Le pare-feu des autorités chinoises est craqué par des chercheurs

Il est encore trop tôt pour dire au revoir à la censure et bonjour à la liberté d'expression. Quoi qu'il en soit, la nouvelle a fait rapidement le tour du monde des sites spécialisés .

Il faut dire que le régime de Pekin s'est encore illustré en ce début d'année par une reprise à la vitesse « V » de sa **chasse aux sorcières**. Mais voilà, des chercheurs britanniques de l'Université de Cambridge ont révélé qu'ils avaient trouvé une faille dans le système de censure chinois. Selon eux il existe un moyen d'utiliser ledit pare-feu pour lancer une attaque par déni de service contre des adresses IP spécifiques.

Le pare-feu utilisé, **signé Cisco**, est en particulier utilisé par les services gouvernementaux pour surveiller le trafic et identifier certains mots clés que les politiques souhaitent interdire sous prétexte qu'ils représentent une menace pour le parti et donc le pays.

Les ingénieurs de Cambridge ont mis à mal le pare-feu en lui envoyant des paquets contenant le **mot « Falun » ou « roue de la loi »**. Ce terme désigne la croyance « Falun Gong », proscrite par les autorités chinoises. Dans les années 1992, on comptait environ 80 millions d'adeptes.

Selon les ingénieurs universitaires, il est possible de tromper le système de détection IDS (Intrusion Detection Systems) chinois en ignorant les paramètres TCP auto configurés par les routeurs chinois qui devraient normalement abandonner ou rejeter la demande de connexion.

Richard Clayton, l'un des universitaires explique dans la presse anglo-saxonne : *« En chine, les ordinateurs autorisent le transfert de paquets (entrant et sortant) seulement ils peuvent fermer la connexion si un mot clé interdit apparaît dans la requête de l'internaute. »*

Pour Clayton, le constat est simple, le pare-feu chinois peut-être utilisé pour lancer des attaques par déni de services et cela même envers des sites du gouvernement. Le système de détection des intrusions ne donne pas d'informations sur l'état du serveur qui lui examine tous les paquets qui transitent par le pare-feu de manière individuel. En identifiant l'adresse de la source ayant fait une requête interdite, des personnes malveillantes pourraient « armer » le pare-feu de façon à interdire la communication entre la source et la destination *« pendant au moins une heure »* précise le chercheur.

Du coup, si notre garnement par chance ou par volonté est capable d'identifier les machines utilisées par le gouvernement il pourrait par exemple bloquer l'accès à Windows Update et même pire ainsi Clayton indique *« Tout cela est lié au design du pare-feu, un seul paquet, destiné à un haut membre du parti pourrait entraîner un déni de service. »*

Cette technique ne concerne que les communications entre deux points sur Internet, mais un attaquant seul qui utiliserait un modem classique pour se connecter à la Toile pourrait provoquer un gros plantage. S'il arme **cent paquets à la seconde**, et que chacun des paquets provoque une interruption de service de 20 minutes, on imagine aisément les dégâts.

Il faut toutefois apporter un bémol qui pourrait décevoir les amoureux de la liberté d'expression prêts à se lancer dans cette aventure périlleuse, puisque l'équipe de Cambridge a communiqué sa découverte au gouvernement chinois. Nul doute donc, que la faille soit rapidement comblée.