CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Campagnes d'arnaques au chantage à la webcam prétendue piratée

31/01/2019

Vous avez reçu un message (mail) d'un supposé « hacker » qui prétend avoir piraté votre ordinateur. Il vous menace de publier des images compromettantes prises à votre insu avec votre webcam et vous demande une rançon en monnaie virtuelle ? Pas de panique, ce n'est qu'une tentative d'arnaque !

Depuis l'été 2018, de très nombreuses vagues de messages de tentatives d'arnaque au chantage à la webcam prétendue piratée ont été recensées.

En janvier 2019, Cybermalveillance.gouv.fr a constaté une forte recrudescence de ces campagnes d'arnaques. Elles ciblent les utilisateurs francophones. Voici un exemple de ce type de message ci-dessous :

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.

Je vou[illegible] je [illegible] vo[illegible] ai pl[illegible] vo[illegible] paie[illegible], vou[illegible] pas ma seule[illegible]. C'[illegible] de [illegible] es h[illegible]

Ne m[illegible] pa[illegible] cha[illegible] so[illegible]
Vou[illegible] oulez [illegible] qu[illegible] ouv[illegible]

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.

De quoi s'agit-il ?

Les utilisateurs victimes de ces arnaques reçoivent un message d'un inconnu qui se présente comme un pirate informatique (« hacker »). Ce prétendu « pirate » prétend avoir pris le contrôle de l'ordinateur de sa victime suite à la consultation d'un site pornographique. Le cybercriminel annonce alors avoir des **vidéos compromettantes de la victime faites avec sa webcam**. Il menace de les publier à ses contacts personnels, ou même professionnels, si la victime ne lui paie pas une rançon. Cette rançon, qui va de quelques centaines à plusieurs milliers d'euros, est réclamée dans une monnaie virtuelle (généralement en Bitcoin).

Pour effrayer encore plus la victime, les cybercriminels vont parfois jusqu'à **écrire à la victime avec sa propre adresse mail** , afin de lui faire croire qu'ils en ont réellement pris le contrôle de son compte.

Dans certaines campagnes, les cybercriminels vont jusqu'à **dévoiler à la victime un de ses mots de passe** pour lui faire croire qu'ils ont bien pris le contrôle de son ordinateur.

Ces messages de chantage sont parfois écrits en anglais, mais ciblent également de plus en plus souvent les victimes dans leur langue natale. On constate une augmentation de messages écrits dans un français plus ou moins correct.

Ces arnaques s'inspirent des chantages à la webcam ciblés, également appelés « **sextorsion »** pour effrayer les victimes. Mais il s'agit ici de messages envoyés en masse par les cybercriminels. Dans les cas réels de sextorsion ciblée, la victime « connaît » son maître chanteur auquel elle a fourni des images ou vidéos compromettantes de son plein gré après avoir été abusée. Vous pouvez consulter les conseils de la CNIL si vous êtes confronté à un cas réel de sextorsion.

Faut-il avoir peur ?

La réponse est simple : **non !** Car il s'agit d'une simple arnaque qui vise à escroquer des victimes crédules en leur faisant peur.

En premier lieu et **si vous y réfléchissez bien, vous n'avez sans doute rien à vous reprocher** de compromettant .

Ensuite, si le « piratage » annoncé par les cybercriminels n'est en théorie pas impossible à réaliser, en pratique, il reste assez complexe techniquement et surtout long à mettre en œuvre. Comme les escrocs ciblent leurs victimes par milliers, on peut donc en déduire qu'ils n'auraient matériellement pas le temps de réaliser ce qu'ils affirment avoir fait.

On peut également noter que de nombreux internautes qui ont reçu ce type de message n'avaient tout simplement pas de webcam, ou que leur adresse de messagerie usurpée ou le mot de passe dévoilé n'étaient plus utilisés depuis plusieurs années.

Enfin, si de très nombreux cas de réception de ces messages de chantage sont rapportés, **aucun cas n'a jamais été signalé jusqu'à présent de victimes qui auraient vu les cybercriminels mettre leurs menaces à exécution**.

Tous ces éléments tendent à démontrer que **ces messages ne sont qu'une tentative d'arnaque**. Autrement dit, si vous recevez un tel message de chantage et que vous ne payez pas, il ne se passera certainement rien de plus.

Mais comment font-ils pour avoir ces informations ?

Là aussi, même si c'est légitimement inquiétant, cela n'est pas très compliqué pour les cybercriminels.

Votre adresse de messagerie circule déjà sur Internet car vous l'utilisez régulièrement sur différents sites pour vous identifier et communiquer. Ces sites ont parfois revendu ou échangé leurs fichiers d'adresses avec différents partenaires plus ou moins scrupuleux dans des objectifs marketing.

Ces fichiers d'adresses de messagerie sont parfois également récupérés par des cybercriminels pour pouvoir être utilisés dans des campagnes publicitaires frauduleuses, pour des attaques par hameçonnage (voir notre article sur ce sujet), ou pour ce type de campagnes de chantage.

Si les cybercriminels vous ont écrit avec votre propre adresse de messagerie pour vous faire croire qu'ils en ont pris le contrôle : sachez que l'adresse de l'émetteur dans un message n'est qu'un simple affichage qui peut facilement être usurpé sans devoir pour autant disposer de beaucoup de compétences techniques.

Si enfin, **les cybercriminels vous dévoilent un de vos mots de passe**, cela ne veut pas forcément dire qu'ils ont piraté votre machine. Ils ont pu avoir accès à un de vos mots de passe qui a été précédemment compromis. Les escrocs jouent sur le fait que malheureusement les victimes ne changent pas assez souvent leur mot de passe et qu'elles réutilisent le même sur différents accès. Or, l'actualité montre que de nombreux sites, parfois très réputés, se font régulièrement pirater leurs bases de comptes utilisateurs qui contiennent des adresses de messagerie et des mots de passe que les cybercriminels se revendent ensuite entre-eux pour pouvoir commettre ce type de méfaits. Autrement dit, le mot de passe qui vous a été dévoilé à certainement été compromis dans une affaire antérieure et les cybercriminels ont donc pu facilement le récupérer.

Que faut-il faire si on reçoit ce type de message ?

1. Ne paniquez pas ! En effet, vous n'avez sans doute rien de réellement compromettant à vous reprocher.

2. Ne répondez pas ! Même si les cybercriminels seraient très probablement incapables de gérer les réponses de toutes leurs victimes, il ne faut jamais répondre à de telles menaces de chantage qui montrent aux cybercriminels que votre adresse de messagerie est « valide » et que vous portez de l'intérêt au message de chantage qu'ils vous ont envoyé.

3. Ne payez pas ! Et ce même si vous aviez un doute. Car comme vu précédemment, aucune mise à exécution des menaces n'a été démontrée jusqu'à présent et vous alimenteriez donc inutilement ce système criminel.

4 – Conservez les preuves ! Faites des copies d'écran, conservez les messages qui pourront vous servir pour signaler cette tentative d'extorsion aux autorités, voire pour déposer plainte si vous l'estimiez nécessaire.

5. Changez votre mot de passe partout où vous l'utilisez s'il a été divulgué ou au moindre doute. Retrouvez tous nos conseils pour bien gérer ses mots de passe dans notre fiche pratique.

6. Signalez cette tentative d'arnaque sur le site du ministère de l'Intérieur Internet-signalement.gouv.fr (Pharos) afin qu'il puisse avoir connaissance du phénomène et envisager les poursuites qui peuvent s'avérer nécessaires.

Et si vous avez payé la rançon ?

Vous êtes alors victime d'une **extorsion**, au sens de l'article 312-1 du code pénal : délit passible de sept ans d'emprisonnement et de 100 000 € d'amende.

1. Contactez votre banque pour essayer de faire annuler la transaction.

2. **Déposez plainte** en vous adressant au commissariat de police ou la brigade de gendarmerie ou encore en adressant votre plainte par écrit au procureur de la République du tribunal de grande instance dont vous dépendez, en fournissant toutes les preuves en votre possession.

Que faire pour éviter qu'un piratage se produise réellement ?

Même si dans le cas évoqué dans cet article, il ne s'agit essentiellement que d'une supercherie, vos équipements sont exposés à de vraies attaques informatiques. Voici quelques mesures simples de sécurité qui permettent de réduire considérablement les risques de piratages :

1. Faites régulièrement les mises à jour de sécurité de tous vos appareils.

2. Utilisez un antivirus et tenez-le à jour.

3. Évitez les sites dangereux tels que les sites de téléchargements ou de vidéos en ligne (*streaming*) illégaux.

4. Utilisez des mots de passe solides, différents sur tous les sites et changez les régulièrement (retrouvez tous nos conseils pour bien gérer ses mots de passe dans notre fiche pratique).

5. Ne répondez pas, ne cliquez pas sur les liens, n'ouvrez pas les pièces jointes de messages d'expéditeurs inconnus ou d'expéditeurs connus mais dont la structure du message est inhabituelle ou vide.

6. Masquer votre webcam quand vous ne vous en servez pas (un simple morceau de ruban adhésif opaque sur l'objectif peut suffire).

Besoin de plus de conseils ?

Vous pouvez contacter les services :

– **Info Escroqueries** au 0 805 805 817 du lundi au vendredi de 9h à 18h30. Numéro vert (appel gratuit). Service du ministère de l'Intérieur.

– **Net Ecoute** au 0 800 200 000 du lundi au vendredi de 9h00 à 19h00. Numéro vert (appel gratuit). Ligne d'écoute nationale anonyme et confidentielle destinée aux internautes confrontés à des problèmes dans leurs usages numériques.