Sécurité l'arnaque à la webcam piratée revient avec le confinement

Félix Marciano - mardi 14 avril 2020 - 11:45

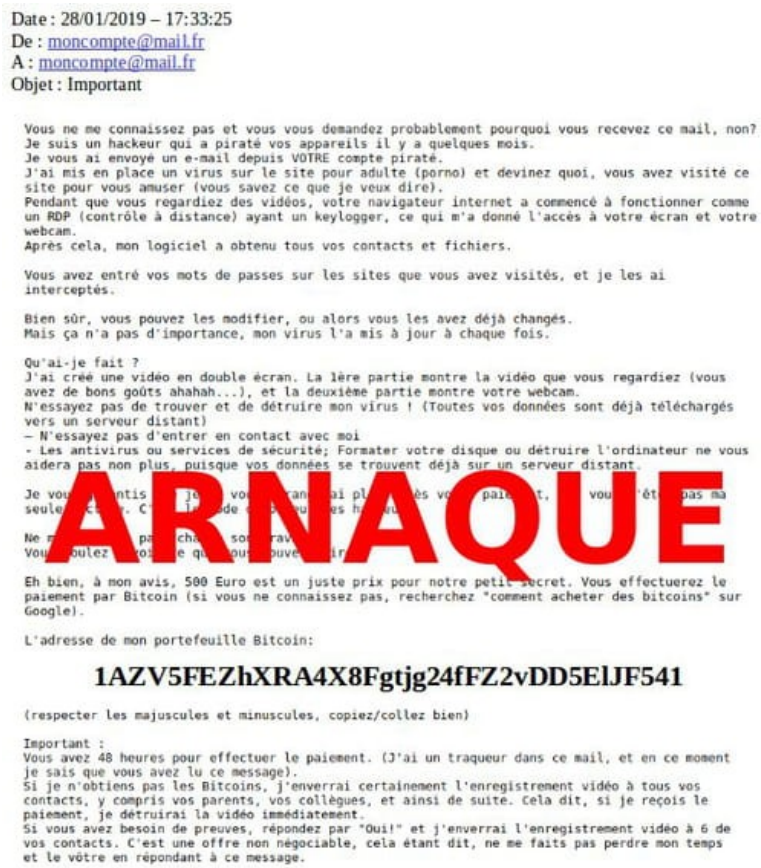
Les tentatives de chantage pour vidéos compromettantes se multiplient depuis la mise en place du confinement. Une escroquerie bien connue qui cible des utilisateurs mal avertis.

Il fallait s'en douter : depuis la mise en place des mesures de confinement à la mi-mars, et avec l'usage intensif de solutions de communication en vidéo, **la fameuse arnaque à la webcam piratée fait son grand retour,les tentatives de chantage se multipliant ces dernières semaines**. C'est la plateforme Cybermalveillance https://www.cybermalveillance.gouv.fr/

qui a donné l'alerte, après avoir relevé un pic de signalements de "sextorsion", avec des plaintes en hausse de 400 %.

Malgré cette brusque recrudescence, l'arnaque, bien connue des services de police, n'a rien de nouveau. Il s'agit simplement d'**une tentative de chantage misant sur la peur et l'ignorance**. La recette est bien rodée. La victime reçoit un mail provenant d'un expéditeur inconnu affirmant avoir pris le contrôle de son ordinateur en y installant des logiciels malveillants. Ne reculant devant rien, **le maitre-chanteur précise qu'il a non seulement récupéré tous les mots de passe et tous les contacts de sa proie**, mais qu'en plus, il a le contrôle de tous ses fichiers et de son ordinateur. **Dans certains cas, l'escroc utilise même l'adresse mail de sa victime pour envoyer son message**, histoire de l'effrayer davantage encore !

Pire encore, **il prétend qu'il l'a filmée "en pleine action" pendant ses visites sur des sites pornographiques en piratant sa webcam**. Bien évidemment, il réclame une rançon allant de quelques centaines à plusieurs milliers d'euros à payer en cryptomonnaie sur un compte dont il fournit les coordonnées sous peine de **tout révéler à l'entourage personnel et professionnel de sa victime** en publiant les fameuses vidéos compromettantes... Pas moins !



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 hackeur 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 téléchargés 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.

ARNAQUE

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:

1AZV5FEZhXRA4X8Fgtjg24fFZ2vDD5ElJF541

(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'enverrai 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'enverrai l'enregistrement vidéo à 6 de vos contacts. C'est une offre non négociable, cela étant dit, ne me faits pas perdre mon temps et le vôtre en répondant à ce message.

Comme l'explique très clairement cybermalveillance.gouv.fr sur sa page dédiée,

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/campagnes-darnaques-au-chantage-a-la-webcam-pretendue-piratee

tout est faux, même quand l'expéditeur du message utilise l'adresse mail de sa victime ou affiche un de ses mots de passe. **Il s'agit simplement d'une tentative d'escroquerie misant sur la crédulité et la peur du chantage** – à caractère sexuel ici, d'où l'appellation sextorsion.

Cybermalveillance indique également l'attitude à adopter en cas de tentative d'escroquerie : **ne pas paniquer, ne pas répondre au message, ne rien payer, changer ses mots de passe, conserver des preuves et porter plainte**, de façon à contribuer aux enquêtes en cours pour identifier et poursuivre les escrocs en justice.

Profitons de l'occasion pour rappeler que **cybermalveillance.gouv.fr est une plateforme en ligne mise en place par le groupement d'intérêt public (GIP) Acyma** (Action contre la cybermalveillance), qui regroupe des membres tels que l'Afnic, l'UFC-Que Choisir, le Clusif, La Poste, Orange, Bouygues Telecom et Google – parmi d'autres acteurs – mais aussi plusieurs ministères. Son tôle principal consiste à informer les utilisateurs – particuliers comme professionnels ou associatifs – des dangers liés à l'usage du numérique en général et d'Internet en particulier. Outre son site Web s,ur lequeul on trouve de précieux conseils pratiques, Cybermalveillance offre deux services téléphoniques :
– **Info Escroqueries, au 0 805 805 817** (appel gratuit) du lundi au vendredi de 9 h 00 à 18 h 30 (service du ministère de l'Intérieur).
– **Net Écoute, au 0 800 200 000** (appel gratuit), du lundi au vendredi de 9 h 00 à 19 h 00, ligne

d’écoute nationale anonyme et confidentielle destinée aux internautes confrontés à des problèmes dans leurs usages numériques.