POLICE
LËTZEBUERG

Service de Police Judiciaire
Cybercrime
L-2957 Luxembourg
Tél. : +352 4997-6422
spj.cy@police.etat.lu

Luxembourg, le 8 mai 2019

Objet: Arnaque / Man in the middle

Madame,
Par la présente, je me permets de vous informer qu'un nombre croissant d'arnaques de type "Man in the middle" sont en cours et ciblent actuellement les départements comptabilités des services communaux.

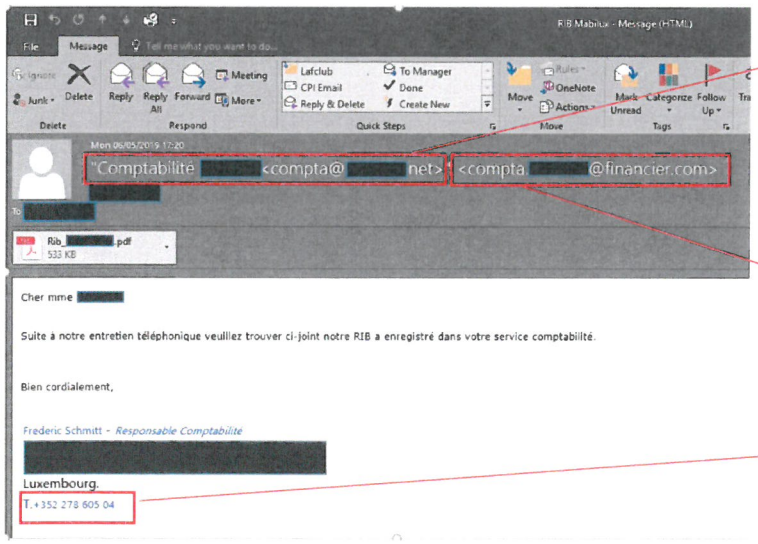
Le mode opératoire des auteurs peut être décrit comme suit:

- L'arnaqueur appelle au nom d'une société, souvent en se faisant passer pour une personne du service comptabilité. Il est très probable que le numéro de téléphone qui s'affiche, correspond au numéro réel de la société en question, mais l'affichage est truqué au niveau de la téléphonie de l'appelant frauduleux.

- En général, les auteurs utilisent un nom d'une entreprise de construction qui est actuellement en charge d'un projet communal.

- Dans une deuxième phase, l'arnaqueur mentionne un changement des coordonnées bancaires de la société. Il demande une adresse E-Mail afin de transmettre les nouvelles coordonnées bancaires.

- L'adresse E-Mail, avec laquelle les auteurs envoient le changement des coordonnées bancaires est souvent similaire à l'adresse de la société et contient une signature falsifiée avec, la plupart du temps, un numéro de contact luxembourgeois "VoIP".



Adresse affichée qui simule le nom de la société, p.ex.

compta@société_xy.lu

adresse réelle p.ex.

compta.société_xy**@financier.com**

numéro de téléphone VoIP luxembourgeois suggérant un numéro fixe

POLICE
LËTZEBUERG

Quelques mesures simples aident à réduire le risque d'être victime de cette arnaque, et augmentent les chances de détecter la fraude :

- sensibiliser le personnel ayant le contact téléphonique avec l'extérieur (secrétariat, réception) à ce type d'attaque,
- demander systématiquement une confirmation par téléphone de toute demande d'envoi de fonds non planifiés, ou pour toute demande concernant un changement de compte bancaire,
- en cas d'une requête par mail, adresser un courriel **à l'adresse habituelle** du donneur d'ordre au lieu de simplement répondre au message initial,
- vérifier la pertinence de tout changement subit de coordonnées téléphoniques, mail ou bancaires,
- être vigilant quant à l'adresse e-mail affichée entre <...> les auteurs utilisent souvent des domaines comme:

  @financier.com. @dr.com, @gmail.com ou créent des domaines similaires au domaine d'une entreprise.

- au cas où un courriel non usuel ou douteux serait envoyé d'une adresse terminant avec '**.lu**', il serait d'autant plus important d'informer sans retard nos services.

Informations supplémentaires:

https://police.public.lu/dam-assets/fr/publications/europol/CEO-fraud-FR.pdf

Service de Police Judiciaire
Section Cybercrime