Les pirates capables de voler des données même si votre ordinateur n’est pas connecté à Internet (ou pire, éteint !)

	Les pirates capables de voler des données même si votre ordinateur n’est pas connecté à Internet (ou pire, éteint !)

Lorsque des institutions gouvernementales ou des entreprises souhaitent stocker des informations confidentielles, elles utilisent le plus souvent un réseau en « air-wall », déconnecté d'internet, et isolé de toute connexion extérieure. Récemment pourtant, plusieurs chercheurs de l'université Ben-Gurion en Israël ont démontré qu'il était possible, une fois ce réseau contaminé par un virus spécifique, d'en récolter les données.

Les pirates informatiques peuvent voler les données de votre ordinateur même s'il est déconnecté et éteint.
Atlantico : Bien que les particuliers soient sans doute moins la cible de ce type d'attaque informatique, sont-ils tout aussi vulnérables ?
Michel Nesterenko : Tout ordinateur est potentiellement vulnérable. Mais les connaissances et la technologie nécessaire pour réussir un tel vol de données font que seules les ordinateurs dans lesquels sont stockés des données stratégiques ou des données commerciales de grande valeur sont vraiment à risque. Donc le consommateur normal n'a pas de grand souci à se faire.
Du temps de la Guerre Froide dans les années 60 les espions américains et russes pouvaient voler toutes les informations passant sur l'écran d'un ordinateur à partir du van stationné dans la rue.
C'est pour cela que certains ministères à Washington avaient blindés l'enveloppe extérieure des ordinateurs détenant des données sensibles de façon à empêcher toute émanation électromagnétique.

Jean-Paul Pinte : En tant que particulier, nous sommes encore plus vulnérables à ce type d'attaque ou d'infiltration qui, une fois installé sur une machine, permet d'y revenir et de se servir. Nous avons en effet moins pensé la sécurité de nos données par rapport à une entreprise par exemple, mais le risque demeure le même, il est même plus grand. Le ver installé sur un PC, il est en effet possible de faire ce que l'on veut, de s'installer confortablement et d'y revenir à sa guise. Une des seules façon de pirater un PC éteint serait d'être en rapport avec la C-MOS et nécessiterait donc un accès physique à la machine. Ce n'est donc à la portée du premier venu.
Comme pour votre Webcam éteinte, il est tout aussi possible d'en prendre la main à distance et certains vont même jusqu'à utiliser un cache ou collant qu'ils posent sur la Webcam pour s'en protéger. Un ordinateur quand il est éteint, c'est juste la boite d'alimentation qui est éteinte mais la carte mère continue à recevoir de l'énergie (un voyant lumineux au niveau de la carte mère est toujours présent). Il est donc toujours plus prudent de débrancher totalement son ordinateur et surtout de ne pas le laisser en mode veille ou veille prolongée. Il est également possible si l'on veut se protéger totalement de fermer son boîtier Wifi mais attention aux mises à jour qui se font parfois la nuit sur ces matériels.

Quelles données peuvent être récupérées ? Quelles sont les marges de manoeuvre des pirates informatiques avec pareil procédé ?
Michel Nesterenko : Potentiellement tout peut être récupéré à terme car le vol des données prends du temps, compte tenu des limitations de la bande passante. Ce type de procédé est fort utile dans un contexte militaire ou d'espionnage industriel. Les informations peuvent être revendues aux concurrents ou utilisées dans des manipulations boursières par exemple.

Jean-Paul Pinte : Une fois dans la machine, on peut tout faire avec quelques manipulations que connaissent bien ces hackers. A la base il y a quelques années, le but était simplement d'avoir pu infiltrer ou craquer une machine.
Aujourd'hui, ce sont tous vos contacts de messagerie, les fichiers stockés, les mots de passe qui peuvent être récupérés par exemple au même titre que tous les documents personnels. Il n'y a donc pas de limites.
Tous ces éléments pourraient se retrouver un jour sur la toile et servir par exemple dans le cas d'adresses de messagerie à des banques de données réutilisées par la suite pour faire des envois en masse comme cela se pratique dans le cas des mails nigérian.
Prendre la main sur votre machine revient à avoir la clé de votre domicile, le code de votre alarme et tout peut alors être envisagé en vue de vous voler des informations et des accès à des sites que vous utilisez et sur lesquels vous passez des actes d'achat par exemple.
Aujourd'hui, on parle même de vol de données qui pourraient vous faire chanter.

Comment savoir si notre ordinateur est infecté par ce type de virus ? Comment s'en apercevoir ?
Michel Nesterenko : Pour tout virus connu, il existe un antidote. Encore faut il que les anti-virus et parre-feu soient mis à jour constamment sur chacun des ordinateurs du réseau indépendamment.

Jean-Paul Pinte : Assurez-vous tout d'abord d'avoir la bonne dernière version officielle de vos logiciels et pensez à utiliser des solutions comme Anti Hacks qui détectera les problèmes de configuration et les logiciels obsolètes sur votre machine et qui, surtout, se chargera de configurer automatiquement les logiciels et vous aidera à les mettre à jour.
Ensuite un anti-virus que vous mettrez à jour tous les jours et pas à la petite semaine comme le font la plupart d'entre nous (beaucoup utilisent celui offert pour une période donnée par le fournisseur du PC mais oublient de le changer ou de l'actualiser dans le temps se retrouvant alors sans protection).

En attendant :
• surveillez vos barres d'outils et les liens que vous n'auriez pas ajouté personnellement ;
• contrôlez votre pointeur de souris qui à certains moments se déplacerait de façon inatendue ;
• regardez l'adresse URL du site que vous consultez car il pourrait changer lors d'une transaction financière par exemple ;
• veillez aux fenêtres intempestives qui s'affichent sur votre PC sans que vous n'interveniez et aux pages qui s'installent en arrière plan et que vous ne découvrez qu'une fois que vous fermez votre session Internet ou machine. Elles pourraient bien être la source d'un début d'installation d'une cyber-surveillance ;
• enfin si tout va plus lentement sur votre ordinateur; pensez à contrôler les fichiers qui se lancent au démarrage et surtour n'oubliez pas que le meilleur anti-virus est parfois de remettre à plat tous les six mois votre PC.

Quel est le niveau d'informatique nécessaire pour mettre en oeuvre correctement cette pratique ? Des solutions simples sont-elles mises à la disposition des amateurs ?
Michel Nesterenko : Le Hacking de haut niveau n'est pas une activité pour amateurs. Il faut des connaissances certaines pour mettre au point le virus adapté a une attaque particulière de même qu'il faut des informations précises obtenues par une opération de reconnaissance informatique et physique pour trouver l'ordinateur cible. Il s'agit d'un travail pour des spécialistes.

Jean-Paul Pinte : Dès que ces cybercriminels ont réussi à installer un virus ou un cheval de Troie (souvent aussi nommé malware ou logiciel malveillant) votre ordinateur devient une source potentielle de revenus. Ils auront accès à toutes vos données personnelles (messages, mails, documents bancaires, mots de passe, photos, vidéos, …) stockées sur votre disque dur et pourront surveiller votre activité sur Internet et sur votre machine.
Aujourd'hui, pas besoin d'être un grand expert sur le sujet en dehors de quelques types d'infiltrations spécifiques sur des sites dits plus sécurisés. En effet, malheureusement, beaucoup d'aide est apportée aux cyberdélinquants par Internet.. Des solutions contenus dans certains forums permettent à des petites mains de se lancer tout d'abord dans le cadre d'arrêt d'une machine en réseau dans une entreprise. Petit à petit, pirates, hackers ou encore crackers découvrent les modes opératoires des plus grands pour se les approprier et pour aller plus loin comme s'il y avait un concours entre eux.
Comment s'en prémunir ? Doit-on se résigner à avoir un ordinateur vierge de toute connexion à internet, avec des protocoles de sécurité stricts, comme par exemple ne pas utiliser de clé usb étrangère ou ne pas prêter les siennes ?
Michel Nesterenko : Absolument. Éviter de connecter à internet un ordinateur détenant des données critiques et stratégiques est la première étape. Interdire l'utilisation de toute clé USB non cryptées avec des codes particuliers est une deuxième étape.
Ensuite, il faudra songer à installer un blindage autour de l'écran pour éviter toute émanation électromagnétique. Surtout, il ne faut jamais oublier de tenir à jour les anti-virus et parre-feu sur chaque ordinateur et crypter toutes les données résidant sur le disque dur.
Le nombre de situations où cela sera vraiment recommandé reste fort restreint. Pour l'écrasante majorité des utilisateurs, cela ne sera jamais nécessaire heureusement.
Jean-Paul Pinte : De plus en plus, il faudra apprendre à se protéger et à avoir une culture sécuritaire en ce qui concerne les materiels que nous utilisons et que nous connectons à notre PC car ils seront autant de sources et de moyens d'attaque pour ces délinquants.
Tout ce qui est installé, introduit et (télé)chargé sur nos machines doit faire l'objet d'une sorte de scan ou contrôle si l'on veut rester dans une protection plus sereine.
Nous en sommes loin aujourd'hui quand nous validons la mise à jour d'un logiciel sans être sûr que l'envoi émane de la société en question. Certains internautes ont découvert tardivement que des exécutables s'étaient installés sur leur PC mais n'ont pu en mesurer l'impact sur leurs données, logiciels, etc.
L'objectif premier du hacker va être d'installer un virus ou un cheval de Troie sur votre ordinateur. Il se présente simplement sous la forme d'un exécutable (par exemple .exe), soit installé suite à l'attaque d'un de vos logiciels mal configurés ou obsolètes (la version installée n'est pas la dernière et contient donc des failles de sécurité). Ces failles sont en général la conséquence d'un bug de programmation dans l'application qu'un hacker saura mettre à profit pour prendre le contrôle de votre ordinateur. Ces logiciels sont très nombreux en voici quelques uns à titre d'exemple :
– Microsoft Windows ;
– Les suites bureautiques (Microsoft Office, OpenOffice) ;
– Les navigateurs (Internet Explorer, Firefox, Chrome, Opera, Safari) ;
– Les logiciels multimedia (Acrobat Reader, Flash, Shockwave, Windows Media Player, Quicktime, RealPlayer, WinAmp, iTunes, VLC) ;
– Les messageries instantanées (Windows Messenger, Pidgin) ;
– Java.

On a pu ainsi découvrir des cas de figure où les PC des internautes sont devenus des serveurs à leur insu se voyant alors stocker à des jours et des heures des données de personnes malveillantes qu'ils ne pouvaient alors contrôler sur leur propre machine.
De même d'autres ont accepté avec trop de simplicité et de naïveté une clé USB offerte avant l'entrée dans un salon ou symposium. Le but étant de garder la clé mais pas son contenu, ils ont ouvert cette dernière sans penser à l'exécutable qui allait s'installer sur la machine et qui allait devenir un moyen d'infiltration sans limite pour l'offreur.
Certaines applications sur ces clés vont même pendant qu'un tiers tente de recopier un fichier à partir de votre machine scruter votre PC pour lui sous-tirer tous vos contacts et ce que vous pouvez imaginer avec sans vous garantir qu'il n'aura pas pris la main sur votre PC pour y revenir ultérieurement.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.atlantico.fr/rdv/minute-tech/pirates-capables-voler-donnees-meme-votre-ordinateur-est-pas-connecte-internet-michel-nesterenko-1893142.html