



ATTENTION

ARNAQUES

LES ARNAQUES ET AUTRES ESCROQUERIES PAR MAILS



I – Les mails provenant soit-disant de la Gendarmerie ou de la Police

En effet, certains ont reçu des mails signés par la Police Nationale ou la Gendarmerie Nationale indiquant que des infractions ont été commises.

Les escrocs envoient via des robots informatiques des mails indiquant que le propriétaire de l'adresse mail recevant ce courrier électronique a :

- soit téléchargé des images pédopornographiques
- soit téléchargé des images pornographiques
- soit commis des délits de cyber pornographie
- ou du trafic sexuel.

Le mail est rempli d'articles du Code Pénal comme le 227-23 – qui lui existe bel et bien – et des logos et/ou noms de ces deux forces de l'ordre françaises. Tout cela pour que cela fasse impression et le plus réel possible. Il est indiqué qu'il faut répondre par mail pour être entendu et donner des justifications (Cf. exemples ci-après).



DIRECTION GÉNÉRALE DE LA POLICE JUDICIAIRE
DIRECTION DE PROTECTION DES MINEURS

Attention !
Paris le 04 Octobre 2020
ARNAQUE

à l'attention :

Je suis **Mme YVETTE BERTRAND**, commissaire divisionnaire, chef de la brigade de protection des mineurs (BPM), je vous contacte peu après une saisie informatique de la Cyber-infiltration (autorisée, notamment en matière de pédopornographie, pédophilie, Cyber pornographie, exhibitionnisme, trafic sexuel depuis 2014) pour vous informer que vous faites l'objet de plusieurs Poursuites Judiciaires en vigueur :

- La pédopornographie
- La pédophilie
- L'exhibitionnisme
- La Cyber pornographie
- Le trafic sexuel

Pour votre information, La loi de mars 2007 aggrave les peines lorsque les propositions, les agressions sexuelles ou les viols ont pu être commis en recourant à internet et vous avez commis les infractions après avoir été ciblé sur internet (site d'annonce), puis pendant des échanges Mails (Messagerie Instantanée) avec plusieurs mineurs, les photos dénudées de vous que vous envoyez aux mineurs ont été enregistrés par notre cyber-gendarme et constituent les preuves de vos infractions.

Vous êtes prié de vous faire entendre par mail en nous écrivant vos justifications pour qu'elles soient mises en examen et vérifiées afin d'évaluer les sanctions, cela dans un délai strict de 72 heures. Passé ce délai nous nous sommes dans l'obligation de transmettre notre rapport à **Mme Myriam Quémener** procureur adjoint au tribunal de première instance de Créteil et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre encontre, le remettre à la Gendarmerie la plus proche de votre lieu de résidence pour votre arrestation et vous fiché comme délinquant sexuel, transmettre votre dossier à plusieurs chaînes de télévision nationale d'information pour une diffusion où votre famille, vos proches et toute la France entière verront ce que vous faites devant votre ordinateur.

Pour tous informations écrivez à cette adresse : protection.mineurs@secretary.net

Maintenant vous êtes prévenu.

Cordialement,
Mme YVETTE BERTRAND, Commissaire Divisionnaire,
Chef de la brigade de protection des mineurs (BPM)

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE
BRIGADE DE PROTECTION DES MINEURS
Adresse: 12 QUAI DE GESVRES 75004 Paris

De: GENDARMERIE NATIONALE [redacted]@outlook.com>
Envoyé: jeudi 17 décembre 2020 02:14
À: [redacted]
Objet: Ordre établie le 17 Décembre 2020

email à vérifier

Je suis [redacted] commissaire divisionnaire, chef de la brigade de protection des mineurs (BPM). Je vous contacte peu après une saisie informatique de cyber-infiltration (autorisée, notamment en matière de pédopornographie, Site Pornographique, Cyber pornographie, pédophilie, exhibitionnisme, trafic sexuel) pour vous informer que vous faites l'objet de plusieurs poursuites judiciaires en vigueur :

- * LA PÉDOPORNOGRAPHIE
- * SITE PORNOGRAPHIQUE
- * Cyber pornographie

L'escroc usurpe l'appellation Gendarmerie Nationale

Pour votre information, la loi de mars 2007 aggrave les peines lorsque les propositions, les agressions sexuelles ou les viols ont pu être commis en recourant à internet et vous avez commis les infractions après avoir été ciblé sur internet.

Vous êtes prié de vous faire entendre par mail en nous écrivant vos justifications afin qu'elles soient mises en examen et vérifiées de sorte à évaluer les sanctions ; cela dans un délai strict de 72 heures. Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport

À Mme [redacted] procureur adjoint au tribunal de première instance de Créteil et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre encontre, le remettre à la Gendarmerie la plus proche de votre lieu de résidence pour votre arrestation et vous fiché comme délinquant sexuel. Votre dossier sera également transmis aux médias nationaux.

Une diffusion où votre famille, vos proches et toute l'Europe entière verront ce que vous faites devant votre ordinateur.

Maintenant vous êtes avertis. Cordialement,

ARNAQUE

En cas de réponse, les auteurs de ces escroqueries demandent le paiement d'amendes pour éviter le passage au tribunal et que l'affaire devienne publique.

Les bons réflexes :

- . Ne pas répondre
- . Placer l'expéditeur en indésirable
- . Vous pouvez signaler les faits sur la plateforme **Pharos** (lien ci-dessous)
- . Supprimer le mail

En cas de paiement d'une quelconque somme d'argent :

- . Conservez le message pour les enquêteurs
- . Porter plainte au commissariat de Police ou à la Gendarmerie
- . Ou prendre contact avec le 116 006 (service d'aide aux victimes - service gratuit)

Petits conseils :

- . La Gendarmerie et la Police ont des adresses mails qui leur sont propres mais jamais de
 - . outlook
 - . wanadoo
 - . gmail
 - . free
- . Il en est de même pour toutes les administrations et services de l'état en France.
- . Dans le doute prenez contact avec les services concernés en leur téléphonant.
- . Et pour votre protection de la Cybermalveillance mettez à jour vos antivirus et changez de temps en temps vos mots de passe.

II – Le chantage à la webcam prétendue piratée

Dans ce genre de tentative d'escroquerie, le prétendu « hacker » transmet un email indiquant avoir pris le contrôle de votre ordinateur et qu'il a des vidéos de la victime qui sont compromettantes qu'il a faites avec sa webcam.

Date: 28/01/2019 – 17:33:25

De : moncompte@mail.fr

A : moncompte@mail.fr

Objet : Important

Vous ne me connaissez pas et vous vous demandez probablement pourquoi vous recevez ce mail, non? Je suis un hacker qui a piraté vos appareils il y a quelques mois. Je vous ai envoyé un e-mail depuis VOTRE compte piraté. J'ai mis en place un virus sur le site pour adulte (porno) et devinez quoi, vous avez visité ce site pour vous amuser (vous savez ce que je veux dire). Pendant que vous regardiez des vidéos, votre navigateur internet a commencé à fonctionner comme un RDP (contrôle à distance) ayant un keylogger, ce qui m'a donné l'accès à votre écran et votre webcam. Après cela, mon logiciel a obtenu tous vos contacts et fichiers.

Vous avez entré vos mots de passes sur les sites que vous avez visités, et je les ai interceptés.

Bien sûr, vous pouvez les modifier, ou alors vous les avez déjà changés. Mais ça n'a pas d'importance, mon virus l'a mis à jour à chaque fois.

Qu'ai-je fait ?

J'ai créé une vidéo en double écran. La 1ère partie montre la vidéo que vous regardiez (vous avez de bons goûts ahahah...), et la deuxième partie montre votre webcam. N'essayez pas de trouver et de détruire mon virus ! (Toutes vos données sont déjà téléchargées vers un serveur distant)

- N'essayez pas d'entrer en contact avec moi
- Les antivirus ou services de sécurité; Formater votre disque ou détruire l'ordinateur ne vous aidera pas non plus, puisque vos données se trouvent déjà sur un serveur distant.

Je vous garantis que si vous n'avez pas payé, je publierai vos vidéos sur Internet, vous n'êtes pas ma seule victime. C'est le rôle de ce virus de vous faire peur.

Ne me contactez pas, ça ne sert à rien. Vous pouvez essayer de me contacter si vous le voulez, mais je ne répondrai pas.

Eh bien, à mon avis, 500 Euro est un juste prix pour notre petit secret. Vous effectuerez le paiement par Bitcoin (si vous ne connaissez pas, recherchez "comment acheter des bitcoins" sur Google).

L'adresse de mon portefeuille Bitcoin:

1AZV5FEZhXRA4X8Fgtjg24fFZ2vDD5EIJF541

(respecter les majuscules et minuscules, copiez/collez bien)

Important :

Vous avez 48 heures pour effectuer le paiement. (J'ai un traqueur dans ce mail, et en ce moment je sais que vous avez lu ce message).

Si je n'obtiens pas les Bitcoins, j'envierai certainement l'enregistrement vidéo à tous vos contacts, y compris vos parents, vos collègues, et ainsi de suite. Cela dit, si je reçois le paiement, je détruirai la vidéo immédiatement.

Si vous avez besoin de preuves, répondez par "Oui!" et j'envierai l'enregistrement vidéo à 6 de vos contacts. C'est une offre non négociable, cela étant dit, ne me faites pas perdre mon temps et le vôtre en répondant à ce message.

Pour donner le change, il lui envoie un mail avec sa propre adresse mail afin de faire croire qu'il est effectivement entré dans son ordinateur.

Il s'agit juste de la modification d'un mail que chacun peut faire avec un minimum de connaissances informatiques.

Dans tous les cas, il ne faut pas avoir peur même si cela peut être le premier réflexe. Les arnaqueurs lancent des milliers de mails à diverses adresses pour avoir le plus de chance de recevoir de l'argent provenant de leur chantage.

Les bons réflexes :

- . Ne pas répondre
- . Ne pas payer
- . Conserver les preuves
- . Changer les mots de passe

En cas de paiement d'une quelconque somme d'argent :

- . Contacter votre banque pour essayer d'annuler la transaction
- . Porter plainte au commissariat de Police ou à la Gendarmerie

Petits conseils :

- . Faire régulièrement les mises à jour de votre ordinateur
- . Avoir un antivirus et le tenir à jour
- . Éviter les sites pouvant être dangereux (téléchargement musiques, films, etc.)
- . Avoir des mots de passes solides et uniques (un par site et non le même pour tous)
- . Ne pas répondre, ouvrir les pièces jointes et de ne pas cliquer sur les liens quand le mail vient d'une personne que vous ne connaissez pas.
- . Masquer la webcam quand elle n'est pas en mode de fonctionnement.

Qui joindre en cas de problèmes :

- . n° 0 805 805 817 Info Escroqueries (appel gratuit) du lundi au vendredi 09h – 18h30
- . 3018 (appel et service gratuit) ligne nationale d'écoute anonyme et confidentielle destinée aux internautes confrontés à des problèmes dans leurs usages numériques.

Toutes les informations se trouvant dans ce document sont aussi consultables sur les sites :

Cyber Malveillance du gouvernement : <https://www.cybermalveillance.gouv.fr/>

Lien Pharos : <https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action>