CHANTAGE À L'ORDINATEUR OU À LA WEBCAM PRÉTENDUMENT PIRATÉS

Définition

Le chantage à l'ordinateur ou à la webcam prétendus piratés (ou « **cryptoporno** ») désigne un type d'escroquerie qui vise à vous faire croire que vos équipements ont été piratés.

Il prend généralement la forme d'un message reçu, essentiellement par courriel (mail), de la part d'un inconnu qui se présente comme un pirate informatique.

Ce « hacker » prétend avoir pris le contrôle de l'ordinateur de la victime suite à la consultation d'un site pornographique et annonce avoir obtenu des vidéos compromettantes avec sa webcam.

Le cybercriminel menace de les publier aux contacts (personnels et/ ou professionnels) de la victime si elle ne lui paie pas une rançon, souvent réclamée en monnaie virtuelle (généralement en Bitcoin).

Parfois, pour attester de la prise de contrôle de l'ordinateur auprès de la victime, les cybercriminels vont jusqu'à lui écrire avec sa propre adresse mail ou lui dévoiler l'un de ses mots de passe.

But recherché

Soutirer de l'argent sous la menace de divulguer des vidéos compromettantes de la victime à ses contacts.

Mesures Préventives

- **Faites régulièrement les mises à jour** de sécurité de tous vos appareil.

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

- **Évitez les sites non sûrs ou illicites** tels ceux hébergeant des contrefaçons (musique, films, logiciels, etc.) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.

- **Utilisez des mots de passe suffisamment complexes** et **changez-les au moindre doute.**

- **N'ouvrez pas les messages suspects, leurs pièces jointes et ne cliquez pas sur les liens** provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu mais dont le contenu est inhabituel ou vide.

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

Si vous êtes victimes

- **NE PANIQUEZ PAS.** En effet, vous n'avez sans doute rien de réellement compromettant à vous reprocher.

- **NE RÉPONDEZ PAS.** 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.

- **NE PAYEZ PAS LA RANÇON.** Et ce, même si vous aviez un doute. En effet, aucune mise à exécution des menaces n'a été démontrée jusqu'à présent et vous alimenteriez donc inutilement ce système criminel.

- **CONSERVEZ LES PREUVES.** Faites des captures d'écran, conservez les messages qui pourront vous servir pour signaler cette tentative d'extorsion aux autorités.

- **CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE** partout où vous l'utilisez s'il a été divulgué ou au moindre doute et choisissez-en un solide.

- **CONTACTEZ VOTRE BANQUE** si vous avez payé la rançon pour essayer de faire annuler la transaction.

- **DÉPOSEZ PLAINTE** au commissariat de police ou à la brigade de gendarmerie ou en adressant votre plainte au procureur de la république du tribunal de grande instance dont vous dépendez.

Les infractions encourues

L'incrimination principale qui peut être retenue est **l'extorsion de fonds. L'article 312-1 du Code pénal** dispose que « l'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque ». L'extorsion est punie de sept ans d'emprisonnement et de 100 000 euros d'amende.