Le piratage est impossible à juguler

L'industrie de la copie illégale de films, de musique, de photos et de logiciel est florissante. Dans des pays comme la Chine, l'Inde ou le Brésil, c'est la contrefaçon qui est la règle et l'achat légal l'exception.

En France, la Loi favorisant la diffusion et la protection de la création sur l'internet ou loi Hadopi (le sigle de « Haute autorité pour la diffusion des œuvres et la protection des droits sur l'internet ») a pour but de lutter contre le piratage. La question est : peut-elle atteindre son but ? La réponse est non. Voici pourquoi.

L'identification de l'expéditeur

Sur l'internet, le seul moyen d'identifier un expéditeur consiste à lire son adresse IP telle qu'elle apparaît dans l'en-tête du paquet de données intercepté.

Le problème est que cette information est invérifiable : le mécanisme de transmission des paquets de données, qui repose sur les protocoles IP et TCP, ne comporte pas de procédure de contrôle de l'adresse de l'expéditeur. Les routeurs qui acheminent le message ne s'intéressent qu'à celle du destinataire.

Il y a cinq méthodes pour brouiller les pistes.

1° Le *ip spoofing*

Il est très facile de remplacer l'adresse de la source par une autre ; c'est ce qu'on appelle le *ip spoofing*, et il existe même utiliser des outils gratuits qui permettent de le faire (rechercher « ip spoofing tool » sur Google).

2° L'accès depuis un *hot spot*

Une autre méthode consiste à travailler depuis un endroit public — place publique, café, gare, aéroport, etc. — où on peut accéder à l'internet. L'anonymité est garantie puisqu'on reçoit une adresse IP volante.

Pour être précis, il y a aussi l'adresse physique qui pourrait être utilisée pour identifier un ordinateur lors d'une enquête pénale, mais on peut également se protéger (rechercher « mac spoofing tool » sur Google).

3° Le *war driving*

Une autre méthode consiste à se connecter sur le réseau sans fil du voisin ou prendre un ordinateur portatif en voiture et rechercher un réseau sans fil. Même dans une petite ville, on en trouve des dizaines.

Si le réseau est protégé par WEP (Wired Equivalent Privacy), on peut aisément casser la protection au moyen d'un outil comme Aircrack-ng (*http://www.aircrack-ng.org*).

4° Les services d'anonymisation des accès

Une quatrième méthode consiste à s'inscrire à un service d'anonymisation des accès à l'internet . Ces services sont très volatiles et ne durent souvent que quelques mois, mais on les trouve toujours en recherchant « anonymous internet access » ou « hide ip » sur Google.

Le mécanisme passe par trois étapes :

1. l'utilisateur se connecte au service en utilisant le VPN (liaison chiffrée et authentifiée) fourni sur le site ;
2. le serveur donne une adresse IP locale à l'utilisateur ;
3. l'utilisateur ouvre son navigateur ou sa messagerie et travaille normalement. Tout paquet de données envoyé aura l'air de venir du site du serveur.

5° Les réseaux sombres

La dernière possibilité consiste à passer par une succession d'ordinateurs relais. Les transmissions sont chiffrées, mais le fait que les paquets passent par une suite de machines qui peuvent être situées n'importe où dans le monde constitue à lui seul une bonne protection. C'est ce qu'on appelle un *black network*, un réseau sombre.

La solution la plus connue est Tor (*http://www.torproject.org*).

Attention, aucune méthode d'anonymisation n'est sûre

De nombreux programmes peuvent contenir l'adresse IP de l'utilisateur, notamment les applets Java, ActiveX, Pdf, Flash, Quicktime, etc., et il en va de même des barres qu'on peut ajouter au navigateur ainsi que des cookies. Cela n'a pas grand sens de passer par un chemin protégé si, à l'arrivée, on affiche d'où on vient.

Il n'y a pas d'anonymisation des accès à l'internet si on n'applique pas toutes les mesures de restriction suivantes :

- désactiver les applets «bavardes» (Java, ActiveX, etc.) ;
- désactiver ou supprimer les cookies indésirables ;
- éviter les applications qui captent l'adresse IP de l'utilisateur (Realplayer, Quicktime, etc.) ;
- ne pas se rendre sur des sites qui utilisent l'adresse IP (YouTube, Facebook, etc.).

Certains sites d'anonymisation incluent les options *no cookies* et *no scripts* (exemples : *http://www.cooltunnel.com*, *http://proxify.co.uk*, *https://www.vtunnel.com*), ce qui résout les deux premiers points, mais le problème de Realplayer ou YouTube reste entier.

Comme on a parfois besoin de naviguer librement et que ce serait impossible de paramétrer et déparamétrer sans arrêt le navigateur, la seule solution pratique consiste à appliquer ces restrictions à un navigateur utilisé pour le surf sécurisé (accès anonyme, e-banking, etc.) et à utiliser un autre navigateur pour le surf normal.

Il existe des sites consacrés à l'anonymisation en général, par exemple *http://www.sneaky.com*.

Les réseaux peer-to-peer

Les réseaux peer-to-peer comme eMule, eDonkey, FastTrack, Gnutella ou BitTorrent ont été beaucoup critiqués parce qu'ils sont massivement utilisés pour la copie illégale, et ils constituent un objectif prioritaire de la lutte contre le piratage.

Le problème est que, même si les autorités parviennent un jour à les fermer tous, cela ne servira pas à grand chose. La méthode de piratage la plus utilisée ne fait appel ni au peer-to-peer, ni à aucun moyen technique élaboré. Elle passe tout simplement par la transmission de main à main d'un CD, d'un DVD, d'une clé USB ou d'une autre mémoire de stockage. Récemment, j'ai vu un échange de musique piratée transiter par un disque dur externe. En quelques minutes, plusieurs milliers de morceaux de musique sont passé d'une personne à l'autre.

Les serveurs

Les efforts portés contre les réseaux peer-to-peer ont eu pour résultat de déplacer le piratage vers les systèmes à serveurs.

En apparence, le contrôle des flux est plus simple avec des serveurs qu'avec des postes de travail fluctuants, mais les pirates jouent avec les frontières pour se protéger et la justice est pratiquement impuissante si le serveur se trouve à l'étranger.

De plus, il y a beaucoup de serveurs privés. Cela commence souvent avec une personne qui a beaucoup d'œuvres piratées et les met à la disposition de ses amis. Après quelque temps, c'est un véritable serveur qui est en place, et il est invisible pour autant que les flux soient chiffrés. Comme les membres du réseau sont cooptés et se connaissent, l'utilisation d'un VPN ne pose pas de problèmes. Un réseau de ce type est indétectable à moins qu'un de ses membres ne vende volontairement ou involontairement la mèche.

Mais que fait la police ?

La surveillance des échanges sur l'internet n'est pas simple. Des milliards de paquets de données transitent sur le réseau chaque minute. La méthode utilisée par la police consiste à se placer sur les principaux routeurs du pays et à espionner les flux avec des logiciels spécialisés. Ces outils repèrent les en-tête qui indiquent que le paquet appartient, par exemple, à un message BitTorrent — le peer-to-peer est la cible numéro une des autorités — et ils analysent les fichiers suspects par ***fingerprinting***. Cette méthode consiste à réduire le fichier en un micro-fichier (son « empreinte digitale ») et à comparer ce dernier avec le contenu d'une base de données des micro-fichiers des œuvres.

Une autre méthode consiste à placer une marque (une suite de bits bien précise) dans l'œuvre originale. Tout fichier intercepté qui contient cette marque est identifié comme une copie pirate. C'est le ***watermarking***.

Mais ces méthodes ne permettent de pêcher que les petits poissons. Les autres sont impossibles à repérer :

- ils chiffrent les échanges, ce qui détruit le fingerprinting comme le watermarking ;

- ils masquent leur identité (serveur d'anonymisation, réseau sombre, etc.), ce qui empêche de les identifier ;
- s'ils veulent éviter tout risque, ils se passent l'œuvre de main à main ou ils envoient le CD ou la clé USB par la poste.

En conclusion

Aujourd'hui, beaucoup d'œuvres se réduisent matériellement à une suite de bits et rien n'est plus simple à copier qu'une suite de bits. C'est une évidence : il faut chercher une autre méthode que la police du web pour protéger les intérêts des créateurs, cela pour l'excellente raison que le piratage des œuvres est impossible à stopper.

La loi Hadopi revient à essayer de vider l'océan avec un filet (citation approximative et hommage aux Frères ennemis, le duo d'humoristes des années soixante : « le pêcheur vit de la mer avec son filet »).