Notes MCC D'ALERTE
DÉPARTEMENT DE RECHERCHE SUR LES MENACES CRIMINELLES CONTEMPORAINES
INSTITUT DE CRIMINOLOGIE DE PARIS-UNIVERSITÉ PARIS II PANTHÉON-ASSAS

N° 10 – mai 2007

Argent criminel ou terroriste ...

*L'avenir radieux du **mandat téléphonique***

FRANÇOIS-BERNARD HUYGHE
contact@huyghe.fr

Nous sommes en 2008…

• Jihadiste français affilié à « al-Qaïda au Maghreb », vous préparez un attentat contre le mufti de Marseille, un modéré. Il vous faut quelques milliers d'euros pour acheter du matériel et de faux papiers, à demander d'urgence à l'organisation mère. Comment opérer ? Envoyer un frère chercher une valise de billets ? faire un virement de banque à banque et aller au guichet ? Simple : vous prenez votre téléphone portable, celui que la police ne peut intercepter parce que vous changez de puce à chaque fois, vous tapez sur le clavier. Quelques minutes plus tard, votre fournisseur regarde son propre portable et hoche la tête : vous pouvez emporter la marchandise, il est payé. Changez la puce – sans jeter votre téléphone : le jour de l'attentat, si vous n'avez pas une vocation de kamikaze, il vous permettra aussi de déclencher la bombe à distance.

• Vous êtes Youri un petit génie de l'informatique. Depuis quelques semaines, vous répandez via Internet un logiciel « cheval de Troie » que les naïfs téléchargent en cherchant des images pornographiques avec leurs GSM. Aujourd'hui vous pressez une touche et attendez quelques minutes. Votre commanditaire assis derrière vous vérifie un compte bancaire puis vous adresse un gentil sourire : des dizaines de milliers de téléphones dans le monde viennent au même moment de le créditer chacun de quelques euros à l'insu de leur propriétaire. Le temps que quiconque réalise ce qui se passe, les fonds ont disparu. Youri aussi, d'ailleurs.

Pure imagination, n'est-ce pas ?

Hélas non. Pour s'en convaincre, revenons à l'actualité récente.

En février de cette année MasterCard et GSM Association (GSMA) ont annoncé la création d'un système destiné à émettre et de recevoir des mandats internationaux par téléphone mobile. Dix-neuf opérateurs représentant environ 600 millions d'usagers dans cent pays s'associent à ce projet pour lequel un programme pilote est déjà lancé. Le but est entre autres de permettre à des

travailleurs migrants qui ne possèdent pas nécessairement de compte en banque d'envoyer facilement de l'argent aux leurs, partant du principe que le réseau mobile couvre bien mieux la planète que le réseau bancaire. Le potentiel de développement est impressionnant : à la fin 2004, GSMA regroupait plus de 660 opérateurs, desservant plus de 1,3 milliard de clients dans 210 pays. Un système qui existe à l'état d'ébauche aux Philippines et dans d'autres pays.

A priori, l'initiative est sympathique : pourquoi les pauvres (ou d'ailleurs les riches) devaient-ils payer des frais importants et attendre des jours pour un mandat ? Des milliards circulent tous les jours de Bourse à Bourse sous forme de bits informatiques et les projets de type « porte monnaie numérique » se développent ; pourquoi un mandat continuerait-il à être un papier mal imprimé, plein de cases mystérieuses, nécessitant force coups de tampons et arrivant avec la prochaine tournée du facteur ?

Donc tout va bien… À moins que…

À moins que la criminalité internationale n'exploite les failles de ce système.

Des milliards de dollars vont circuler de pays à pays, vite, souvent, par petites sommes qui n'attirent guère l'attention, de ou vers des zones où il n'existe pas forcément des administrations fiscales et policières tatillonnes et incorruptibles. La traçabilité des opérations dépendra des disques durs d'opérateurs, téléphoniques ou bancaires, dispersés, soumis à des législations ou à des normes légales et à des techniques de contrôle très différentes. La vérification des noms et des adresses des acteurs (voire celle de leur simple existence) sera complexe. Tout se passera entre correspondants virtuels identifiés par un numéro et dont personne ne verra la tête.

Certains appartiendront à des communautés exilées et vivront des conditions où ils pourront être facilement soumis aux pressions. Pense-t-on sérieusement qu'un Pakistanais ou Vietnamien travailleur pauvre à des milliers de kilomètres de chez lui a les moyens de résister à l'amicale pression de gens qui lui demanderont de leur rendre un petit service tous les mois ? S'imagine-t-on que tout le dispositif technique chez les fournisseurs d'accès, les opérateurs, mémoires commutateurs, concentrateurs (*hubs*), routeurs pourra être visité par un cyber-gabelou ?

> ***• Ce système complexe représentera d'incroyables opportunités pour tous les trafics et blanchissements. En tant que réseau planétaire, instantané, à multiples entrées, facilement anonyme, il est intrinsèquement vulnérable.***

S'ajoute un second facteur. Un combiné GSM est par nature un objet nomade, presque intime puisqu'on le porte toujours avec soi. Il est aussi un terminal relié à des flux numériques de voix, de textes, d'images, de données et maintenant d'argent circulant sous forme numérique, via une multitude de relais et vecteurs. Il conjugue toutes les faiblesses d'un ordinateur en termes de sécurité plus d'autres qui sont liées à son statut d'objet hybride.

Ces dernières années, les affaires touchant à la sécurité des mobiles se sont multipliées. Certaines, très « haut de gamme », visaient par exemple à faire de l'espionnage économique (forcément coûteux) sur les téléphones des responsables économiques ou autres. Mais d'autres s'adressaient en masse à des utilisateurs ordinaires pour leur faire dépenser quelques cents, un petit vol presque invisible sur une facture, mais très rentables pour celui qui en recueille le résultat à grande échelle.

Tout ce qui peut se faire sur un ordinateur (virus, chevaux de Troie et autres logiciels malveillants, consultation de données confidentielles, vol de code, substitution d'identité, prise de commande sur l'appareil ou un réseau d'appareils, interception des messages, phishing qui consiste à attirer sa victime sur un faux site ou un faux central téléphonique pour l'escroquer..) tout cela se fait sur un téléphone mobile. Celui-ci acquiert de plus en plus de fonction d'un PC (y compris

celle d'aller sur Internet), est mal protégé par des puces et des codes et est accessible par de multiples vecteurs y compris les ondes de Bluettooh ou Wifi, peu réputées pour leur sécurité.

En d'autres termes, ce sont autant de possibilités de substitution, de prélèvement et d'opérations non autorisées. Mais aussi de prédation et de sabotage pouvant donner lieu à chantage et extorsion. De la mini-ecroquerie pour voler quelques roupies numériques à un malheureux aux grandes opérations coordonnées portant simultanément sur la prise de commande de milliers de comptes : le champ est vaste qui vient de s'ouvrir à l'imagination criminelle. Il couvre aussi bien des actions sophistiquées reposant sur la cryptologie que des escroqueries basées sur la naïveté ou la faillibilité humaines.

S'il est un cas où le décèlement précoce doit s'appliquer, c'est bien à celui-là.

Nous voyons la conjonction d'une technique encore mal sécurisée, d'une multiplicité de maillons faibles - qu'ils soient matériels ou humains- d'une dispersion internationale et d'une multiplication des cibles mal protégées, de gros enjeux financiers, de risque minimal et de possibilités d'expansion et de profits grâce aux réseaux pour des organisations travaillant en réseaux. Certes, on se doute que des organismes comme Mastercard qui ont assez payé pour savoir ne vont pas négliger la sécurité. Mais il reste que les problèmes posés par les mandats internationaux virtuels ne se résoudront pas forcément par davantage de protection technologique ou de meilleurs algorithmes : beaucoup seront simples voire rustiques tout en se posant à l'échelle planétaire. Raison de plus pour en surveiller les développements.

***

Version complète du document sur le site du Département de Recherche sur les Menaces Criminelles Contemporaines :

www.drmcc.org

(cliquer sur *Notes d'alerte* en page d'accueil)