Quand l'industrie culturelle US veut attaquer les « pirates » à l'artillerie lourde !

Une nouvelle traduction de Cory Doctorow

L'industrie américaine du divertissement au Congrès : autorisez-nous légalement à déployer des rootkits, des mouchards, des logiciels rançonneurs et des chevaux de Troie pour attaquer les pirates !

US entertainment industry to Congress: make it legal for us to deploy rootkits, spyware, ransomware and trojans to attack pirates!

Cory Doctorow – 26 mai 2013 – BoingBoing.net
(Traduction : Mowee, ehsavoie, audionuma, Asta)

La « Commission sur le Vol de la Propriété Intellectuelle Américaine », qui porte bien comiquement son nom, a finalement rendu son rapport de 84 pages complètement folles. Mais dans toute cette folie, il y a une part qui l'est encore plus que le reste : une proposition pour légaliser l'usage des logiciels malveillants afin de punir les personnes soupçonnées de copies illégales. Le rapport propose en effet que ce logiciel soit chargé sur les ordinateurs et qu'il détermine si vous êtes un pirate ou non. S'il soupçonne que c'est le cas, il verrouillera votre ordinateur et prendra toutes vos données en otage jusqu'à ce que vous appeliez la police pour confesser vos crimes. C'est ce mécanisme qu'utilisent les escrocs lorsqu'ils déploient des logiciels rançonneurs *(NdT :*

ransomware).

Voilà une preuve supplémentaire que les stratégies en terme de réseau des défenseurs du copyright sont les mêmes que celles utilisées par les dictateurs et les criminels. En 2011, la MPAA (Motion Picture Association of America) a dit au Congrès qu'ils souhaitaient l'adoption de la loi SOPA (Stop Online Piracy Act). Selon eux, cela ne pouvait que fonctionner vu que la même tactique est utilisée par les gouvernements en « Chine, Iran, Émirats Arabes Unis, Arménie, Éthiopie, Arabie Saoudite, Yémen, Bahreïn, Birmanie, Syrie, Turkménistan, Ouzbékistan et Vietnam. » Ils exigent désormais du Congrès que soit légalisé un outil d'extorsion inventé par le crime organisé.

> *De plus, un logiciel peut être écrit de manière à ce que seuls des utilisateurs autorisés puissent ouvrir des fichiers contenant des informations intéressantes. Si une personne non autorisée accède à l'information, un ensemble d'actions peuvent alors être mises en œuvre. Par exemple, le fichier pourrait être rendu inaccessible et l'ordinateur de la personne non autorisée verrouillé, avec des instructions indiquant comment prendre contact avec les autorités pour obtenir le mot de passe permettant le déverrouillage du compte. Ces mesures ne violent pas les lois existantes sur l'usage d'Internet, elles servent cependant à atténuer les attaques et à stabiliser un cyber-incident, pour fournir à la fois du temps et des preuves, afin que les autorités puissent être impliquées.*

De mieux en mieux :

> *Alors que la loi américaine interdit actuellement ces pratiques, il y a de plus en plus de demandes pour la création d'un environnement légal de défense des systèmes d'informations beaucoup plus permissif. Cela permettrait aux entreprises de non seulement stabiliser la situation, mais*

aussi de prendre des mesures radicales, comme retrouver par elles-mêmes les informations volées pouvant aller jusqu'à altérer voire détruire ces dernières dans un réseau dans lequel elles n'ont pourtant aucun droit. Certaines mesures envisagées vont encore plus loin : photographier le hacker avec sa propre webcam, infecter son réseau en y implantant un logiciel malveillant ou même désactiver voire détériorer physiquement le matériel utilisé pour commettre les infractions (comme son ordinateur).

Source : *La Commission sur le Vol de la Propriété Intellectuelle Américaine recommande les malwares !*