



Forum: Trucs en vrac

Topic: La justice Française condamne ZATAZ.COM à se taire

Subject: Re: La justice Française condamne ZATAZ.COM à se taire

Publié par: doc

Contribution le : 30/01/2009 14:35:36

Premier point : on n'a pas tous les éléments, et cela ne nous regarde pas car c'est dans le dossier de l'instruction, donc secret pour ceux qui n'y sont pas impliqués. Donc tout ce qu'on pourra avancer sera forcément faux car nous n'avons ni les tenants, ni les aboutissants, ni les modalités des faits. Ce ne sont qu'allégations et autres propos qui alimentent la chronique et qui, au final, ne peuvent que desservir la défense de cette personne. Quelle qu'en fût la notoriété de la personne inculpée, nul n'est au-dessus des lois. Laissons la justice suivre son cours.

Deuxième point : l'intrusion dans un SI est puni par la loi. Je crois me souvenir que c'est dans les articles 323-xx et suivants du nouveau code pénal que le problème est évoqué et traité. Il n'y a pas, à ma connaissance, de clause légale permettant une intrusion, même pour démontrer la perméabilité d'un système, même après un accord tacite entre les deux parties. Par extension, l'introduction d'un virus dans un ordinateur d'une entreprise est considéré comme une introduction de données frauduleuses, donc répréhensible au vu des mêmes articles du même nouveau code pénal.

Troisième point : ce genre d'exemple est très caractéristique du fait que la sécurité des systèmes d'information est une réalité et que les moyens pour s'en prémunir, sont ceux qu'ils sont, mais qu'ils existent et que la justice a pris en compte cette cybercriminalité. Et cela, c'est une bonne chose. Le jour où une société mettra au chômage ne serait-ce qu'un seul employé car elle s'est fait hacker son compte et qu'elle n'a donc plus de liquidités pour payer les fournisseurs et les salaires de ses employés, on espère tous que la justice retrouvera les coupables, car on sera peut-être concerné par ce chômage forcé et non désiré. Le seul piaffement qu'il nous est autorisé décemment et humblement permis de faire publiquement, c'est justement de dire, "ouh là, ça ne rigole pas dans le domaine de la S.S.I."

S.S.I. : Sécurité des Systèmes d'Information (des fois que...)

@zorro51 : les procédures bancaires commencent à changer dans le domaine des "numéros de cartes bleues qui se promènent".

Je m'explique, ou plutôt je cite l'avertissement que certaines banques mettent sur leur site depuis plusieurs mois :

"Une nouvelle réglementation de MasterCard et de VISA, destinée à renforcer la sécurité des paiements par carte bancaire sur Internet, est entrée en vigueur. Les commerçants affichant les logos "MasterCard Secure Code" ou "Verified by Visa" nous demandent désormais de contrôler votre identité lorsque vous payez vos achats par carte bancaire sur leur site.

A cette fin, vous devez adhérer au service gratuit d'authentification des paiements carte bancaire. Vous bénéficierez ainsi d'une sécurité accrue et vous pourrez continuer d'acheter sur Internet avec votre carte bancaire auprès de vos marchands habituels.

A défaut d'adhésion à ce service, vous ne pourrez plus utiliser votre carte bancaire pour payer sur les sites internet qui demandent une telle authentification."

Cela se traduit par l'utilisation (bien) connue des e-cartes bleues fournissant un numéro virtuel, de sorte que si le véritable numéro est livré en pâture sur le net, cela devient de la responsabilité du titulaire de ladite carte.

De plus, alors là, méf de chez méf à propos des hotspots gratuits non sécurisés : on s'y connecte en wifi, et on y fait des achats croyant que la transaction est sécurisée. Mais non, elle l'est du hotspot vers le net, mais entre l'internaute et son point de raccordement wifi hotspot, tout passe "en clair". Je ne donnerai pas de nom d'utilitaires permettant le snif des trames, on les connaît, mais c'est d'une incroyable réalité.

Maintenant, il est vrai que les organismes financiers se doivent de sécuriser nos transactions et toutes les infos qu'on leur confie, sinon j'appelle Rambo et SuperMario !