CRIMISCOPE

ESC - UNIL - 1015 Lausanne Nummer 26 – Dezember 2004

Operationelle und strategische Auswertung der E-Mails Typ "Nigerian Connection"

Der "Nigerian Connection" Betrug ist ein kriminelles Phänomen von bedeutendem Ausmass. Grundsätzlich werden die Opfer mit einer grosszügigen Belohnung im Austausch für verschiedene Dienstleistungen geködert. Um die Opfer zu kontaktieren wird die elektronische Datenübermittlung benutzt, die parallel zur Verallgemeinerung dieses Kommunikationsmittels an Bedeutung gewonnen hat. Die Täter sind sehr schwer zu verfolgen, da die Komplizen, welche an der Betrugsverwirklichung teilnehmen, sich in verschiedenen Ländern aufhalten. Bürger, die den Betrug wittern, leiten diese Mitteilungen (E-Mails) oft an die Polizei weiter. Diese Informationsquelle erlaubt es potentiell, ein einschlägiges Bild des Phänomens zu erhalten. Sie wird aber momentan wenig genutzt.

Im Rahmen einer Studie hat die Ecole des Sciences Criminelles in Zusammenarbeit mit der Kantonspolizei Waadt ein System eingeführt, um solche elektronischen Mitteilungen zu erhalten, zu erfassen und zu analysieren. Jedes E-Mail wird nach folgenden Kriterien klassifiziert:

- dem **Text der Mitteilung** (z. B. vom Autor angekündigtes Ursprungsland, angekündigtes Aufnahmeland, benutzte Sprache, Nummer des Kontakttelefons, elektronische Kontaktadresse usw..)
- den **Informationen, die mit den E-Mails zusammenhängen** (E-Mail Adresse des Absenders, Datum/Zeitpunkt des Versands, Provider der Internetadresse, IP-Adresse [1] usw..)
- nach der **IP Adresse des Computers**, der vom Täter benutzt wird, um seine Mailbox zu verwalten.

Die IP Adresse erlaubt es im allgemeinen, das Land zu bestimmen, wo sich der von den Autoren benutzte Internet Service Provider[2] befindet.

Eine vereinfachte Struktur der Datenbank, welche die gewonnenen Angaben aus den E-Mails aufnimmt, wird durch Abb. 1 illustriert.

Die Analyse und Interpretation der 438 E-Mails zeigen insbesondere:

- das Land, welches im Szenario der Mitteilung erscheint und die mögliche Lokalisierung, die anhand der IP-Nummer ermittelt wurde, ist verschieden;
  - die **Ursprungsländer,** in denen sich angeblich das Szenario abspielt sind mehrheitlich: Nigeria, Sierra Leone, die Elfenbeinküste, Kongo und Südafrika;
  - die **Aufnahmeländer**, wo sich die Protagonisten angeblich aufhalten, sind hauptsächlich die Elfenbeinküste, die Niederlande und Südafrika;
  - die **IP-Adresse** zeigt im allgemeinen eine Lokalisierung in den Niederlanden, in Nigeria, in den USA, in Israel, in der Elfenbeinküste und in Südafrika.
- Die Gesamtheit aller Verknüpfungen (individuelle), zwischen den Mitteilungen (IP, Nummer des Telefons/Fax, E-Mail-Adresse) hat es ermöglicht, die E-Mails in Gruppen zu gliedern. Des weiteren wäre es sinnvoll die Datenmenge zu vergrössern, um festzustellen, ob grössere Gruppen entstehen, welche auf die Existenz einer oder mehreren Organisationen hindeuten würden.
- Ein Zusammenhang zwischen den typischen Szenarien der N-Connection (z.B.: Familienangehöriger [next of kin], Bauern auf der Flucht [farmer], abgesetzter Diktator [dictator]) und den Mitteilungen vom Typ "Lotterie" konnte bewiesen werden (Abb. 2). Diese Verbindung zeigt auf, dass die Autoren ihr Szenario weiterentwickeln, um neue Opfer zu ködern. Das immer häufigere Auftreten von französischen Mails, die eine bestimmte Zielgruppe visieren, ist ein anderes Zeichen dieser Adaptationsfähigkeit.
- Im Datensatz befand sich eine Schweizer IP Adresse. Dies ist ein Zeichen, dass Ermittlungen auf nationaler Ebene aufgenommen werden können.

Diese Resultate, auf eine beschränkte Datenmenge gestützt, sind sowohl von einem operationellen wie auch strategischem Gesichtspunkt aus vielversprechend. Sie weisen auf das Potential einer systematischeren Behandlung der Daten in grösserem Umfang hin. Zu diesem Zweck wird gegenwärtig die Möglichkeit evaluiert, den Vorgang der E-Mailbearbeitung vermehrt zu automatisieren.

Abbildung 1 : *vereinfachte Darstellung der Datenbank*

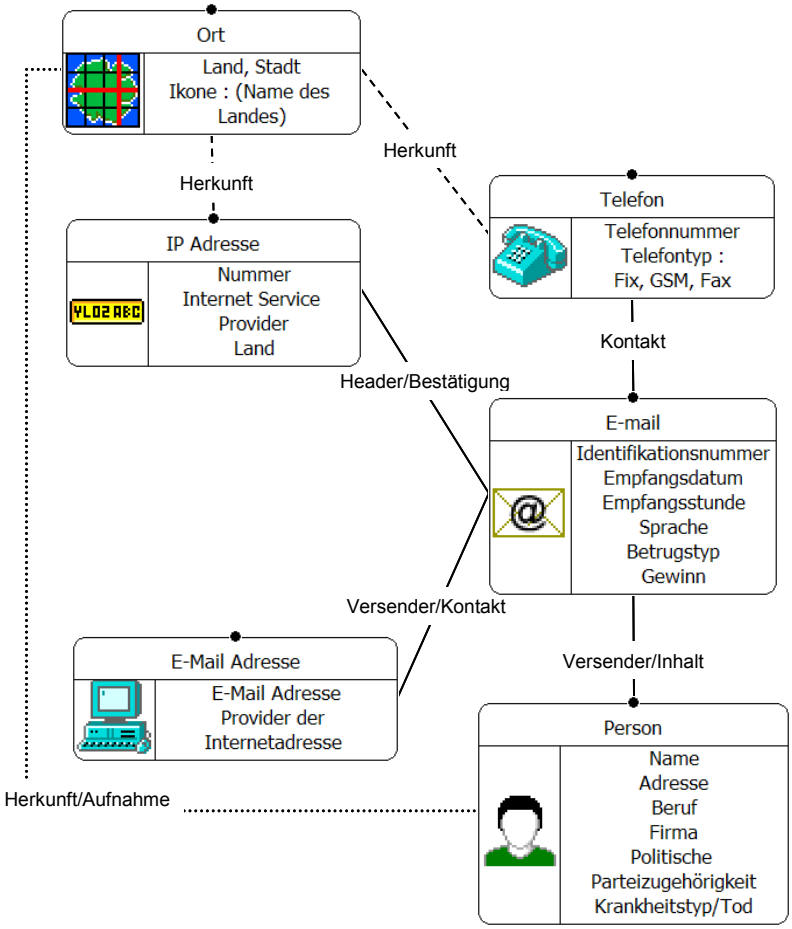
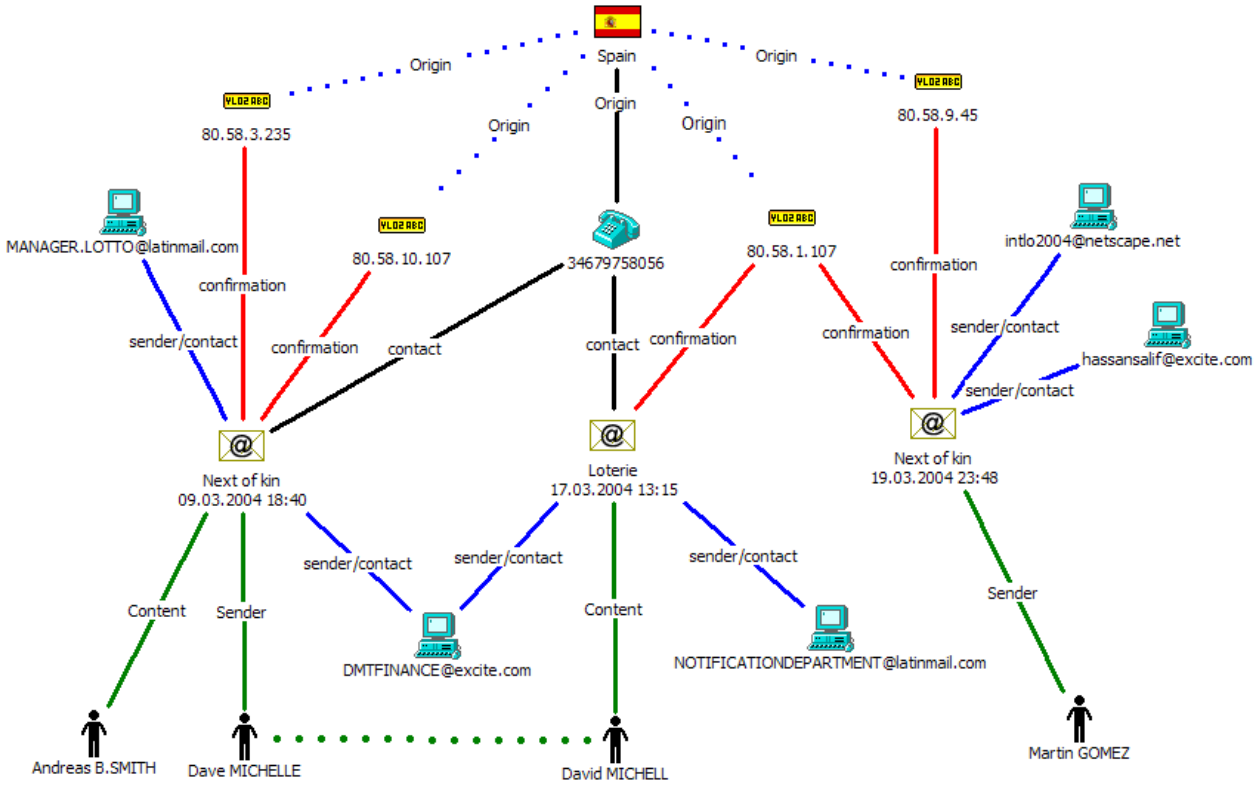


Abbildung 2 : *Visualisierung von Beziehungen zwischen den Mitteilungen vom Typ « N-Connection » und « Lotterie »*



Referenz :

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.

Weitere Auskünfte :

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

Noten

[1] Die Internet Protocol Addresse ist eine einmalige Nummer, die jeder Maschine die sich auf Internet einwählt zugeteilt wird.
[2] Meistens ist der Internet Service Provider nahe des eingewählten Computers, so dass die Verbindungskosten möglichst klein gehalten werden können.

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

Bitte senden Sie Ihre Bemerkungen und Mitteilungen an:

Sekretariat *Crimiscope* % (021) 692 46 44
UNIL – Ecole des sciences criminelles Fax (021) 692 46 05
CH–1015 LAUSANNE Int. (+ 41 21) 692 46 44