

Quels sont les moyens techniques de surveillance numérique à disposition des Forces de l'Ordre ? (Wiki en chantier ☐☐)

Vers où tendent les moyens techniques ?

Les autorités françaises étaient en 2020 dans les dernières étapes de négociations pour l'achat du système de surveillance Pegasus avant d'y renoncer. Bien que l'achat ne se soit pas fait, cela montre la volonté des autorités françaises d'obtenir les moyens techniques de surveillance les plus poussés.

Qu'est-ce que le logiciel espion Pegasus ?

Le superviseur européen de la protection des données a publié [un rapport très complet sur Pegasus](#).

Pour résumer, Pegasus est* le logiciel espion connu le plus performant et cela pour les raisons suivantes:

- il donne un accès total au téléphone espionné. Il a accès à aux caméras, aux micros, aux fichiers, aux applications, etc.
- il peut infecter un appareil avec une attaque "Zéro Click" c'est-à-dire sans aucune action de la victime. Donc quelque soit votre vigilance, si vous êtes visé.es vous ne pouvez pas empêcher l'infection de votre téléphone.
- il est indétectable par l'utilisateur et seule une analyse technique très poussée a permit d'identifier les téléphones infectés.

Ce logiciel espion a notamment été utilisé en Europe contre des citoyen.ne.s européen.nes incluant des journalistes, des politiques, des avocat.es.

*: Suite aux enquêtes, les failles de sécurités utilisés par Pegasus ont été réparées par les entreprises logiciels (Google et Apple). Si vous avez sur votre smartphone la dernière version du système d'exploitation, il est possible que vous soyez protégé.e. Cependant, les fabricants de téléphone (autres que Apple et Google) proposent rarement la dernière version du système d'exploitation. Votre téléphone est donc probablement toujours vulnérable. De plus, d'autres failles non détectées pourraient être utilisées. Il semble donc pertinent de considérer que le logiciel espion Pegasus est encore efficace et utilisé.

Quelles sont les pratiques et outils de hacking des FDO ?

Selon un [rapport de 2017 demandé par le parlement européen](#), les enregistreurs de frappe ou Key Logger, c'est-à-dire un système qui enregistre l'utilisation d'un ordinateur ou téléphone [cf: wikipedia](#), sont les outils les plus utilisés par les Forces De l'Ordre. En 2017, ce rapport concluant que les outils de "hacking" n'étaient pas énormément utilisés.

Selon un [autre rapport du Superviseur européen de la protection des données](#) de 2013, la France a un système de surveillance de masse en collectant directement les données sur les infrastructures. Cependant en 2013, les moyens étaient bien plus faibles que les agences de surveillance américaines et Britanniques. La France était alors considéré comme le 5ième pays collectant le plus de [metadonnées](#).

Cadre légal du hacking en France

En France, les techniques de piratage informatique sont autorisées par les articles 706-102-1 et 706-102-2 du Code de procédure pénale. Elles permettent entre autre aux forces de l'ordre d'accéder à distance aux ordinateurs et autres appareils.

En vertu de l'article 706-102-1, les opérations ne peuvent être autorisées que pour une période maximale d'un mois. Le renouvellement est possible une fois dans les mêmes conditions.

En vertu de l'article 706-102-2, les opérations sont autorisées pour une durée plus longue, dans la limite d'une période initiale maximale de quatre mois, renouvelable dans les mêmes conditions dans la limite d'une période totale de quatre mois.

La gouvernance diffère selon ces dispositions puisque l'article 706-102-1 concerne les enquêtes menées par le procureur de la République, alors que l'article 706-102-2 concerne les enquêtes menées par le juge d'instruction.

Le hacking peut être utilisé par les fdo pour les crimes avec des peines d'au moins 2 ans de prison. Pour rappel, de nombreuses méthodes d'action de DCNV (par exemple [l'entrave à la circulation](#)) peuvent théoriquement conduire à des peines de prison de 2 ans ou plus. **Le "hacking" est donc légal pour prévenir des actions de DCNV.**

A noter, l'article 163 garantit un inventaire judiciaire des preuves électroniques pouvant être exploitées par des experts techniques. Il précise que les experts qui effectuent des opérations d'exploitation doivent rédiger un rapport qui contient une description des opérations et leurs conclusions. L'inventaire et les rapports sont fournis à la juridiction et enregistrés dans le procès-verbal. Si procès, il peut donc être intéressant de vérifier la présence d'un tel procès-verbal.

Révision #1

Créé 8 September 2023 18:15:40 par julien

Mis à jour 8 September 2023 18:15:40 par julien