CRIMISCOPE

ESC - UNIL - 1015 Lausanne Numéro 26 – Décembre 2004

Exploitation opérationnelle et stratégique des courriers électroniques de la « Nigerian Connection »

L'escroquerie de type « Nigerian Connection » est un phénomène criminel d'envergure dont le principe est d'appâter les victimes en leur proposant une forte récompense en échange de différents services. L'utilisation de la messagerie électronique pour contacter les victimes s'est développée avec la généralisation de ce moyen de communication. Les auteurs sont très difficiles à poursuivre, car les complices qui participent à la réalisation de l'escroquerie se situent dans des pays différents. Des citoyens qui flairent l'arnaque transmettent fréquemment ces messages (courriels) à la police. Ce jeu d'informations permet potentiellement de disposer d'une image pertinente de ce phénomène, mais est actuellement peu exploité.

Dans le cadre d'une recherche, l'École des Sciences Criminelles, en collaboration avec la police cantonale vaudoise, a mis en place une structure pour recevoir, traiter et analyser ces messages électroniques. Chaque courriel reçu est classifié en fonction :

- du **texte du message** (par ex. pays d'origine annoncé par l'auteur, pays d'accueil annoncé, langue utilisée, numéro de téléphone de contact, adresse électronique de contact, etc.)
- des **informations liées au courrier électronique** (adresse électronique de l'expéditeur, date/heure d'envoi, service de messagerie, adresse IP[1], etc.)
- de l'**adresse IP de l'ordinateur utilisé** par l'auteur pour gérer sa messagerie.

L'adresse IP permet généralement de déterminer le pays où se trouve le fournisseur d'accès[2] utilisé par le/les auteurs.

La structure simplifiée de la base de données qui accueille les informations extraites des courriels est illustrée par la figure 1.

L'analyse et l'interprétation de 438 courriels ont notamment permis d'obtenir les renseignements suivants :

- le pays qui apparaît dans le scénario du message et la localisation supposée au moyen du numéro IP sont différents;
  - les **pays d'origine** dans lequel le scénario est censé se dérouler sont majoritairement : le Nigeria, la Sierra Leone, la Côte d'Ivoire, le Congo et l'Afrique du Sud ;
  - les **pays d'accueil** où les protagonistes sont censés se trouver sont principalement la Côte d'Ivoire, les Pays-Bas et l'Afrique du Sud ;
  - les **adresses IP** montrent généralement une localisation aux Pays-Bas, au Nigeria, aux USA, en Israël, en Côte d'Ivoire et en Afrique du Sud.
- L'ensemble des liens (individuels) entre les messages (IP, numéro de téléphone/fax, adresse électronique) a permis de créer quelques groupes de message électronique. Il conviendrait d'augmenter l'échantillon de données pour constater si des groupes plus conséquents indiquant l'existence d'une ou plusieurs organisation(s) apparaîtraient.
- Une relation entre les scénarios typiques de la N-Connection (par ex : familier [next of kin], paysans en fuite [farmer], dictateur déchu [dictator]) et les messages de type « loterie » a pu être démontrée (figure 2). Celle-ci montre bien que les auteurs font évoluer leur scénario pour piéger de nouvelles victimes. L'apparition toujours plus fréquente de messages en Français, donc plus ciblés, est un autre signe de cette capacité d'adaptation.
- Dans le jeu de données, une adresse IP située en Suisse a été trouvée, ce qui montre la possibilité d'ouvrir des enquêtes à l'échelle du pays.

Ces résultats obtenus au moyen d'un échantillon de données restreint sont prometteurs tant d'un point de vue opérationnel que stratégique. Ils indiquent ainsi le potentiel d'un traitement plus systématique et à plus large échelle. Pour cela les possibilités d'automatiser davantage le processus de traitement des messages sont actuellement évaluée

Figure 1 : *Structure simplifiée de la base de données*

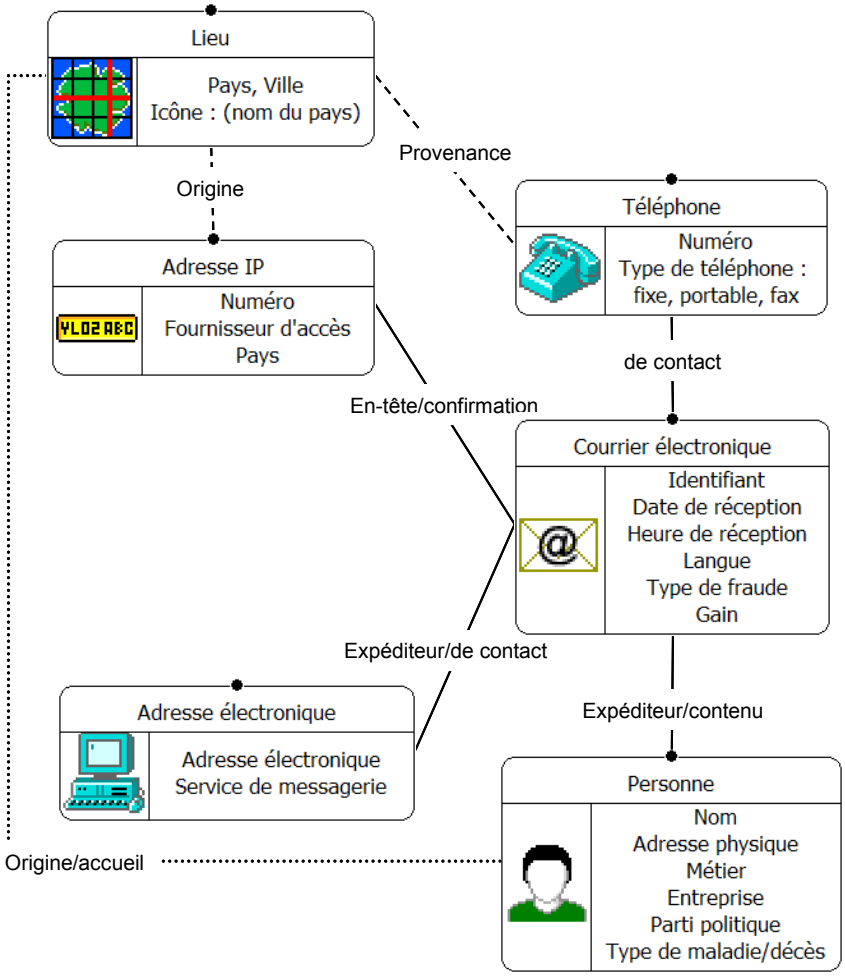
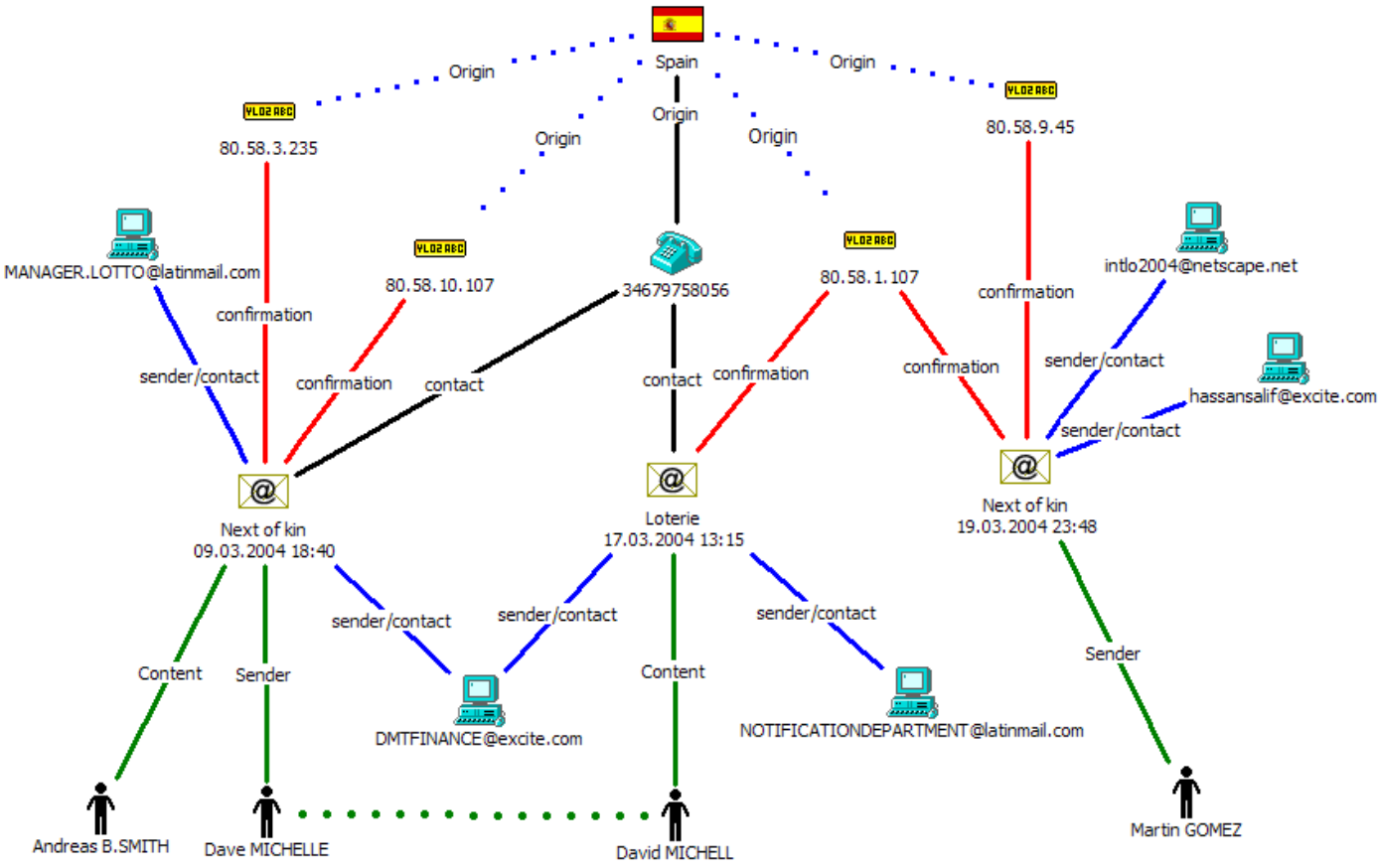


Figure 2 : *Relations entre messages du type « N-Connection » et du type « Loterie »*



Errata

Violences contre les femmes (CRIMISCOPE n°25):
Une fâcheuse erreur s'est glissée dans la version française du dernier n° de CRIMISCOPE. En fait, les taux de violences dirigées contre des partenaires sont inférieurs à ceux constatés dans d'autres pays (Australie, Danemark, Tchéquie), et non pas l'inverse. Nous prions nos lecteurs d'excuser cette méprise.

Référence :

Schiffer B., Birrer S., Cartier J., Capt S., Ribaux O. (2004), *"Analyse de la forme, du contenu et de la provenance des courriers électroniques.",* Revue internationale de criminologie et de police technique et scientifique(2): 148-158.

Renseignements :

Ecole de Sciences Criminelles - Institut de Police Scientifique – BCH - 1015 Lausanne-Dorigny Tél. 0041 21 692.46.00 - Fax 0041 21 692.46.05 – stephane.birrer@unil.ch

Notes

[1] L'Internet Protocol Address est un numéro unique attribué à chaque machine qui se connecte sur Internet.
[2] Généralement, le fournisseur d'accès (ou Internet Service Provider) se situe proche de l'ordinateur connecté, cette proximité permettant de diminuer les coûts de liaison entre eux.

Rédaction: Prof. P. Margot et Prof. M. Killias, ESC, UNIL, 1015 Lausanne

Veuillez adresser vos remarques et communications à:

Secrétariat du Crimiscope
UNIL – Ecole des sciences criminelles
CH–1015 LAUSANNE

(021) 692 46 44
Fax (021) 692 46 05
Int. (+ 41 21) 692 46 44