nos contre-mesures si nous voulons cacher quelque chose.

Comment garder tout cela secret ? Je ne sais pas. Mais essayons de comprendre toute cette merde. Ce sont mes premières réflexions sur ce à quoi devrait correspondre une culture de la sécurité dans une époque d'analyse moderne de grands panels de données, et je serais très contents de recevoir des compléments de la part de camarades qui ont des idées à ce propos.

Aussi, sentez-vous libres de diffuser et modifier ce texte sans références.