Analyse de la forme, du contenu et de la provenance des courriers électroniques de la «Nigerian Connection» (1)

par **Beatrice SCHIFFER*, Stéphane BIRRER*, Julien CARTIER**, Sébastien CAPT* et Olivier RIBAUX***

Résumé
La "Nigerian Connection" est une escroquerie 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. Des citoyens qui flairent l'arnaque transmettent fréquemment ces messages à la police. Ce jeu d'informations permet potentiellement de disposer d'une image pertinente de ce phénomène, mais est actuellement peu exploité. Cette étude propose le développement d'une méthode d'analyse en temps réel de la forme, du contenu et de la provenance de ces courriels. L'étude préliminaire de 233 messages met en évidence principalement les types de fraudes et l'emplacement réel des escrocs. L'utilisation d'un système de confirmation de lecture des courriers électroniques permet notamment d'obtenir l'emplacement des escrocs lorsqu'ils lisent leurs courriels.

Abstract
The "Nigerian Connection" is a large swindle which principle is to attract victims in their proposer a strong reward in exchange of various services. The use of electronic mails to contact victims is developing with the generalization of this type of communication. Citizens who smell frauds frequently transmit these messages to law enforcement agencies. This information could potentially be exploited to give a relevant image of this phenomenon, but it is little used nowadays. This study proposes an analysis of the form, contents and origin of these electronic mails. The analysis of 233 messages highlights particular types of frauds and the real origin of the swindlers. The use of a reading confirmation system makes it possible to obtain the swindlers' position when they read their electronic mails.

Introduction

La Nigerian Connection (Nigerian Advance Fee Fraud) ou "419 scam" (en référence à l'article du code pénal nigérian réprimant ce comportement) est une escroquerie (scam) d'envergure, perpétrée à large échelle, et qui rapporte à leurs auteurs des montants estimés à plusieurs millions de dollars (National White Collar Crime Center and the Federal Bureau of Investigation 2001). Son principe consiste à appâter les victimes en leur proposant une forte récompense en échange de différents services. Un des subterfuges le plus couramment utilisé consiste à demander de l'aide pour débloquer la fortune d'un chef d'Etat

* Ecole des Sciences Criminelles (ESC), Université de Lausanne (Suisse)
** Police Cantonale Vaudoise (Suisse)

africain déchu immobilisée dans un paradis fiscal ou dans le pays qu'il a dû fuir (Bureau of International Narcotics and Law Enforcement Affairs 1997). Une commission de 10 à 35% du montant total de la fortune est proposée à ceux qui acceptent de servir d'intermédiaires pour faire transiter cette forte somme d'argent. Une fois qu'une victime est intéressée par ce gain facile, les escrocs cherchent à lui faire verser à l'étranger une succession de montants qui paraissent proportionnellement ridicules par rapport aux sommes en jeu, comme des «avances pour frais de dossier». Bien sûr, dès que suffisamment d'argent est versé, le soi-disant fortuné dictateur disparaît sans laisser d'adresse.

Les malfaiteurs prenaient initialement contact par des lettres et des fax au moyen desquels ils sondaient des entreprises ou des individus. Le courrier électronique leur permet maintenant d'atteindre sous forme de spam (2) de grandes quantités de victimes potentielles (Buchanan et Grant 2001) résidant dans n'importe quel pays (figure 1).

FROM: BARRISTER AKINI ABBEY
OKEAYA INNEH LAW FIRM
ATTORNEYS/LEGAL PRACTITIONERS.
NIGERIA

ATTENTION: XXXXXXXXXX
DEAR SIR/MADAM,

COMPLIMENTS OF THE SEASON. GRACE AND PEACE AND LOVE FROM THIS PART OF THE ATLANTIC TO YOU. I HOPE MY LETTER DOES NOT CAUSE YOU TOO MUCH EMBARRASSMENT AS I WRITE TO YOU IN GOOD FAITH BASED ON THE CONTACT ADDRESS GIVEN TO ME BY A FRIEND WHO WORKS AT THE
NIGERIAN EMBASSYIN YOUR COUNTRY. PLEASE EXCUSE MY INTRUSION INTO YOUR PRIVATE LIFE.

I AM BARRISTER AKINI ABBEY , I REPRESENT MOHAMMED ABACHA, SON OF THE LATE GEN. SANI ABACHA, WHO WAS THE FORMER MILITARY HEAD OF STATE IN NIGERIA. HE DIED IN 1998. SINCE HIS DEATH, THE FAMILY HAS BEEN LOSING A LOT OF MONEY DUE TO VINDICTIVE GOVERNMENT OFFICIALS WHO ARE BENT ON DEALING WITH THE FAMILY. BASED ON THIS THEREFORE, THE FAMILY HAS ASKED ME TO SEEK FOR A FOREIGN PARTNER WHO CAN WORK WITH US AS TO MOVE OUT THE TOTAL SUM OF US$75,000,000.00 (SEVENTY FIVE MILLION UNITED STATES DOLLARS), PRESENTLY IN THEIR POSSESSION. THIS MONEY WAS OF COURSE, ACQUIRED BY THE LATE PRESIDENT AND IS NOW KEPT SECRETLY BY THE FAMILY. THE SWISS GOVERNMENT HAS ALREADY FROZEN ALL THE ACCOUNTS OF THE FAMILY IN SWITZERLAND, AND SOME OTHER COUNTRIES WOULD SOON FOLLOW TO DO THE SAME. THIS BID BY SOME GOVERNMENT OFFICIALS TO DEAL WITHTHIS FAMILYHAS MADE IT NECESSARY THAT WE SEEK YOUR ASSISITANCE IN
RECEIVING THIS MONEY AND IN INVESTING IT ON BEHALF OF THE FAMILY.

THIS MUST BE A JOINT VENTURE TRANSACTION AND WE MUST ALL WORK TOGETHER. SINCE THIS MONEY IS STILL CASH, EXTRA SECURITY MEASURES HAVE BEEN TAKEN TO PROTECT IT FROM THEFT OR SEIZURE, PENDING WHEN AGREEMENT IS REACHED ON WHEN AND HOW TO MOVE IT INTO ANY OF YOUR NOMINATED BANK ACCOUNTS. I HAVE PERSONALLY WORKED OUT
ALL MODALITIES FOR THE PEACEFUL CONCLUSION OF THIS TRANSACTION. THE TRANSACTION DEFINITELY WOULD BE HANDLED IN PHASES AND THE FIRST PHASE WILL INVOLVE THE MOVING OF US$25,000,000.00(TWENTY FIVE MILLION UNITED STATES DOLLARS).

MY CLIENTS ARE WILLING TO GIVE YOU A REASONABLE PERCENTAGE OF THIS MONEY AS SOON AS THE TRANSACTIONIS CONCLUDED. I WILL, HOWEVER, BASED ON THE GROUNDS THAT YOU ARE WILLING TO WORK WITH US AND ALSO ALL CONTENTIOUS ISSUES DISCUSSED BEFORE THE COMMENCEMENT OF THIS TRANSACTION. YOU MAY ALSO DISCUSS YOUR PERCENTAGE BEFORE WE START TO WORK. AS SOON AS I HEAR FROM YOU, I WILL GIVE YOU ALL NECESSARY DETAILS AS TO HOW WE INTEND TO CARRY OUT THE WHOLE TRANSACTION.

PLEASE, DO NOT ENTERTAIN ANY FEARS,AS ALL NECESSARY MODALITIES ARE IN PLACE, AND I ASSURE YOU OF ALL SUCCESS AND SAFETY IN THIS TRANSACTION.

PLEASE, THIS TRANSACTION REQUIRES ABSOLUTE CONFIDENTIALITY AND YOU WOULD BE EXPECTED TO TREAT IT AS SUCH UNTIL THE FUNDS ARE MOVED OUT OF THIS COUNTRY.

PLEASE, YOU WILL ALSO IGNORE THIS LETTER AND RESPECT OUR TRUST IN YOU BY NOT EXPOSING THIS TRANSACTION, EVEN IF YOU ARE NOT INTERESTED.

I LOOK FORWARD TO WORKING WITH YOU.

THANK YOU.

TRULY YOURS,

AKINI ABBEY ESQ

Figure 1: Exemple d'un courrier électronique de la Nigerian Connection

Il est généralement supposé que les auteurs proviennent du Nigéria ou d'autres pays de l'Ouest africain tels que le Ghana, le Togo, le Libéria, la Sierra-Leone ou la Côte-d'Ivoire (3). D'autres sources (4) mentionnent également l'Angleterre, les Pays-Bas et les Etats-Unis.

La honte, l'illégalité de l'arrangement et la peur d'éventuelles représailles dissuadent les lésés de se plaindre à la police même s'ils ont perdu des sommes conséquentes (Smith *et al.* 1999). Le déclenchement d'enquêtes est donc relativement rare et celles qui sont menées aboutissent difficilement car les investigateurs doivent agir dans plusieurs systèmes judiciaires différents et l'origine des courriers, les rencontres avec les escrocs, les comptes transitoires et les comptes sur lesquels les victimes versent de l'argent se situent généralement dans des pays différents. De même, l'ampleur réelle de cette escroquerie et son évolution ne sont pas connues car la dimension géographique empêche une analyse stratégique fondée de ce phénomène. La lutte contre cette escroquerie est donc difficile.

Toutefois, les citoyens qui flairent l'arnaque n'hésitent pas à transmettre à la police de nombreux courriers électroniques envoyés par les escrocs qui incitent ainsi les utilisateurs de la toile à tomber dans leur piège. Ces messages constituent une source d'information souvent inexploitée. Dans le cadre de cette étude, leur potentiel informatif a été évalué par un traitement systématique des messages transmis à une police suisse qui couvre une région de 600'000 habitants environ (figure 2).

Méthode

Durant une période de 3 mois, tous les courriers électroniques transmis à la police ont été analysés selon leur forme, leur contenu et leur provenance. Une base de données informatisée qui répertorie 233 courriers reçus a été construite et a aidé à traiter les messages.

Détermination de la provenance d'un courrier électronique

Les endroits depuis lesquels les courriers électroniques sont envoyés constituent une information évidemment cruciale car elle peut largement influencer les

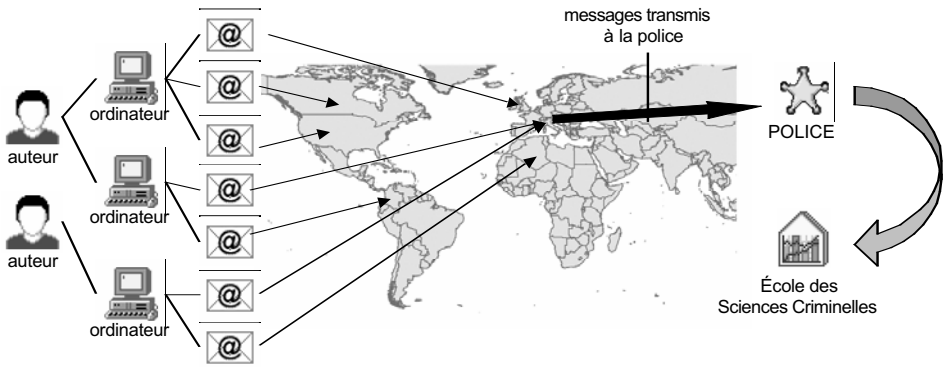

Figure 2: Déroulement de l'envoi de message électronique avec réception par la police et analyse par l'École des Sciences Criminelles (ESC)

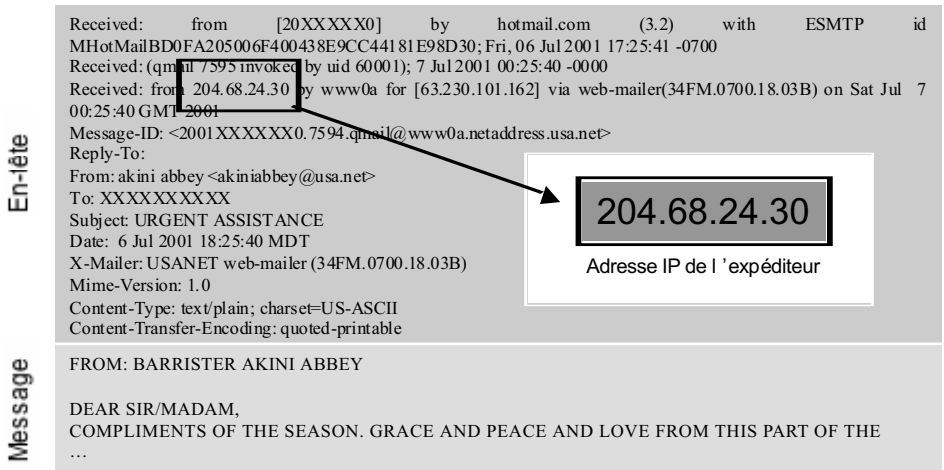

Figure 3: Exemple de visualisation de l'adresse IP d'un courrier électronique

possibilités pour le système judiciaire de lutter contre ces escroqueries. L'en-tête (header) des messages reçus contient potentiellement cette information grâce à un numéro, appelé numéro IP (Internet Protocol) qui attribue une identité à chaque ordinateur connecté au réseau: il n'y a pas deux ordinateurs connectés en même temps sur INTERNET qui peuvent porter le même numéro. Ces adresses sont gérées et distribuées par une agence selon une logique qui permet de situer la machine qui porte un certain numéro et qui communique sur le réseau (figure 3).

Mais la localisation n'est pas immédiate car un ordinateur se voit généralement attribuer un numéro différent à chaque connexion; de plus, certains fournisseurs de service de messagerie gratuits on-line ne font pas toujours figurer le numéro de la machine utilisée pour rédiger le message (Hotmail.com le fait, mais pas Ziplip.com par exemple) et les messages reçus par la police sont souvent amputés de l'en-tête, donc de l'adresse IP; enfin, il existe des possibilités de tromper le destinataire sur l'origine d'un message, au moyen de différentes techniques, notamment par l'utilisation d'un service d'anonymisation qui attribue un nouveau numéro IP à l'ordinateur ou un service de remailing qui renvoie les courriers électroniques en remplaçant l'adresse IP d'origine par une autre.

L'information contenue dans l'en-tête ne suffit donc pas à notre analyse. C'est la raison pour laquelle une étude plus approfondie a été réalisée en répondant aux messages reçus tout en intégrant à notre courrier un mécanisme de confirmation de lecture qui, lui-même, renseigne sur l'adresse IP de notre destinataire. Pour cela, nous avons utilisé un site web commercial qui propose ce service. La figure 4 explique ce système.

Les variables

La base de données a été structurée principalement selon les dimensions suivantes:

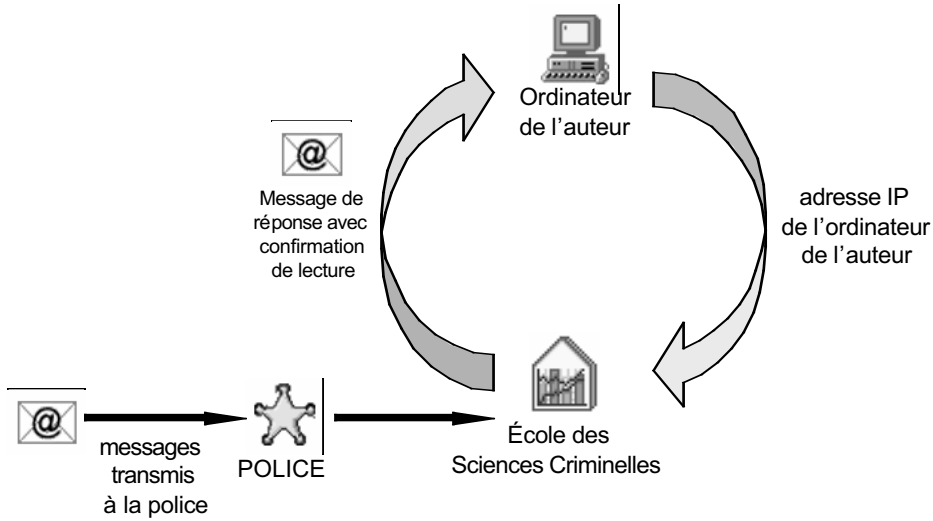

Figure 4: Système de confirmation de lecture avec extraction de l'adresse IP

- Présence ou absence d'un en-tête
  Cette variable permet de savoir si les courriers reçus contiennent un en-tête ou pas. Cette variable est liée au mode de transmission du message de la victime vers la police, certaines victimes imprimant le message sans l'en-tête ou ne transmettant électroniquement que le texte du message.
- Adresses IP
  Les adresses IP peuvent parfois être obtenues par les informations contenues dans l'en-tête ou par l'utilisation du service de confirmation. Elles permettent de supposer l'emplacement de la machine ayant envoyé le message frauduleux.
  Par ailleurs, l'obtention d'une adresse IP par le service de confirmation indique que le courrier a été lu et qu'il sert à une prise de contact.
- Adresses électroniques des fraudeurs
  Les escrocs utilisent différents services de messagerie électronique et différentes adresses.
- Date et heure d'envoi
  L'historique des messages est évidemment crucial pour l'analyse. Par exemple le traitement des courriels envoyés le même jour peut amener à s'intéresser aux messages identiques, mais transmis par plusieurs contributeurs différents. L'apparition et la durée de vie d'une «légende» (5) ou d'une adresse électronique peuvent être observées et des particularités tels des jours de la semaine préférés pour les envois ou la fréquence avec laquelle les boîtes aux lettres électroniques sont relevées par les malfaiteurs peuvent être mis en évidence.
- Pays mentionnés
  Généralement la «légende» indique un pays d'origine et l'auteur indique un pays d'accueil; cette variable permet donc entre autres de vérifier si le pays

d'accueil qui apparaît dans l'histoire racontée par les escrocs concorde avec celui de l'adresse IP.

- Nom donné
  Les noms choisis par les fraudeurs peuvent être de deux types: ou bien liés à un personnage réel tel que Mobutu Sese Seko (dictateur) ou bien être de type imaginaire.
  Dans le premier cas, le nom a une importance et restera le même d'un message à un autre tant que la même histoire est exploitée, tandis que dans le deuxième cas le nom varie selon l'imagination de l'auteur.
- Sujet
  Le sujet a pour but de persuader la victime potentielle de lire le message; les mots utilisés sont souvent les mêmes, ils sont donc facilement classifiables (par exemple: BUSINESS, CONFIDENTIAL, URGENT ASSISTANCE).
- Type de contact
  Trois moyens de contact sont proposés par les malfaiteurs: courriel, téléphone et fax. Il s'agit de savoir si le courrier électronique sert effectivement de moyen de contact ou si les escrocs utilisent de préférence des téléphones et fax. Cette variable donne des indications sur le *modus operandi*.
- Numéro de téléphone/fax
  Permet d'analyser les numéros de téléphone ou de fax et de les comparer entre eux afin de déterminer leur origine et si les mêmes numéros apparaissent plusieurs fois.
- Type de fraude
  Les fraudes les plus communes ont été classifiées par un terme générique typique de la légende. Parfois des sous-groupes d'un type de fraude peuvent être définia. La classification proposée s'est inspirée de celle utilisée sur le site www.internet-fraud.com et a été adaptée en fonction des courriers électroniques analysés.

    next of kin / proche: un étranger mort n'a pas d'héritiers, la victime remplacera les proches manquants du décédé, il s'agit de la version générale du «general auditor».

    general auditor: il s'agit d'un sous-groupe du type «next of kin / proche», mais avec un contenu très spécifique tel l'utilisation du terme «general auditor» ayant l'Afrique du Sud comme origine.

    over invoice: une somme d'argent a pu être détournée en surévaluant un contrat par des personnes dans le service de l'Etat ou autre, en majorité des Nigérians. Ils ont besoin d'aide pour déposer cette somme hors du pays.

    dictateur: tous les familiers, avocats et autres personnes se référant à un dictateur.

    farmer: familiers de «paysans», souvent du Zimbabwe, qui se sont réfugiés dans un autre pays et qui ont besoin d'aide pour accéder à leur argent.

    enfant seul: enfant qui sait souvent mal écrire et qui cherche une personne pour l'aider, entre autre pour améliorer son éducation et accéder à l'argent hérité de ses parents décédés.

maladie: cas isolés de personne ayant une maladie et joue sur la pitié, une connotation religieuse est possible.
autre: histoire n'ayant pas pu être classifiée autrement.

- Majuscule/Minuscule
  Selon l'hypothèse du copier/coller ou de l'effort minimum pour modifier le texte des courriers, il est imaginable que les messages majuscules vont se retrouver modifiés dans des messages majuscules et la même chose pour ceux en minuscules.
- Institutions mentionnées
  Les institutions les plus citées ont été classifiées. Elles sont souvent couplées à un type de fraude. Les principales institutions mentionnées sont:
  NNPC: «National Nigerian Petroleum Company»
  Gouvernement Nig.: des gens du gouvernement nigérian en général (sans NNPC)
  SA minerals: département de minéraux de l'Afrique du Sud
    - Finance of mineral resources and energy South Africa

  Banque: beaucoup de banques (in)existantes mentionnées
  SA: Afrique du Sud en général
  Les entreprises de «sécurité» n'ont pas été retenues, n'étant pas spécifiques à un type de fraude.
- **Signes de modification**
  Sous l'hypothèse que les courriers sont souvent modifiés par copier/coller, ceci peut donner lieu à des incohérences de contenu (ex. nom, sexe, etc.) ou de mise en page tel qu'une phrase ou un mot coupé au milieu.

Résultats

Caractéristiques du destinataire

Le système de classification a été appliqué à 233 courriels reçus par une police suisse durant les mois de janvier à mars 2003. Seuls 29 messages reçus comportaient l'en-tête (header), soit 12% des messages. Ces 233 courriers viennent de plus de 50 contributeurs différents. Le principal contributeur a transmis à la police 16 messages durant la période retenue.

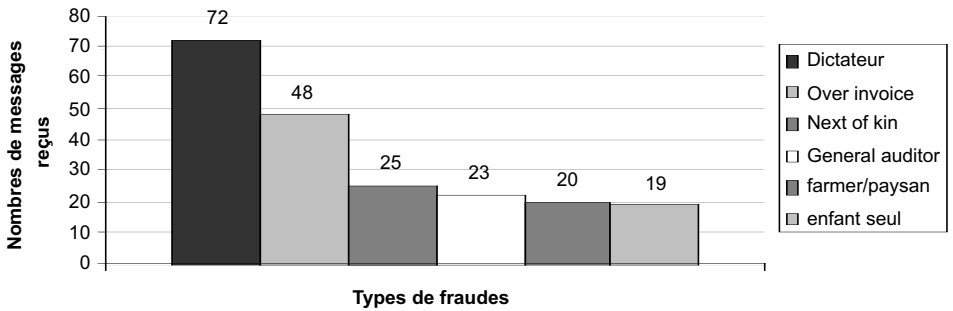

Figure 5: Principaux types de fraudes rencontrées

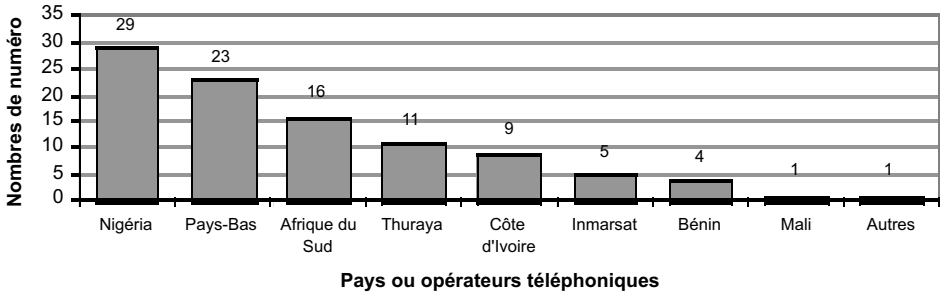

Figure 6: Origine des numéros de téléphone ou de fax mentionnés dans les messages

Caractéristiques du message

La langue des messages reçus est essentiellement l'anglais; seuls 5% (12) sont en français. Dans le sujet du message, les mots les plus fréquents sont: «urgent, assistance, business, confidential». Les textes écrits entièrement en majuscules représentent 20% (47) des messages.

Le type de fraude majoritaire est celui lié à un dictateur, suivi des «over invoice» et des «next of kin» (figure 5).

Caractéristiques de l'expéditeur

Les services de messageries les plus utilisées par les auteurs des messages sont: rediffmail.com (26), yahoo.com ou .fr (25), netscape.net (24), hotmail.com (17), caramail.com (16) et spinfinder.com (8). Dans 36% des messages, plusieurs adresses de contact possible sont fournies par l'auteur.

Pour les 99 courriers proposant des contacts par téléphone ou fax, 6 pays et 2 entreprises de téléphones par satellite ont pu être identifiés. La figure 6 montre le nombre de messages contenant au moins un numéro de téléphone ou de fax par pays (6).

Le fraudeur indique souvent un pays d'origine, mais aussi un pays de résidence actuelle (accueil); dans un tiers des cas, ces deux pays sont identiques. Les pays d'origine cités fréquemment sont: le Nigéria (61), l'Afrique du Sud (32), le Zaïre/Congo (30), la Sierra-Leone (25) et le Zimbabwe (21). Les pays d'accueil cités sont principalement le Nigéria (56), les Pays-Bas (42), l'Afrique du Sud (40) et la Côte-d'Ivoire (29).

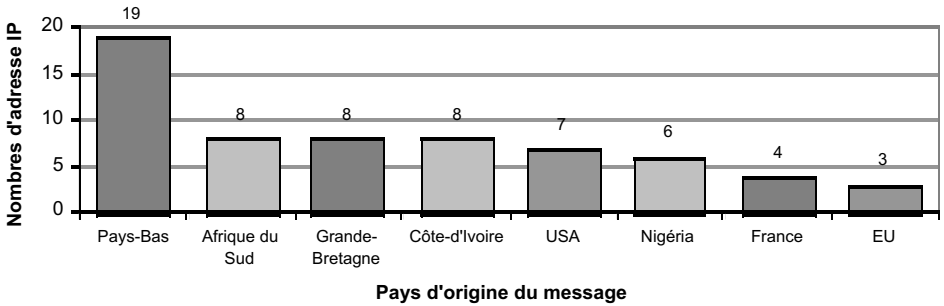

Figure 7: Origine des adresses IP obtenues par le système de confirmation

L'analyse de la provenance des adresses IP fournies par le système de confirmation des messages montre que les courriels sont lus prioritairement aux Pays-Bas. La figure 7 montre la provenance des 63 adresses IP obtenues.

Discussion

La police reçoit de nombreux courriers électroniques transmis par des personnes qui ont reçu un message provenant des escrocs. Cette information est généralement très peu exploitée, car la police ne peut procéder préventivement à une localisation par l'envoi d'un courriel. La méthode proposée à l'ESC permet de traiter ces messages selon leur forme, leur contenu et leur provenance et a permis de donner une image utile de ce phénomène.

Les informations obtenues par l'analyse de 233 courriers reçus par la police de la région retenue durant les mois de janvier à mars 2003 montre que la majorité sont écrits en anglais (seulement 5% en français), que les types d'histoires sont variés, le principal étant basé sur les difficultés d'un dictateur déchu. Les pays mentionnés dans le texte ou déterminés par l'analyse de l'origine des courriers se répartissent selon le tableau présenté dans la figure 8.

La méthode utilisée permet donc de montrer que, durant notre étude, les Pays-Bas étaient une plateforme importante pour les escrocs prenant contact avec des victimes potentielles qui se trouvent en Suisse, notamment. Ceci contredit les informations sur la localisation des escrocs circulant sur Internet qui indiquent le lieu de résidence plutôt en Afrique de l'Ouest. De plus, lors de cette étude, aucune adresse IP analysée ne venait d'un ordinateur situé en Suisse.

Les renseignements apportés par la méthode proposée permettent potentiellement d'améliorer les démarches préventives proposées actuellement (7) par une meilleure connaissance du phénomène touchant la région concernée. Elle permet également de surveiller l'évolution des types de fraude. La mise en évidence de pays touchés proches de la région analysée permet de faciliter les coopérations internationales lors d'investigations.

Une analyse de liens est également possible (même adresse électronique, même adresse IP, même nom, même numéro de téléphone, …) au moyen du jeu de données disponible, mais cette analyse fera l'objet d'une publication ultérieure.

Position	Adresse IP	N° téléphone ou fax	Pays d'accueil	Pays d'origine
1	Pays-Bas	Nigéria	Nigéria	Nigéria
2	Côte-d'Ivoire	Pays-Bas	Pays-Bas	Afrique du Sud
3	Grande-Bretagne	Afrique du Sud	Afrique du Sud	Zaïre/Congo
4	Afrique du Sud	Tél. par satellite	Côte-d'Ivoire	Sierra-Leone

Figure 8: Classement des pays les plus courants

Limitations

Ce travail repose sur un échantillon recueilli durant une période limitée (3 mois) et dans une région particulière. La généralisation des résultats obtenus nécessiterait préalablement d'effectuer une nouvelle recherche basée sur un échantillon de données plus représentatif. Sous l'hypothèse que les escrocs n'envoient jamais de courriers dans les pays qui les héberge, il n'est pas exclu que les auteurs agissent depuis d'autres bases situées en Europe. Il serait donc intéressant d'effectuer une étude semblable dans plusieurs pays différents.

De nombreux courriers reçus par la police sont incomplets et limitent donc les possibilités d'analyse. Notamment les messages sont fréquemment amputés de leur en-tête. Il a été démontré comment cette information pouvait être complétée par le mécanisme de confirmation de la réception des courriers. Toutefois, la possibilité d'exploiter ce service dépend du temps entre la réception du message par la victime et la réponse avec confirmation envoyée par l'ESC.

Plusieurs informations sont difficiles à déterminer; l'heure d'envoi se présente sous différents formats. Il est souvent difficile de différencier les noms et les prénoms qui apparaissent dans les messages. Enfin, le format des numéros de téléphone et de fax peut aussi poser des problèmes.

Conclusions

Cette recherche montre qu'un traitement systématique des courriers électroniques provenant des escrocs de la "Nigerian Connection" est possible et qu'il permet d'obtenir une bonne image du phénomène. L'expérience menée démontre que de nombreux envois reçus dans la région suisse retenue provenaient, au moment de l'étude, des Pays-Bas, contrairement à ce qui était préalablement supposé. Une extension de cette étude serait souhaitable pour augmenter l'échantillon de données et étudier les relations entre les messages afin de détecter les différents groupes d'auteurs actifs. Enfin, une comparaison internationale permanente des mécanismes utilisés par les malfaiteurs serait un atout supplémentaire pour disposer d'une image plus précise de ce phénomène.

Bibliographie

Buchanan J., Grant A. J. (2001). "Investigating and Prosecuting Nigerian Fraud." United States Attorneys'Bulletin **49**(6): 39.

Bureau of International Narcotics and Law Enforcement Affairs (1997). Nigerian Advance Fee Fraud, United States Departement of State. **2003**.

National White Collar Crime Center and the Federal Bureau of Investigation (2001). IFCC 2001 Internet Fraud Report.

Smith R. G., Holmes M. N., Kaufmann P. (1999). "Nigerian Advance Fee Fraud." Trends & Issues in Crime and Criminal Justice(121).

Sur Internet:
http://home.rica.net/alphae/419coal/
www.nigerianscams.org
www.internet-fraud.com
www.419fraud.com

Notes

1 Nous souhaitons remercier la Police Cantonale Vaudoise pour sa précieuse collaboration lors de cette étude, ainsi que la société I2 Ltd® pour la mise à disposition des nouvelles versions de leur logiciel qui nous a aidés dans cette recherche

2 Courrier non sollicité envoyé à de très nombreuses personnes

3 http://home.rica.net/alphae/419coal/; http://www.climate.unibe.ch/~beyerle/emails/

4 www.nigerianscams.org

5 histoire racontée par le message

6 Thuraya et Inmarsat sont des entreprises de téléphonie par satellite, la localisation du téléphone n'est donc pas possible

7 Par exemple: http://www.stoppbetrug.ch/french/index.html