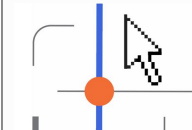


Mon ordinateur ou mon téléphone est-il espionné ? Des informations me sont-elles volées ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT RGPD CYBER MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Denis JACOPINI VOUS INFORME		Mon ordinateur ou mon téléphone est-il espionné ? Des informations me sont-elles volées ?			

Quelqu'un sait des choses qu'il ne devrait pas savoir ?

Comment savoir si mon ordinateur est espionné ?

Comment savoir si je suis victime de fuites d'information ?

Il est clair que si vous êtes en conflit avec quelqu'un, il y a de fortes chances, qu'il cherche, tout comme vous, à savoir ce qui peut bien se mijoter chez la partie adverse.

Il est clair que si vous êtes en conflit avec quelqu'un, il y a de fortes chances, qu'il cherche, tel que vous, à savoir ce qui peut bien se mijoter chez la partie adverse.

Le premier réflexe que vous aurez sera probablement de penser que **vosre ordinateur est espionné** ou que **vosre téléphone est espionné**. Sans à ce que vous ayez anticipé la fuite d'informations en plaçant dans votre installation informatique des systèmes destinée à détecter la fuite d'informations et éventuellement à vous alerter, il faudra passer vosre téléphone ou vosre ordinateur au peigne fin pour détecter à posteriori des traces d'intrusion ou des traces d'exfiltration de données.

Quelle est notre technique ?

Quelle est notre technique ?
Nous n'allons pas vous dévoiler nos petits secrets, mais notre technique est basée sur la recherche et la détection de détails et fonctionnements anormaux. C'est par une bonne connaissance des techniques utilisées par les pirates informatique et par une connaissance approfondie d'un système sain que nous pouvons identifier un système modifié, altéré, trafiqué, piégé.

Des informations dans le système d'exploitation (base de registre, journaux des événements, journaux divers) et dans tous les lieux dans lesquels le malveillant peut laisser des traces, sont collectées, analysées et traitées. Une analyse sur une « Timeline » des actions déroulées dans votre ordinateur permet aussi parfois de pouvoir découvrir la chronologie des actions et confondre les éléments recueillis avec d'autres preuves.

Comment devrez-vous vous organiser ?

Afin de vous aider à en organiser le cœur net sur l'existence ou non d'éléments douteux dans votre système, il est d'abord indispensable de pouvoir disposer des équipements à expertiser. Nous nous organisons pour vous priver de votre appareil le moins possible mais cette étape est nécessaire pour faire une photocopie de votre appareil et les premières mesures.

En fonction de vos besoins, il se peut aussi que nous déposions dans vos locaux un appareil enregistreur avec lequel nous pourrions collecter en temps réel l'ensemble des données suspectes.

Nos rapports sont-ils utilisables en justice ?
Et vous avez peut-être la réponse dans votre

Si vous avez opté pour la rédaction d'un rapport d'expertise privé (non judiciaire), nous le construisons sur le même modèle que les rapports d'expertise que nous produisons pour la justice. Si par la suite vous avez décidé d'aller en justice, le juge qui sera en charge de votre affaire, même s'il ne pourra pas se fier aux seuls éléments figurant dans notre rapport expertise, aura tout de même l'obligation d'en tenir compte dans son jugement.

Que faire avant qu'il ne soit trop tard ?

Par exemple, en France, 6 employés sur 10 ayant quitté leur entreprise au cours des 12 derniers mois conservent des données confidentielles appartenant à leur ancienne entreprise. Le départ d'un collaborateur constitue souvent un maillon faible de la sécurité du patrimoine informationnel qu'il faut donc s'efforcer de renforcer.

- Hiérarchiser vos documents et restreindre les accès;

- Ne pas avoir d'utilisateurs qui peuvent travailler sur leur ordinateur en mode administrateur;
- Fournir les informations les plus sensibles sur votre système informatique ou utiliser des com

- Crypter les informations les plus sensibles sur votre système informatique ou utiliser des containers cryptés;
- Utiliser toutes les connaissances de sécurité relatives aux mails piégés, aux sites internet piégés et aux techniques d'ingénierie sociale évitant de donner un accès complet à votre ordinateur.

De plus, depuis le 6 janvier 1978, la loi Informatique et Libertés vous oblige, sauf si vous êtes un particulier, à protéger l'ensemble des données personnelles dont vous disposez (fichier client, contacts, fichiers fournisseurs, fichiers salariés, tableaux de congés...). Vous vous exposez à ce jour à une amende de 150 000 euros et 5 ans de prison. A compter du 24 mai 2018, l'amende pourra être portée jusqu'à 20 millions d'euros ou 2% du chiffre d'affaire mondial.

Pensez à anticiper ce risque en mettant en oeuvre des procédures visant à protéger les données personnelles que renferme votre système informatique et des moyens techniques destinés de vous protéger contre la fuite de données.

Que faire s'il est déjà trop tard ?

Que faire s'il est déjà trop tard ?
Vous pensez être espionné, épié par l'intermédiaire de votre ordinateur ou de votre téléphone ?

N'attendez pas, il est nécessaire de réagir vite, compte tenu que les traces peuvent disparaître rapidement.

Deux priorités se présentent à vous et en fonction de votre

1. rechercher l'auteur de cet espionnage;
2. faire stopper l'acte de surveillance illicite;

Article de Denis JACOPINI (expert informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles).



Denis JACOBIE est Expert Informatique, notamment spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (crimes, espions, piratages, fraudeurs, groupes Internet...) et polices (investigations téléphoniques, drogues durs, e-mails, cyberdélits, délinquants de chambre...) ;

- Expertise de systèmes de vote électronique ;

- Formations et conditions de sphérisabilité ;
- Évaluation de C.E. : Mesurements différentiels

- Formation de C.I.L. (Correspondants Informatique et Liberté);



[Contact us now](#)

Réagir à cet article

Original de l'article mis en page : Comment se protéger contre la fuite d'informations avec le départ des collaborateurs ? – Lexsi Security Hub