ZOOM

ENQUÊTE SUR LES LOGICIELS ESPIONS DANS LE CADRE DES VIOLENCES CONJUGALES

centre hubertine auclert

ilede France

Le Centre Hubertine Auclert a conduit en 2018 une enquête sur les logiciels espions dans le cadre de sa recherche-action sur les cyberviolences conjugales.

Les logiciels espions permettent de surveiller les activités, les communications et les déplacements. Téléchargés sur un téléphone ou un ordinateur, ils ne sont pas facilement détectables. L'installation et l'utilisation d'un logiciel espion à l'insu et sans le consentement de la personne surveillée est illégal (délit de violation du secret des correspondances, art. 226-15 du Code pénal). De plus, ces logiciels ne respectent pas les règles des magasins d'applications officiels (AppStore, Google Play) qui exigent que toute application soit visible à son installation sur la page d'accueil du téléphone. Ces logiciels espions se trouvent donc dans des magasins d'applications alternatifs et/ou sur le web.

1. OBJECTIFS DE L'ENQUÊTE

- identifier les principaux logiciels espions disponibles en France utilisables dans le contexte de violences conjugales
- comprendre les principales fonctionnalités de ces logiciels espions et les possibilités de désinstallation

2. MÉTHODOLOGIE

L'analyse s'est concentrée sur le moteur de recherche Google à partir d'une recherche par mots-clés[1]. Une recherche complémentaire a été effectuée grâce à des articles de presse qui abordent le sujet des logiciels espions.
Les logiciels analysés sont les plus référencés sur les trois premières pages proposées par Google France. Au total **14 applications ont été identifiées et analysées**[2]. Il ne s'agit pas d'une recherche exhaustive mais d'un aperçu du fonctionnement des logiciels espions à partir d'un échantillon des logiciels présents sur le marché français. Les données sont celles qui sont présentées sur les sites marchands (ou forums) des logiciels. Aucune donnée sur le nombre de vente de ces logiciels n'a été trouvée.

3. PRINCIPAUX RÉSULTATS

INSTALLATION

Un accès physique au téléphone ou à l'ordinateur est nécessaire pour installer un logiciel espion. Sans accès physique au téléphone, il est possible d'avoir accès à l'iCloud sur les iPhones grâce à un logiciel espion à condition de connaître l'identifiant et le mot de passe du compte.

Il existe deux manières d'installer un logiciel espion :

- **via un lien qui lance un téléchargement**. Pour cette opération, un débridage du téléphone est parfois nécessaire, ce qui demande des connaissances techniques avancées ou la consultation d'un professionnel
- **via l'iCloud de l'iPhone**. Cette installation nécessite de connaître l'identifiant et le mot de passe, que la sauvegarde iCloud soit activée et que l'identification à deux facteurs ne soit pas activée.

COMMENT ÇA FONCTIONNE ?

Une fois le logiciel installé, la personne surveillant le téléphone peut accéder aux données du téléphone cible via un tableau de bord accessible sur le site du logiciel ou via SMS. Le transfert des données du téléphone cible à la personne surveillant se fait par Internet.

LES FONCTIONNALITÉS DES LOGICIELS ESPIONS

Un logiciel espion peut donner accès aux contacts, au journal d'appels, aux photos, aux vidéos, aux SMS et à la localisation (via GPS si celui-ci est activé ou via le réseau Wifi auquel le téléphone est connecté). Les forfaits de base permettent l'accès aux fonctionnalités et aux applications d'origine du téléphone. Les fonctionnalités supplémentaires sont généralement payantes. 6 logiciels sur les 14 étudiés, soit près de la moitié, proposent une assistance technique via email, chat ou téléphone.

Tous les logiciels permettent :

- l'accès au **journal d'appel** et au **répertoire de contact**
- l'**accès aux applications** du téléphone cible
- l'accès aux **SMS**
- l'accès à la **localisation** (via le réseau Wifi ou GPS)

Suite au verso >

La plupart des logiciels proposent des fonctionnalités supplémentaires comme :

- l'accès au **navigateur Internet** du téléphone cible (12/14)
- l'accès aux **emails** (11/14) (si l'application email du téléphone est utilisée).
- l'accès à la **galerie médias du téléphone cible** (10/14) (photos, vidéos, musiques, images enregistrées).
- l'accès au **micro s'il est activé**, (8/14) et **l'activation du micro à distance** (7/14)
- l'**écoute des conversations** téléphoniques (8/14)

Quelques logiciels proposent des fonctionnalités plus avancées :

- 3 logiciels proposent de **cracker les codes de déverrouillage du téléphone cible**
- 3 logiciels proposent une fonction d'**enregistrement de frappe** qui peut permettre de récupérer tous les identifiants et mots de passe tapés sur le téléphone.
- 4 logiciels peuvent **bloquer certaines applications**.
- 3 logiciels peuvent avoir accès au **calendrier** sans le mot de passe du cloud.
- 2 logiciels peuvent **bloquer les sms** et 2 permettent d'**envoyer un sms via le numéro de la victime** (*spoof* SMS).
- 2 logiciels peuvent **bloquer les appels entrants**.
- 2 logiciels peuvent **activer la géolocalisation à distance** et 2 proposent de mettre en place des **zones d'alerte** (*geofencing* : une notification est envoyée sur le téléphone de l'agresseur si le téléphone de la victime quitte ou entre une zone précise).
- 2 logiciels proposent une **alerte par mots clé tapés** (dans un sms, une application ou le navigateur).
- 2 logiciels peuvent **bloquer certains sites**.
- 1 logiciel permet de verrouiller **le téléphone cible à distance**.

4. RÉFÉRENCE À LA LOI ET PRÉVENTION DES UTILISATIONS ABUSIVES

Aucun logiciel ne cible dans sa présentation directement la surveillance de sa partenaire. Certains (4/14) sont vendus comme des logiciels de contrôle parental, la majorité (8/14) comme des logiciels de **contrôle parental** ou **professionnel**.

Plus de la moitié des logiciels (8/14) annonce clairement que le logiciel peut être caché sur le téléphone cible.

La majorité des logiciels (11/14) a inséré un rappel à la loi sur le site, mais celui-ci se trouve souvent en note de bas de page (6/11) ou bien dans les rubriques.

5. DÉSINSTALLATION

La désinstallation à distance n'est pas possible pour la plupart des logiciels, une trace est laissée sur le téléphone.

Seulement 2 logiciels peuvent être désinstallés par la victime dont 1 avec une alerte de désinstallation envoyée à l'agresseur. Aucun ne propose d'assistance à la victime pour le faire.

6. CONCLUSION

- **L'utilisation de ces logiciels implique un accès physique au portable de la victime, ce qui est facilité dans le cadre du couple**. Une assistance est généralement proposée sur les sites de vente. Leur installation peut également se faire sur le téléphone des enfants, notamment après une séparation. Ces logiciels sont généralement très difficiles à détecter et à désinstaller par la victime.
- **Une fois installé le logiciel est très intrusif**. Il permet d'avoir accès à de nombreuses informations et de contrôler des fonctionnalités sur le téléphone, dès les forfaits de base disponibles à des prix très accessibles.
- **Les logiciels espions sont l'un des dispositifs de surveillance, mais de nombreuses applications disponibles légalement dans les magasins d'applications peuvent être facilement détournées pour surveiller** les communications et les déplacements de sa partenaire ou ex-partenaire, à son insu ou de manière imposée (applications de contrôle parental, de surveillance mutuelle dans le cadre du couple, ou encore des logiciels anti-vol d'appareils numérique). Une récente étude américaine[3] démontre que ces logiciels, facilement accessibles par l'agresseur de manière légale - bien que leur utilisation à l'insu de la victime soit illégale- permettent une cybersurveillance plus simple mais avec des fonctionnalités proches de celles des logiciels espions.

1 *« Logiciels surveillance Android », « Logiciel surveillance iPhone », « Appli surveillance » ; « Surveiller sms » ; « Comment suivre le portable de ma femme/copine » ; « Comment lire les sms de ma femme/copine » ; « Savoir où est ma femme/copine » ; « Savoir avec qui parle ma femme/copine ».*

2 Voir liste de logiciels espions en annexe n°3 du rapport.

3 «The spyware used in intimate partner violence », R. Chatterjee et al. , 39th IEEE *Symposium on Security and Privacy*, 21 mai 2018.

centre hubertine auclert

*Cette étude réalisée par l'Observatoire régional des violences faites aux femmes du Centre Hubertine Auclert est extraite du rapport « Cyberviolences conjugales, recherche-action menée auprès de femmes victimes de violences conjugales et de professionnel-le-s les accompagnant » (pages 63 à 65). Elle a été réalisée par Mégane Le Provôt et Iman Karzabi. Le rapport complet est accessible en ligne : **https://www.centre-hubertine-auclert/fr/observatoire-regional-des-violences-faites-aux-femmes***

*Pour des conseils sur comment mieux protéger sa vie privée, consulter le site : **www.guide-protection-numerique.com***

ile de France

www.centre-hubertine-auclert.fr