David Aitel, Immunity: ‘ Le full-disclosure n’est pas bien vu ‘

Qui est Immunity Inc. Quel est votre objet social? Qui êtes-vous? « *Je suis fondateur et dirigeant de la société Immunity, Inc. (www.immunitysec.com). J’ai lancé la société il y a plus de deux ans et l’ai financée jusqu’à présent sur fonds propres. Précédemment, j’ai été ingénieur en sécurité auprès de la NSA (National Security Agency) et consultant chez @stake. Nous sommes aujourd’hui quatre personnes, localisées respectivement à New-York, en Californie, en Argentine et en Hollande.* **Quel est le coeur de métier d’Immunity ?** *ImmunitySec a pour vocation première de proposer aux entreprises du conseil en sécurité informatique. Par ailleurs nous dispensons des sessions de formation et développons un outil d’intrusion appelé «Canvas» qui propose une base regroupant près de 90 « exploits ». Nous avons également fondé le fameux « Vulnerability Sharing Club ».* **Quel est votre avis sur le « Full-Disclosure » ?** *Ce que la société Immunity soutient n’est pas directement le « Full-Disclosure » mais plutôt le droit de déterminer ce que l’on veut faire de l’information dont on dispose. Que l’on souhaite la conserver pour soit, la diffuser à un cercle restreint d’individus, la diffuser ouvertement ou encore la vendre, chacun est libre de faire ce qu’il veut de l’information qu’il possède. Lorsqu’une vulnérabilité est découverte, l’éditeur concerné ne veut évidemment aucune publicité. Cependant ses clients ont besoin d’être informé sur les problèmes qu’ils doivent affronter. Quoi qu’on puisse en penser le « Full-Disclosure » n’est pas toujours bien vu chez les « hackers ». Ne pensez-vous pas qu’ils préfèrent disposer d’une vulnérabilité telle que RPC DCOM, plutôt que de voir un ver tel que « Nachi » arriver sur la toile et imposer que la quasi-totalité des machines vulnérables se voient patchées ?* **Vous avez créé un service appelé le « Vulnerability Sharing Club », pouvez-vous nous en dire davantage ?** *Le « Vulnerability Sharing Club » est un service qui permet de proposer, aux entreprises abonnées, des informations sur des vulnérabilités jusqu’alors inconnues. Nous cherchons continuellement des failles sur les systèmes et diffusons nos découvertes au sein de ce groupe.* **Quel est le ticket d’entrée pour être membre ?** *C’est un abonnement annuel et le montant varie en fonction de la taille de l’entreprise cliente. Nous mettons en place un contrat de confidentialité dès lors qu’une entreprise devient cliente qui lui interdit de diffuser la moindre information à un tiers. Toutefois nous considérons que plus l’entreprise est importante plus la probabilité qu’il y ait une fuite est grande. Le tarif varie donc entre $50.000 et $100.000 par an.* **Pensez-vous qu’il s’agisse d’un moyen éthique de diffuser l’information ?** *Chacun possède sa propre éthique. C’est à celle-ci que Immunity adhère. Pour être franc, le but est financier. Ne nous voilons pas la face, c’est grâce aux vulnérabilités, aux virus, aux vers et au piratage que toute entreprise spécialisée dans ce domaine vit.* **Quel est le profil du client type du « Vulnerability Sharing Club » ?** *Il s’agit de larges organisations et d’agences gouvernementales américaines. Une vingtaine au total.* **Considérant qu’on peut mettre à genoux Internet lorsque l’on dispose d’une vulnérabilité de ce type, qu’arriverait-il si un «pays à haut risque» souhaitait s’abonner a cette liste?** *Immunity, Inc est une société américaine et nous ne pouvons pas, pour des raisons légales, revendre nos services à n’importe quel pays. Par exemple, la loi américaine interdit d’établir une relation commerciale avec Cuba ou encore l’Iran. Aujourd’hui tous nos clients sont américains.* **En ce qui concerne la faille dans le service WINS sur Microsoft Windows, la découverte avait été faite en mai 2004 par votre équipe et vous l’avez annoncée à Microsoft et au public fin novembre 2004. Pourquoi avoir attendu autant de temps ?** *Nous n’avons pas établi de règles quant à l’annonce des failles que nous découvrons et je dirais même qu’en règle générale, nous ne publions pas les vulnérabilités que nous découvrons. Ce qui s’est passé et que personne n’a vraiment remarqué, c’est que la société «Core Impact» a publié une annonce où ils*

affirmaient mettre à jour leur produit en raison d'une nouvelle vulnérabilité sur le service WINS. Le problème est qu'ils en ont fait l'annonce le soir de Thanks Giving à l'heure du dîner. Nous avons donc décidé de nous exprimer et de fournir tous les détails sur cette vulnérabilité. Pour information, les problèmes de sécurité sur WINS sont bien connus, d'autres sociétés comme « HbGary » avaient publié des captures d'écrans « d'exploit » sans fournir de détails sur la faille. **Combien de vulnérabilités critiques n'avez-vous pas encore rendues publiques ?** *Je dirais entre 10 et 20 vulnérabilités critiques qui peuvent toucher HP-UX, dtlogin, ou des solutions de Web Management. Nous avons en notre possession des failles aussi dangereuses que celles qui touchaient RPC DCOM pour Windows ou Solaris. Nous avons également décelé une faille très critique au niveau du noyau de Microsoft Windows sur une installation par défaut.* **Pouvez-vous nous donner plus de détails sur ces vulnérabilités ?** *Vous avez 50.000 dollars ?...* **(*) pour Vulnerabilite.com**