

Extrait du Spyworld Actu

<http://spyworld.spyworld-actu.com/spip.php?article2054>

Les barbouzes se mettent à la VoIP

- Terrorisme - International -



Date de mise en ligne : vendredi 2 juin 2006

Spyworld Actu

[Homeland Stupidity](#) nous raconte une histoire fort instructive sur un usage inattendu des réseaux de téléphonie sur IP. L'affaire commence avec la publication d'une petite annonce, rédigée comme suit : « Ma Fraulein, je n'ai pas de nouvelles de toi depuis un certain temps...Pourrais tu m'appeler au 212 796 0735 ? » Inutile de préciser qu'immédiatement, ce numéro public fut immédiatement « testé » par une armée de cybercurieux. Lesquels ont eu la surprise d'entendre [une voix égrener une série de chiffres regroupés par paquets de 5](#). Les habitués des ondes courtes se souviennent avec nostalgie de cette voix féminine expédiant des datagrammes semblables destinés aux agents en opération à l'étranger. La « voix du KGB », avec ses « Arrrrrtung arrrrtung, funeuf, neuheun, Tzvo, Koma, noul, heinss » évoquait des rivages où d'abominables Günther Schmetz affrontaient OSS117.

A noter que la voix synthétique annonce son chiffre en anglais, et non en allemand (langue qui « passe » mieux les brouillages radio). Que le message est assez court. Que sa méthode de mise en oeuvre comportent une faille... Non pas sa « visibilité publique », mais le fait que la ruée d'internautes sur le numéro de téléphone en question ait épuisé le compte prépayé, et donc rendu l'accès à l'information impossible. Que son en-tête et sa fin comporte une plage musicale insipide destinée à tromper les contrôles automatiques de contenu... mais d'une qualité tellement abominable que cela ne peut que provoquer une curiosité certaine. Un ensemble d'éléments qui sentent un peu l'amateurisme ou la procédure d'urgence. Mais même les espions les plus chevronnés commettent des bourdes et des enfantillages. Souvenons-nous des plombiers du Canard, des touristes du Rainbow Warrior, des conseillers militaires Comoriens égarés ou les professionnels de l'intox à la sauce Clearstream.

Le principe technique, en revanche, est redoutable d'efficacité. Il est anonyme... du moins tant qu'il règne un certain capharnaüm dans la législation internationale VoIP. Il n'oblige pas le ou les correspondants à posséder un équipement informatique permanent, une adresse « traçable » ou un numéro de cellulaire particulier. Il autorise tout autant le « multicast » d'ordres ou de consignes. Et surtout, l'appel VoIP élimine le principal inconvénient des émissions de Radio Karl-Marx-Stadt, à savoir le respect de l'heure de vacation. La ToIP constitue donc une boîte à lettre idéale pour les taupes en tous genres.

Mais la médiatisation de cette affaire est également à prendre avec des pincettes. Elle rappelle étrangement la mode de « la stéganographie, outil préféré des agents d'Al Quaida » qui servit d'argument -entre autres- pour justifier le filtrage, l'écoute et la rétention de toutes les données qui passent sur Internet, et ce, dans la plupart des pays du bloc de l'Ouest. Or, l'histoire du « numéro 212 » intervient précisément au moment où les faucons de Dick Cheney réclament à cors et à cris la généralisation des infrastructures d'enregistrement sur les réseaux VoIP. L'affaire des écoutes de la Maison Blanche avait donné un sérieux coup de frein à ce genre de demande, il fallait bien une menace pour relancer le débat. De là à penser que le contenu de ce message est un « bidon » monumental...Ajoutons que ce n'est pas en « fliquant » le trafic IP que les services de renseignements pourront acquérir une longueur d'avance sur les « méchants d'en face ». Les chefs de la Stasi se moquaient que l'on écoute leurs messages -un code est bien plus complexe à casser qu'un cryptage- et leurs héritiers spirituels doivent sourire à la seule évocation du coût que provoquera l'organisation d'une telle machine à surveiller dans le camp adverse. Usine à gaz aussi coûteuse qu'inefficace de surcroît, car il est plus rapide de changer de technique ou de procédure de transmission que de verrouiller tous les accès Internet d'un pays sur une simple présomption d'usage frauduleux.

Avec les NTIC, les agents de renseignement se sont vus offrir toute une panoplie d'appareils qui auraient fait se pâmer « Q » et son agent 007 : Nokia remplace Minox et PGP Enigma. La chaussure gauche de Max la Menace s'est changée en U.A. de mail, la VoIP prend la relève de l'émetteur morse, romantisme en moins, et la pose de microphones espions se transforme de nos jours en diffusion de Troyens et spywares. Et il est peu probable que le phénomène date de cette année. Les plus malheureux sont bien les auteurs de romans noirs. Ca vous casse un suspens, l'envoi de secrets par MMS. Ca vous flingue une intrigue, une course-poursuite par TraceRoute IP. Et quand çà défouraille, c'est à coup d'Interrupts et de buffer overflows. Fatal, c'est moins sanglant, ca va pas passionner les foules. Monsieur Philippe Rondo, Monsieur Pierre de Bousquet de Florian, rendez nous nos services « moustache » d'antan.

Post-scriptum :

<http://www.reseaux-telecoms.net/act...>