

**TRIBUNAL DE GRANDE INSTANCE  
DE PARIS,**  
12<sup>ème</sup> ch. 2 juin 2006

COLT TELECOMMUNICATIONS c/ M. B.

PROCEDURE

M. B. est prévenu de :

D'avoir à Montpellier et Paris, courant août à septembre 2002, en tout cas sur le territoire national et depuis temps non prescrit, frauduleusement accédé dans tout ou partie d'un système de traitement automatisé de données et s'être maintenu frauduleusement dans le système, en l'espèce le serveur répondant à l'adresse IP 195.68.78.155 et ce au préjudice de la société Colt Telecommunications, faits prévus et réprimés par les articles 323-1 et 323-5 du code pénal, dans leur rédaction en vigueur à l'époque des faits.

D'avoir à Montpellier et Paris, courant août à septembre 2002, en tout cas sur le territoire national et depuis temps non prescrit, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données en l'espèce le serveur répondant à l'adresse IP 195.68.78.155, en l'ayant détourné de sa finalité pour consacrer ses ressources à la recherche et l'exploitation de vulnérabilités sur des serveurs gouvernementaux, et ce au préjudice de la société Colt Telecommunications, faits prévus et réprimés par les articles 323-2 et 323-5 du code pénal, dans leur rédaction en vigueur à l'époque des faits. D'avoir à Montpellier et Paris, courant août à septembre 2002, en tout cas sur le territoire national et depuis temps non prescrit, introduit ou supprimé frauduleusement des données d'un système de traitement automatisé de données en l'espèce, en ayant introduit sur le serveur répondant à l'adresse IP 195.68.78.155 des outils d'administration à distance (Dameware) de recherches de vulnérabilités (SSS) et des données utiles à des attaques (listes de serveurs gouvernementaux ciblés et texte de revendication), et ce au préjudice de la société Colt Telecommunications, faits prévus et réprimés par l'article 323-3 du code pénal, dans sa rédaction en vigueur à l'époque des faits.

D'avoir tenté, à Montpellier et Paris, et sur l'ensemble du territoire national courant septembre 2002, et depuis temps non prescrit, d'accéder frauduleusement à tout ou partie d'un système de traitement automatisé de données, en l'espèce 385 sites gouvernementaux (les 394 des listes jointes D11 D12 moins les 9 grisés sur le tableau récapitulatif), ladite tentative ayant été caractérisée par un commencement d'exécution, en l'espèce la recherche active de vulnérabilités à l'aide d'un outil par nature intrusif (SSS) à partir d'une machine compromise chez Colt Telecommunications, et n'ayant manqué son

effet que par circonstance échappant à la volonté de son auteur, en l'espèce la mise hors réseau de la machine compromise, faits prévus et réprimés par les articles 323-1, 323-5 et 323-7 du code pénal, dans leur rédaction en vigueur à l'époque des faits. D'avoir sur le territoire national, courant 2002 et depuis temps non prescrit, accédé frauduleusement à tout ou partie d'un système de traitement automatisé de données, ou s'être maintenu frauduleusement dans le système, en l'espèce les serveurs indiqués au tableau récapitulatif joint et numérotés de 1 à 72, au préjudice des victimes indiquées dans le même tableau, faits prévus et réprimés par les articles 323-1 et 323-5 du code pénal, dans leur rédaction en vigueur à l'époque des faits. D'avoir sur le territoire national, courant 2002 et depuis temps non prescrit, introduit frauduleusement des données dans un système de traitement automatisé de données, en l'espèce dans 72 serveurs indiqués au tableau récapitulatif joint et numérotés de 1 à 72, au préjudice des victimes indiquées dans le même tableau, s'agissant de données relatives à des revendications au nom de Reyn 0 ou des correctifs de vulnérabilités, faits prévus et réprimés par les articles 323-3 et 323-5 du code pénal, dans leur rédaction en vigueur à l'époque des faits.

DISCUSSION

Sur l'action publique :

Il est reproché au prévenu d'avoir à Montpellier et Paris courant août à septembre 2002, accédé frauduleusement à tout ou partie d'un système de traitement automatisé de données et de s'être maintenu frauduleusement dans le système, en l'espèce le serveur répondant à l'adresse IP 195.68.78.155, et ce, au préjudice de la société Colt Telecommunications, ;

- courant août à septembre 2002, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données en l'espèce le serveur répondant à l'adresse IP 195.68.78.755, en l'ayant détourné de sa finalité pour consacrer ses ressources à la recherche et l'exploitation de vulnérabilités sur des serveurs gouvernementaux et ce, au préjudice de la société Colt Telecommunications, ;  
- courant août à septembre 2002, introduit ou supprimé frauduleusement des données d'un Système de traitement automatisé de données en l'espèce, en ayant introduit sur le serveur répondant à l'adresse IP 195.68.78.155 des outils d'administration à distance (Dameware) de recherches de vulnérabilités (SSS) et des données utiles à des attaques (listes de serveurs gouvernementaux ciblés et texte de revendication), et ce au préjudice de la société Colt Telecommunications, ;  
- courant septembre 2002, tenté d'accéder frauduleusement à tout ou partie d'un système de traitement automatisé de données, en

l'espèce 385 sites gouvernementaux , ladite tentative ayant été caractérisée par un commencement d'exécution, en l'espèce la recherche active de vulnérabilité à l'aide d'un outil par nature intrusif (SSS), à partir d'une machine compromise chez Colt Telecommunications, n'ayant manqué son effet que par circonstance échappant à la volonté de son auteur, en l'espèce la mise hors réseau de la machine compromise, - courant 2002, accédé frauduleusement à tout ou partie d'un Système de traitement automatisé de données, ou s'être maintenu frauduleusement dans le système, en l'espèce les serveurs indiqués au tableau joint à l'ordonnance de renvoi, au préjudice des victimes indiquées, - courant 2002, introduit frauduleusement des données dans un Système de traitement automatisé de données, en l'espèce dans 72 serveurs indiqués au tableau récapitulatif annexé à l'ordonnance de renvoi, au préjudice des victimes indiquées, s'agissant de données relatives à des revendications au nom de Reyn0 ou des correctifs de vulnérabilités.

#### Résumé du dossier d'instruction

Les investigations menées par les services spécialisés ont très rapidement localisé les attaques menées sur plusieurs sites gouvernementaux le 18 septembre 2002 dans la matinée. Ils sont remontés sans difficultés à l'ordinateur de M. B. dit Reyn0 qui a reconnu intégralement ces faits et d'autres du même type dont il tenait soigneusement la trace.

M. B. a pris le contrôle en août 2002 du serveur de la société Colt Telecommunications sis à Paris. A partir de ce serveur il a lancé des attaques systématiques vers des centaines de sites gouvernementaux pour explorer leurs failles. Pour cela, il a introduit dans le serveur divers programmes, en particulier l'outil d'administration à distance dit Dameware qui lui permettait de contrôler le serveur à distance et le scruteur de vulnérabilité SSS (Shadow Security Scanner, logiciel commercial testant plus de 1200 vulnérabilités connues). Il a pu ensuite introduire la liste des cibles choisies ainsi que sa revendication avec son nom de hawker, Reyn0, emprunté à une série télévisée américaine (d'où la qualification de "modification"). La revendication était la suivante : "bonjour, je viens de découvrir une faille dangereuse sur les serveurs suivants... Vous devez appliquer les services Packs de Microsoft et mettre à jour le serveur en urgence... Si vous avez besoin d'autres informations contactez-moi, et si vous n'avez besoin d'autre info n'oubliez pas de dire merci".

C'est le 18 septembre que le serveur du Casier judiciaire national a été victime des requêtes caractéristiques de recherches de vulnérabilité. Le même jour le Centre d'expertises

gouvernemental de Réponse et de Traitement des Attaques Informatiques dépendant du Secrétariat Général à la défense Nationale était lui aussi victime de 1215 attaques du même type ayant la même origine. La déconnexion du serveur Colt le 19 septembre 2002 a permis de mettre fin aux attaques. M. B. a déclaré avoir agi dans un esprit de sécurisation des serveurs pour en alerter l'administrateur. Il a d'ailleurs de lui-même affirmé avoir attaqué d'autres serveurs pour compromettre des sites d'entreprises ou de grandes écoles. Il apparaissait qu'il avait commis les mêmes faits en 2002 et notamment fin juillet au préjudice du ministère de l'agriculture. L'expertise de son ordinateur permettait de retrouver la trace précise de chacune de ces attaques. Au total 394 serveurs gouvernementaux ont été attaqués et 63 autres serveurs publics ou privés (notamment ceux des parties civiles). L'accusation estime que les motivations de M. B. sont plus complexes qu'il ne le dit. Il est rappelé qu'il présente sa société de manière trompeuse sur internet et que son activité principale est en fait d'exploiter des vulnérabilités. M. B. nourrirait une certaine amertume du fait que sa valeur n'est pas reconnue et qu'il n'a pas trouvé de travail dans le secteur.

Le prévenu déclare : *"tout d'abord je reconnais tous les faits reprochés. Au départ j'étais passionné par la sécurité informatique. Je voulais alerter les administrateurs de l'insécurité de leur système. Je ne voulais pas prouver de compétences exceptionnelles dans le domaine de la sécurité. En effet, les failles que j'ai mis en évidence étaient déjà connues et auraient dû être réparées depuis lors. Il y avait la volonté d'assouvir une passion personnelle. J'ai créé une SARL en sécurité informatique. Je suis gérant et consultant. Je ne voulais pas détruire. Le serveur qui a subi des inconvénients c'est celui de Colt mais ce serveur n'était pas sécurisé"*.

#### Sur la culpabilité

Les investigations techniques ont permis d'identifier sans le moindre doute l'origine des attaques. L'examen de l'ordinateur de M. B. a confirmé, si besoin était, la source de l'infraction. Le prévenu a reconnu les faits, lors de l'enquête, devant le juge d'instruction puis à l'audience. La culpabilité est donc évidente.

M. B., 25 ans, est marié depuis 3 ans, sa femme travaille comme comptable. Ils n'ont pas d'enfants. Il a un salaire de 2000 € par mois comme gérant d'une société de sécurité informatique. Ses parents sont en Algérie. Son père est directeur général d'une société de pétrochimie. Il a un bac+2. Le casier judiciaire est vierge.

Madame le procureur de la République a requis 4 mois d'emprisonnement avec sursis. Cette peine apparaît effectivement au préjudice subi, au trouble à l'ordre public et à la personnalité du prévenu. Elle sera donc prononcée à son encontre. Il a été demandé une non inscription au Bulletin n°2 du casier judiciaire mais l'intéressé ne justifie pas d'un intérêt actuel à bénéficier de cette mesure. Elle sera donc rejetée.

M. B. n'ayant pas été condamné au cours des cinq années précédant les faits pour crime ou délit de droit commun aux peines prévues par les articles 132-30, 132-31 et 132-33 du code pénal peut bénéficier du sursis simple dans les conditions prévues par les articles 132-29 à 132-34 de ce même code.

#### Sur l'action civile :

Le tribunal dit y avoir lieu à déclarer recevable en la forme la constitution de partie civile du Ministère de l'écologie et du développement durable, le Ministère de l'agriculture en la personne de l'agent judiciaire du Trésor et l'association française contre les myopathies, les sociétés Microsoft Portugal et Microsoft Corée.

#### Parties civiles :

L'agent judiciaire du Trésor, ès qualité de représentant du ministère de l'écologie et du développement durable, et du ministère de l'agriculture demande 15 000 € et 1000 € au titre de l'article 475-1. Au vu des arguments avancés, le préjudice causé sera évalué plus justement à la somme de 1000 €, 500 € étant alloué sur le fondement de l'article 475-1. L'AFM demande une somme de 5000 € et 15 000 € au titre de l'article 475-1. Là encore pour les mêmes raisons, il sera alloué une indemnité de 1000 € et 500 € pour les frais irrépétibles. Les sociétés Microsoft Portugal et Microsoft Corée demandent une somme de 5000 € à titre de dommages-intérêts, la publication du dispositif du jugement à intervenir dans deux journaux ou magazines papier, à hauteur de 2000 € par support, la publication du dispositif du jugement, dans le délai de 15 jours à compter du prononcé du jugement, en en tête de la page d'accueil et sur une surface égale à au moins 30% de celle-ci du site internet [www.frsirt.com](http://www.frsirt.com) ainsi que tous autres sites qui pourraient lui être substitués, pendant une durée de deux mois et sous astreinte de 5000 € sous astreinte par jour de retard ainsi que la somme de 1500 € à verser à chaque société sur le fondement de l'article 475-1 du code de procédure pénale, ainsi qu'aux entiers dépens. Il sera alloué une indemnité de 1000 € et 500 € pour les frais irrépétibles et le surplus sera rejeté.

Vu les dispositions de l'article 425 du code de procédure pénale, il convient de présumer le

désistement de la constitution des parties civiles des Assurances Ginet-Chomel, Air Ambiance assistance, EMI Music France, Reuters France, Gie EMI France.

#### **DECISION**

Le tribunal statuant publiquement, en matière correctionnelle, en premier ressort et par jugement contradictoire à l'encontre de M. B. prévenu, à l'égard du Ministère de l'écologie et du développement durable, le Ministère de l'agriculture et l'association française contre les myopathies, les sociétés Microsoft Portugal et Microsoft Corée parties civiles ; par jugement de défaut en application des dispositions de l'article 425 du code de procédure pénale à l'encontre des Assurances Ginet-Chomel, Air Ambiance assistance, Reuters France, Gie EMI Music France ;

#### Sur l'action publique :

Déclare M. B. coupable pour les faits qualifiés de :

- accès frauduleux dans un Système de traitement automatisé de données, faits commis courant août à 30 septembre 2002 et depuis temps non prescrit, à Paris, et à Montpellier et sur le territoire national,
- entrave au fonctionnement d'un Système de traitement automatisé de données, faits commis courant août à 30 septembre 2002 et depuis temps non prescrit, à Paris, et à Montpellier et sur le territoire national,
- introduction frauduleuse de données dans un Système de traitement automatisé de données, faits commis courant août à 30 septembre 2002 et depuis temps non prescrit, à Paris, et à Montpellier et sur le territoire national,
- tentative d'introduction frauduleuse de données dans un Système de traitement automatisé de données, faits commis courant août à 30 septembre 2002 et depuis temps non prescrit, à Paris, et à Montpellier et sur le territoire national,
- accès frauduleux dans un Système de traitement automatisé de données, faits commis courant 2002 et depuis temps non prescrit, sur le territoire national,
- introduction frauduleuse de données dans un Système de traitement automatisé de données, faits commis courant 2002 et depuis temps non prescrit, sur le territoire national,

Vu les articles susvisés ;

Condamne M. B. à 4 mois d'emprisonnement.

Vu les articles 132-29 à 132-34 du code pénal :

Dit qu'il sera sursis totalement à l'exécution de cette peine dans les conditions prévues par ces articles.

Et aussitôt, le président, suite à cette condamnation assortie du sursis simple, a

donné l'avertissement, prévu à l'article 132-29 du code pénal, au condamné que s'il commet une nouvelle infraction, il pourra faire l'objet d'une condamnation qui sera susceptible d'entraîner l'exécution de la première peine sans confusion avec la seconde et qu'il encourra les peines de la récidive dans les termes des articles 132-9 et 132-10 du code pénal.

Rejette la demande de non mention de cette décision au bulletin N°2 du casier judiciaire.

La présente décision est assujettie à un droit fixe de procédure d'un montant de 90 € dont est redevable M. B.

Sur l'action civile :

Déclare recevable, en la forme, la constitution de partie civile du Ministère de l'écologie et du développement durable, le Ministère de l'agriculture en la personne de l'agent judiciaire du Trésor et l'association française contre les myopathies, les sociétés Microsoft Portugal et Microsoft Corée ;

Condamne M. B. à payer Ministère de l'écologie et du développement durable, partie civile, la somme de 1000 € à titre de dommages-intérêts, et en outre la somme de 500 € au titre de l'article 475-1 du code de procédure pénale ;

Condamne M. B. à payer Ministère de l'agriculture, partie civile, la somme de 1000 € à titre de dommages-intérêts, et en outre la somme de 500 € au titre de l'article 475-1 du code de procédure pénale ;

Condamne M. B. à payer à l'association française contre les myopathies, partie civile, la somme de 1000 € à titre de dommages-intérêts, et en outre la somme de 500 € au titre de l'article 475-1 du code de procédure pénale ;

Condamne M. B. à payer aux sociétés Microsoft Portugal et Microsoft Corée, parties civiles, la somme de 1000 € à titre de dommages-intérêts, et en outre la somme de 500 € au titre de l'article 475-1 du code de procédure pénale ;

Rejette le surplus des demandes ;

Présume le désistement des Assurances Ginet-Chomel, Air Ambiance assistance, Reuters France, Gie EMI Music France.