Lenovo accusé d’infecter ses propres PC. Le protocole sécurisé SSL aurait été atteint

	Lenovo accusé d’infecter ses propres PC. Le protocole sécurisé SSL aurait été atteint

Très mauvaise publicité pour le premier fabricant mondial. Lenovo a été contraint d'admettre qu'il a installé secrètement un logiciel de publicité sur ses ordinateurs, lors de leur fabrication. Problème : ce logiciel aurait un effet pervers en mettant en péril la sécurité du protocole de sécurisation SSL. Face au tollé, Lenovo fait une courbe rentrante.

Lenovo, ce n'est pas n'importe qui. Il s'agit ni plus ni moins du premier fabricant mondial de PC. 60 millions de PC vendus l'an passé tout de même… Le groupe chinois est connu pour avoir racheté il y a quelques années la division PC d'IBM, ce qui lui a permis de faire son entrée dans la cour des grands. Ensuite, il a particulièrement bien tiré son épingle du jeu grâce à du matériel de qualité. Mais là, son image en prend un coup …

Toujours plus gourmand ?
Le logiciel installé secrètement par Lenovo, appelé Superfish, aurait pour but de créer un canal d'affichage de publicités ciblées lors des recherches effectuées sur certains moteurs de recherche. On appelle cela un « Adware ».

Le but ? Probablement faire de la concurrence à des systèmes bien connus comme Adwords, et créer une source de revenus complémentaires pour le fabricant qui pourrait ainsi entrer dans le marché très rentable de la publicité en ligne. Un péché de gourmandise ?
Le groupe ne nie pas mais minimise. Selon lui, il s'agirait d'améliorer « l'expérience utilisateur » selon l'expression consacrée, en permettant d'afficher du contenu publicitaire qui lui convient vraiment. Du marketing ciblé en un mot.

Contre publicité
Jusque-là, les enjeux sont éthiques (les publicitaires diront que les enjeux touchent l'image de l'entreprise), outre bien entendu un problème potentiel au niveau de la protection des données personnelles de l'utilisateur. Il y a tout de même des règles à respecter dans le cas de l'utilisation de données à caractère personnel à des fins de marketing. Il y a aussi des développements potentiels en droit des contrats si l'on considère que le PC livré ne correspond pas à ce qui a été vendu puisqu'un module supplémentaire, secret et indiscret est livré avec.
Il s'agit toutefois d'une contre-publicité remarquable, car plusieurs commentateurs rappellent que Lenovo a déjà été accusé plusieurs fois d'infecter ses PC lors de leur fabrication en modifiant les microprocesseurs afin de créer une porte d'entrée dérobée. Derrière cela, il y aurait le gouvernement chinois et de sombres opérations d'espionnage et/ou de cyber-guerre. Difficile de savoir si ces accusations ont quelque fondement ou s'il s'agit d'un fantasme lié à l'origine chinoise du fabricant, mais la rumeur est solide. Tel le monstre du Loch Ness, la rumeur est réapparue plus forte que jamais ces jours-ci, suite à l'affaire Superfish.

Un risque grave pour la sécurité
L'affaire Superfish se corse car des chercheurs ont révélé un effet pervers majeur du logiciel superfish : il mettrait en péril le protocole de sécurisation SSL.

Le protocole SSL – abréviation de Secure Socket Layer – est une application des outils cryptographiques, largement utilisée pour les paiements électroniques en ligne, bien qu'il n'a pas été créé spécifiquement pour cela. Le système – intégré par défaut à presque tous les logiciels de navigation – crée un canal de communication sécurisé entre le serveur du vendeur et l'ordinateur du client, assurant entre eux la transmission cryptée des informations communiquées (par exemple : le numéro facial de la carte de crédit, la date d'expiration et le nom du titulaire).

Le protocole SSL présente principalement les avantages suivants :
• coût réduit : le protocole est intégré dans les logiciels récents de navigation sur l'internet (MS Internet Explorer, Netscape, Opera, etc.) et ne requiert donc pas d'équipement particulier ;
• simplicité d'utilisation : l'intégration au logiciel de navigation dispense l'acheteur de toute démarche particulière. La présence d'un logo représentant un cadenas fermé sur l'écran du logiciel confirme le recours à une transmission cryptée ;
• authentification du vendeur : le protocole SSL assure avant tout l'authentification du vendeur ce qui permet, dans une certaine mesure, de décourager les escrocs qui se font généralement vite repérer par les sociétés émettrices de cartes de crédit ;
• cryptage : l'utilisation de la cryptographie asymétrique permet de sécuriser les transmissions sur le réseau.

Toute médaille ayant son revers, ces avantages et la simplicité d'utilisation constituent également les principales faiblesses du système :
• il n'y a aucune vérification de l'identité du client ;
• le numéro apparent de la carte est transmis au vendeur, ce qui laisse subsister le risque d'une utilisation frauduleuse par ce dernier, ni ne résout le danger d'une intrusion dans le serveur du vendeur par un tiers désireux de faire main basse sur les informations bancaires des clients ;
• l'efficacité de la protection en cours de transmission dépend essentiellement de la clef de cryptage retenue.
• L'importance de SSL est considérable. S'il fallait l'exprimer en quelques mots, on pourrait dire qu'à l'heure actuelle, ce protocole protège quasiment toutes les transactions sur l'internet. Qu'il s'agisse d'acheter des billets de trains, de réserver un spectacle, de télécharger de la musique payante, de commander un livre … SSL est derrière l'immense majorité des opérations. Presque tous les sites qui opèrent le paiement par la transmission du numéro facial de carte de crédit, utilisent SSL. Ce protocole n'est pourtant pas le seul, mais il est le plus utilisé.

En raison de sa conception (recours à des certificats auto signés, en utilisant de surcroît la même clef privée sur tous les ordinateurs équipés de ce logiciel), le logiciel Superfish peut déchiffrer des connexions supposées sécurisées afin d'insérer des contenus publicitaires sans que l'utilisateur ne soit averti d'une telle intrusion, et briser ainsi la sécurité du protocole (plus d'infos en faisant une recherche sur votre moteur préféré avec les mots-clef « superfish ssl »).

Lenovo fait une courbe rentrante
Face au tollé général, le fabricant chinois a été contrainte de reconnaître les faits en les minimisant, et d'assurer que depuis ce mois de janvier, les nouvelles machines ne sont plus équipées de ce logiciel. (voir le communiqué http://news.lenovo.com/article_display.cfm?article_id=1929)

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

Source : http://www.droit-technologie.org/actuality-1698/lenovo-accuse-d-infecter-ses-propres-pc-le-protocole-de-securise-ssl.html
Par Etienne Wery, Avocat aux barreaux de Bruxelles et Paris (cabinet Ulys)