



ASSEMBLÉE NATIONALE

11ème législature

Internet

Question écrite n° 49153

Texte de la question

M. André Thien Ah Koon souhaite attirer l'attention de M. le ministre de l'intérieur sur la propagation des virus informatiques sur Internet. Après le virus « Love Bug » qui a fait des ravages dans les ordinateurs du monde entier, un nouveau virus baptisé « SouthPark » se répand actuellement sur Internet. Il semblerait que le potentiel destructeur de ce nouveau virus soit encore plus important que celui de « Love Bug » : alors que celui-ci était doté de l'extension « vbs » (visual basic script), relativement peu fréquente, « SouthPark » est un fichier « exe », nettement plus répandu. Etant donné que ce virus a pour seule finalité de se dupliquer (qui, une fois ouvert, utilise le carnet de l'internaute pour se répandre instantanément dans d'autres ordinateurs), il représente un réel danger pour les réseaux informatiques des administrations et des entreprises. En conséquence, il le remercie de bien vouloir lui indiquer si des mesures sont envisagées pour protéger les réseaux informatiques contre ces virus, sources de nuisances pour les administrations et les entreprises.

Texte de la réponse

La lutte contre la cybercriminalité, et notamment celle visant à propager des virus informatiques ou d'autres programmes malveillants comme les Chevaux de Troie, doit s'adapter à la rapidité de transmission ou à la difficulté de repérer l'origine du virus, faute d'une traçabilité des connexions distincte de celle effectuée par le destinataire (dont les données sont le plus souvent détruites). Les logiciels anti-virus ne peuvent détecter un programme malveillant que si sa structure exécutable est déjà connue (extension, taille, secteur infecté : macros, scripts, boots, etc.) et enregistrée dans la base de signatures du programme anti-virus. En complément de cette approche technique de la lutte anti-virus (recherche, détection et destruction par un logiciel anti-virus), les entreprises ou les organismes publics victimes de ces attaques doivent les porter à la connaissance des services spécialisés dans la lutte contre la cybercriminalité. En effet, les diffusions de virus visant directement les réseaux d'entreprise peuvent avoir des mobiles très différents, qu'une enquête est susceptible de faire apparaître : destruction des traces laissées au cours d'une intrusion, malveillance d'un salarié, perturbation de l'action d'un concurrent, dissimulation d'une négligence en matière de sécurité, etc. L'office central de lutte contre les infractions liées aux technologies de l'information et de la communication a été créé par décret interministériel du 15 mai 2000. Cet office interministériel, rattaché à la direction centrale de la police judiciaire, est composé de policiers spécialisés prochainement renforcés par des gendarmes, des douaniers, et des ingénieurs réseau spécialisés. Outre son action en matière de lutte contre la cybercriminalité internationale, cet office a pour mission au plan national de contribuer à la sécurité informatique des particuliers et des entreprises. Le Gouvernement entend poursuivre une coopération active dans la lutte contre la cybercriminalité au sein du G8, du Conseil de l'Europe ou de l'Union européenne, et encourager la mise en place de points de contact nationaux spécialisés pouvant agir d'urgence 24 heures sur 24 et 7 jours sur 7. En matière de lutte contre les programmes malveillants, l'information rapide par les autorités concernées des entreprises et des particuliers susceptibles d'être visés est à la base d'une limitation des conséquences de ces actions. C'est pour assurer le recueil de ces informations qu'ont été mis en place des centres d'alerte et d'assistance sur Internet dont la mission est la détection et la résolution d'incidents concernant la sécurité des systèmes d'information. Le

CERTA (Center Emergency Response Team - Administration), mis en place début 2000 auprès du service central de sécurité des systèmes d'information du secrétariat général de la défense nationale, répertorie tous les incidents liés à la sécurité des réseaux de l'administration puis répercute cette information vers les administrateurs des autres réseaux de l'Etat en proposant des solutions techniques. Le CERT-Industrie regroupe des entreprises du secteur privé et répond aux mêmes impératifs.

Données clés

Auteur : [M. André Thien Ah Koon](#)

Circonscription : Réunion (3^e circonscription) - Députés n'appartenant à aucun groupe

Type de question : Question écrite

Numéro de la question : 49153

Rubrique : Télécommunications

Ministère interrogé : intérieur

Ministère attributaire : intérieur

Date(s) clé(s)

Question publiée le : 24 juillet 2000, page 4347

Réponse publiée le : 16 octobre 2000, page 5931