Après avoir effectuer plusieurs vérification dans notre parc informatique, j’ai pu identifier le type de cyber-attaque que l’entreprise à subi. Il s’aggit d’un spoofing : Cette forme d’attaque consiste à faire substituer l’adresse IP de la machine de l’expéditeur par celle d’une autre machine, afin de contourner le système de pare-feu ou « firewall » de la machine de l’utilisateur victime. Cette attaque peut se traduire par des paquets de données identiques à ceux d’une machine de confiance. Les pirates ont fait croire au réseaux que leur machine n’étaient pas étrangère et ils ont pus ainsi accéder à plusieurs données.

Pour se protéger, L'utilisation de logiciels comme arpwatch est recommandé. Il permet de centraliser les associations MAC/IP, et de contrôler en temps réel les messages pour vérifier qu'une menace n'est pas en cours. Des alertes sont alors générées en cas de divergence. Il pourrait même être envisagé un système de contre mesure consistant à repositionner la bonne association MAC/IP sur une machine venant de se faire attaquer. Ce repositionnement pourrait s'effectuer par le même processus que celui qui a permis l'attaque!

Having to make several check our computer equipment, i was able to identify the type of cyber-attack that the company in undergone. He aggit of a spoofing : this form of attack consists in making substitute the IP adress of the machine of the sender by that of another machine, to by-pass the system of firewall of the machine the user victim. This attack can be translated by packages of data identical to those of a reliable machine. The pirates persuaded in networks that their machine were not foreign and they have pus so to reach several data.

To protect itself, the users of software as arpwatch is recommended. He allows to centralize PIMP/IP associations, and to check in real time messages to verify that a threat is not in progress. Alerts are then generated in case of différence. He could be even envisaged a system of against measure consisting in repositionning the good PIMP/IP association on a machine coming be attacked. This repositioning could be made by the same process as the one who allowed the attack !